Università
Ca'Foscari
Venezia

Corso di Laurea Magistrale

In Amministrazione, Finanza e Controllo

Tesi di Laurea

Il ruolo del revisore nel comprendere e valutare l'ambiente IT delle società in conformità al principio di revisione internazionale 315

Relatrice

Ch.ma Prof.ssa Rigo Sabrina

Laureanda

Alessia Semenzato

Matricola 868443

Anno Accademico

2022 / 2023

INDICE

INTRODUZIONE

L'obiettivo della seguente trattazione è quello di analizzare il ruolo del revisore nel comprendere e valutare l'ambiente IT delle società, alla luce dell'aggiornamento avvenuto nel 2022 del principio di revisione internazionale ISA 315. Tale aggiornamento ha infatti definito delle procedure specifiche e degli aspetti che il revisore deve considerare e valutare relativi all'ambiente IT implementato nelle società al fine di individuare e valutare rischi di errori significativi nel bilancio. L'utilizzo crescente della tecnologia all'interno delle società ha reso necessario che il revisore ponesse maggior attenzione alla componente IT delle società, in quanto, oltre ad apportare numerosi benefici, apporta anche numerosi rischi derivanti dall'utilizzo dell'IT che potrebbero influenzare negativamente l'informativa finanziaria.

Nel 2019 a cura dello IAASB (*International Auditing and Assurance Standards Board*), ovvero l'organismo che si occupa di elaborare i principi di revisione a livello internazionale, sono stati aggiornati i principi di revisione con l'obiettivo di rinnovarli, anche alla luce del costante aumento dell'utilizzo della tecnologia all'interno delle aziende. Un aggiornamento era necessario in quanto la tecnologia e l'automazione, oltre ad aver reso le operazioni aziendali più efficienti, hanno sottoposto le società a nuovi rischi IT. I rischi derivanti dall'uso dell'IT hanno, la maggior parte delle volte, un effetto diretto sulle informazioni aziendali e, di conseguenza, sull'informativa di bilancio; proprio per questo è necessario che il revisore consideri tali aspetti.
L'Italia ha recepito l'aggiornamento internazionale nel 2022 (è perciò applicabile nella revisione dei bilanci relativi ai periodi amministrativi che iniziano il 1° gennaio 2022 e successivi) e la novità maggiore è stata apportata all'ISA 315 ovvero il principio che si occupa di trattare il ruolo del revisore nell'identificare e valutare i rischi di errori significativi mediante la comprensione dell'impresa e del suo sistema di controllo interno. Oggi, oltre a tali aspetti, il revisore dovrà comprendere anche le componenti IT e i processi IT aziendali al fine di individuare i rischi derivanti dall'utilizzo dell'IT, considerando anche i controlli IT progettati e attuati dalle società per contrastare tali rischi.

Se l'ambiente IT è complesso e il revisore non ha le competenze adeguate al fine di poterlo comprendere, interverrà un *IT Auditor*, ovvero un revisore con competenze tecniche in campo tecnologico.

Nel primo capitolo dell'elaborato, sarà introdotta la figura del revisore al fine di evidenziare lo scopo della revisione e il processo di revisore. Capire come si struttura il lavoro del revisore, infatti, aiuta a comprendere in quali fasi del processo sono eseguite le procedure legate alla comprensione e alla valutazione dell'ambiente IT.
Si analizzerà inoltre nel dettaglio l'aggiornamento che ha coinvolto i principi di revisione internazionale, evidenziandone gli obiettivi e le finalità. Sarà prestata maggior attenzione all'ISA Italia 315 e alle modifiche che sono state apportate per stare al passo dell'avanzamento tecnologico. Saranno poi evidenziati gli aspetti chiave dell'ISA Italia 315: il rischio di revisione e le sue componenti, il concetto di asserzione, le procedure di valutazione del rischio e la documentazione richiesta in questa fase della revisione.
In tal senso sarà ampiamente descritto il rischio di errori significativi in quanto è l'oggetto dell'ISA Italia 315, il quale può essere definito come il rischio che il bilancio contenga errori prima che esso sia sottoposto a revisione. Questo rischio si compone di due rischi: il rischio interseco e il rischio di controllo. Il revisore analizzerà il rischio intrinseco e, sulla base di questo, individuerà i controlli posti in essere dalla società, al fine di valutare il rischio di controllo.

Nel secondo capitolo si entrerà nel vivo della trattazione, evidenziando l'importanza dell'uso della tecnologia all'interno delle aziende attraverso l'analisi dell'evoluzione storica dell'uso dell'IT in ambito aziendale, dei benefici che ha apportato e, infine, dei rischi derivanti dal suo utilizzo. Questi rischi, anche se non sempre in modo diretto, possono influenzare le informazioni aziendali, incidendo così sulla veridicità e la correttezza del bilancio d'esercizio. Si analizzeranno poi due rischi IT molto diffusi e dannosi: il rischio legato alla sicurezza digitale (*cybersecurity*) e il rischio legato al *cloud*.
In relazione alla *cybersicurezza*, si esamineranno inoltre due certificazioni che attestano la sicurezza digitale di una società, ovvero la certificazione ISO 2700, la quale è volontaria, e la certificazione GDPR, obbligatoria.
Nello stesso capitolo, saranno esaminati due strumenti e una disciplina fondamentali e riconosciuti a livello mondiale riguardo il tema trattato: il *framework* COSO, il *framework*

COBIT e la normativa SOX. Il *framework* COSO è uno strumento che definisce come un'azienda dovrebbe strutturare il proprio sistema di controllo interno e, invece, il *framework* COBIT è uno strumento che definisce come dovrebbe strutturarsi un sistema di controllo interno in un'ottica IT, focalizzandosi maggiormente sulla governance e sul management dei sistemi IT.
Infine, la normativa SOX, di origine statunitense, ha permesso la diffusione dei *framework* precedenti in quanto ha introdotto per le aziende l'obbligo di implementare un sistema di controllo interno, il quale dovrà essere documentato e certificato da un revisore esterno.

Nel terzo capitolo della trattazione saranno evidenziate le procedure di revisione che il revisore dovrà svolgere in relazione all'ambiente IT in conformità al principio di revisione 315. Il revisore, infatti, sarà chiamato innanzitutto a comprendere la società in oggetto, il suo ambiente IT e come la tecnologia si implementa all'interno del suo sistema di controllo interno. Saranno puntualmente trattati gli aspetti che il revisore deve considerare e comprendere, grazie anche ai numerosi esempi forniti dall'ISA Italia 315.
A seguire, il revisore dovrà individuare i rischi derivanti dall'IT con l'obiettivo di intercettare i controlli generali IT e i controlli applicativi IT definiti e attuati dalle società per contrastarli.
Nella fase successiva il revisore dovrà testare i controlli: testerà innanzitutto il *design* del controllo e successivamente la sua effettività. Questi test hanno l'obiettivo di valutare se il revisore può fare affidamento sui controlli nello svolgimento delle procedure di revisione oppure no, in questo caso dovrà svolgere ulteriori procedure, definite procedure di validità. Al termine del processo di revisione, il revisore emetterà un giudizio di revisione su quanto rilevato.
In questo capitolo sono state analizzate inoltre delle tecniche computerizzate che vengono applicate solitamente in questo ambito, definite CAAT's *(Computer Assisted Audit Techniques*), ovvero tecniche sofisticate e altamente automatizzate che supportano il revisore nella conduzione dell'attività di *audit*.

In conclusione, il quarto capitolo verterà sulla figura dell'*IT Auditor*, ovvero un revisore che ha competenze specifiche in campo informatico e in particolare nei sistemi IT delle

aziende. Dopo una breve introduzione relativa a questa figura professionale, è riportata un'intervista condotta ad un *IT Auditor* con un'esperienza consolidata in questo campo. Il soggetto intervistato è il Dottor Iannucci Sandro, revisore Partner della società di revisione Crowe Bompani Spa presso la sede di Roma.
Le domande sottoposte al revisore hanno avuto come oggetto tre temi ampi: il suo lavoro e come si svolge all'interno del gruppo di *audit*, l'aggiornamento relativo all'ISA 315 e i principali rischi IT. Date le sue competenze e la sua esperienza, le risposte del revisore hanno evidenziato degli aspetti e dei temi importanti, tra cui quello della cybersicurezza, dell'importanza del lavoro in *team*, del rapporto tra *team* di *audit* finanziario e team di IT *audit* e soprattutto della percezione che hanno le aziende sulla componente IT. L'intervista è stata molto formativa in quanto ha approfondito il tema trattato in questo elaborato, evidenziando come viene effettivamente svolta l'attività nella pratica e quali sono le criticità riscontrate.

Per concludere, è fondamentale porsi delle domande: come cambia il ruolo revisore a causa del costante aumento dell'automazione? Com'è implementata la tecnologia all'interno dell'azienda? Quanto la tecnologia incide nella produzione dell'informativa finanziaria? Quali sono i nuovi rischi che il revisore si trova ad affrontare relativi all'utilizzo della tecnologia? Quali sono i nuovi aspetti che il revisore deve considerare? Quali sono le competenze che dovrebbe avere un revisore per poter comprendere e valutare un sistema IT?
A queste domande, si cercherà di rispondere attraverso il seguente elaborato.

CAPITOLO 1: IL RUOLO DEL REVISORE E INTRUDUZIONE ALL'ISA 315

1.1 Il ruolo del revisore legale

Al fine di comprendere il ruolo del revisore nella comprensione dell'ambiente IT delle società è importante chiarire prima di tutto cos'è la revisione legale, chi è il revisore e quali sono le società obbligate alla revisione. I concetti che sono affrontati in questo capitolo saranno utili per comprendere i vari temi trattati nel corso del presente elaborato.

Il revisore contabile è quel soggetto chiamato ad esprimere un giudizio sul bilancio di una società e lo fa mediante lo svolgimento di un insieme di procedure di revisione svolte in conformità ai principi di revisione internazionali. L'obiettivo è quello di verificare se il bilancio riflette in modo corretto e veritiero la situazione economica e patrimoniale della società.

Il revisore è tenuto a verificare «*nel corso dell'esercizio la regolare tenuta della contabilità sociale e la corretta rilevazione dei fatti di gestione nelle scritture contabili*»[1].

Per "regolare tenuta della contabilità", si intende la verifica dell'osservanza degli obblighi civilistici e fiscali a cui una società è sottoposta, i quali stabiliscono in che modo e con quale scadenza devono essere rilevate le scritture contabili. Per "corretta rilevazione dei fatti di gestione", si intende verificare che i fatti di gestione siano rilevati in conformità ai principi contabili nazionali disciplinati dall'OIC (Organismo Italiano di Contabilità) o internazionali (IAS/IFRS) in base alla società di riferimento.

Questa attività è obbligatoria in Italia dal 7 aprile 2010 con l'entrata in vigore del Decreto Legislativo 39 del 2010 recependo la direttiva europea 2006/43/CE[2]. Inizialmente l'attività di revisione era un'attività svolta dal Collegio Sindacale, ma con tale decreto viene affidata ad un revisore unico o ad una società di revisione con soggetti indipendenti ed esterni alla società.

L'attività di revisione è svolta nel rispetto dei principi di revisione, detti *ISA* ovvero *International Standard Auditing.* Gli ISA definiscono i principi etici e professionali a cui

[1]Decreto Legislativo 27 gennaio 2010, n. 39.

[2]Direttiva 2006/43/CE del Parlamento Europeo e del Consiglio del 17 maggio 2006 relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio.

deve sottostare il revisore, le norme sullo svolgimento dell'incarico e le norme sulla redazione della relazione di revisione.

Lo IAASB (*International Auditing and Assurance Standards Board*)[3]è un organo interno all'IFAC (*International Federation of Accountants*) che elabora i principi di revisione internazionale, i quali poi verranno tradotti e recepiti da ogni Stato.

Tale organismo si occupa di definire, nell'interesse pubblico, i principi di revisione, i principi per il controllo di qualità[4] e i principi per le altre attività di Assurance agevolando l'adozione di tali principi dagli Stati. Il suo obiettivo generale è quello di migliorare la qualità della revisione e di uniformarla in tutto il mondo, rafforzando così la fiducia del pubblico nei confronti della figura del revisore e dell'Assurance globale.

Gli ISA adottati in Italia sono definiti "ISA Italia" e sono una versione tradotta in lingua italiana, con poche variazioni, dei principi di revisione internazionali. Essi conservano la medesima numerazione e regolamentano in egual modo gli aspetti della revisione.

Al fine di conformare la disciplina italiana con le discipline europee, il Decreto Lgs. 39/100[5] dispone che l'attività di revisione dei conti debba essere svolta in conformità ai principi di revisione sviluppati dagli ordini professionali[6], convenzionati con il Ministero dell'Economia e delle Finanze (MEF), e dalla Commissione Nazionale per le Società e la Borsa, la CONSOB.[7] Questi soggetti si occupano di recepire in Italia gli aggiornamenti dei principi internazionali definiti dallo IAASB. [8]

Gli ISA Italia in vigore oggi sono stati aggiornati il 1° settembre 2022, la quinta versione rispetto alla prima adozione. La prima adozione, infatti, è stata adottata per la revisione dei bilanci riferiti agli esercizi dal 01 gennaio 2015 dopo una determina della Ragioneria dello Stato avvenuta il 23 dicembre 2014.

---

[3]L'International Auditing and Assurance Standards Board è un organismo di standardizzazione indipendente preposto all'emissione di standard, come gli International Standards on Auditing (ISA), le linee guida per il controllo della qualità e altri servizi di Assurance.

[4]I principi per il controllo della qualità si occupano di definire il controllo della qualità per i soggetti abilitati che svolgono revisioni contabili e altri incarichi di *assurance* che hanno l'obiettivo di fornire un alto livello di attendibilità. In Italia se ne occupa l'ISQC 1 Italia (principio internazionale sul controllo della qualità).

[5]Decreto Legislativo 39/2010, art. 11 comma 3.

[6]Tra questi soggetti rientrano il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC), l'Associazione Italiana Revisori Contabili (Assirevi) e l'Istituto Nazionale Revisori Legali (INRL).

[7]Ministero dell'Economia e delle Finanze, *Principi di Revisione Legale Handbook 2020. Edizione in lingua italiana*, Roma, ottobre 2020.

[8]AA. VV., *Introduzione ai Principi di Revisione Internazionali (ISA Italia) elaborati ai sensi dell'art. 11 del Decreto Legislativo 27 gennaio 2010, n. 39,* Documento in pubblica consultazione, Ministero dell'Economia e delle Finanze, 2022.

Come definito dall'ISA Italia 200[9], l'obiettivo generale del revisore è quello di «*[..]acquisire una ragionevole sicurezza che il bilancio nel suo complesso non contenga errori significativi, dovuti a frodi o a comportamenti o eventi non intenzionali [..]*»[10] al fine di poter esprimere un giudizio sul bilancio di esercizio. Il revisore deve appurare che il bilancio sia conforme al quadro normativo sull'informativa finanziaria con lo scopo finale di emettere una relazione di revisione redatta in conformità ai principi di revisione e ai risultati ottenuti dalle procedure di revisione. La relazione di revisione descrive le attività esercitate dal revisore e conferisce un giudizio imparziale sul bilancio: attesta se rappresenta correttamente la situazione economica e patrimoniale della società.

Al fine di acquisire il grado di sicurezza richiesto, il revisore deve acquisire elementi probativi sufficienti e appropriati con lo scopo di ridurre ad un livello accettabilmente basso il rischio di revisione[11]. La sicurezza richiesta non è assoluta, ma viene richiesta una sicurezza "ragionevole", ossia elevata.

La revisione contabile è importante perché ha l'obiettivo di accrescere il grado di fiducia dei fruitori del bilancio e di qualsiasi soggetto interessato ad avere rapporti con la società; allo stesso tempo però non è un giudizio sulle prospettive future della società e non è un giudizio di merito sulle scelte aziendali, ma attesta la veridicità e la correttezza dei dati contenuti nel bilancio.

In base alla provenienza della persona preposta all'attività di revisione, la revisione può essere: interna oppure esterna.

Per revisione interna, in inglese *internal audit*, si intende l'attività svolta da organi interni alla società e ha ragione di esistere nelle società di medie e grandi dimensioni, soprattutto se divise.

I revisori interni sono soggetti dipendenti della società, ma allo stesso tempo, sono indipendenti alla direzione aziendale. Il fine di questa attività è quello di garantire un alto livello di attendibilità delle informazioni aziendali e di valutare l'efficacia dei

[9]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale".

[10]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale", paragrafo 11, pag. 5.

[11]Per la definizione del rischio di revisione e delle sue componenti si rimanda al Capitolo 1, par. 1.4, da pagina 20 della seguente trattazione.

processi di governance, di gestione del rischio e del controllo interno della società, e come vedremo in seguito, anche dei processi IT e dell'infrastruttura IT. Le considerazioni raccolte da questa attività dovranno poi essere riportate ai massimi organi amministrativi e funzionali.

Per revisione esterna si intende l'attività svolta da un revisore esterno ed indipendente alla società, questa può essere obbligatoria oppure volontaria.

Il revisore esterno può scegliere di utilizzare la documentazione prodotta dal revisore interno, se presente e se la ritiene adeguata ai fini della revisione e, in questo caso, in sede di pianificazione delle procedure di revisione deve tenerne conto nella definizione dell'estensione, della natura e delle tempistiche delle procedure.[12]

È obbligatoria, ovvero prevista per legge, per i seguenti soggetti:

1) Per le società per azioni (Spa) l'obbligo è sempre previsto e la revisione è esercitata da un revisore unico oppure da una società di revisione; può essere esercitata anche dal Collegio sindacale composto da tutti membri iscritti al registro dei revisori legali se ciò viene indicato espressamente nello statuto della società e nel caso in cui la società non sia obbligata a redigere il bilancio consolidato.[13]
2) Per gli Enti di Interesse Pubblico (EIP)[14], per società controllate da EIP e per società che appartengono ad un gruppo in cui fa parte anche un EIP. In questi casi la revisione può essere affidata solo ad un revisore unico o ad una società di revisione, non al Collegio Sindacale. Tra le società che rientrano in questa categoria ci sono le società quotate in borsa, le banche e le imprese di assicurazione e riassicurazione. [15]
3) Per gli Enti Sottoposti a Regime Intermedio (ESRI)[16]. A questo tipo di società si applica parte della disciplina prevista per gli EIP e la revisione può essere affidata solo ad un revisore unico o ad una società di revisione.
4) Per le Società a Responsabilità Limitata (Srl) l'obbligo è previsto nel caso in cui la società sia obbligata a redigere il bilancio consolidato, nel caso in cui sia controllata da una società obbligata alla revisione e nel caso in cui superi uno dei

[12]Tale attività è regolamentata dal Principio di Revisione Internazionale (ISA Italia) 610: "Utilizzo del lavoro dei revisori interni".
[13]Art 2409-bis del c.c..
[14]Agli EIP si applica integralmente il Regolamento europeo n. 537/2014.
[15]L'art 16, comma 1, del D.Lgs. n. 39/10 elenca gli EIP.
[16]L'art 19-bis, comma 1, del D.Lgs. n. 39/10 elenca gli ESRI.

tre limiti dimensionali[17] previsti dall'art. 2477 c.c. per due esercizi consecutivi. In questi casi la revisione può essere svolta sia da una società di revisione, che da un revisore unico, sia dal collegio sindacale, che da un sindaco unico.

La revisione volontaria invece può essere svolta da qualsiasi altro soggetto che non è legalmente obbligato alla revisione legale. Può essere utile per le società che vogliono consolidare la propria credibilità sul mercato e che vogliono aumentare il grado di fiducia degli *stakeholder*.

1.2 Il processo di revisione

La revisione legale è un processo articolato che si concretizza in un insieme di verifiche e di procedure che inizia con la fase di accettazione dell'incarico e termina con l'emissione di un giudizio sul bilancio d'esercizio. Per comprendere al meglio il tema trattato in questa tesi, è importante comprendere in quale fase del processo di revisione il revisore dovrà svolgere procedure specifiche sull'ambiente IT.

Il processo di revisione è costituito da tre fasi principali: inizia con la fase di valutazione del rischio, successivamente sussiste la fase di risposta ai rischi individuati nella prima fase e termina con l'attività di *reporting*.

La fase di valutazione del rischio è fondamentale in quanto ha l'obiettivo di definire la strategia di revisione. Inizialmente, il revisore dovrà raccogliere informazioni preliminari sull'azienda e sui rischi ad essa correlati al fine di valutare quanto sia conveniente e opportuno accettare l'incarico.

I fattori di rischio che potrebbero impedirne l'accettazione potrebbero essere correlati alla figura del revisore, ad esempio, la mancanza di indipendenza[18] da parte del *team* di revisione o la mancanza di personale competente per seguire un'impresa che opera in un settore particolare, oppure legati alla società, ad esempio, caratteristiche rischiose legate al settore di appartenenza o legate al sistema di controllo interno[19].

---

[17]Art 2477 c.c. definisce i limiti dimensionali, i quali sono i seguenti: il totale dell'attivo dello stato patrimoniale pari a 4 milioni di euro; i ricavi delle vendite e delle prestazioni a pari 4 milioni di euro; dipendenti occupati in media durante l'esercizio pari a 20 unità. Se la società supera almeno uno dei tre limiti per due esercizi consecutivi è obbligata alla revisione legale.

[18]L'indipendenza è sancita dal D. Lgs. 39/10. Per indipendenza si intende che il revisore non deve avere alcun potere decisionale nell'azienda e non deve avere rapporti personali, di parentela, finanziari, d'affari e di lavoro con la società sottoposta a revisione.

[19]Luciano Marchi, Revisione aziendale e sistemi di controllo interno, Quarta edizione, Giuffrè Francis Lefebvre, Milano, 2019, pag.26.

Dopo aver accettato l'incarico, il revisore emetterà una "Lettera d'incarico" al cliente con la quale definirà i termini, le tempistiche e la natura delle procedure di revisione che svolgerà.

Successivamente il *team* di revisione dovrà pianificare l'attività di revisione, elaborando una strategia generale di revisione e un piano di revisione sulla base del livello di significatività[20] stabilito al fine di garantire l'efficacia del processo di revisione.

La fase di valutazione del rischio si conclude con l'elaborazione di procedure di identificazione e valutazione di rischi di errori significativi svolte attraverso la comprensione dell'impresa, del suo quadro normativo di riferimento, del suo sistema di controllo interno e dei processi IT con il fine ultimo di definire le risposte di revisione adatte.

È proprio in questa fase che entra in gioco il principio di revisione ISA 315[21], ovvero il principio che definisce l'obiettivo del revisore nell'identificare e valutare i rischi di errori significativi attraverso un'attività di comprensione dell'impresa e del suo sistema di controllo interno e, grazie all'aggiornamento del 2022, il revisore è tenuto a comprendere anche come il cliente utilizza la componente IT per elaborare le informazioni contabili. La crescente digitalizzazione ha richiesto, infatti, che fossero predisposte delle procedure specifiche che il revisore deve seguire in riferimento all'ambiente IT delle società. Se il livello di automatizzazione fosse elevato, potrebbe essere necessario per il revisore servirsi di uno specialista IT. Nei paragrafi seguenti sarà analizzato l'ISA 315 in tutti i suoi punti ponendo maggior attenzione alle procedure e alle novità riguardanti l'ambiente IT.

Dopo la fase di valutazione del rischio, il revisore dovrà definire delle risposte generali ai rischi di errori significativi precedentemente identificati e dovrà metterle in atto per ridurre il rischio di revisione ad un livello accettabilmente basso.

Infine, nella fase di *reporting*, il revisore valuterà gli elementi probativi acquisiti durante le attività di revisione e, alla luce di quanto acquisito, valuterà se è necessario svolgere ulteriori procedure.

[20]La significatività è sancita dal principio di revisione internazionale (ISA Italia) 320: "Significatività nella pianificazione e nello svolgimento della revisione contabile". Per significatività si intende una soglia definita come un importo sotto del quale si ritiene che un errore non sia significativo, ovvero che non modifica o influenza il giudizio del revisore e le decisioni dei terzi che fanno affidamento sul bilancio.

[21]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi".

Nel caso non fosse necessario, il revisore sarà pronto per predisporre la relazione di revisione in cui formulerà un giudizio sulla base dei risultati ottenuti durante tutto il processo di revisione.

1.3 Il principio di revisione internazionale 315

Come detto nel paragrafo precedente, il principio di revisione internazionale ISA 315 si occupa di trattare la responsabilità del revisore nell'individuare ed esaminare rischi di errori significativi nel bilancio. L'obiettivo del revisore in tal senso è infatti quello di «*identificare e valutare i rischi di errori significativi, siano essi dovuti a frodi o a comportamenti o eventi non intenzionali, a livello di bilancio e di asserzioni, conseguendo in tal modo una base per definire e mettere in atto risposte di revisione a fronte dei rischi di errori significativi identificati e valutati*»[22].

Mediante la definizione e lo svolgimento di procedure di valutazione del rischio, il revisore deve acquisire elementi probativi sufficienti ed appropriati per identificare i rischi di errori significativi a livello di bilancio e di asserzioni e per definire, di conseguenza, le procedure di revisione in risposta ai rischi identificati. I rischi sono identificati e valutati attraverso un'attività di comprensione dell'impresa, del contesto in cui opera, del quadro normativo e del sistema di controllo interno. Grazie alla comprensione di questi aspetti, il revisore svilupperà delle aspettative iniziali che si modificheranno nel corso della revisione con l'acquisizione di nuovi elementi probativi.

Lo IAASB avviò un processo di revisione di questo principio all'inizio del 2016 per rispondere ai risultati che aveva ottenuto attraverso un progetto con cui stava monitorando come erano implementati e messi in atto i principi di revisione nella pratica. Lo IAASB ha intrapreso un progetto strategico negli anni 2015- 2019[23] con il quale ha appurato che era necessario migliorare alcuni ISA per ottenere una maggiore coerenza ed efficacia nella loro applicazione. Dopo aver raccolto informazioni e dati dagli organismi di regolamentazione dell'attività di *audit*, notò che l'area di competenza dell'ISA 315 richiedeva dei perfezionamenti per migliorare le prestazioni *dell'audit* generale.

[22]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", pag. 4.

[23]Il progetto strategico prendeva il nome di "Strategy for 2015–2019: Fulfilling Our Public Interest Mandate in an Evolving World".

Per raggiungere questo obiettivo, l'istituto coinvolse gli organismi di regolamentazione dell'attività di *audit* e piccole-medie imprese per avere dei *feedback* sulle sfide e sui problemi legati all'applicazione di questo principio. L'aggiornamento era necessario in quanto alcuni aspetti previsti in precedenza erano difficili da applicare dal punto di vista pratico ed erano difficili da estendere a tutte le società. C'era infatti incoerenza nella natura e nel numero dei rischi di errori significativi identificati nella pratica, le attività volte alla comprensione del sistema di controllo interno erano difficili da applicare e non era stato considerato il rischio informatico (IT), in crescita negli ultimi anni.
Gli obiettivi che lo IAASB si poneva durante questa fase di aggiornamento erano i seguenti:

1) stabilire requisiti più solidi e linee guida adeguatamente dettagliate per guidare i revisori a eseguire procedure di valutazione del rischio efficienti commisurate alle dimensioni e alla natura della società di riferimento. Nel comprendere la società e il suo sistema di controllo interno, il revisore avrebbe dovuto adottare un approccio che teneva conto dell'evoluzione costante dell'ambiente esterno;
2) prevedere procedure di valutazione del rischio più efficienti;
3) procedere ad una modifica degli altri principi di revisione alla luce delle modifiche apportate all'ISA 315 (come ISA 220[24], ISA 240[25], ISA 330[26], ISA 540[27]). Si parla in questo caso di un'attività di "*conforming amendments*"[28];
4) definire degli strumenti di supporto non autorevoli per le società, soprattutto per le piccole medie imprese, al fine di guidarle e di favorire la corretta applicazione dell'aggiornamento. Questi strumenti sono ad esempio le note pratiche sulle procedure di revisione, le illustrazioni oppure esempi che potrebbero rispondere alle domande dei revisori;
5) era necessario che il nuovo ISA rispecchiasse il contesto attuale, ma che fosse anche sufficientemente adattabile per far fronte alla rapida evoluzione del contesto aziendale di revisione soprattutto in ambito tecnologico.[29]

[24]Principio di Revisione Internazionale (Isa Italia) 220: "Controllo della qualità dell'incarico di revisione contabile del bilancio".
[25]Principio di Revisione Internazionale (Isa Italia) 240: "Le responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio".
[26]Principio di Revisione Internazionale (Isa Italia) 330: "Le risposte del revisore ai rischi identificati e valutati".
[27]Principio di Revisione Internazionale (Isa Italia) 540: "Revisione delle stime contabili, incluse le stime contabili del fair value, e della relativa informativa".
[28]L'attività di conforming amandament è quell'attività che prevede la correzione della totalità degli ISA a seguito della modifica apportata all'ISA 315.

L'aggiornamento fu pubblicato ufficialmente nel dicembre del 2019 e successivamente l'Italia lo ha recepito il 01 settembre 2022 tramite una determina del Ministero dell'Economia e delle Finanze traducendolo in lingua italiana e tenendo in considerazione le specificità del nostro sistema normativo. Il principio, ad oggi, risulta essere molto più esteso rispetto alla versione precedente (da 53 a 93 pagine), più dettagliato e più concreto in quanto fornisce molti esempi pratici e sei appendici che possono guidare il revisore nello svolgimento dell'incarico.

Nei prossimi paragrafi verranno esaminate nello specifico le novità apportate dall'ISA in merito all'ambiente IT messo in atto nelle società e verrà analizzato un nuovo concetto introdotto, quello di scalabilità.

1.3.1 Modernizzazione dell'ISA 315 per un ambiente IT in costante evoluzione

Uno degli obiettivi dell'aggiornamento del 2019 era quello di stare al passo con i cambiamenti dell'economia globale, la quale era, ed è tuttora, in costante evoluzione.

L'ambiente nel quale operano le aziende sta diventando sempre più complesso e cambia significativamente e costantemente dal punto di vista tecnologico e normativo. Le imprese infatti sono sempre più digitalizzate ed era necessario per il revisore comprendere come le società utilizzassero la componente IT nello svolgimento del business aziendale e all'interno del sistema di controllo interno.

I tre acronimi maggiormente utilizzati in campo tecnologico sono ICT, IT e TLC; quello più comunemente adottato è l'acronimo "IT".

ICT sta per "*Information and Communication Technology*", letteralmente Tecnologia dell'informazione e della comunicazione, fenomeno che si sviluppa intorno agli anni Sessanta con l'avvento della "convergenza ICT", precursore della "convergenza digitale", che sarebbe iniziata qualche anno dopo. È un fenomeno che vede l'uso combinato delle telecomunicazioni (TLC) e dell'informatica (IT) al fine di permettere lo scambio di informazioni in formato digitale. Non esistono definizioni univoche per questi termini in quanto hanno tutte e tre un significato molto ampio. [30]

---

[29]IAASB, *Basis for conclusions (october 2019) preparared by the staff of the IAASB, Internation Standard on Auditing 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement Including Conforming and consequential amendments to other international standards,* Documento in Pubblica Consultazione, pag. 4.

[30]Pighin M., Marzona A., *Sistemi informativi aziendali, ERP e sistemi di data analysis, Terza edizione*, Pearson, Milano, 2018.

Lo IAASB ha rinnovato il principio in modo tale che il revisore fosse tenuto a comprendere il sistema IT delle società con il fine di identificare e valutare i rischi di errori significativi derivanti dall'uso dell'IT ed eventuali controlli informatici generali pertinenti messi in atto dalla società per affrontare tali rischi.

Nel fare questa attività però, lo IAASB ha dovuto tener conto della velocità con cui cambia e si evolve il mercato IT e proprio per questo c'era il rischio che il principio potesse diventare obsoleto in un breve lasso di tempo. [31]

Nell'aggiornare questo principio sono state introdotte nuove definizioni per comprendere al meglio il tema: sono stati definiti, in primo luogo, i concetti di "controlli sull'elaborazione delle informazioni", ovvero quei controlli diretti a garantire l'integrità delle informazioni prodotte dai sistemi informativi e dalle applicazioni IT, e "controlli generali IT" per spiegare nello specifico cosa si intende per controlli relativi all'ambiente IT. È stato poi, di conseguenza, definito e circoscritto il termine ampio di "ambiente IT", definendo anche le sue tre componenti: le applicazioni IT, le infrastrutture IT e i processi IT. Infine, venne definito il termine "rischi derivanti dall'utilizzo dell'IT", ovvero il rischio che i controlli sull'elaborazione delle informazioni non operino in modo efficiente a causa di un ambiente IT non adeguato.

Le ultime due appendici dell'ISA sono dedicate proprio al tema IT. L'Appendice 5, denominata "Considerazioni relative alla comprensione dell'IT" [32], tratta degli aspetti che potrebbero aiutare il revisore nel comprendere come un'impresa utilizza la tecnologia all'interno del proprio sistema di controllo, ponendo attenzione alle diversità che ci potrebbero essere sulla base della complessità dell'azienda revisionata. Si occupa anche di trattare gli aspetti dell'ambiente IT che sono soggetti a rischi IT, introducendo per la prima volta all'interno dell'ISA il concetto di *cybersecurity*.

L'Appendice 6, denominata invece "Considerazioni relative alla comprensione dei controlli generali IT" [33], tratta degli aspetti che il revisore potrebbe considerare nel valutare l'efficacia dei controlli IT messi in atto dalle società, fornendo anche esempi di

[31]IAASB, *Basis for conclusions (october 2019) preparared by the staff of the IAASB, Internation Standard on Auditing 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement Including Conforming and consequential amendments to other international standards,* Documento in Pubblica Consultazione, pag. 11-13.

[32]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", "Appendice 5: Considerazioni relative alla comprensione dell'IT", pag. 78.

[33]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", "Appendice 6: Considerazioni relative alla comprensione dei controlli generali IT", pag. 87.

controlli generali IT per processo IT, tutti concetti che verranno ripresi dettagliatamente nel terzo capitolo.
Il principio 315 ha perciò modificato sostanzialmente il modo in cui devono essere trattati gli aspetti IT, in quanto non erano mai stati considerati in precedenza, e ha fornito del materiale applicativo che il revisore deve considerare durante lo svolgimento dell'incarico.

1.3.2 Il principio di scalabilità

Nel mettere in pratica l'ISA 315, il revisore deve avere la capacità di applicarlo alle revisioni contabili dei bilanci di tutte le società: dalle società piccole, semplici e non complesse alle società grandi, complesse e multinazionali. Lo IAASB, infatti, si è posto l'obiettivo di rendere i principi di revisione fruibili da qualsiasi tipo di società.
Nella versione precedente erano presenti dei paragrafi intitolati "Considerazioni specifiche per le imprese di dimensioni minori" nei quali erano definite delle linee guide più specifiche per imprese di dimensioni minori.
Nella nuova versione, invece, lo IAASB ha definito come parametro distintivo delle aziende il loro grado di complessità e non più la loro dimensione. Nello svolgere le procedure di revisione, infatti, il revisore deve considerare le specificità delle aziende che ha di fronte sulla base della loro complessità. La complessità è spesso strettamente correlata alla dimensione della società, ma questo non è sempre vero, in quanto ci possono essere aziende di dimensioni minori molto complesse e aziende di grandi dimensioni poco complesse.
È stato introdotto così il concetto di scalabilità, ovvero la capacità dei principi di revisione di adattarsi ad ogni tipo di società. Sulla base della complessità varieranno la natura e l'estensione delle procedure di revisione e, nell'applicare questo concetto, il revisore userà il proprio giudizio e la propria esperienza professionale.
Al fine di guidare il revisore nell'ISA 315 e in tutti gli altri principi di revisione sono state predisposte delle disposizioni ad hoc per l'applicazione della regola della scalabilità: per ogni tema trattato è stato predisposto un capitolo specifico in cui vengono date specifiche direttive su come trattare sia le imprese più complesse sia quelle meno complesse, piuttosto che concentrandosi solo su "imprese di dimensioni minori".

Per definire uno spartiacque tra imprese di grandi dimensioni (più complesse generalmente) e imprese di piccole dimensioni interviene l'ISA Italia 200, il quale definisce come "impresa di dimensioni minori" essenzialmente un'azienda non quotata. Lo stesso ISA esplicita le caratteristiche qualitative di queste società che il revisore userà come guida per verificare se le imprese rientrano in questa categoria. Tali requisiti sono:

1) se la proprietà e la direzione sono nelle mani di un numero circoscritto di soggetti;
2) se le operazioni che svolge la società sono semplici e chiare;
3) se le registrazioni contabili sono semplici;
4) se il sistema di controllo interno è ridotto e poco complesso;
5) se sono poche le persone che hanno poteri direzionali, le quali singolarmente esercitano un vasto numero di controlli;
6) se sono pochi i dipendenti assunti, i quali svolgono singolarmente molteplici mansioni.[34]

I requisiti evidenziati non sono da considerarsi né in modo esaustivo, né in modo esclusivo; inoltre, non è necessario che un'azienda sia in possesso di tutte le caratteristiche sopra elencate, ma è sufficiente che ne possieda almeno una.

Il tema della scalabilità è stato utilizzato ampiamente anche in relazione alle nuove disposizioni in tema IT. In tal senso, è stato definito che il grado di comprensione dei processi informatici e il grado di valutazione dei controlli generali IT messi in atto dalla società varieranno in base alla natura, alle dimensioni e alle circostanze della singola impresa e del suo ambiente IT[35]. È possibile che la complessità dei sistemi IT sia così elevata da richiedere membri del *team* con competenze informatiche specializzate.

[34]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale", par. A69-A72, pag. 22-23.

[35]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", par. A170, pag. 47.

1.3.3 Lo scetticismo professionale

L'aggiornamento dell'ISA 315 ha rafforzato il concetto di scetticismo professionale per incoraggiare i cambiamenti comportamentali dei revisori.

Nello svolgere l'attività di revisione, il revisore deve esercitare lo scetticismo professionale, ovvero adottare un atteggiamento dubitativo, critico e attento soprattutto nelle situazioni che potrebbero segnalare la presenza di possibili errori dovuti a comportamenti intenzionali o non intenzionali. [36]

L'ISA Italia 315 evidenzia che, nello svolgimento delle procedure di valutazione del rischio, il revisore non può adottare un comportamento orientato all'ottenimento di elementi probativi corroborati oppure orientato all'esclusione di elementi probativi contraddittori.

Nella valutazione degli elementi probabili acquisiti, il revisore deve essere critico e deve interrogarsi costantemente sull'attendibilità della documentazione e delle informazioni raccolte dalla direzione aziendale, escludendo eventuali elementi probativi che potrebbero essere incerti e ambigui.

Lo scetticismo si applica:

1) interrogandosi su eventuali informazioni contraddittorie e sull'affidabilità dei documenti raccolti;
2) esaminando le informazioni acquisite dalla direzione aziendale, tra cui anche le risposte alle indagini;
3) ponendo attenzione alle situazioni che potrebbero denotare probabili errori dovuti a frodi o a comportamenti non intenzionali;
4) sulla base della comprensione acquisita, valutando se gli elementi probativi supportano adeguatamente l'individuazione e la valutazione dei rischi di errori significativi.[37]

[36]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale", par. 15, pag. 8.
[37]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale", par A21-A25, pag. 14-15.

1.4 Il rischio di revisione

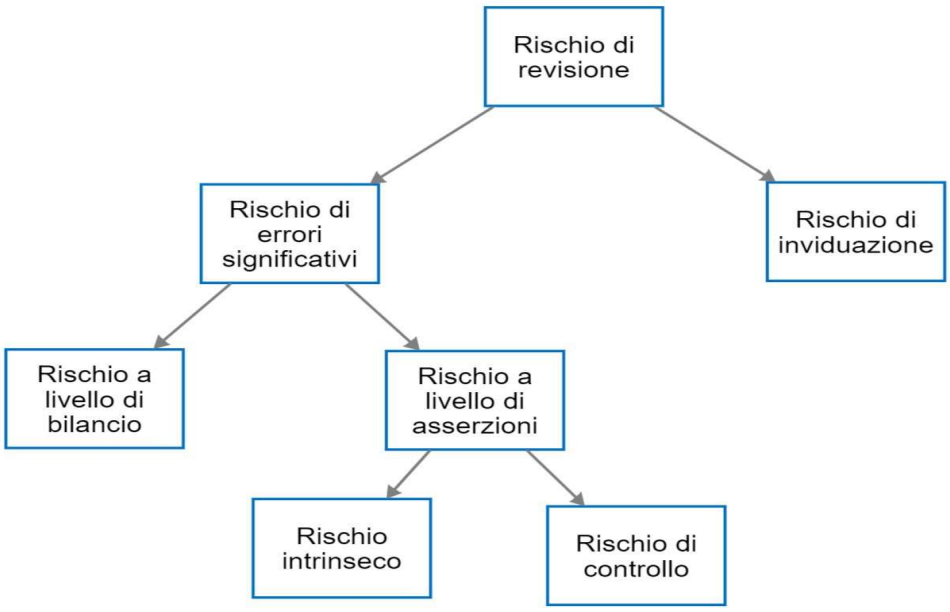
Come detto in precedenza, con l'applicazione dell'ISA 315 il revisore ha l'obiettivo di individuare e valutare i rischi di errori significativi. In questo capitolo sarà analizzeremo cosa sono i rischi di errori significativi e, più in generale, cos'è il rischio di revisione.

Il revisore utilizza un approccio *"risk based",* ovvero basato sul rischio; durante la sua attività deve sempre identificare e valutare il rischio di errori significativi al fine di definire e attuare le risposte adatte per ridurre il rischio di revisione ad un livello accettabile. Per "rischio di revisione", si intende il rischio di emettere un giudizio positivo su un bilancio che contiene errori significativi e, allo stesso tempo, il rischio di non emettere un giudizio positivo su un bilancio che non contiene errori significativi[38].

Soprattutto nella fase di pianificazione dell'attività di revisione, il revisore deve identificare i rischi per definire le procedure di revisione corrette per gestirli. Nello svolgere queste attività è importante che il revisore applichi il proprio giudizio professionale piuttosto che svolga analisi quantitative.

Il rischio di revisione può essere schematizzato dalla figura che segue:

Figura 1.4 La composizione del rischio di revisione



Fonte: Principio di revisione internazionale ISA Italia 315: "Identificazione e valutazione dei rischi di errori significativi"

[38]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale", pag. 6.

È bene evidenziare che con il termine "rischio di revisione" non si intende il rischio d'impresa a cui è sottoposto il revisore nello svolgimento della sua professione come, per esempio, il rischio di incorrere a perdite d'esercizio, perdite di clienti o altri eventi negativi connessi alla sua attività.
Come possiamo vedere dalla figura sovrastante, il rischio di revisione si compone di due rischi: il rischio di errori significativi e il rischio di individuazione.

Il rischio di errori significativi è il rischio che il bilancio contenga degli errori prima che quest'ultimo venga sottoposto a revisione contabile, ed è quel rischio che, secondo il giudizio del revisore, derivante dalla propria esperienza professionale, richiede una considerazione specifica.
Siamo davanti a questo tipo di rischio quando è ragionevole affermare che c'è una probabilità ragionevole che un errore si verificherà e che l'entità di tale errore sia significativa. [39]
Si articola su due livelli: a livello di asserzioni e a livello di bilancio.
Il rischio a livello di asserzioni colpisce nello specifico un'asserzione. Le asserzioni sono definite dall'ISA 315 come: «*attestazioni, esplicite e non, relative alla rilevazione, quantificazione, presentazione ed esposizione in bilancio di informazioni che sono insite nella dichiarazione della direzione sul fatto che il bilancio è redatto in conformità al quadro normativo sull'informazione finanziaria applicabile*»[40].
Sono fondamentali da identificare perché permettono al revisore di determinare la natura, la tempistica e l'estensione delle procedure di revisione conseguenti al fine di acquisire gli elementi probativi necessari a ridurre il rischio di revisione ad un livello accettabilmente basso. Nel prossimo paragrafo sarà analizzato nello specifico cosa sono e quali sono le asserzioni.
Il rischio a livello di bilancio colpisce il bilancio nel suo complesso e di conseguenza colpisce più asserzioni. Questo rischio non è identificabile necessariamente in una determinata operazione o classe di operazioni, ma si tratta solitamente di circostanze che potrebbero aumentare in modo pervasivo il rischio a livello di asserzioni. Questo

[39]Principio di revisione internazionale (ISA Italia) 200: "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionale", paragrafo A16 pagine 13.
[40]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", definizione a), pag. 5.

rischio può derivare da carenze dell'ambiente di controllo oppure da eventi esterni all'azienda, come ad esempio un peggioramento delle condizioni economiche esterne. [41]

Il rischio a livello di asserzioni si compone a sua volta di due rischi, strettamente correlati al rischio d'impresa, ovvero il rischio intrinseco e rischio di controllo.
Il rischio intrinseco consiste nella probabilità che un'asserzione contenga un errore significativo a prescindere da qualsiasi controllo posto in essere dal revisore responsabile dell'incarico. Risulta maggiore per alcune asserzioni rispetto che per altre in quanto, per loro natura, sono soggette a stime o valutazioni da parte della società, come per esempio i fondi rischi e i fondi oneri; può dipendere anche da fattori esterni alla società, legati per esempio al settore di appartenenza, che potrebbero dar luogo ad un rischio di *business*.
L'aggiornamento dell'ISA 315 ha apportato delle novità anche all'individuazione e alla valutazione del rischio intrinseco. Innanzitutto, per facilitarne l'individuazione, ha introdotto dei fattori di rischio intrinseco che, se presenti, aumentano la possibilità che un'asserzione contenga un errore; in secondo luogo, ne ha modificato la modalità di valutazione introducendo lo "spettro del rischio intrinseco" costruito sulla base dell'entità e della probabilità di manifestazione dei fattori.

Il rischio di controllo è quella probabilità che un errore significativo non venga individuato e corretto dal sistema di controllo interno della società. La direzione aziendale infatti progetta, mette in atto e mantiene dei controlli per affrontare i rischi che ostacolano il raggiungimento degli obiettivi aziendali correlati alla redazione del bilancio. Questi rischi, però, sono impossibili da eliminare totalmente, possono solo essere ridotti a causa dei limiti intrinseci legati ai controlli, come per esempio la possibilità di forzatura dei controlli oppure la possibilità di errori umani.
Questo rischio, perciò, è strettamente correlato a carenze nel sistema di controllo della società e il revisore può verificare l'efficacia operativa dei controlli con lo scopo di definire le procedure di validità[42] da eseguire.

[41]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", pag. 53.
[42]Le procedure di validità sono delle procedure che il revisore svolge nel caso in cui i controlli posti in essere dalla società siano inefficaci oppure nel caso in cui non si voglia fare affidamento sui controlli. Hanno l'obiettivo di individuare rischi di errori significativi a livello di asserzioni e si concretizzano in: test di dettaglio e procedure di analisi comparativa.

L'aggiornamento dell'ISA 315 ha previsto inoltre una valutazione separata dei due rischi e non più congiunta come la versione precedente: prima il revisore valuterà il rischio intrinseco e successivamente, sulla base di esso, si occuperà del rischio di controllo.[43]

Il rischio di individuazione invece è il rischio che il revisore non identifichi, attraverso le procedure di revisione, un errore che potrebbe essere significativo. È perciò la possibilità oggettiva che un errore non venga individuato dal revisore.
Questo rischio dipende dalla natura, dalla tempistica e dall'estensione delle procedure che sono state definite dal revisore per ridurre il rischio di revisione. Le procedure, perciò, devono essere efficaci e per fare in modo che lo siano, è importante che vengono considerati i seguenti fattori:

1) l'attività di revisione deve essere pianificata in modo adeguato;
2) il personale assegnato al *team* di revisione deve essere appropriato;
3) il revisore deve applicare lo scetticismo professionale durante tutto l'incarico;
4) le carte di lavoro e l'intera attività devono essere supervisionati e riesaminati dai membri più competenti del gruppo.

Il rischio di individuazione e il rischio di errori significativi sono inversamente proporzionali tra loro in quanto al crescere del rischio di errori significativi che è stato definito, il revisore deve ridurre il rischio di individuazione acquisendo elementi probativi sufficienti ed appropriati e mettendo in atto le procedure di revisione adeguate. Nemmeno il rischio di individuazione può essere annullato totalmente ma può essere solo ridotto in quanto le procedure di revisione hanno dei limiti intrinseci che non possono essere eliminati. Questi limiti dipendono dalla natura delle procedure di revisione e dell'informativa finanziaria, ma anche dall'esigenza che la revisione sia svolta con tempi e costi adeguati.

Oltre a tali rischi, il revisore è tenuto a comprendere anche il rischio legato all'utilizzo dell'IT. Nel secondo capitolo sarà analizzato con precisione cosa si intende per rischio IT e che aspetti deve considerare il revisore per individuarlo ed analizzarlo.

[43]Per la trattazione di questi argomenti si rimanda al Capitolo 1, par. 1.4.2, pag. 26 della seguente trattazione.

1.4.1 Le asserzioni

Le asserzioni[44] sono delle dichiarazioni, sia implicite che esplicite, che una società fa in relazione alle informazioni che sono contenute nel bilancio. Predisponendo il bilancio una società attesta che tutte le operazioni aziendali siano state riportate e siano state rappresentate in bilancio in modo adeguato e nell'esercizio corretto.

Il revisore utilizza le asserzioni perché hanno l'obiettivo di evidenziare i diversi tipi di errori potenziali che potremmo riscontrare in un bilancio. Un'asserzione è considerata rilevante se ad essa è connesso un rischio di errore significativo e queste si dividono in due categorie principali.

Nella prima categoria rientrano le asserzioni relative a classi di operazioni ed eventi e l'informativa finanziaria connessa ad esse nel periodo amministrativo di riferimento che sono:

1) manifestazione: le operazioni e gli eventi che sono stati contabilizzati e che sono stati riportati nell'informativa finanziaria sono avvenuti e sono relativi all'azienda;
2) completezza: tutte le operazioni e gli eventi che sono realmente accaduti sono stati effettivamente contabilizzati e sono stati riportati nell'informativa inclusa nel bilancio;
3) accuratezza: gli importi connessi alle operazioni e agli eventi sono stati contabilizzati adeguatamente e la relativa informativa è stata predisposta e descritta adeguatamente;
4) competenza: la contabilizzazione delle operazioni e degli eventi è avvenuta nel periodo amministrativo corretto;
5) classificazione: sono stati utilizzati i conti corretti per contabilizzare le operazioni e gli eventi;
6) presentazione: le aggregazioni e disaggregazioni dei dati relativi alle operazioni e agli eventi sono state svolte in modo adeguato e sono state descritte in modo chiaro.

Nella seconda categoria rientrano invece le asserzioni relative ai saldi contabili e all'informativa finanziaria connessa ai saldi ed esse sono:

[44]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", par. A188- s.s., pag.51.

1) esistenza: ciò che rientra nell'attivo, nel passivo e nel patrimonio netto esiste;
2) diritti e obblighi: i diritti e gli obblighi sono posseduti dalla società. Nello specifico, la società ha il diritto di possedere o controllare le attività iscritte in bilancio e ha assunto personalmente le passività iscritte in bilancio;
3) completezza: la società ha contabilizzato tutte le attività, passività e componenti di patrimonio netto che avrebbero dovuto essere contabilizzate e la relativa informativa è stata predisposta e descritta adeguatamente;
4) accuratezza, valutazione e allocazione: gli importi e le rettifiche di valutazione e di allocazione connesse alle attività, alle passività e alle componenti di patrimonio netto sono state contabilizzate adeguatamente e la relativa informativa è stata predisposta e descritta adeguatamente;
5) classificazione: sono stati utilizzati i conti corretti per contabilizzare le attività, le passività e le componenti di patrimonio netto;
6) presentazione: le aggregazioni e le disaggregazioni dei dati relativi alle attività, passività e componenti di patrimonio netto sono state svolte in modo adeguato e sono state descritte in modo chiaro.

Le asserzioni sono perciò utilizzate come base per identificare eventuali errori potenziali e per individuare e valutare rischi di errori significativi. L'obiettivo sarà quello di definire le procedure di revisione che il revisore dovrà eseguire a fronte dei rischi individuati.

L'ISA 315 definisce il concetto di "asserzione rilevante", quando un'asserzione presenta un rischio di errori significativi identificato. Si determina la rilevanza di un'asserzione prima di considerare i relativi controlli sulla base del rischio intrinseco. Una classe di operazioni, un saldo contabile oppure l'informativa è detta rilevante per la revisione se per essa esistono una o più asserzioni rilevanti. [45]

La loro individuazione permette al revisore di determinare in quale misura dovrà comprendere il sistema informativo aziendale.

[45]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", par. A202, pag. 54.

1.4.2 Il rischio di errori significativi: individuazione e valutazione del rischio intrinseco

Il revisore deve identificare e valutare i rischi di errori significativi con lo scopo di definire le procedure di revisione conseguenti. Con tali procedure il revisore dovrà raccogliere gli elementi probativi che gli consentiranno di ridurre il rischio di revisione ad un livello accettabilmente basso[46].

Riguardo i rischi a livello di bilancio, il revisore deve identificare gli errori che hanno un effetto pervasivo nel bilancio e che richiedono, di conseguenza, delle risposte generali di revisione. Questa attività potrebbe aiutare il revisore nell'individuare i rischi a livello di asserzioni.

Nell'identificare il rischio a livello di asserzioni, il revisore deve valutare separatamente il rischio intrinseco e il rischio di controllo. Il revisore deve considerare innanzitutto il rischio intrinseco senza considerare i controlli posti in essere dalla società, ovvero effettuando delle considerazioni preliminari non considerando i controlli, al fine di identificare gli errori probabili e significativi.[47]

Nel valutare il rischio intrinseco, il revisore determinerà innanzitutto la probabilità del verificarsi di un errore potenziale e la sua entità. La combinazione di queste due componenti determinerà la significatività dell'errore che si collocherà in una scala di rischio: lo spettro del rischio intrinseco. Per probabilità si intende l'eventualità che un errore possa verificarsi. Il revisore fa questa considerazione sulla base dei fattori di rischio intrinseco, che vedremo a seguire.

Per entità dell'errore invece si intende la portata dell'errore sulla base della dimensione, della natura e delle circostanze. Il livello di significatività, ovvero il risultato della combinazione delle due componenti, è usato dal revisore per stabilire in che punto dello spettro del rischio intrinseco si trova quell'errore.

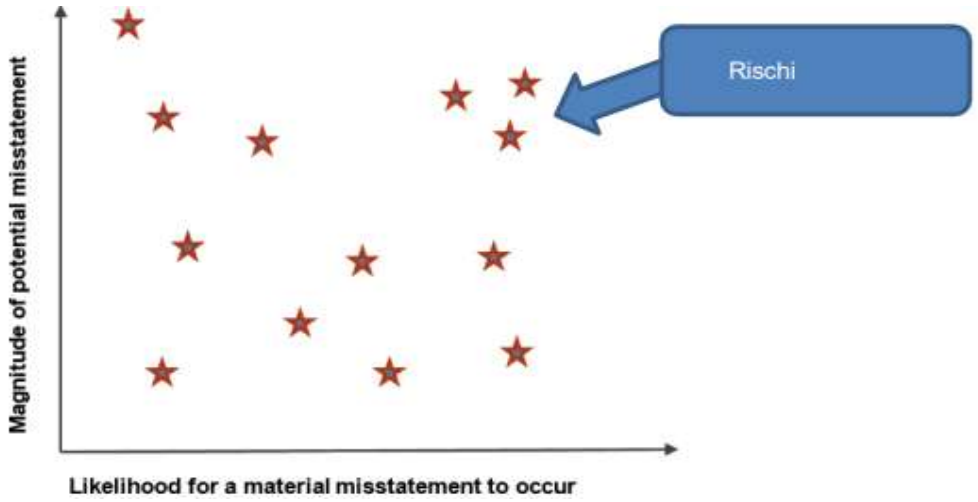
Lo spettro è un intervallo all'interno del quale si valuta il rischio intrinseco: più alto sarà il livello di significatività e più alto sarà il rischio; al contrario, più basso sarà il livello e più basso sarà il rischio. Se un rischio è valutato come elevato significa che la combinazione di probabilità ed entità di quell'errore è valutata come elevata. Questo non significa che entrambe le componenti sono elevate, ma che è elevata la sua

[46]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", par A185, pag. 51.

[47]La valutazione separata del rischio intrinseco e del rischio di controllo è una novità introdotta dall'aggiornamento dell'ISA 315.

combinazione; perciò, un determinato punto nello spettro può derivare da combinazioni diverse: entità elevata ma probabilità bassa e viceversa.
Lo spettro del rischio intrinseco può essere rappresentato dal grafico che segue:

Figura 1.4.3 Grafico dello spettro del rischio intrinseco



Fonte: IAASB, ISA 315 (Revised 2019) Identifying and Assessing the Risk of Material Missestment, First implementation Guide, July 2022.

Come si può vedere dal grafico sovrastante, nell'asse delle ascisse c'è la probabilità del verificarsi di un errore significativo e in quella delle ordinate l'entità potenziale di un errore significativo: la loro combinazione darà luogo ad un rischio
Lo spettro e i suoi estremi variano da azienda ad azienda e, per la stessa azienda, potrebbero variare da un periodo amministrativo all'altro in quanto dipendono dalla dimensione e dalla complessità dell'azienda, sarà il revisore a determinarli con il proprio giudizio professionale.

Nel considerare il rischio intrinseco, il revisore deve considerare anche i cosiddetti "fattori del rischio intrinseco", ovvero quelle caratteristiche, sia qualitative che quantitative, che potrebbero influenzare la probabilità che un'asserzione contenga errori, senza aver prima considerato i controlli. [48]
I fattori correlati alla predisposizione dell'informativa finanziaria sono cinque.

[48]L'appendice 2 del principio di revisione internazionale ISA Italia 315 tratta il rischio intrinseco, riportando degli esempi che potrebbero aiutare il revisore. Gli esempi forniti non devono essere considerati né in modo esaustivo e né in modo esclusivo.

Il primo fattore è la complessità relativa alla natura delle informazioni e alla modalità di predisposizione delle stesse. Si presenta, ad esempio, quando la società calcola accantonamenti oppure stime contabili. In queste due circostanze è possibile che i processi di predisposizione delle informazioni possano essere complessi da applicare.
Alcuni esempi di complessità possono essere i seguenti:

- ➔ l'impresa è soggetta ad una regolamentazione complessa a causa dell'attività svolta;
- ➔ la società fa parte di alleanze e *joint venture* complesse;
- ➔ processi complessi che richiedono una relativa quantificazione finanziaria complessa;
- ➔ operazioni aziendali complesse.

Il secondo fattore è la soggettività legata alla capacità di predisporre in modo obiettivo le informazioni. Un limite relativo alla predisposizione delle informazioni è dato dalla soggettività delle scelte o valutazioni elaborate dalla direzione aziendale in merito all'approccio appropriato da adottare per predisporre le informazioni che saranno incluse nel bilancio. Gli approcci utilizzati potrebbero essere diversi portando risultati diversi rispetto a quanto previsto dall'informativa finanziaria. Maggiori sono i limiti legati alla conoscenza, maggiore sarà la valutazione soggettiva e maggiore sarà la diversità dei risultati. La soggettività potrebbe essere relativa, ad esempio, al criterio di quantificazione delle stime contabili oppure ad una metodologia di valutazione

Il terzo fattore è il cambiamento relativo a tutti quegli eventi e quelle condizioni che influenzano sia l'impresa direttamente che i suoi aspetti contabili, regolamentari ed economici. Il cambiamento può avvenire nel corso di un esercizio oppure tra due esercizi differenti. Anche cambiamenti nell'ambiente IT potrebbero influenzare l'impresa come, ad esempio, l'implementazione di nuovi sistemi IT condizionerebbe la predisposizione dell'informativa finanziaria. Il cambiamento può dipendere, ad esempio:

- ➔ dall'instabilità dell'area economica, del mercato oppure del settore di appartenenza dell'azienda;
- ➔ dalla possibilità di perdere clienti e fornitori;
- ➔ da un problema di continuità aziendale;
- ➔ dall'ingresso in nuovi mercati o in nuove aree di business;

- ➔ da cambiamenti relativi al personale: nuove assunzioni oppure licenziamenti di personale qualificato e di personale in posizioni apicali;
- ➔ dalla componente IT: cambiamenti dell'infrastruttura IT oppure installazioni di nuovi programmi o software;
- ➔ da cambiamenti relativi alle normative vigenti.

Il quarto fattore è l'incertezza che si manifesta nei casi in cui le informazioni aziendali vengano prodotte sulla base di dati poco precisi e poco completi, i quali non possono essere verificati per mezzo dell'osservazione diretta. Le informazioni, infatti, devono essere predisposte sulla base di dati precisi e completi, se disponibili, ma nei casi in cui non lo siano, la società dovrà fare delle previsioni ragionevoli a supporto dei dati disponibili. La mancanza di disponibilità di dati completi è un limite delle società che provoca incertezza nella predisposizione dell'informativa finanziaria. L'incertezza può essere relativa, ad esempio, a contenziosi potenziali oppure nella quantificazione e rilevazione contabile di nuove operazioni aziendali.

Il quinto, e ultimo, fattore è *"la possibilità di errori dovuti a ingerenze da parte della direzione o ad altri fattori di rischio di frodi nella misura in cui influenzano il rischio intrinseco"*[49], ovvero la possibilità che le informazioni aziendali contengano errori a causa di un'intromissione della direzione aziendale nella predisposizione delle informazioni. Gli errori sono causati da una mancanza di neutralità, intenzionale o meno, della direzione aziendale che può essere intercettata da fattori come incentivi o pressioni, come ad esempio l'esercizio di una pressione eccessiva per il raggiungimento degli obiettivi aziendali può indurre a falsificare le informazioni aziendali.
Se questi comportamenti sono intenzionali si tratta di comportamenti fraudolenti e nello specifico l'ISA Italia 240 evidenzia i fattori che potrebbero segnalare errori dovuti a frodi legate alla falsa informativa finanziaria.[50]
Esempi di questi comportamenti possono essere relativi:

- ➔ alla possibilità per la direzione aziendale, data la posizione apicale, di emettere una falsa informativa finanziaria oppure di omettere operazioni significative;

[49]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", Appendice 2, par. 2, pag. 66.
[50]Le attività sono descritte ai paragrafi A1-A5 del principio di revisione internazionale (ISA Italia) n. 240.

- ➔ operazioni con parte correlate, ovvero quei soggetti che hanno la possibilità, per la posizione in cui si trovano, di controllare o influenzare le decisioni finanziarie di un'impresa;
- ➔ operazioni straordinarie, come ad esempio le operazioni infragruppo.

È possibile che i fattori siano tra loro interconnessi, ad esempio, se il rischio di soggettività è elevato è più probabile che sia alto anche il rischio di ingerenze da parte della direzione aziendale nel produrre le informazioni finanziarie.

Il revisore deve considerare i rischi di errori significativi che si trovano nell'estremo superiore dello spettro del rischio intrinseco per numerosi motivi e perché da essi derivano svariati obblighi successivi in capo al revisore.
Innanzitutto, a fronte dei rischi identificati, il revisore deve individuare i controlli delineati dalla società[51], successivamente deve valutare se sono stati messi in atto e se sono efficaci[52], e questi devono essere verificati nell'esercizio in cui sono stati istituiti.
Successivamente, in conformità all'ISA Italia 330, il revisore deve mettere in atto delle procedure in risposta ai rischi identificati: deve pianificare e svolgere procedure di validità e deve acquisire elementi probativi sufficienti e appropriati.
In conformità all'ISA 260[53], il revisore deve comunicare alla direzione aziendale e ai responsabili dell'attività di governance i rischi identificati e come intende fronteggiarli.
Inoltre, in conformità all'ISA 701[54], il revisore deve tener presente i rischi identificati al fine di stabilire gli aspetti che gli hanno richiesto un'attenzione particolare e che potrebbero essere significativi per la revisione.
Infine, il responsabile dell'incarico di revisione deve riesaminare tempestivamente la documentazione prodotta e raccolta durante la revisione con l'obiettivo di risolvere in tempo e in modo efficace gli aspetti che sono stati considerati significativi, tra cui anche i rischi significativi.

[51]I controlli che fronteggiano i rischi devono essere istituiti in conformità al paragrafo 26 a) - i) dell'ISA Italia 315.
[52]L'attività deve essere svolta in conformità al paragrafo 26 d) dell'ISA 315.
[53]Principio di revisione internazionale (ISA Italia) 260: "Comunicazione con i responsabili dell'attività di governance".
[54]Principio di revisione internazionale (ISA Italia) 701: "Comunicazione degli aspetti chiave della revisione contabile nella relazione di revisione indipendente".

1.4.3 Il rischio di controllo: valutazione

Dopo aver identificato il rischio intrinseco, il revisore potrà verificare l'efficacia operativa dei controlli al fine di identificare e valutare il rischio di controllo. Il revisore può anche non pianificare di valutare i controlli e in questo caso il rischio di errori significativi sarà pari al rischio intrinseco.

In relazione ai controlli, il revisore si creerà, innanzitutto, un'aspettativa iniziale sulla base dei controlli definiti e configurati dalla componente "attività di controllo" del sistema di controllo interno. Successivamente verificherà se i controlli sono stati messi in atto effettivamente e se sono efficaci con l'obiettivo di confermare o meno l'aspettativa iniziale.

La valutazione del rischio di controllo è perciò strettamente correlata al sistema di controllo interno delle società in quanto il revisore lo comprenderà al fine di individuare i controlli configurati sui quali testerà l'efficacia.

Se le aspettative non sono confermate e i controlli non operano in modo efficace, il revisore dovrà riconsiderare l'identificazione e la valutazione del rischio acquisendo nuove informazioni.

Il revisore può utilizzare diverse tecniche e diversi metodi per valutare il rischio di controllo.

Nella pianificazione delle verifiche, il revisore definirà quali controlli valutare: può valutare i controlli diretti, i controlli indiretti e i controlli generali IT, considerando anche come vengono combinati tra di loro. Se il controllo messo in atto non contrasta in modo efficace il rischio intrinseco, il revisore dovrà definire delle risposte conseguenti per il ridurre il rischio di revisione ad un livello accettabilmente basso.

L'aggiornamento dell'ISA 315 ha apportato novità in merito ai controlli IT in quanto ha definito delle procedure specifiche e degli aspetti che il revisore dovrà considerare nell'identificazione e nella valutazione dei controlli IT.[55] Il revisore, infatti, dovrà valutare la progettazione e successivamente l'efficacia dei controlli generali IT che supportano la società nel fronteggiare i rischi derivanti dall'uso dell'IT all'interno di una società.

Se i controlli generali IT non sono stati configurati e messi in atto in modo efficace, aumenterà il rischio di errori significativi a livello di asserzioni. Sarà compito del

[55]L'appendice 6 dell'ISA Italia 315 si occupa di trattare il ruolo del revisore nel verificare i controlli IT.

revisore pianificare delle procedure conseguenti in conformità all'ISA 330. I controlli generali IT e i test sui controlli sono approfonditi nel terzo capitolo di questo elaborato.

1.5. Le procedure di valutazione del rischio

L'attività di identificazione e di valutazione del rischio viene messa in atto mediante procedure di valutazione del rischio, ovvero procedure "*definite e svolte per identificare e valutare i rischi di errori significativi, dovuti a frodi o a comportamenti o eventi non intenzionali, a livello di bilancio e di asserzioni"*[56].

Nello svolgere queste procedure, il revisore acquisisce elementi probativi sufficienti e appropriati, i quali saranno anche elementi probativi della revisione. Essi guideranno il revisore nell'individuazione dei rischi di errori significativi ma lo guideranno anche nella definizione delle risposte ai rischi.

Il revisore deve acquisire elementi probativi in maniera imparziale al fine di esercitare lo scetticismo professionale richiesto dall'incarico. La fonte degli elementi può essere sia interna che esterna: le informazioni raccolte possono provenire infatti dalla direzione aziendale, dai revisori interni, o da altro personale aziendale; oppure possono essere informazioni che sono disponibili al pubblico esterno alla società come, ad esempio, analisi di consulenti esterni, comunicati stampa, comunicati per gli investitori. Indipendentemente dalla fonte però, gli elementi probativi devono essere pertinenti e attendibili.

Nel definire quali procedure svolgere, il revisore deve definirne la natura e l'estensione in base alla società che ha di fronte, applicando costantemente il proprio giudizio professionale.

È possibile che la natura e l'estensione di tali procedure siano più vaste nel caso di primo incarico e più limitate negli esercizi seguenti e successivi, in quanto il revisore potrebbe poi concentrarsi principalmente sulle variazioni avvenute tra due esercizi. [57]

Le procedure di valutazione del rischio sono principalmente tre:

1) indagini presso la direzione aziendale e verso qualsiasi altro soggetto in azienda, anche verso il personale preposto alla funzione di revisione interna se presente;
2) procedure di analisi comparativa;

[56]Principio di revisione internazionale (ISA Italia)315: "Identificazione e valutazione dei rischi di errori significativi", definizione j, pag. 6.

[57]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", par. A14-A18, pag. 15-16.

3) osservazioni e ispezioni.[58]

Per indagine si intende la ricerca di dati e informazioni finanziarie e non finanziarie svolta dal revisore presso i membri della società di riferimento.[59] Possono essere svolte presso la direzione aziendale, presso la funzione di revisione interna e presso qualsiasi altro soggetto dipendente. Svolgere la stessa indagine verso diversi livelli di autorità può aiutare il revisore ad individuare e valutare i rischi di errori significativi. Ad esempio, le indagini svolte presso la direzione aziendale potrebbero aiutare il revisore nella comprensione del grado di supervisione che la direzione applica nella redazione del bilancio. Le indagini svolte nei confronti dei dipendenti che si occupano di rilevare e contabilizzare operazioni complesse potrebbero aiutare il revisore a comprendere la modalità con cui sono state rilevate. Invece, per avere maggiori informazioni riguardo controversie legali, garanzie, accordi commerciali, frodi o sospette frodi e qualsiasi altro aspetto legale, il revisore potrebbe rivolgersi al consulente legale interno della società. Per avere informazioni riguardo eventuali rischi a cui è esposta la società, potrebbe svolgere indagini presso il personale addetto alla gestione del rischio.

Per avere, invece, informazioni riguardo i sistemi IT implementati nella società e gli eventuali rischi connessi, il revisore potrà avere come figura di riferimento il personale addetto all'IT.

Le indagini vengono svolte anche verso il personale addetto alla funzione di revisione interna, se presente nella società, in quanto possono aiutare il revisore nella comprensione dell'impresa, del contesto in cui opera e del suo sistema di controllo interno.

Per procedure di analisi comparativa, invece, si intendono tutte quelle valutazioni delle informazioni finanziarie attraverso l'analisi di legami tra dati finanziari e non finanziari.[60] Queste procedure sono vantaggiose perché portano alla luce eventuali incoerenze, relazioni inusuali oppure andamenti che potrebbero aiutare il revisore nell'identificare rischi di errori significativi. Sono utili perché mediante esse è facile che il revisore prenda in considerazione nuovi aspetti che inizialmente non considerava.

[58]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", pag. 7.
[59]Principio di revisione internazionale (ISA Italia) 500: "Elementi probativi", par. A26-A29, pag. 10.
[60]Principio di revisione internazionale (ISA Italia) 500: "Elementi probativi", par. A25, pag. 10

Queste procedure, perciò, si concretizzano nella comparazione di dati. I dati possono riguardare singole informazioni, finanziarie e non finanziarie, oppure possono riguardare informazioni aggregate ad alto livello. Un esempio di analisi comparativa è la comparazione dei saldi contabili trimestrali rispetto ai saldi dei periodi amministrativi precedenti per evidenziare eventuali aree più a rischio rispetto ad altre.
Il revisore può servirsi di strumenti e tecniche automatizzate per svolgere tali procedure, soprattutto se deve comparare un grande numero di dati[61]. Può infatti utilizzare fogli di calcolo oppure tecniche di visualizzazione per evidenziare saldi contabili oppure classi di operazioni inusuali per i quali sono necessari ulteriori approfondimenti.

Gli obiettivi delle osservazioni e delle ispezioni sono principalmente due: innanzitutto, confermare oppure contraddire le informazioni raccolte dal revisore tramite le indagini; e, in seguito, fornire ulteriori informazioni sull'impresa e sui controlli interni.
Il revisore svolge un'osservazione quando assiste ad un processo o ad una procedura svolta dalla società acquisendo elementi probativi sull'esecuzione di tale processo o procedura. Un classico esempio di osservazione è il controllo del personale dell'azienda nello svolgere una conta fisica delle rimanenze. È importante evidenziare che gli elementi probativi acquisiti potrebbero non essere veritieri in quanto l'essere osservati influenza il modo in cui viene eseguita una determinata procedurea. [62]
Un'ispezione, invece, è un'analisi di registrazioni contabili e di documenti aziendali. La documentazione esaminata potrebbe provenire sia dall'interno che dall'esterno dell'impresa e potrebbe essere sia cartacea che elettronica. Le ispezioni forniscono elementi probativi ma in base alla provenienza, alla natura e al formato delle informazioni esaminate varia il loro grado di attendibilità.
Le osservazioni e le ispezioni aiutano il revisore ad acquisire elementi probativi anche sui controlli nel caso in cui la direzione aziendale abbia messo in atto controlli poco formalizzati oppure direttive non documentate. Ad esempio, se il revisore vuole verificare che controlli vengono messi in atto durante una conta fisica, in quanto poco formalizzati, potrebbe osservare direttamente come viene effettuata. Se invece vuole

[61]Si usa l'espressione "data analytics" quando le procedure di analisi comparativa di applicano ai dati.
[62]Principio di revisione internazionale (ISA Italia) 500: "Elementi probativi", par. A18-A21, pag. 9.

verificare come sono separate le funzioni in azienda, lo può osservare direttamente sul campo.

Le osservazioni e le ispezioni svolte come procedure di valutazione del rischio riguardano:

- lo svolgimento di attività aziendali;
- documenti redatti dalla direzione aziendale e dai responsabili delle attività di governance come, ad esempio, l'ispezione dei bilanci intermedi oppure dei verbali predisposti dal Consiglio di amministrazione;
- documentazione interna predisposta dall'azienda, registrazioni contabili e manuali relativi al sistema di controllo interno;
- documenti e informazioni acquisite da fonti esterne all'azienda come ad esempio banche, consulenti, agenzie di rating, riviste economiche;
- l'atteggiamento tenuto dalla direzione aziendale, come ad esempio l'osservazione di una riunione del consiglio istituito per il controllo interno. Anche in questo caso potrebbero essere svolte per mezzo di strumenti automatizzati, come ad esempio con strumenti che consentono l'osservazione da remoto, come i droni.

Al fine di acquisire elementi probativi sufficienti e appropriati, il revisore può esaminare anche informazioni proventi da altre fonti[63] se sono rilevanti al fine di comprendere, ad esempio, i rischi di *business* dell'impresa, il quadro normativo applicabile, i valori etici, l'integrità della direzione aziendale ed eventuali cambiamenti rispetto ad esercizi precedenti.

Le fonti potrebbero riferirsi ad informazioni che il revisore aveva acquisito al fine di valutare se accettare o se mantenere l'incarico di revisione con la società di riferimento oppure che aveva acquisito svolgendo altri incarichi per la società. Per altri incarichi si intendono, ad esempio, incarichi di revisioni precedenti, incarichi di *Assurance* oppure altri incarichi obbligatori previsti dalle norme giuridiche.

Se le informazioni provengono da incarichi o esperienze precedentemente svolte, il revisore deve valutare se sono opportune e adatte per essere utilizzate anche nell'incarico di revisione in corso. Infatti, alcune situazioni potrebbero essere variate e perciò le informazioni raccolte in precedenza potrebbero non essere pertinenti e, perciò,

[63]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", par.15 e par. A37-A41, pag. 7 e pag. 19-20.

utilizzabili. Per valutarne l'appropriatezza, il revisore potrebbe svolgere verifiche "*walk-through*", ovvero test che prevedono la verifica di un'informazione contabile passo dopo passo attraverso il sistema contabile dal suo inizio alla disposizione finale.
In ogni caso le esperienze passate con la società potrebbero fornire informazioni importanti riguardo errori individuati in passato, informazioni riguardo l'impresa e il suo sistema di controllo interno, informazioni riguardo cambiamenti avvenuti tra due esercizi oppure informazioni riguardo situazioni ed operazioni complesse.

1.6 La documentazione

L'ISA Italia 315 include un obbligo di documentazione delle procedure svolte e delle informazioni raccolte in questa fase della revisione.
Il revisore infatti deve documentare:

1) ciò che è stato discusso all'interno del *team* di revisione e le decisioni significative che sono state assunte, anche in relazione al quadro normativo sull'informativa finanziaria applicato;
2) gli aspetti importanti recepiti dal revisore nella fase di comprensione[64] dell'impresa e del suo sistema di controllo interno e le relative fonti di informazione;
3) la valutazione dei controlli identificati: come sono stati configurati, come sono stati messi in atto e la loro efficacia[65];
4) i rischi di errori significativi a livello di bilancio e a livello di asserzioni che sono stati individuati e valutati nel corso delle procedure di revisione.

Se l'incarico è ricorrente, il revisore può utilizzare e aggiornare la documentazione raccolta in incarichi precedenti al fine di evidenziare i cambiamenti che sono avvenuti da un esercizio all'altro.
Una corretta e accurata documentazione è importante per dare evidenza dello scetticismo professionale tenuto dal revisore[66] . Se, ad esempio, durante le procedure di valutazione del rischio vengono raccolti elementi probativi in contrasto con le asserzioni, il revisore deve dare evidenza della fonte da cui provengono tali elementi e deve dare un giudizio professionale al fine di valutare il rischio di errori significativi.

[64]L'attività deve essere svolta in conformità dei paragrafi 19, 21, 22, 24 e 25 dell'ISA Italia 315.
[65]L'attività deve essere svolta in conformità alle regole del paragrafo 26 dell'ISA Italia 315.
[66]Principio di revisione internazionale (ISA Italia) 230: "La documentazione della revisione contabile".

La documentazione deve essere predisposta dal revisore sulla base del proprio giudizio professionale[67] e ha lo scopo di permettere ad un revisore esterno all'incarico ed esperto di comprendere le tempistiche, l'estensione e la natura delle procedure di revisione programmate e svolte dal revisore dell'incarico. Deve essere molto dettagliata nei casi in cui il revisore abbia formulato dei giudizi complessi e articolati.

Il livello di dettaglio richiesto per la documentazione dipende anche dalla complessità dell'impresa sottoposta a revisione: se l'impresa è poco complessa anche la documentazione necessaria sarà più semplice. La complessità della documentazione è strettamente correlata alle dimensioni dell'azienda, alla complessità dell'azienda e del suo sistema di controllo interno, alle tecniche e alle procedure di revisione svolte.

Il revisore non deve documentare tutta l'attività di revisione ma è necessario che documenti solo gli elementi che stanno alla base della sua valutazione dei rischi di errori significativi.

[67]L'attività deve essere svolta nel rispetto delle regole contenute nel paragrafo 38 dell'ISA 315.

CAPITOLO 2: TECNOLOGIA E NORMATIVE VIGENTI

2.1 Informazione e progresso tecnologico

Come definito dall'aggiornamento dell'ISA 315, il revisore dovrà svolgere delle procedure specifiche al fine di comprendere la componente IT della società, con l'obiettivo di individuare eventuali rischi di errori significativi.

Siccome i processi amministrativi e contabili sono sempre più automatizzati e svolti all'interno di sistemi informatici automatizzati, c'era bisogno di maggior certezza relativa alla correttezza dei dati e delle informazioni contenute nell'informativa di bilancio. Per svolgere tali verifiche, però, sono necessarie delle competenze e delle conoscenze specifiche, che vanno oltre la sola conoscenza economica, e perciò è necessario l'intervento di un *IT Auditor*, ovvero un revisore con competenze specifiche relative alla componente IT[68].

Le informazioni aziendali, perciò, sono degli elementi essenziali per le organizzazioni e, ad oggi, l'informatica svolge un ruolo chiave per l'informativa finanziaria prodotta dalle società: la tecnologia è fondamentale in quanto segue il processo dell'informazione dal momento in cui viene creata, partendo dai dati, fino al momento della sua distruzione. L'"Informatica" (Informazione automatica) è, infatti, la scienza che studia come, attraverso strumenti tecnologici, i dati vengono raccolti, analizzati ed elaborati e come le informazioni vengono prodotte. "Dato" e "informazione" non sono tra loro sinonimi. Per dato si intende una rappresentazione concreta e oggettiva della realtà, il quale può essere raccolto per mezzo di osservazioni interne o esterne alla società oppure attraverso test su eventi specifici. Il dato visto singolarmente non ha alcun significato ma lo assume nel momento in cui viene elaborato e interpretato, trasformandosi così in informazione. L'informazione è quel risultato che permette alla società di poter prendere delle decisioni sulla base dei dati che sono stati raccolti[69].

L'informatica si è diffusa rapidamente in quanto risulta sempre più evidente la necessità di trasformare i dati in risultati in modo economico, veloce e sicuro al fine di sfruttarli in base ai bisogni delle persone ma soprattutto delle aziende. L'avvento dell'IT ha reso i

[68]Il ruolo dell'IT Auditor sarà ampiamente descritto nei Capitoli 3 e 4 della seguente trattazione.
[69]Pighin M., Marzona A., *Sistemi informativi aziendali, ERP e sistemi di data analysis, Terza edizione*, Pearson, Milano, 2018, pag. 2-3.

processi aziendali più efficienti ed efficaci ma allo stesso tempo ha portato con sé anche nuovi rischi che le aziende si sono trovate ad affrontare.
I sistemi IT, essendo strettamente correlati ai dati aziendali, devono operare in modo adeguato al fine di garantire un'informativa finanziaria veritiera e corretta. È necessario, infatti, che i sistemi IT siano affidabili al fine di prevenire perdite economiche e danni reputazionali per l'azienda.
Proprio per questi motivi è necessaria l'attività di *audit* della componente IT al fine di garantire la continuità aziendale e la verifica della qualità dei processi.
Nel prossimo paragrafo è stato analizzato come l'utilizzo dell'informatica si è evoluto all'interno delle aziende, dall'avvento del primo prototipo di computer alle tecnologie avanzate che abbiamo oggi.

2.1.1 Evoluzione storica della tecnologia all'interno delle società

L'adozione della componente informativa all'interno delle società è cambiata e si è evoluta nel tempo a pari passo con l'evoluzione storica delle tecnologie informatiche e della comunicazione.
L'informatica nasce nel 1945, ovvero l'anno in cui è stato prodotto il primo prototipo di computer, e da quell'anno in poi l'evoluzione è stata velocissima: siamo passati da calcolatori giganteschi con pochissima memoria ed esigue funzionalità ai sistemi potentissimi che abbiamo oggi.
La prima adozione a livello aziendale dell'informatica avvenne intorno agli anni Sessanta, quando IBM[70] produsse il "Sistema 360", ovvero un computer adibito anche ad uso commerciale, che ebbe fin da subito un forte successo. Le prime società a servirsene furono le grandi imprese perché avevano la necessità di elaborare una grande quantità di dati al fine di sviluppare informazioni in modo efficiente ed efficace. La prima area aziendale in cui fu integrato l'uso dell'informatica fu quella amministrativa in quanto c'era la necessità di velocizzare lo svolgimento delle operazioni standard come, per esempio, la registrazione delle fatture. Successivamente i sistemi informativi aziendali iniziano a supportare anche le attività di pianificazione e di controllo perché, grazie alla grande quantità di dati raccolti, le società erano in grado di calcolare indici di

[70]L'International Business Machines Corporation (IBM) è un'azienda statunitense, la più anziana e tra le più conosciute e rispettabili al mondo nel settore informatico.

performance necessari per pianificare le azioni future e per verificare l'andamento aziendale con il fine ultimo di redigere il bilancio.
L'informatica divenne a portata delle imprese di piccole e medie dimensioni intorno agli anni Ottanta grazie alla diffusione dei personal computer, ovvero calcolatori più piccoli che potevano stare nelle scrivanie di chi li usava; e grazie all'introduzione dei sistemi di rete. La crescente diffusione dei computer portò ad un conseguente abbattimento dei costi informatici, facendo in modo che potessero essere accessibili a tutte le imprese.
Cresce però il bisogno da parte delle società di aumentare la velocità e la flessibilità dei sistemi informatici e intorno agli anni Novanta si diffondono, in risposta ai bisogni delle società, i sistemi ERP (*Enterprise Resource Planning*). Per ERP (in italiano si usa comunemente il termine "gestionale") si intende un *software* che ha l'obiettivo di integrare tutti i processi aziendali: ciclo attivo, ciclo passivo, contabilità e bilancio, finanza, gestione del personale, produzione e commercializzazione dei beni e servizi.
Dagli anni 2000, l'informatica ha cambiato anche il rapporto delle società con l'ambiente esterno: le società, infatti, sfruttando la connessione ad Internet, si aprono a nuove opportunità. Per esempio, aprono canali di vendita online, impensabili senza l'avvento di Internet, e iniziano a sfruttare i canali social a fini promozionali. [71]

Ad oggi, la politica è fortemente orientata a sostenere la transizione verso un'"Industria 4.0" e questo fenomeno è detto Quarta Rivoluzione Industriale, la quale ha lo scopo di creare un nuovo prototipo di industria. L'obiettivo della rivoluzione è quello di creare un'industria sempre più automatizzata e interconnessa grazie a due strumenti: la tecnologia e l'innovazione.
Non è uno scenario futuro, ma è una realtà che stanno affrontando le aziende e i manager devono adeguarsi a questi mutamenti per non perdere competitività nel mercato e per creare valore. Per restare al passo con i tempi, le società devono superare il modello di business "tradizionale" e devono passare necessariamente ad un modello di business intelligente e innovativo. Ciò non significa semplicemente introdurre in azienda nuove tecnologie ma il cambiamento deve riguardare l'intera impresa.
Un evento che ha dato una forte spinta a ciò è stata sicuramente la pandemia da Covid-19 grazie alla quale le aziende si sono rese conto dell'importanza della digitalizzazione,

[71]Pighin M., Marzona A., *Sistemi informativi aziendali, ERP e sistemi di data analysis, Terza edizione*, Pearson, Milano, 2018, pag. 10-16.

in quanto era vitale per affrontare quella situazione e per non interrompere totalmente l'attività lavorativa. Ha costretto le aziende meno sviluppate dal punto di vista tecnologico a focalizzarsi su nuovi investimenti innovativi per migliorare la connessione dell'impresa con l'ambiente esterno, per consentire sempre di più il lavoro da remoto e per incentivare le vendite online. Infatti, uno studio svolto dall' *European Investment Bank*[72], ha dimostrato che le aziende digitali hanno avuto meno ripercussioni negative provocate dalla pandemia rispetto ad altre aziende.

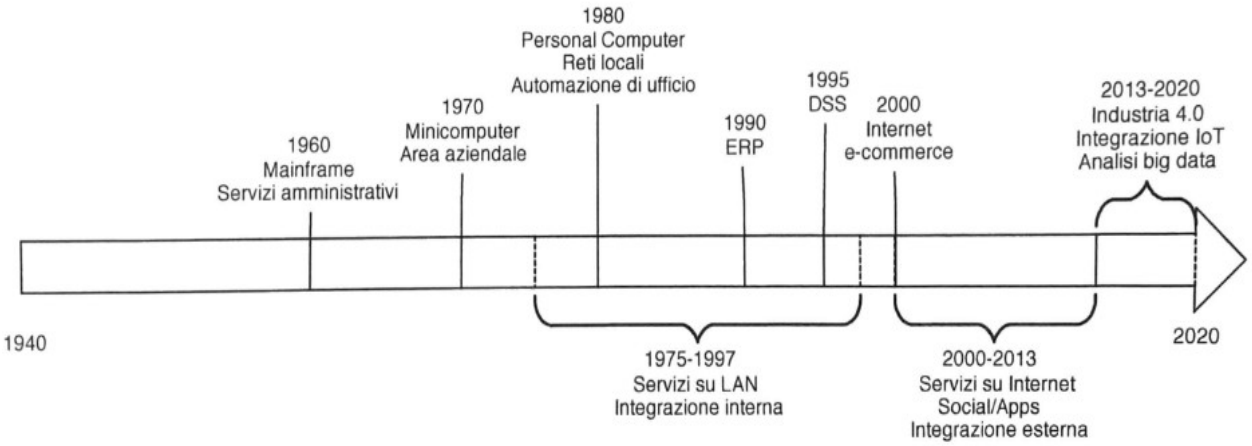
La costante automazione ha permesso inoltre lo sviluppo di tecnologie emergenti come le *blockchain*, la robotica e l'Intelligenza Artificiale.
Per *blockchain*, letteralmente "catena a blocchi", si intende un grande registro virtuale e immutabile utilizzato per tracciare le risorse e le transazioni di una realtà aziendale. Ciò permette di aumentare la sicurezza delle informazioni aziendali e allo stesso tempo di ridurre i costi di gestione delle informazioni. È utile in quanto fornisce informazioni in modo immediato, condiviso e trasparente in quanto tali informazioni sono memorizzate in un registro in cui possono accedere solo i soggetti autorizzati. Le informazioni che possono essere scambiate sono svariate, tra cui ad esempio gli ordini, gli acquisti, i pagamenti, le risorse in magazzino.
Ogni transazione deve essere considerata come un "blocco" della catena, il quale deve essere collegato al blocco precedente e in seguito al blocco successivo. Per ogni blocco può essere indicato ad esempio il luogo della transazione, l'importo, l'ora e tali dati devono essere coerenti con il blocco precedente, al fine di confermarne la validità. Ogni blocco infatti deve verificare e confermare la legittimità dei dati del blocco precedente affinché l'ultimo blocco possa essere aggiunto alla catena: ogni blocco aggiuntivo, infatti, rafforza la validità del blocco precedente e perciò di tutta la *blockchain*. Ciò permette di aumentare la sicurezza e la fiducia nei dati inseriti[73].
Per robotica invece si intende quella branca dell'ingegneria che si occupa di progettare dei robot con l'obiettivo di riprodurre e svolgere dei compiti in modo automatico senza che essi siano svolti dall'uomo. Sono utilizzati soprattutto in campo industriale per svolgere azioni ripetitive, come quelle svolte in una catena di montaggio. Possono aumentare l'efficienza del lavoro svolto portando benefici in termini di costi e di tempo.

[72]European Investment Bank, *"Digitalisation in Europe 2021-2022, Evidence from the EIB Survey",* Documento di Pubblica Consultazione, 2022.
[73]Nasce nel mondo delle criptovalute al fine di tracciare e convalidare ogni transazione di bitcoin.

Per Intelligenza Artificiale (IA) si intende quella branca della tecnologia che ha l'obiettivo di progettare e creare dei sistemi che abbiano le caratteristiche tipiche della mente umana, ovvero che abbiano ad esempio competenze decisionali, capacità di *problem-solving* e di pianificazione, capacità creative e di relazione.
Viene utilizzata in moltissimi campi, ma in campo aziendale permette ad esempio di analizzare i dati al fine di prevedere le tendenze e le situazioni future, permettendo allo stesso tempo di utilizzare i dati recepiti in modo vantaggioso. Ad esempio, la società Netflix, società statunitense che distribuisce in streaming film e serie TV, grazie all'IA ha offerto ai suoi clienti un servizio sempre più personalizzato, aumentando così la sua base clienti del 25%.

Di seguito è riportata graficamente una linea del tempo che evidenzia l'evoluzione storica dell'utilizzo dell'informatica all'interno dei contesti aziendali, dalla prima adozione alle tecnologie emergenti che ci sono oggi.

Figura 2.1. L'evoluzione storica della tecnologia all'interno dell'azienda



Fonte: Pighin M., Marzona A., Sistemi informativi aziendali, ERP e sistemi di data analysis, Terza edizione, Pearson, Milano, 2018, pag.16.

2.2 I benefici e i rischi IT

I benefici apportati dall'utilizzo di strumenti tecnologici e automatizzati sono molteplici.
In primis, l'uso della tecnologia nello svolgimento dei processi operativi permette di ridurre il costo della manodopera grazie all'uso di procedure automatizzate. Tali procedure rendono il lavoro più veloce, garantiscono il miglioramento dei processi rendendoli più controllati e veloci e infine permettono di aumentare la qualità e la quantità dei dati raccolti. L'area aziendale in cui sono stati utilizzati questi processi per la prima volta è stata quella amministrativa, in quanto è caratterizzata da procedure standard dettate da norme di legge e di conseguenza comuni a tutte le società. Successivamente, i processi automatizzati si sono estesi a tutte le aree aziendali.
Un secondo beneficio riguarda il fatto che la grande quantità di dati raccolti per mezzo dell'automazione permette di migliorare le procedure di pianificazione che una società è tenuta a svolgere. Conoscere dati storici e attuali della società permette di definire gli obiettivi e di pianificare le politiche conseguenti in modo più accurato e consapevole.
Un terzo beneficio riguarda la veridicità dei dati raccolti in quanto vengono sottoposti ad un costante controllo. Il controllo può avvenire in modo automatico oppure può essere condotto in modo esplicito e manuale da parte della direzione.
In conclusione, oltre a portare benefici agli operatori aziendali nello svolgimento del proprio lavoro, i sistemi informativi aziendali supportano la direzione nel prendere decisioni grazie ai dati, ai sistemi di *reporting* e di trasmissione delle informazioni. I manager, infatti, sono guidati dai sistemi informativi nella risoluzione dei problemi, nella definizione di nuove strategie e nella creazione di nuovi prodotti e servizi.

Oltre ai benefici precedentemente descritti, ci sono anche molti rischi relativi all'IT che il revisore deve considerare.
Esistono varie definizioni di rischio IT, ma l'ISACA *(Information Systems Audit and Control Association),* ovvero un'associazione riconosciuta a livello globale in quanto molto attiva riguardo i temi IT, definisce tale rischio come un rischio operativo relativo all'utilizzo dell'IT che si concretizza in eventi e situazioni causate dalla tecnologiache potrebbero influenzare negativamente il raggiungimento degli obiettivi aziendali definiti dalla società.[74]

[74]ISACA, *IT Risk Framework, 2009.*

Il termine rischio IT è molto ampio in quanto al suo interno sono comprese tutte le fonti di rischio che influenzano le risorse informatiche e tecnologiche di un'azienda. La conseguenza principale del rischio informatico è l'impatto diretto sull'integrità, sulla riservatezza e sulla disponibilità dei dati e delle informazioni aziendali contenute all'interno dei sistemi informativi aziendali.

I rischi informatici possono essere suddivisi in quattro fonti di rischio:

1) Le azioni delle persone. Esse possono essere azioni involontarie, ovvero azioni dannose ma non intenzionali (come, ad esempio, errori ed omissioni); intenzionali, ovvero azioni intraprese con la volontà di provocare un danno (come, ad esempio furti informatici, sabotaggio, frode) oppure la mancanza dello svolgimento di un'azione, dovuta ad esempio dalla mancanza di conoscenze e competenze del personale IT.
2) Guasti nel sistema e nella tecnologia. I guasti possono riguardare la componente *hardware*, ovvero la componente fisica del sistema e possono impattare, ad esempio, sulle capacità della componente, sulle prestazioni e possono essere dovuti a manutenzioni non eseguite oppure all'obsolescenza. In secondo luogo, i guasti possono riguardare anche la componente *software*, ovvero i programmi, le applicazioni e sistemi operativi e possono riguardare la compatibilità, la configurazione, la gestione delle modifiche, le impostazioni di sicurezza e dei codici di accesso. Infine, i guasti possono riguardare il sistema, provocando problemi di integrazione della tecnologia IT.
3) Il fallimento dei processi interni. I processi principali riguardanti la tecnologia sono tre: il processo di configurazione ed esecuzione, il processo di controllo e il processo di supporto ai precedenti. Un fallimento nel primo processo può provocare errori nel flusso delle informazioni e dei processi, nell'archiviazione dei dati, nella documentazione del processo, nell'attività di avviso e notifica. Un fallimento nel secondo processo è dovuto a controlli non adeguati provocando errori nelle attività di monitoraggio e di reporting periodico. Infine, un errore nel terzo processo provocherà squilibri a livello generale.
4) Eventi esterni. Tali eventi comprendono le catastrofi, come ad esempio eventi naturali che l'organizzazione non può prevedere e perciò controllare; questioni legali, come ad esempio il cambio di normativa vigente e infine i cambiamenti del business.

Tali fattori di rischio, seppur generali, hanno un impatto diretto sull'integrità e la riservatezza dei dati che a loro volta posso provocare perdite monetarie, reputazionali nei confronti degli *stakeholder* e a volte possono provocare persino l'interruzione dell'attività. [75]

Il revisore deve valutare la misura in cui tali rischi informatici impattano l'informativa di bilancio e i dati aziendali. I rischi strettamente correlati alle informazioni aziendali sono correlati:

- alla gestione degli accessi, in quanto gli accessi non autorizzati ai dati potrebbero provocare la loro distruzione o modifica non appropriata oppure la contabilizzazione di operazioni non autorizzate, inesistenti oppure non esatte. Altri rischi specifici potrebbero verificarsi nelle situazioni in cui più soggetti possono aver accesso ad un database comune;
- alla violazione del principio di separazione delle funzioni nei casi in cui, ad esempio, il personale IT sia in possesso di privilegi di accesso troppo estesi rispetto alle funzioni per le quali era stato assegnato;
- alle modifiche non autorizzate a dati presenti nei master file[76], alle modifiche non autorizzate ad applicazioni IT oppure ad interventi non opportuni effettuati manualmente;
- ad un ambiente IT obsoleto causato dal mancato aggiornamento necessario delle applicazioni IT oppure di altri aspetti dell'ambiente IT;
- a perdite potenziali di dati o all'impossibilità di accedere ai dati aziendali.

Il revisore è tenuto perciò a valutare i rischi correlati all'informativa finanziaria ma è importante sottolineare che i rischi IT, anche se possono sembrare distanti dall'informativa finanziaria è difficile che non vadano ad intaccare i dati aziendali e, perciò, il bilancio. [77]

Nel prossimo paragrafo sono analizzati due rischi correlati a due fenomeni molto diffusi che è importante prendere in considerazione: la cybersecurity e il *cloud*.

[75]Biener C., Eling M., Hendrik Wirfs J., Insurability of Cyber Risk: An Empirical, Vol. 40, Springer, Giugno 2014, pag. 5.

[76]Per master file si intende un formato particolare di file utilizzato comunemente per inviare informazioni aziendali confidenziali che devono essere protette. Tale formato viene utilizzato, per esempio, per inviare file all'Agenzia delle Entrate.

[77]Principio di revisione internazionale 315: "Identificazione e valutazione dei rischi di errori significativi", App.5, pag. 85-86.

2.2.1 Cybersecurity e cloud

Il costante sviluppo della tecnologia e dell'automazione ha apportato anche nuovi rischi e nuovi problemi che le società devono affrontare. In questo paragrafo sono trattati due temi interessanti: la cybersicurezza e il *cloud*.

Innanzitutto, è importante trattare è il tema della cybersicurezza in quanto gli accessi possono essere violati sia da soggetti interni all'azienda che da soggetti esterni: in quest'ultimo caso si entra nel campo della *cybersecurity*. Per *cybersecurity* si intendono quelle pratiche e quegli strumenti utilizzati per proteggere un sistema da attacchi esterni.

Le strategie che una società potrebbe attuare per garantire la sicurezza digitale sono svariate, ma dovrebbe basarsi sempre su tre principi, i quali, se rispettati, garantiscono la sicurezza di un sistema, ovvero:

- ➔ confidenzialità (*confidentiality*): la strategia che prevede la tutela e la protezione dei dati aziendali, dal momento in cui sono immagazzinati fino a quando vengono diffusi. Ha lo scopo di garantire la *privacy* dei dati aziendali da eventuali attacchi hacker. Rientra in questa strategia la gestione degli accessi ai dati aziendali;
- ➔ integrità (*integrity*): la strategia che prevede la tutela dell'incolumità dei dati. Secondo tale principio, infatti, i dati devono essere protetti da eventuali modifiche o cancellazioni inappropriate, le quali potrebbero ledere la veridicità dei dati. Rientrano in questa strategia il monitoraggio degli accessi e la formazione adeguata dei dipendenti;
- ➔ disponibilità (*availability*): tale strategia è volta a garantire che i dati siano disponibili agli utenti quando necessario e per la durata necessaria, senza che si verifichino interruzioni.[78]

Si parla di attacchi alla sicurezza digitale, nelle situazioni in cui viene violata o minacciata una pratica di sicurezza standard o una politica interna definita dalla società messa in atto per garantire la sicurezza informatica. Per attacchi alla cybersicurezza, detti anche *cybercrime* (attacchi cibernetici), si intendono tutte quelle attività illecite che includono l'estorsione di dati aziendali sensibili, la distruzione o danneggiamento di dati, le frodi online oppure l'accesso non autorizzato all'infrastruttura IT.

[78] Rigoni A., *I 3 principi chiave della sicurezza informatica: la triade CIA*, Cyberment, https://cyberment.it/sicurezza-informatica/3-principi-chiave-della-sicurezza-informatica/

Tra i cyber attacchi più diffusi e famosi sono due: i *malware* e il fenomeno del *phishing*.

I *malware* (il termine deriva dalle parole *malicious* e *software,* ossia software malevolo) sono dei *software* che hanno l'obiettivo di recare danni al dispositivo al quale sono inviati con il fine di spiare, danneggiare oppure rubare i dati riservati contenuti in tale dispositivo, compromettendone le funzioni e i dati stessi.
I *malware* possono accedere ad un sistema aziendale attraverso diversi mezzi: attraverso internet, attraverso le *e-mail* (in questo caso si tratterà di un attacco tramite *phishing,* il quale sarà analizzato a seguire in questo paragrafo), oppure anche offline, attraverso ad esempio chiavette USB (*Universal Serial Bus*). È possibile, infatti, scaricare un *malware* quando si scarica un *software* oppure un file dannoso da internet, visitando siti web oppure cliccando su *pop-up*[79] dannosi.
A seconda del mezzo di diffusione possono essere suddivisi in tre categorie:

1) *Malware* a diffusione: in questa categoria rientrano i *virus* e i *worm*.
   I *virus* sono dei *software* che si attivano all'interno del sistema nel momento in cui l'utente apre il file o il *software* dannoso, diffondendosi su tutti i file presenti nel computer. L'effetto si traduce nella distruzione o nel danneggiamento di file presenti nel computer oppure nel rallentamento del sistema operativo. I *worm* sono simili ai *virus* ma si diffondono nel computer senza il bisogno di un'azione umana, ma solo attraverso la connessione ad una rete internet, rendono i computer inutilizzabili.
2) *Malware* strumentali: in questa categoria rientrano i *trojan*, *backdoor* e *spyware*.
   I *trojan* sono dei *software* che si presentano come utili all'utente ma sono in realtà utilizzati dagli hacker per eseguire *malware* dannosi, come ad esempio le *backdoor*, ovvero *malware* che hanno l'obiettivo di accedere al sistema dell'utente attaccato per danneggiarlo.
   Gli *spyware* invece hanno l'obiettivo di spiare e registrare le attività svolte nei dispositivi per poi diffonderle a terzi soggetti. Sono dannosi soprattutto nel caso siano in oggetto dati sensibili.
   Diversamente dalla prima categoria, questi *software* non si diffondono all'interno di un sistema.

[79] I pop-up sono delle interfacce che compaiono automaticamente durante la visualizzazione di un sito web con l'obiettivo di attirare l'attenzione del soggetto che sta visualizzando il sito.

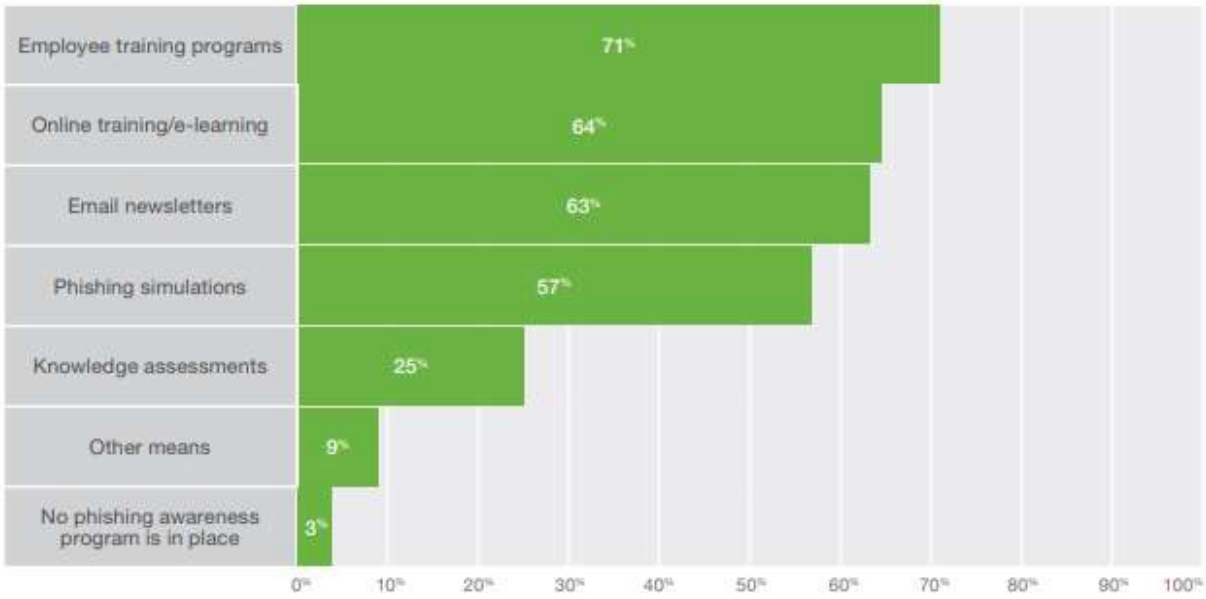
3) *Malware* per il controllo. In questa categoria ne rientrano molti, ma il più diffuso è il *ransomware*, ovvero *software* dannosi che hanno l'obiettivo di bloccare, oppure minacciare di bloccare, il dispositivo della vittima. In questi casi, l'hacker chiederà un riscatto monetario per sbloccare il dispositivo sottoposto ad attacco[80].

Il secondo cyberattacco più frequente e comune alla sicurezza digitale è il fenomeno comunemente chiamato "*phishing",* tradotto "frode online". Il *Phishing* è un attacco che vede l'utilizzo delle *e-mail* come strumento per l'ottenimento di informazioni sensibili (come, ad esempio, i dettagli di una carta di credito oppure informazioni personali) oppure per l'invio di *malware*. Questi attacchi sono molti dannosi e sono rivolti direttamente al personale aziendale attraverso la posta elettronica; perciò, se non vengono attuati i giusti controlli aziendali e se non viene eseguita un'adeguata formazione ai dipendenti la società sarà esposta in modo elevato al rischio.
Oltre ad essere dannosi sono anche molto diffusi. Secondo un Report dell'FBI (*Federal Bureau of Investigation*), infatti, le *e-mail* di *phishing* sono lo strumento più usato dagli hacker per inviare *ransomware,* inoltre, secondo un Report svolto nel 2018 definito "*The Symantec Internet Security Threat*"[81] è stato dimostrato che in media nel 2017 un utente utilizzatore di *e-mail* ha ricevuto 16 *e-mail* dannose al mese.
Infine, secondo un Report di IBM svolto nel 2021, l'attacco *phishing* è il quarto attacco cyber più comune riguardante la violazione dei dati aziendali e il secondo attacco più costoso da sistemare per le aziende: nel 2021 infatti la spesa per il ripristino del sistema e dei dati dopo un attacco ammontava mediamente a circa 4,65 milioni di dollari per attacco.[82]
Le società devono mettere in pratica delle azioni in azienda per mitigare tale rischio, soprattutto attraverso l'aumento della consapevolezza dei dipendenti verso tale problema. Secondo un sondaggio svolto dall'ISACA nel 2018, il 71% delle aziende intervistate, come dimostra il grafico 2.2, svolgeva corsi di formazione per sensibilizzare

[80] Antonielli A, *Riconoscere e difendersi dai Malware: significato, esempi e tipologie più comuni*, Politecnico di Milano, 21 Gennaio 2021, https://blog.osservatori.net/it_it/malware-significato-esempi-riconoscerli
[81]Symantec, *Internet Security Threat Report*, volume 23, March 2018, www.symantec.com/security-center/threat-report
[82] IBM, *Cos'è il Phishing?*, 2022, https://www.ibm.com/it-it/topics/phishing
https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/top-risks-and-rewards-of-moving-to-the-cloud

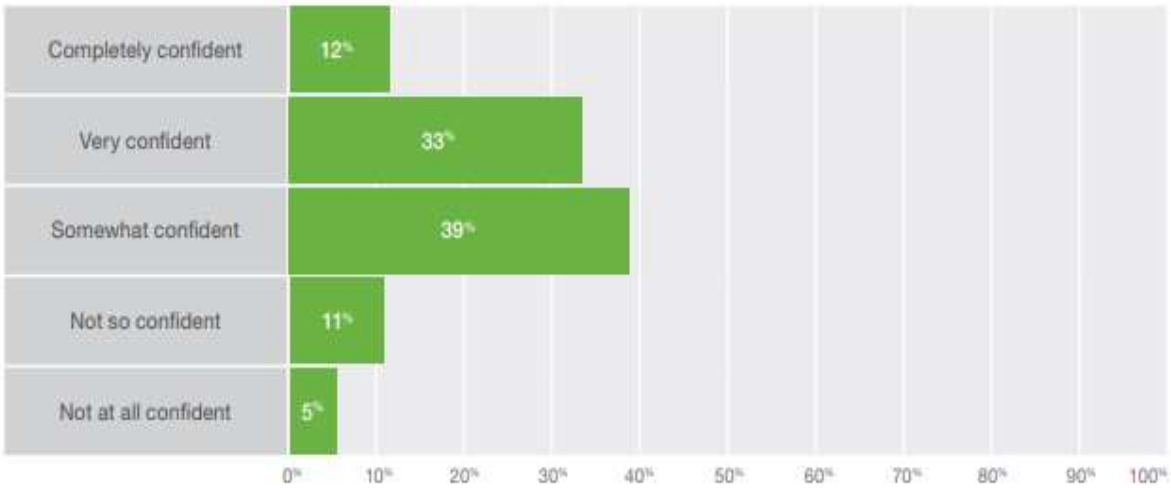
i dipendenti al tema ma solo il 12% degli intervistati, come mostra il grafico 2.3, si sentiva sicuro al riguardo. È importante, perciò, che tale tema si integri maggiormente all'interno delle società per evitare che il rischio di attacchi di *phishing* diventi elevato. Nei due grafici sottostanti è possibile vedere i risultati completi dei sondaggi analizzati.

Figura 2.2: Metodi utilizzati per promuovere la consapevolezza al fenomeno del *phishing*



Fonte: ISACA, Phishing defense and governance, How to Improve User Awareness, Enhance Controls and Build Process Maturity, Documento di Pubblica Consultazione, 2019, pag. 5.

Figura 2.3: Valutazione dell'efficacia da parte dei soggetti intervistati dei metodi per promuovere la consapevolezza al fenomeno del *phishing*



Fonte: ISACA, Phishing defense and governance, How to Improve User Awareness, Enhance Controls and Build Process Maturity, Documento di Pubblica Consultazione, 2019, pag. 5.

Gli attacchi, di norma, hanno luogo a livello della rete perimetrale[83] e della rete interna, le quali sono solitamente lontane dalle componenti IT strettamente correlate alla redazione del bilancio. Non per forza, perciò, questi rischi influenzano l'informativa di bilancio in quanto una società può utilizzare le componenti IT anche per sostenere processi diversi dalla produzione dell'informativa, come ad esempio per sostenere le attività operative. Perciò, ogni qual volta che si verifica un attacco, il revisore deve valutare in quale misura tale attacco poteva condizionare l'informativa di bilancio. Se lo ritiene necessario, il revisore può:

1) comprendere e identificare i controlli IT messi in atto dalla società;
2) definire l'eventuale errore potenziale che incide sull'informativa finanziaria;
3) valutare se l'organizzazione aziendale fornisce un'adeguata informativa riguardo l'attacco alla sicurezza digitale accaduto. [84]

Un secondo tema che è importante trattare in tema di rischi IT è quello del *cloud*. Per *cloud* si intende un accesso tramite Internet a risorse che si trovano in un centro di dati remoto, il quale è gestito da un fornitore esterno di servizi *cloud*: viene attuata una vera e propria "migrazione" dei dati aziendali verso uno spazio remoto.[85]Le risorse possono riguardare applicazioni, dati, server oppure strumenti di sviluppo. È uno strumento che ha cambiato profondamente il modo in cui lavorano le aziende ed è stato uno strumento chiave per la transizione digitale.

I vantaggi relativi al *cloud* sono svariati come, ad esempio, la maggior flessibilità e la riduzione dei costi ma ci sono anche svariati rischi. Uno dei rischi principali riguarda la mancanza di sicurezza dei dati presenti nel *cloud*, infatti, i fornitori archiviano i dati in uno spazio remoto e per questo le aziende sono preoccupate in quanto non possiedono il controllo dei dati.

Un secondo rischio è relativo, invece, alla gestione degli accessi e delle identità (definito comunemente IAM) in quanto solo gli utenti autorizzati dovrebbero avere accesso ai dati presenti nel *cloud* e allo stesso tempo i soggetti amministratori con privilegi d'accesso dovrebbero essere monitorati. Infatti, secondo una ricerca condotta da Delinea[86], il 74%

[83]Per rete perimetrale si intende un sistema di sicurezza che viene posto per proteggere la rete aziendale da attacchi esterni, come una sorta di mura.
[84]Principio di revisione internazionale (ISA Italia) 315, App. 5, par. 19, pag. 85.
[85]IBM, *Cloud Computing*, 2022, https://www.ibm.com/it-it/topics/cloud-computing
[86]Delinea, *Delinea recognized as a Leader again in the 2022 Gartner Magic Quadrant for Privileged Access Management, Documento di ricerca, 19 Luglio 2022,* Message from Delinea

delle violazioni dei dati è riconducibile ad abusi relativi agli accessi privilegiati degli utenti. Gli accessi privilegiati infatti possono raffigurare una minaccia e proprio per questo è importante che le aziende disabilitino tempestivamente gli account dei dipendenti cessati per limitare i rischi.
Un rischio ulteriore è relativo alla necessità di conformità dell'ambiente IT e delle applicazioni IT di una società per poter accedere al *cloud*. Questa non sempre viene messa in atto dalla società definendo così dei sistemi non efficienti.
A causa di questi rischi, il revisore IT deve affrontare nuove sfide per verificare la conformità, la *privacy* dei dati, la gestione degli accessi e la disponibilità dei dati presenti nel *cloud*. [87]

2.2.2 Certificazioni e attività del revisore relative alla cybersicurezza

Come è stato definito dal paragrafo precedente, gli attacchi alla cybersicurezza sono molto diffusi e soprattutto molto pericolosi in quanto hanno l'obiettivo di spiare, danneggiare oppure eliminare i dati di un'azienda. I dati per un'azienda sono fondamentali e proprio per questo le società devono mettere in atto dei processi e delle procedure al fine di difendersi da tali attacchi. A causa dell'aumento degli attacchi alla *cybersecurity*, sono sorte diverse normative, certificazioni e regolamenti a cui le società devono sottostare in tema di protezione dei dati e delle informazioni.
La certificazione più importante in questo ambito è la certificazione ISO 27001, ovvero una certificazione volontaria riconosciuta a livello internazionale che definisce una serie di attività che le aziende devono mettere in pratica per poter progettare un sistema di sicurezza delle informazioni aziendali. Non è una certificazione obbligatoria, ma possederla aumenta la fiducia dei soggetti che si interfacciano con le aziende.
L'obiettivo è quello di definire un sistema di protezione che consideri l'azienda a 360° (tecnologia, personale, documenti e processi aziendali) al fine di garantire l'integrità, la disponibilità e la riservatezza dei dati aziendali; fornisce pertanto delle *best practice* che supportano le aziende nel definire un sistema di protezione efficiente sulla base dell'ambiente esterno dell'azienda.

[87] AA. VV., *Top Risks and Rewards of Moving to the Cloud, ISACA, 14 Marzo 2023* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/top-risks-and-rewards-of-moving-to-the-cloud

Il sistema si caratterizza da un insieme di politiche e procedure che hanno l'obiettivo di gestire, controllare e monitorare la sicurezza dei dati aziendali per poter contrastare il rischio IT legato alla loro sicurezza: la società identifica e valuta tali rischi per stabilire i controlli adeguati al fine di contrastarli.
Il revisore IT, attraverso l'attività di comprensione, dovrà valutare se la società ha messo in atto dei controlli per garantire la sicurezza digitale. Se una società è certificata ISO 27001 avrà la garanzia (non assoluta) che la società sta attuando le politiche necessarie per contrastare gli attacchi alla sicurezza digitale; se invece non lo è potrà utilizzare tale certificazione come base per comprendere se la società si difende adeguatamente da tali rischi. [88]

Una normativa che è importante citare è il Regolamento UE 679/2016, definito comunemente GDPR (*General Data Protection Regulation*) ovvero un Regolamento generale sulla protezione dei dati, il quale entra in vigore per gli Stati membri dell'Unione Europea il 25 maggio 2018.
Si applica a tutte le aziende che operano all'interno dell'UE che trattano dati personali e a tutte le aziende extra-UE che operano e scambiano dati personali con aziende UE, inoltre, le aziende che gestiscono una quantità elevata di dati sensibili devono nominare un soggetto rappresentante che sia responsabile, definito *Data Protection Officer* (DPO).
Questo soggetto ha il compito di implementare una strategia di protezione dei dati nel rispetto della normativa GDPR, ovvero sarà responsabile delle attività di sviluppo, attuazione e monitoraggio di politiche sulla privacy dei dati trattati dalla società, da quando il dato è raccolto a quando esce dall'azienda. [89]
Per dato personale si intende qualsiasi informazione riguardante un individuo specifico o identificabile (ad esempio, anche i dati dei dipendenti sono dati personali che devono essere trattati adeguatamente).
Gli obiettivi del regolamento sono principalmente due:

- ➔ aumentare la fiducia dei consumatori verso le aziende che possiedono e utilizzano le proprie informazioni personali, ponendo attenzione soprattutto alla *privacy*. Al centro della norma, infatti, ci sono i cittadini dell'UE e loro dati;

[88] AA. VV., *Sicurezza delle informazioni e ISO 27001*, Documento di Pubblica Consultazione, IT Governance, Gennaio 2018.
[89] AA. VV, *Assirevi Monografie – L'evoluzione della governance e dei rischi di Information Technology, Modelli di governo da considerare per un'efficace gestione dei rischi legati alla tecnologia*, Documento di Ricerca, Assirevi, 04 Maggio 2023.

- ➔ facilitare lo scambio di dati tra gli Stati membri, in quanto si applica a tutti gli Stati allo stesso modo.

Al centro della norma ci sono perciò i dati personali, i quali devono essere trattati in modo lecito, trasparente, corretto e il titolare del dato deve essere a conoscenza delle finalità della raccolta. Allo stesso tempo, il dato deve essere conservato solo per il periodo di tempo necessario per adempiere al fine prestabilito e deve essere mantenuto integro, protetto e disponibile.

Il dato può essere trattato solo se si rientra in queste circostanze:

- ➔ consenso: il titolare del dato ha dato il suo consenso per il trattamento specificandone il fine;
- ➔ contratto: i dati sono trattati per poter stipulare ed eseguire un contratto;
- ➔ obbligo di legge: il trattamento deriva da un obbligo di legge;
- ➔ interessi vitali: i dati sono trattati al fine di proteggere la vita del titolare;
- ➔ pubblico interesse: il trattamento deriva da un interesse pubblico;
- ➔ legittimo interesse: il dato è trattato nelle situazioni in cui l'interesse della società prevale sull'interesse del singolo.

Le società devono risultare conformi a tale normativa e il revisore dovrà verificarne obbligatoriamente la conformità; solitamente il revisore IT si occupa di tale verifica in quanto i dati sono strettamente correlati ai sistemi informativi.

È importante che le imprese comprendano che ottenere la conformità non deve essere solamente fine a sé stessa ma deve essere un pretesto per garantire la *privacy*, la protezione e la sicurezza dei dati aziendali. Tale garanzia aiuterà le aziende ad utilizzare i dati raccolti adeguatamente e permetterà di trarre dei benefici.[90]

La certificazione ISO 27001 è volontaria a differenza della GDPR, ma la prima potrebbe essere strumentale per rispettare la seconda, nonostante abbiano per oggetto elementi diversi.

La GDPR ha al centro i cittadini appartenenti all'Unione Europea e i loro dati personali in quanto sensibili; invece, la certificazione ISO 27001 ha l'obiettivo di fornire degli strumenti che se applicati garantiscono la sicurezza da attacchi esterni del proprio sistema, tra cui anche i dati sensibili raccolti. La certificazione, infatti, consente di

[90] AA. VV., *Regolamento generale sulla protezione dei dati (GDPR), Guida alla conformità,* Documento di Pubblica Consultazione, IT governance, Maggio 2018.

ottenere la sicurezza digitale relativa a tutti i dati aziendali, non sono i dati personali, diffondendo all'interno dell'azienda una cultura orientata alla *privacy* e alla protezione delle informazioni sensibili. Certificarsi aiuta ad ottenere la conformità al regolamento in quanto permette di fornire elementi probativi utili.

Anche le società di revisione, come tutte le organizzazioni, devono essere conformi alla GDPR in quanto, per svolgere i loro incarichi, si servono di un'enorme quantità di dati sensibili. Basti pensare che revisionando un'azienda si ottengono i dati dell'azienda stessa, dei suoi dipendenti, dei suoi clienti, dei suoi fornitori e dei suoi legali. [91]

2.3 Progresso IT e normative vigenti

Il progresso IT e l'ampio uso della tecnologia ha influenzato le aziende e i loro manager, ponendo nuovi obiettivi e nuove sfide da affrontare. Innanzitutto, l'azienda deve garantire un'alta qualità delle informazioni aziendali prodotte grazie alla tecnologia al fine di supportare adeguatamente le decisioni aziendali. Inoltre, investendo in sistemi IT strategici ed innovativi, l'azienda potrà creare valore raggiungendo obiettivi strategici e benefici che non sarebbe riuscita a raggiungere senza tali investimenti e, allo stesso, potrebbe eccellere nelle attività legate al suo core business grazie all'uso affidabile ed efficiente della tecnologia.
Tuttavia, è importante che le organizzazioni tengano conto anche dei rischi legati all'IT e che questi siano mantenuti ad un livello accettabilmente basso; inoltre, non vanno trascurati i costi legati alla tecnologia, in quanto il rapporto costi-benefici deve risultare ottimale.
Le organizzazioni aziendali, inoltre, devono occuparsi di un nuovo tema che ha assunto una forte importanza nell'ultimo decennio, anche a fronte dei fallimenti che hanno coinvolto aziende di successo a livello globale, ovvero quello della governance dei sistemi IT. Le imprese, infatti, hanno appreso che i manager aziendali dovevano considerare l'IT come parte fondamentale e integrata all'interno dell'attività aziendale. La cooperazione tra le attività aziendali e la tecnologia è necessaria al fine di garantire il

[91]AA.VV*., Normativa "protezione dei dati personali" per i casi di revisione (legale e volontaria) e incarichi disciplinati da legge o regolamenti*, Documenti di Ricerca n.227, Assirevi, Febbraio 2019.

successo dell'azienda e proprio per questo l'IT deve essere incluso nell'approccio di governance aziendale. [92]

Un'efficace governance permette anche la riduzione dei rischi relativi all'IT, i quali possono essere diretti, ovvero strettamente correlati al malfunzionamento della tecnologia ma anche indiretti, ovvero correlati alle attività operative aziendali.

Ad esempio, i rischi possono essere correlati alla gestione degli accessi dei dipendenti di una società ad applicazioni IT strettamente correlate all'elaborazione di informazioni aziendali, soprattutto se sensibili. In tal senso, la società dovrebbe mettere in atto dei controlli al fine di monitorare il corretto funzionamento dell'IT e al fine di valutarne l'adeguatezza e l'efficacia perché eventuali errori potrebbero portare perdite significative per l'azienda.

A fronte dei rischi in relazione all'ambiente IT, furono fissate delle norme per garantire che le società emettessero una corretta e adeguata informativa finanziaria al fine di salvaguardare gli investitori sociali. A tal fine nasce il concetto di sistema di controllo interno, ovvero una struttura di controllo che le società avrebbero dovuto implementare per ridurre i rischi aziendali e che avrebbe permesso di raggiungere di conseguenza gli obiettivi aziendali.

Le normative e modelli di rifermento più importanti che sono analizzati nei paragrafi seguenti sono tre, i quali sono stati predisposti per contrastare gli scandali finanziari che accaddero in quegli anni, ovvero il *framework "COSO",* il *framework "COBIT"* e la normativa *SOX*.

Il *framework COSO* (*Committee of Sponsoring Organizations of the Treadway Commission)* è uno strumento basato sul sistema di controllo interno delle società e si concretizza in un modello che le società possono adottare al fine di configurare un sistema controllo efficace per il conseguimento degli obiettivi aziendali. La sua prima versione, definita "*COSO Report 1*" fu pubblicata nel 1992 a cura di una commissione nata nel 1985. Questo modello è utilizzato ancora oggi dai revisori aziendali per individuare e valutare il sistema di controllo interno di una società, come definito dall'ISA Italia 315.

Nel 1996 fu pubblicata a cura dell'ISACA la prima versione del *framework COBIT* (*Control Objectives for Information and related Technology*), il quale può essere considerato come

[92]AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 13.

un'evoluzione del *framework COSO* in quanto considera l'IT nella governance dell'azienda e nei controlli che la società deve mettere in atto per contrastare i rischi IT. È diventato lo standard per lo sviluppo di strategie di controllo e governance dell'IT per prevenire le frodi aziendali. Può essere considerato come un manuale di istruzioni per la creazione di un sistema IT sicuro per il *reporting* dei rischi finanziari, ben integrato nella gestione e nella governance aziendale.
La normativa *SOX* (*Sarbanes – Oxley Act*), pubblicata nel 2002, ha mutato profondamente il concetto di trasparenza relativa all'informazione finanziaria e ha previsto strumenti per contrastare le frodi aziendali e contabili, numerose negli anni precedenti alla sua entrata in vigore. La trasparenza richiesta da tale normativa doveva essere messa in pratica attraverso la progettazione e l'attuazione di un sistema di controllo interno efficiente, il quale doveva essere documentato dai responsabili aziendali e successivamente revisionato da un revisore esterno. Nonostante non menzioni esplicitamente la componente IT, è stata una legge rilevante perché ha determinato la diffusione del *framework* COBIT come mezzo per governare in modo efficace l'ambiente IT delle società.
I due strumenti e la normativa SOX sono strettamente correlate in quanto il *framework* COBIT rappresenta uno strumento fondamentale in ambito IT in quanto consente di sviluppare un sistema di controllo interno che tenga conto della componente informatica e la sua applicazione permette di ottenere la conformità alla normativa SOX. Allo stesso tempo, COBIT consente di riconoscere il valore e i rischi associati alle risorse IT in un'azienda.
Nei paragrafi seguenti saranno analizzati gli strumenti e la normativa definiti in precedenza al fine di comprendere la loro importanza e la loro correlazione.

2.4 Sistema di controllo interno e framework "COSO"

Già negli anni Ottanta, a seguito delle prime frodi aziendali e dei primi falsi di bilancio nacque la necessità per le aziende di definire un proprio sistema di controllo interno al fine di gestire i rischi aziendali. Il principale rischio era quello di presentare nel bilancio una situazione che non fosse una veritiera rappresentazione della realtà aziendale a discapito degli *stakeholder*, i quali avevano interesse nel buon funzionamento della società.

Una definizione puntuale di sistema di controllo interno (comunemente abbreviato nella sigla SCI) ci viene data dall'ISA Italia 315, definendolo come un "*sistema configurato, messo in atto e mantenuto dai responsabili delle attività di governance, dalla direzione e da altro personale dell'impresa al fine di fornire una ragionevole sicurezza sul raggiungimento degli obiettivi aziendali con riferimento all'attendibilità dell'informativa finanziaria, all'efficacia e all'efficienza delle sue attività operative ed alla conformità alle leggi e ai regolamenti applicabili*"[93].

Si concretizza perciò in tutte quelle politiche e procedure definite dalla direzione di una società che garantiscono con ragionevole sicurezza il raggiungimento degli obiettivi aziendali e la salvaguardia del patrimonio aziendale. È importante sottolineare che con ragionevole sicurezza non si intende una sicurezza assoluta in quanto ci sono limiti intrinseci legati al giudizio umano nella definizione degli obiettivi e nell'attuazione dei controlli, in quanto potrebbero essere forzati dal personale della società.

Gli obiettivi del SCI sono principalmente tre:

a) garantire il raggiungimento degli obiettivi aziendali attraverso l'uso efficace ed efficiente delle risorse aziendali (come personale, disponibilità liquide, ecc.);
b) garantire l'attendibilità della rendicontazione interna ed esterna all'azienda, sia finanziaria che non finanziaria;
c) garantire la conformità alle norme e ai regolamenti.

È importante evidenziare che il sistema di controllo interno è un processo e può essere considerato come il mezzo per svolgere un'attività di controllo e di garanzia al buon funzionamento di una società, non il fine ultimo del sistema. Proprio per questo non è una procedura indipendente oppure un'attività isolata ma si interseca all'interno dell'intera attività aziendale. È efficace proprio nel momento in cui riesce ad integrarsi all'interno dell'organizzazione e a far parte della cultura aziendale.

Inoltre, al centro del sistema di controllo interno ci sono le persone di una società. Non deve essere considerato come un insieme di procedure manuali o come la sola compilazione di check-list, ma è un processo in cui il personale aziendale è in una posizione di rilievo. Tutti i membri di un'impresa sono responsabili dei controlli interni nella loro area di attività e del loro efficace funzionamento.

[93]Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", pag. 6.

L'impresa si compone di un insieme di processi aziendali in funzione, come i processi operativi, le operazioni contabili e anche i sistemi IT. Il management aziendale deve gestire correttamente questi processi altrimenti l'impresa potrebbe andare fuori controllo e non funzionare adeguatamente.[94]
Tutti i soggetti che lavorano in una società devono conoscere e comprendere i sistemi di controlli e comprendere se c'è una connessione tra aree di controllo adeguata al fine di gestire correttamente l'impresa.

Come detto in precedenza, il concetto di SCI nasce per prevenire le frodi aziendali accadute, soprattutto in America, negli anni Ottanta. Negli USA, infatti, nel 1985 nasce un'organizzazione anticorruzione composta dalle cinque organizzazioni[95] più importanti americane in campo contabile e di revisione dei conti con l'obiettivo di migliorare la qualità dell'informativa finanziaria prodotta dalle società in favore degli *stakeholder*. Questa commissione, denominata *"Committee of Sponsoring Organizations of the Treadway Commission"* (abbreviata comunemente in *"COSO")*[96], voleva identificare le cause principali che permettevano alle società di emettere bilanci fraudolenti con l'obiettivo di definire delle raccomandazioni per ridurne l'incidenza.
Nel 1987 pubblicò una relazione finale con numerose raccomandazioni per le aziende e per i revisori esterni delle aziende, chiedendo anche ai dirigenti aziendali di valutare l'efficacia dei loro controlli interni. La commissione inoltre definì gli elementi chiave che doveva possedere un sistema di controllo interno efficace, tra cui un solido ambiente di controllo, dei codici di condotta, un comitato di revisione competente e una forte funzione di revisione interna.
Nel 1992 pubblicò ufficialmente il cosiddetto *"COSO Report 1"*, ovvero un report che è diventato nel tempo un punto di riferimento in tema di sistema di controllo interno sia per le società che per i revisori esterni. Viene considerato una guida per le imprese al fine di mettere in atto e sviluppare un sistema di controllo interno efficiente ed efficace. A livello mondiale, è diventato un modello di riferimento per l'elaborazione di norme,

94 Moeller R., Executive's guide to governance – Improving Systems Processes with Service Management, COBIT and ITIL, Libro, Wiley Corporate F&A, 2013, pag. 51.

[95]Le cinque società che fanno parte della commissione sono: American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), American Accounting Association (AAA), Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA).

[96]La commissione prende il nome dal suo presidente James C. Treadway.

codici di autodisciplina e altri documenti inerenti ai controlli interni di molte nazioni, tra cui anche l'Italia.

Questo report scompone il sistema di controllo interno in cinque componenti:

1) l'ambiente di controllo, ovvero tutti i soggetti presenti in un'azienda, la loro cultura aziendale e i valori aziendali che sono stati diffusi. È una componente fondamentale in quanto costituisce la base per le altre componenti del SCI;
2) valutazione del rischio, ovvero il processo che si concretizza nell'individuazione e nella gestione dei rischi aziendali con l'obiettivo di definire le risposte adeguate ai rischi identificati. La società dovrebbe innanzitutto individuare e stimare i rischi significativi a cui è esposta, successivamente dovrebbe valutare la probabilità di tali rischi e infine dovrebbe valutare le azioni da intraprendere per contrastarli;
3) attività di controllo, ovvero le procedure messe in atto per garantire che vengano messe in atto le azioni identificate per affrontare i rischi. I controlli possono essere manuali o IT;
4) informazione e comunicazione, ovvero le attività focalizzate sull'elaborazione di informazioni adeguate e sulla comunicazione efficace delle stesse;
5) attività di monitoraggio, ovvero il monitoraggio dell'intero sistema con l'obiettivo di individuare eventuali carenze da correggere.[97]

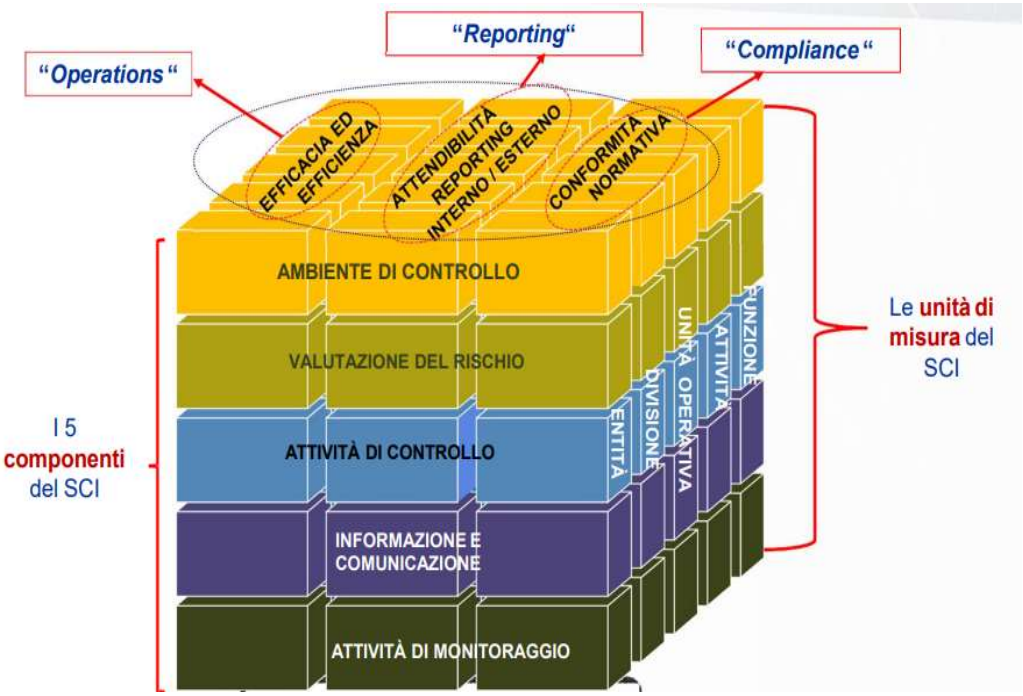
Ogni società ha il suo sistema di controllo interno e differirà da quello delle altre società in quanto tutte le società si differenziano per dimensioni, caratteristiche e cultura aziendale ma è importante che tutte le cinque componenti siano implementate al fine di assicurarne il buon funzionamento.

Nell'immagine riportata di seguito è riportato il cosiddetto *"COSO Cube"*, ovvero un cubo con cui viene rappresentato di norma il *COSO Report:* nella parte frontale del cubo sono riportate le cinque componenti del controllo interno, nella parte superiore i tre obiettivi generali del controllo interno e nel lato destro invece sono state rappresentate le componenti strutturali di un'impresa, le quali variano a seconda della struttura aziendale. Il cubo rappresenta dal punto di vista grafico come deve essere configurato un controllo: per ogni aspetto aziendale devono essere valutate e configurate le cinque componenti del controllo rappresentate nella parte frontale, le quali devono essere

[97]Le cinque componenti del sistema di controllo interno sono utilizzate anche dai revisori esterni per comprendere e valutare il sistema di controllo interno. L'ISA 315 descrive le procedure e gli aspetti che il revisore deve valutare per ogni componente.

predisposte per ogni componente aziendale rappresentata nel lato destro, tutto ciò nel rispetto dei tre obiettivi generali (presenti nella parte superiore del cubo). Ogni componente del SCI deve essere collegata e deve comunicare con le altre componenti.

Figura 2.4: Il cubo "COSO"



Fonte: Pastorino S., Webinar Il sistema di controllo interno, L'applicazione dei principi del CoSO 2013 - Introduzione al CoSO Report 2013, Istituto Nazionale Revisori Legali (INRL), 2022.

La commissione negli anni seguenti aggiornò il report del 1992 in quanto il contesto globale era cambiato e perciò un aggiornamento era necessario. In quegli anni, infatti, la complessità dei processi aziendali stava aumentando, la tecnologia stava assumendo un ruolo sempre più importante, gli adempimenti normativi erano aumentati e si riteneva necessario un approccio maggiormente concentrato sul rischio e che ponesse più attenzione al rischio di frode.

Nel settembre 2004 la commissione *COSO* pubblicò un nuovo *framework* denominato l'*"Enterprise Risk Management (ERM) – Integrated Framework"* con l'obiettivo di fornire un supporto alle aziende maggiormente orientato al rischio. Secondo questa nuova versione, il sistema di controllo interno doveva essere progettato con l'obiettivo di identificare, valutare e rispondere ai rischi identificati in riferimento all'attendibilità

dell'informativa finanziaria, all'efficacia delle attività operative e alla conformità alla normativa di riferimento.

È una rivisitazione dei concetti presentati dal *COSO Report* del 1992 perché mette in evidenza il tema della valutazione del rischio come presupposto per la progettazione efficiente di un sistema di controllo interno.

Un'ulteriore novità è l'enfatizzazione del ruolo del management nel processo di implementazione del sistema di controllo interno e sposta su di lui la responsabilità di eventuali pratiche illecite o fraudolente svolte dalla società.

I controlli, infatti, si svolgono su tre linee di difesa integrate tra loro, ovvero:

1) la prima linea di controllo spetta al Consiglio di Amministrazione e alla direzione che hanno l'incarico di mettere in atto i controlli al fine di gestire i rischi aziendali;
2) la seconda linea spetta a coloro che in azienda hanno funzioni di controllo, ovvero soggetti che monitorano i rischi e i controlli posti in essere dalla prima linea di controllo. Questi soggetti hanno libertà di giudizio, modesta indipendenza e svolgono principalmente attività di controllo di gestione, di qualità e soprattutto di gestione dei rischi;
3) la terza linea di controllo spetta a coloro che svolgono attività di *Audit*, sia interna che esterna all'azienda, ovvero soggetti indipendenti alla società che valutano l'adeguatezza del sistema di controllo interno della società, comunicando eventuali carenze alla direzione aziendale. Tra questi soggetti ci sono l'Organismo di vigilanza, il revisore esterno e il collegio sindacale. [98]

Il *COSO Report 1* e il *COSO Framework ERM* sono stati dei documenti fondamentali per l'attività di revisione esterna in quanto definiscono una guida per comprendere e valutare la composizione e l'efficacia di un sistema di controllo interno.

Il revisore dovrà svolgere delle procedure specifiche per ogni componente del SCI e, come definito dall'ISA 315, dovrà comprendere il sistema di controllo interno delle società al fine di individuare e valutare rischi di errori significativi a livello di bilancio e a livello di asserzioni.

[98]Pesenato A., *COSO Report I e COSO Framework SCIGR: loro applicazione nella revisione legale e nel MOGC ex D.Lgs 231/2001*, Documento di Pubblica Consultazione n. 256, Periodico "Il commercialista veneto", Associazione dei Dottori Commercialisti e degli Esperti Contabili delle Tre Venezie, 2020.

Le cinque aree possono essere presenti in imprese di grandi, medie o piccole dimensioni ma in forme diverse a seconda della natura e delle dimensioni della società. Le aziende più piccole e meno strutturate avranno messo in atto dei controlli più semplici e meno articolati a differenza delle imprese più grandi. Non per forza in un'azienda sono presenti tutte le aree e non per forza vengono definite dalla società con questa terminologia, sarà perciò compito del revisore identificarle applicando il proprio giudizio professionale.

2.5 Dal COSO Report al framework COBIT

Il COSO Report fu un quadro di riferimento per il controllo interno ma era necessaria una guida più orientata all'ambiente IT, in quanto era in costante crescita l'utilizzo di infrastrutture IT da parte delle società.
Senior manager e professionisti dell'IT, infatti, erano preoccupati nell'utilizzare il COSO Report nelle società odierne maggiormente orientate all'IT in quanto non poneva sufficiente enfasi sugli strumenti IT e sui rischi correlati. C'erano bisogno, perciò, di ulteriori linee guide più specifiche.

Nel 1996 fu emanato un *framework* chiamato COBIT (*Control Objectives for Information and related Technology*), vale a dire un quadro di valutazione e una guida per la comprensione dei controlli interni con particolare attenzione alla componente IT delle società. Tale *framework* non sostituisce il COSO Report, ma costituisce un modo differente e talvolta preferibile di guardare i controlli interni, in quanto la digitalizzazione ha travolto le aziende e il loro modo di operare nel mercato.
Nonostante sia stato pubblicato prima della normativa SOX, è uno strumento utilizzato dalle imprese per conformarsi alle procedure di controllo interno previste da tale normativa.
È uno strumento che nasce soprattutto per i revisori IT interni ed esterni al fine di esaminare i controlli IT ma, allo stesso tempo, è uno strumento importante per aiutare l'alta direzione aziendale nello stabilire pratiche di governance IT efficaci. Sia i soggetti che svolgono *internal audit* che i manager aziendali dovrebbero conoscere tale *framework* per governare e controllare in modo efficace l'implementazione degli strumenti IT in azienda.

È uno strumento fondamentale in quanto non considera solo la tecnologia fine a sé stessa ma considerare l'organizzazione nel suo complesso e come usa la tecnologia per gestire le informazioni aziendali, alla luce degli obiettivi aziendali.

L'emissione e i successivi aggiornamenti del COBIT sono stati svolti a cura dell'IT Governance Institute (ITGI) e dall'organizzazione professionale strettamente affiliata, *l'Information Systems Audit and Control Association* (ISACA). L'ISACA è un'organizzazione più focalizzata sull'IT *audit* invece l'ITGI è un istituto maggiormente focalizzato sui processi di ricerca. [99]

L'ISACA si occupa anche di gestire l'esame e la nomina professionale di *Certified Information Systems Auditor* (CISA), ovvero certifica a livello mondiale gli *IT Auditors*: soggetti che si occupano di *audit*, controllo, monitoraggio e valutazione dei sistemi IT e dei sistemi aziendali di un'organizzazione.

Negli anni si sono succedute diverse versioni del *framework* COBIT e l'ultima versione, la numero 5, risale al 2011 definita COBIT 5. Il suo obiettivo generale è quello di costruire un'infrastruttura IT che aiuti le imprese a creare valore per l'intera organizzazione grazie all'ottenimento di un equilibrio tra i benefici ottenuti da una parte e il livello di rischio e le risorse utilizzate dall'altra. Può essere applicato a tutte le organizzazioni a livello generale, sia di grandi che di piccole dimensioni, sia commerciali che non a scopo di lucro e sia private che pubbliche. [100]

L'ultima versione del modello COBIT, oltre ad aver integrato le versioni dei *framework* precedenti, ha integrato anche altri modelli e standard comunemente utilizzati in riferimento ai sistemi IT ovvero:

a) TOGAF (*The Open Group Architecture Framework*), ovvero uno modello di architettura aziendale che si occupa ad allineare gli obiettivi aziendali con gli obiettivi IT, con l'obiettivo finale di sviluppare un *software* aziendale adatto;
b) ITIL (*Information Technology Infrastructure Library*), il quale si occupa di IT *service Management.* È un modello che si focalizza sul creare valore per i clienti attraverso servizi definendo linee guida di gestione dei servizi IT;

[99]Moeller R., *Executive's guide to governance, Improving Systems Processes with Service Management, COBIT and ITIL,* Libro, Wiley Corporate F&A, 2013.pag. 84-85.
[100]AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 13.

c) ISO 27000, il quale è uno standard di sicurezza digitale emanato dalla ISO (in inglese, *International Organization for Standardization)* ovvero l'organizzazione internazionale per la normazione;
d) PMBOK, ovvero una guida emanata dal PMP (*Project Management Professional*) che si occupa di *project management*, ovvero gestione e controllo di progetti;
e) ISO 31000, ovvero uno standard ISO che si occupa di *risk management*.

COBIT 5 si basa su cinque principi che evidenziano le principali aree di interesse del *framework*, ovvero:

1) Principio 1: soddisfare le esigenze degli *stakeholder*;
2) Principio 2: considerare l'organizzazione nel suo complesso;
3) Principio 3: applicare un'infrastruttura integrata;
4) Principio 4: adottare un approccio globale (olistico);
5) Principio 5: separare la governance dal management. [101]

Questi cinque principi, o aree di enfasi, definiscono gli elementi del *framework* COBIT fornendo una definizione degli elementi chiave per governare il sistema IT, per documentarlo e per definire tutti i controlli interni in tema IT. Fornisce un approccio alternativo rispetto a quello fornito dal *framework* COSO in quanto enfatizza il tema dell'IT. Le informazioni e i processi a loro supporto sono risorse preziose per ogni impresa e proprio per questo è importante per la direzione aziendale che le gestisca e le controlli in modo efficiente.

COBIT fornisce una visione olistica sul modo di gestire la tecnologia: l'IT deve essere implementato in modo globale in tutta la società tenendo conto di tutte le sue aree di business. Implementando correttamente il *framework* COBIT, le società creeranno sicuramente valore.

La governance dell'IT può essere descritta come la gestione dei *software* e della componente *hardware* di un'azienda perché si prevede che sviluppare e migliorare la redditività del sistema informativo contribuisca ad aumentare i benefici a lungo termine per le organizzazioni. L'utilizzo dell'IT non solo deve essere gestito, ma deve anche essere controllato per aumentare l'affidabilità del patrimonio informativo delle aziende e perciò dell'informativa finanziaria prodotta. Pertanto, sia la governance che i controlli

[101] AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 13.

IT devono essere valutati da un soggetto esterno ed indipendente, ovvero da un *IT Auditor*. COBIT 5 è il quadro di riferimento per l'attività di *audit* dei sistemi IT e per il monitoraggio costante dell'allineamento degli obiettivi IT alle esigenze degli *stakeholder*. L'*IT Auditing* è un processo di raccolta di elementi probativi con l'obiettivo di migliorare la sicurezza degli asset, mantenere l'integrità dei dati, l'efficacia del sistema IT e infine l'efficienza dell'utilizzo della componente IT all'interno delle organizzazioni aziendali.[102][103]

Nel paragrafo seguente sono analizzati nel dettaglio i cinque principi del COBIT 5.

2.5.1 I cinque principi del framework COBIT 5

Con lo sviluppo della digitalizzazione, la tecnologia è diventata un fattore abilitante per il business ed ha assunto un ruolo importante per la creazione di valore per gli *stakeholder*. Proprio loro, in quanto destinatari del valore, necessitano una gestione efficiente delle risorse IT al fine di ottimizzare i rischi e le risorse utilizzate. COBIT 5 per definire un *framework* di successo ha creato uno strumento integrato con le altre discipline in tema IT e considera l'impresa a livello globale. Infine, definisce in maniera dettagliata i processi fondamentali di management e di governance IT, considerandoli separatamente. Questi concetti fondamentali sono stati schematizzati nei cinque principi definiti nel paragrafo precedente.

Il primo principio consiste nella soddisfazione delle esigenze degli *stakeholder*. L'obiettivo generale di un'azienda è infatti quello di creare valore per i propri *stakeholder*, bilanciando i benefici con i rischi e con le risorse da impiegare.

Le imprese hanno però obiettivi diversi e possono interfacciarsi con diverse categorie di *stakeholder*, le quali potrebbero avere interessi diversi nei confronti dell'impresa anche in conflitto tra loro; pertanto, la società dovrà definire un sistema di governance che tenga conto di tutti i portatori di interesse. COBIT 5 deve poter essere applicato a qualsiasi società e viene, perciò, definita una sequenza "a cascata" di obiettivi (la sequenza è composta da 4 fasi) che le società devono seguire con l'obiettivo di

[102] AA. VV., Analyzing COBIT 5 IT Audit Framework Implementation using AHP Methodology Mutiara, Documento di Ricerca, Vol 1 N. 2, JOIV:International Journal on Informatics Visualization, 2017, pag. 33-34.

[103] Il processo di IT Auditing sarà descritto nel dettaglio nel capitolo 3.1 della seguente trattazione.

trasformare le esigenze degli investitori in obiettivi specifici al fine di definire una strategia realizzabile.

La prima fase consiste nell'identificare gli elementi che condizionano le esigenze degli *stakeholder*, i quali variano in base alle caratteristiche delle società. I fattori possono essere esterni, come ad esempio il mercato o il settore di riferimento; oppure interni, come ad esempio la cultura aziendale e la propensione al rischio degli investitori.

La seconda fase consiste nel mettere in relazione le esigenze degli *stakeholder* con gli obiettivi generali dell'organizzazione di riferimento e, per poterlo fare, COBIT 5 ha definito un elenco non esaustivo di obiettivi comuni e generici (utilizzando la tecnica della *Balanced Scorecard*) nei quali ogni impresa può riconoscersi. Per *Balanced Scorecard* (in italiano "schema di valutazione bilanciata") si intende uno strumento di misurazione strategica che si impegna a definire, pianificare e monitorare la strategia aziendale, la quale viene definita tenendo conto degli obiettivi di lungo termine e di breve termine dell'azienda. È uno strumento avanzato in quanto, per la definizione degli obiettivi strategici, non tiene conto solo dei misuratori di performance economico-finanziari ma considera l'azienda nel suo complesso.

Gli obiettivi definiti sono 17 e sono stati suddivisi innanzitutto per macroarea aziendale all'interno della quale si inserisce l'obiettivo.

Le aree sono quattro: l'area clienti, l'area finanziaria, i fattori esterni e infine l'area di apprendimento e crescita. Per ognuno, la società dovrà poi definire il rapporto tra obiettivo e obiettivo di governance definito in termini di generazione di benefici, riduzione del rischio e ottimizzazione delle risorse. Il rapporto può essere definito come primario oppure secondario, se meno forte.

Nella terza fase invece la società deve mettere in relazione gli obiettivi della società con gli obiettivi IT. Anche in questo caso, sono stati definiti 17 obiettivi correlati all'IT, ovvero obiettivi di informazione e tecnologia che la società potrebbe perseguire. La società dovrà associare gli obiettivi definiti nella seconda fase con quelli definiti nella terza, i quali saranno individuati e scelti a supporto dei primi.

Nella tabella seguente sono stati riportati i 17 obiettivi IT definiti dal COBIT 5.

Figura 2.5: COBIT e obiettivi IT

Dimensione IT in BSC	Obiettivi dell'informazione e della tecnologia correlata	
Aspetti finanziari	01	Allineamento tra strategia IT e strategia aziendale
	02	Conformità IT e supporto alla conformità aziendale rispetto alle leggi e alle normative vigenti
	03	Impegno da parte dell'alta direzione nella gestione delle decisioni relative all'IT
	04	Gestione del rischio aziendale correlato all'IT
	05	Realizzazione di benefici grazie a portafoglio di investimenti e servizi supportati da IT
	06	Trasparenza di costi, benefici e rischi relativi all'IT
Cliente	07	Erogazione dei servizi IT in linea con i requisiti aziendali
	08	Uso adeguato di applicazioni, informazioni e soluzioni tecnologiche
Fattori interni	09	Prontezza dell'IT
	10	Sicurezza delle informazioni, dell'infrastruttura di elaborazione e delle applicazioni
	11	Ottimizzazione di cespiti, risorse e funzionalità IT
	12	Attivazione e supporto di processi aziendali, integrando in essi applicazioni e tecnologia
	13	Erogazione di programmi che apportano benefici, entro scadenze e budget stabiliti e nel rispetto dei requisiti e degli standard di qualità.
	14	Disponibilità di informazioni affidabili e utili per il processo decisionale
	15	Conformità IT con le policy interne
Apprendimento e crescita	16	Personale aziendale e IT competente e motivato
	17	Conoscenze, competenze e iniziative per l'innovazione aziendale

Fonte: AA. VV., Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 19.

Nella quarta fase, la società deve identificare gli attivatori necessari per raggiungere gli obiettivi IT. Con attivatori, il COBIT 5 intende le risorse organizzative per la governance aziendali, tra cui ad esempio le infrastrutture, i processi, i principi che una società utilizza per raggiungere gli obiettivi. Rientrano tra gli attivatori anche le risorse dell'organizzazione come, ad esempio, le persone e le informazioni. Se le risorse sono carenti è possibile che sarà compromessa la capacità dell'impresa di creare valore. Per ogni attivatore saranno individuati degli obiettivi rilevanti per supportare gli obiettivi correlati IT.

COBIT 5 definisce questa sequenza "a cascata" in quanto permette alle società di definire le proprie priorità in termini di governance IT sulla base degli obiettivi aziendali e dei rischi correlati. Permette infatti di definire innanzitutto gli obiettivi specifici delle società, di associarli agli obiettivi IT e di identificare le risorse necessarie, ovvero gli attivatori, per poterli raggiungere. [104]

[104] AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 17-22.

Il secondo principio prevede la considerazione dell'organizzazione nel suo complesso, ovvero la gestione dei sistemi IT e delle informazioni aziendali deve essere progettata tenendo conto dell'intera azienda. Dunque, COBIT 5 si pone l'obiettivo di integrare la governance IT con la governance aziendale e di occuparsi di tutti i processi necessari per la gestione delle informazioni aziendali e delle tecnologie ad esse correlate; pertanto, affronta l'insieme dei servizi IT importanti, sia interni che esterni. Ci viene fornita perciò una visione a 360° sulla governance e management IT e l'approccio di governance è descritto dall'immagine seguente che evidenzia i tre elementi chiave per definirlo: gli attivatori, l'ambito di governance e infine i ruoli, le attività e le funzioni.

Figura 2.6: Obiettivi di governance

Figura: AA. VV., Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 23.

Come detto in precedenza, gli attivatori sono le risorse aziendali, le quali comprendono ogni persona, cosa, attività e funzione aziendale rilevante per la gestione dell'IT.[105]

La società deve poi definire l'ambito di governance: come ambito si intende "a cosa" si applica la governance in quanto può essere applicata ad un'azienda nel suo complesso, ad una sua entità oppure ad una singola attività.

L'ultimo fattore chiave comprende i ruoli, le attività e le relazioni delle persone coinvolte nella governance. È importante definire chi sono tali soggetti, le loro mansioni, le loro responsabilità e come interagiscono tra di loro. Nell'immagine sottostante si evidenzia

[105] Gli attivatori saranno descritti ampiamente dal principio 4 a pagina 18

come interagiscono i quattro soggetti principali coinvolti nelle attività di governance e di management.

Figura 2.7: Ruoli, attività e relazioni fondamentali

Fonte: AA. VV., Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag.24.

Il terzo principio prevede l'applicazione di un'infrastruttura unica e integrata perché COBIT 5:

a) è uno strumento conforme agli altri standard e *framework* di governance dei sistemi IT;
b) è uno strumento ad ampio spettro che può essere utilizzato per qualsiasi organizzazione e allo stesso tempo può essere integrato facilmente con altri standard utilizzati comunemente in campo IT;
c) offre linee guida facilmente utilizzabili dalle società in quanto è stato redatto con un linguaggio semplice e non tecnico;
d) integra al suo interno i framework precedentemente pubblicati dall'ISACA. [106]

Il quarto principio prevede l'adozione di un approccio di governance integrato.
Per descrivere questo principio partiamo innanzitutto dagli attivatori, ovvero quei fattori che influiscono sul funzionamento della governance e del management dell'IT e, come definito dal primo principio, sono definiti sulla base degli obiettivi IT.
COBIT 5 li suddivide in sette categorie:

1) principi, policy e strutture, ovvero il mezzo con cui si traduce la condotta desiderata in regole da applicare quotidianamente in azienda;

[106]AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 25-26.

2) processi, ovvero tutte le attività definite e organizzate per conseguire sia gli obiettivi dell'organizzazione a livello aziendale che gli obiettivi IT;
3) strutture organizzative, ovvero la componente aziendale con potere decisionale;
4) cultura, etica e comportamento delle singole persone dell'organizzazione aziendale. Spesso, non viene dato il giusto valore a questi tre fattori nelle attività di governance;
5) informazioni prodotte e utilizzate dall'organizzazione. Sono un elemento fondamentale delle organizzazioni in quanto ne consentono la corretta direzione e il corretto funzionamento;
6) servizi, infrastruttura e applicazioni, ovvero le infrastrutture e le applicazioni che consentono la produzione di servizi informatici;
7) le persone, le loro abilità e le loro competenze: sono fondamentali per condurre correttamente l'organizzazione aziendale e per pronunciarsi correttamente sulle questioni aziendali.[107]

Gli attivatori sono tra loro interconnessi: per operare in modo efficace hanno bisogno di input da altri attivatori e allo stesso tempo producono output per altri attivatori, ad esempio, la struttura organizzativa ha bisogno di persone e abilità, le quali rendono efficaci i processi.

COBIT 5 definisce anche delle dimensioni comuni per fornire una visione strutturata di trattamento degli attivatori e per agevolare le società nel gestire in modo efficiente gli attivatori e le loro interconnessioni. Le dimensioni sono 4: *stakeholder*, obiettivi, ciclo di vita e nuove prassi.

Gli *stakeholder*, interni o esterni all'azienda, hanno degli interessi e dei bisogni e la società deve definire degli attivatori per ognuno di loro tenendo conto delle loro esigenze.

Per obiettivi invece, si intende che la società deve definire per ogni attivatore degli obiettivi al fine di creare valore per il perseguimento degli obiettivi generali. Sono definiti in relazione al risultato che ci si attende dall'attivatore e in base al funzionamento dell'attivatore.

Gli obiettivi degli attivatori si suddividono a loro volta in tre categorie, sulla base di tre caratteristiche:

[107] AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 27.

1) la loro qualità intrinseca, ovvero il livello di precisione degli attivatori e il livello di accuratezza, affidabilità e oggettività dei risultati;
2) la loro qualità contestuale, ovvero il livello di coerenza degli attivatori e dei risultati ottenuti con lo scopo. I risultati dovrebbero essere idonei, precisi, completi e inerenti al contesto;
3) l'accesso e la sicurezza, ovvero il livello di accessibilità e sicurezza degli attivatori.

Per ciclo di vita si intende il ciclo di vita degli attivatori, ovvero ogni attivatore nasce, svolge la propria attività e infine viene smaltito. Le fasi comprendono innanzitutto la pianificazione e la progettazione dell'attivatore, il quale successivamente viene acquistato o costruito dalla società. Poi viene utilizzato e contemporaneamente monitorato. Infine, completato il suo ciclo di vita, sarà smaltito.

La quarta dimensione riguarda le buone prassi che devono essere definite per ogni attivatore al fine di supportare il conseguimento degli obiettivi degli attivatori. Per buone prassi si intendono esempi o suggerimenti per migliorare l'implementazione degli attivatori. Anche il *framework* COBIT 5 fornisce degli esempi che possono guidare le società.

Pertanto, per implementare al meglio gli attivatori, sulla base delle quattro dimensioni le società dovrebbero chiedersi se le esigenze degli *stakeholder* sono state considerate, se gli obiettivi sono stati raggiunti, se il ciclo di vita dell'attivatore è stato gestito e se le buone prassi sono state applicate. [108]

Il quinto principio invece tratta la separazione della funzione di governance con quella di management, delineando innanzitutto la differenza tra le due funzioni.

Infatti, i responsabili dell'attività di governance garantiscono che la definizione degli obiettivi sia stata svolta in relazione alle esigenze degli *stakeholder*; guidano l'attività prendendo decisioni e definendo le priorità e infine supervisionano le prestazioni e il raggiungimento degli obiettivi. Tale attività è spesso svolta dal consiglio di amministrazione.

Diversamente, i responsabili dell'attività di management pianificano, sviluppano, eseguono e monitorano le attività sulla base di ciò che è stato predisposto dai

[108] AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, pag. 27 – 30.

responsabili di governance. Tale attività è spesso svolta dall'alta direzione con alla guida l'amministratore delegato.

Al fine di ottenere una struttura efficiente, le due funzioni devono essere interconnesse e devono interagire. Le società dovrebbero strutturare i processi di governance e processi di management in modo opportuno tenendo conto di tutti gli obiettivi in gioco; pertanto, COBIT 5 fornisce un modello di riferimento che rappresenta tali processi in relazione alla componente IT.

Questo modello è completo e facilmente comprensibile dal personale IT e dalla direzione aziendale, ma non è un modello universale in quanto non è l'unico possibile e le società devono in ogni caso tener conto delle proprie specificità nell'applicarlo. Il modello fornisce una guida operativa per le applicazioni IT e allo stesso tempo permette di valutare le prestazioni IT, assicurarne il funzionamento e integrarlo con le altre attività aziendali.

COBIT 5 suddivide i processi in processi di governance IT e i processi di management IT.

I processi di governance sono a loro volta suddivisi in cinque processi e per ogni processo devono essere definire delle procedure di valutazione, direzione e monitoraggio. I cinque processi sono i seguenti: assicurare l'impostazione e la manutenzione dell'infrastruttura IT, assicurare la realizzazione dei benefici, assicurare l'ottimizzazione del rischio, assicurare l'ottimizzazione delle risorse e infine assicurare la trasparenza per gli *stakeholder*.

I processi di management comprendono invece quattro "domini" strettamente correlati alle aree di pianificazione, costituzione, esecuzione e monitoraggio del controllo interno al fine di tener conto di tutti gli aspetti IT. I quattro domini sono i seguenti:[109]

1) allineamento, pianificazione e organizzazione (APO), ovvero la fase strategica nella quale si definisce il piano IT migliore e più adatto per il raggiungimento dell'obiettivo aziendale. Per raggiungere tale obiettivo, infatti, il piano deve essere pianificato, comunicato e gestito per poter essere messo in atto;
2) costruzione, acquisto e implementazione (BAI), ovvero la fase in cui, dopo aver definito il piano IT, si acquisiscono le risorse necessarie per metterlo in pratica e successivamente viene messo in atto. Per realizzare la strategia, infatti, devono essere create internamente oppure acquistate esternamente le risorse per

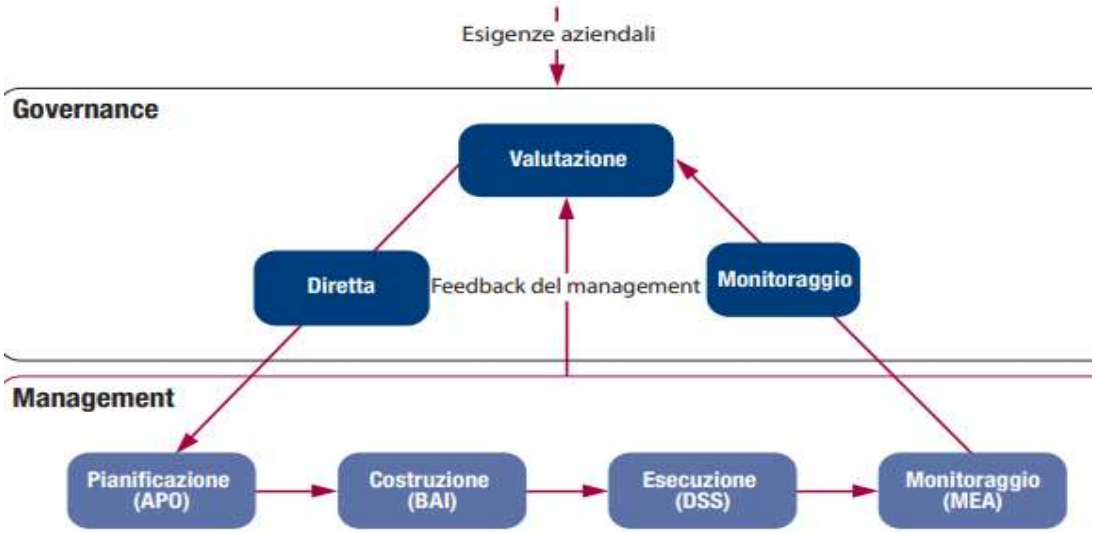
[109]AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, capitolo 6, 31-33

applicarlo, le quali poi vengono successivamente implementate e integrate all'interno del processo aziendale. In questo dominio rientrano anche tutte quelle attività di modifica e di manutenzione necessarie per assicurare il corretto funzionamento dei sistemi;

3) erogazione, servizio e supporto (DSS), ovvero la fase grazie alla quale viene garantito il funzionamento del piano. Questo dominio permetto di emettere i servizi definiti dalla strategia sotto forma di operazioni aziendali e attraverso l'elaborazione dei dati da parte dei sistemi operativi;
4) monitoraggio, valutazione e rilevazione (MEA), ovvero la fase che consente di monitorare, valutare e raccoglie dati in merito al piano attuato per verificarne l'efficacia. Infatti, è importante valutare regolarmente la qualità e la conformità ai controlli dei processi IT. [110]

COBIT 5, inoltre, si impegna a definire 37 processi di governance e di management che le società dovrebbero, o meglio potrebbero, mettere in atto sulla base del contesto di riferimento e delle caratteristiche uniche della società che intendono metterlo in atto.
I fattori che ne influenzano l'applicazione sono diversi tra cui le leggi e la normativa a cui è sottoposta quel tipo di società, l'etica e la cultura aziendale, la mission e la vision aziendale, la propensione al rischio e le strategie aziendali.

Figura 2.8: Interazione tra processi di governance e processi di management



[110]Lahti C., Peterson R., *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools*, Synngress, 2015, pag. 35-37.

Fonte: AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di pubblica consultazione, traduzione italiana, ISACA, 2012, capitolo 6, 32.

Nell'immagine sovrastante, sono schematizzati i due processi, formalmente separati tra loro ma con dei punti di collegamento che ne permettono l'efficienza. Entrambi i processi sono costituiti in risposta alle esigenze aziendali.

2.5.2 COBIT e revisione

COBIT è uno strumento che si è diffuso ampiamente negli ultimi anni e che è in continua crescita in tutti i settori economici, sia tra gli *IT auditor* che tra le società.
COBIT 5, e in generale i suoi predecessori, sono stati dei *framework* di controllo per il management e per la governance IT perché è importante che l'ambiente IT sia ben strutturato e organizzato, in quanto la società deve soddisfare i bisogni e gli obiettivi degli *stakeholder* alla luce dei rischi IT. Oltre ad una struttura efficiente però, sono necessari anche dei controlli efficienti che garantiscano il corretto funzionamento del sistema. COBIT 5 infatti, è un esempio di policy e di buone pratiche per definire dei processi IT che si integrano all'interno di una struttura IT gestibile e logica e che allo stesso tempo utilizzano in modo ottimale le risorse aziendali.

Tale strumento, però, si focalizza maggiormente sulle attività di controllo piuttosto che sulle attività operative per definire il sistema e proprio per questo rappresenta una guida per le attività di *audit*. Il framework COBIT è, infatti, uno strumento che è stato definito principalmente per due soggetti: il management aziendale e i revisori esterni ed interni all'azienda. Per il management costituisce una guida per la definizione di un ambiente IT strutturato ed efficiente. Per i revisori, invece, rappresenta una guida per poter emettere un'opinione sul management dell'IT precisa in quanto, definendo come dovrebbe essere un ambiente IT efficiente, il revisore ha la capacità di comprendere l'ambiente IT che ha di fronte individuando eventuali carenze e possibili soluzioni per migliorare l'IT.
Il *framework* fornisce anche delle linee guida di *audit* a sostegno dell'attività di valutazione dei processi e dei controlli. COBIT ci fornisce un approccio ben preciso: il

revisore deve comprendere il processo, successivamente deve valutare i controlli definiti dalla società e i rischi che potrebbero ostacolare il raggiungimento degli obiettivi. Tale attività deve essere svolta per i 37 processi definiti dal quinto principio del *framework*. Rappresenta perciò uno strumento che può essere utilizzato dal revisore come guida per l'attività di *audit*. Per poter essere applicato in modo efficace però, è necessario che l'*IT Auditor* abbia il giusto livello di formazione e istruzione.

È importante ricordare che tale strumento è scalabile e perciò può essere utilizzato per qualsiasi organizzazione e per qualsiasi ambiente IT: può essere infatti personalizzato sulla base delle caratteristiche specifiche di ogni singola azienda.

Tale strumento però inizialmente fu poco utilizzato. A diffonderlo fu la normativa *"Sarbanes – Oxley Act",* successiva alla normativa COBIT, ovvero una legge americana che introdusse per la prima volta l'obbligo di definire dei controlli interni all'interno delle società a garanzia degli *stakeholder*.

2.6 Sarbanes – Oxley Act

Il *"Sarbanes – Oxley Act*" (comunemente chiamata normativa SOX)[111] è una legge statunitense emanata nel 2002 per migliorare i processi di rendicontazione finanziaria, *audit* e governance aziendale delle società pubbliche. Nasce negli Stati Uniti in risposta ad una serie di fallimenti aziendali e scandali finanziari avvenuti in quel periodo, tra cui quelli che hanno coinvolto due società famose: Enron[112] e Worldcom[113]. Si applica a tutte le società americane ed estere quotate alla borsa americana e alle società controllate da società quotate alla borsa americana. [114]

L'obiettivo della legge è quello di migliorare l'accuratezza e la veridicità delle informazioni finanziarie prodotte dalle società per proteggere gli investitori aziendali da

[111]Il Sarbanes– Oxley Act prende il nome dal senatore statunitense Paul Sarbanes e dal rappresentante statunitense Micheal Oxley che l'hanno approvata.

[112]Enron era un'azienda multinazionale statunitense che si occupava di distribuzione di gas. Fallì inaspettatamente nel 2001 smascherando un bilancio fasullo e società di comodo situate all'esterno con l'obiettivo di occultare il denaro nascosto. Questo fallimento fu significativo per l'opinione pubblica e, in risposta a questo fatto, il presidente Bush varò delle leggi al fine di contrastare e punire il reato di falso di bilancio.

[113] Worldcom era un'azienda leader nel mercato delle telecomunicazioni. Tale azienda puntava a crescere attraverso operazioni straordinarie di acquisizioni di nuove aziende. Dopo una serie di acquisizioni, nel 2002 crollò il sistema messo in atto dal suo CEO e fallì, smascherando un falso di bilancio. Per poter fare ciò, l'azienda aveva sovrastimato le proprie azioni aziendali attraverso investimenti fittizi arrivando ad un valore di 60 dollari per azione; nel momento del fallimento arrivarono a 20 centesimi. Il CEO di Worldcom fu condannato a 25 anni di reclusione.

[114]Per borsa americana si intende il NYSE, ovvero il New York Security Exchange.

possibili frodi. Il risultato si concretizza nell'aumento di credibilità e di trasparenza dell'informativa finanziaria, traducendosi così in una riforma di Corporate Governance. Si vuole infatti rafforzare il concetto di responsabilità aziendale introducendo nuovi obblighi in capo alle società e nuove sanzioni applicabili in caso di comportamenti fraudolenti da parte della direzione aziendale.
È suddiviso in sezioni e le sue sezioni più importanti per i temi affrontati in questa tesi sono principalmente tre, le quali introducono nuove responsabilità e nuovi obblighi per la direzione aziendale. Le sezioni che saranno analizzate sono: la sezione 302, la sezione 404 e la sezione 906.

La sezione 302 delinea un obbligo da parte della direzione di certificare che la documentazione annuale e trimestrale obbligatoria non contenga errori, omissioni, notizie false o fuorvianti. Allo stesso tempo deve attestare che l'informativa finanziaria fornisce una rappresentazione veritiera e corretta della situazione patrimoniale ed economica della società. Tale sezione rende anche la direzione responsabile nella definizione, nell'attuazione e nella valutazione di controlli messi in atto per garantire una corretta informativa. La novità è proprio questa: per la prima volta c'è un obbligo da parte della direzione aziendale di valutare i controlli posti in essere per migliorare l'informativa finanziaria. La direzione, infatti, è tenuta a comunicare al revisore esterno eventuali carenze nei controlli.
Il CEO e il CFO devono periodicamente certificare:

- la loro responsabilità relativamente ai controlli;
- che hanno progettato e valutato i controlli messi in atto per garantire un'informativa finanziaria efficiente;
- che hanno comunicato le loro conclusioni relativamente all'efficacia dei controlli e che hanno comunicato ai revisori esterni ed interni eventuali carenze significative riscontrate.

La sezione 404 invece introduce il concetto di sistema di controllo interno prevedendo un obbligo da parte della direzione di valutare l'efficacia dei controlli interni messi in atto con l'obbligo di predisporre un report annuale su quanto valutato. Il CEO e il CFO devono annualmente:

- dichiararsi responsabili dell'efficacia del sistema di controllo interno definito e mantenuto in azienda;
- valutare al termine dell'esercizio il sistema di controllo interno.

La sezione 906 prevede invece la certificazione, e perciò l'attribuzione della responsabilità alla direzione aziendale, del rendiconto finanziario annualmente predisposto dalla società. Una mancata certificazione prevederà delle multe per la società fino ad un massimo di 5 milioni di dollari e può essere prevista anche la reclusione fino a 20 anni per non conformità se l'omissione è intenzionale e fraudolenta.

La normativa SOX attribuisce un ruolo importante anche ai revisori esterni legali della società, i quali devono valutare e attestare, attraverso una relazione separata, quanto dichiarato dal management in merito ai controlli interni. Devono infatti analizzare il sistema di controllo interno definito, attuato e valutato dalla società raccogliendo elementi probativi sufficienti e appropriati. L'obiettivo è quello di emettere una relazione che attesti l'effettività dei controlli definiti dalla direzione aziendale. [115]
Per valutare l'adeguatezza del sistema di controllo interno, il revisore deve servirsi di un quadro di riferimento riconosciuto a livello globale. La normativa SOX, però, non specifica quale sia lo strumento da utilizzare ma gli strumenti maggiormente utilizzati e riconosciuti sono quelli precedentemente analizzati, ovvero il *framework* COSO e il *framework* COBIT.

La direzione non può attestare come efficaci dei controlli che presentano delle carenze sostanziali (nel linguaggio tecnico queste carenze sono definite "*material weakness*") ma deve mettere in atto un processo strutturato per valutarne l'efficacia, definito "*Managment Assessment Process"*. Questo processo prevede innanzitutto l'individuazione dei controlli messi in atto per contrastare eventuali errori significativi. Successivamente deve essere valutata l'efficacia e l'operatività dei controlli al fine di individuare eventuali carenze significative. Infine, deve documentare quanto valutato ai revisori esterni che ne attesteranno la correttezza.

[115]Nel paragrafo 3.6 della presente trattazione sono definiti i test sui controlli che devono essere svolti dal revisore.

Il revisore, nell'attestarne la correttezza, valuterà innanzitutto i controlli messi in atto a livello aziendale (i cosiddetti "*Entity Level Control*") che hanno un effetto pervasivo nell'intera valutazione, successivamente valuterà i controlli messi in atto per prevenire comportamenti fraudolenti e infine i controlli definiti per determinati elementi chiave o transazioni rilevanti per la società di riferimento.[116]
Il costante aumento dell'automazione ha introdotto un sistema di controllo interno più orientato all'IT e dei nuovi controlli IT che le società dovranno progettare e mettere in atto. Di conseguenza, il revisore sarà chiamato ad individuare e a valutare anche questo nuovo tipo di controllo.

La legge SOX è stata recepita dalla normativa italiana attraverso la Legge sul Risparmio 262/2005[117] introducendo la figura del Dirigente Preposto ovvero una figura che redige l'informativa finanziaria e se ne assume la responsabilità.
Il Dirigente preposto infatti ha la responsabilità di definire e mettere in atto procedure amministrative e contabili adeguate alla predisposizione del bilancio d'esercizio e di ogni documentazione economico-finanziaria destinata al mercato. Le procedure devono essere adeguatamente formalizzate e devono essere sottoscritte dal direttore generale e dal dirigente preposto, i quali ne attestano la veridicità.
Il Dirigente ha inoltre la responsabilità di valutare l'efficacia delle procedure definite e infine deve attestare con una relazione apposita la loro adeguatezza e la loro effettiva applicazione.
Lo strumento di riferimento per rispondere a queste responsabilità è la definizione di un sistema di controllo efficiente, mediante l'applicazione del COSO *Framework*. Esso rappresenta la *best practice* per la progettazione e la valutazione del sistema di controllo interno, nonostante non sia esplicitamente menzionato dalla normativa. Nel caso in cui invece le imprese siano maggiormente automatizzate e perciò abbiano un ambiente aziendale tecnologico, il *framework* più opportuno da utilizzare sarà il COBIT.

[116]Bozzola M, Faedo I., Sarbanes- Oxley Act, Sezione 404 (Internal control over Financial reporting), Documento in Pubblica Consultazione, E&Y, 22 novembre 2010.
[117]Legge 28 dicembre 2005, n. 262 " Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari", art. 14.

2.6.1 Sox e IT Auditing

La normativa SOX è importante in quanto permette di valutare e testare i controlli interni che una società definisce al fine di attestare l'accuratezza dei dati finanziari. Questi controlli devono essere progettati e attuati in modo adeguato dalle società in quanto il revisore successivamente valuterà e testerà tali controlli al fine di assicurarne l'adeguatezza.

Come abbiamo visto in precedenza però, il progresso tecnologico ha integrato sempre di più la tecnologia e la componente IT all'interno del sistema di controllo interno. Nel valutare perciò il controllo interno, il revisore dovrà monitorare anche le risorse IT utilizzando il *framework* COBIT come strumento di riferimento.

Tra gli elementi IT che il revisore dovrà verificare ci sono i seguenti:

1) La sicurezza informatica. Il revisore dovrà verificare se la società ha definito dei controlli per prevenire i rischi IT legati alla sicurezza informatica e perciò correlati alla violazione dei dati aziendali. Allo stesso tempo dovrà verificare se la società possiede degli strumenti per contrastare eventuali attacchi informatici.
2) Il controllo degli accessi. Il revisore dovrà verificare se la società ha definito dei controlli in relazione agli accessi che impediscano agli utenti non autorizzati di visualizzare le informazioni aziendali sensibili. Tali controlli possono riguardare l'accesso a server e database oppure possono riguardare i sistemi di autenticazione (ID e password).
3) Al *backup* dei dati. Il revisore verificherà i controlli relativi ai *backup* dei dati, considerando anche i dati archiviati esternamente (come, ad esempio, i dati in *cloud*). Per *backup* si intende un'operazione finalizzata alla messa in sicurezza di un determinato ammontare di dati attraverso la duplicazione degli stessi su un supporto esterno.
4) Cambio gestionale. Il revisore in questo caso dovrà verificare come il reparto IT attuerà tale processo in termini di: aggiornamento e installazione del nuovo *software*, autenticazione di nuovi utenti, modifica di database oppure di altri elementi di dati. Sarà importante verificare anche se le verifiche sono state eseguite da un utente che aveva l'autorizzazione per farlo.[118]

[118]Sarbanes Oxley Act, Sarbanes- (SOX) Audit Requirements (sarbanes-oxley-101.com)

2.7 Le tre normative vigenti

Quando la normativa SOX è diventata efficace per la prima volta negli Stati Uniti, non erano state definite delle disposizioni precise su come implementare e gestire la revisione dei sistemi di controllo interno in conformità alla Sezione 404; era solo stato definito che dovevano essere utilizzati dei quadri di riferimento globalmente riconosciuti e ufficiali ma non erano state date ulteriori direttive.

Le prime versioni dei *framework* COSO e COBIT sono precedenti rispetto alla normativa SOX, ma per poter adempiere ad essa le società hanno applicato i due strumenti.

Il quadro COSO è uno strumento che può essere utilizzato al fine di definire e valutare i controlli interni attraverso le cinque componenti. Il quadro COBIT invece è uno strumento che rappresenta come dovrebbe essere definito e valutato il controllo interno in un ambiente fortemente orientato alla tecnologia. Sia lo strumento COSO che COBIT possono essere descritti come *framework* multidimensionali che descrivono la progettazione di un sistema di controllo interno.

I due framework hanno avuto un forte sviluppo e diffusione in seguito alla normativa SOX, in quanto erano i due unici strumenti riconosciuti a livello globale che emanavano regole di *best practice* sulla progettazione e l'attuazione di controlli interni efficienti.

Una conseguenza della legge SOX, dato anche l'obbligo di certificazione da parte della direzione e di verifica da parte di un revisore, è una maggior attenzione nella definizione di controlli interni per il conseguimento degli obiettivi aziendali e una maggior attenzione globale relativa alla governance IT ed ai rischi IT.

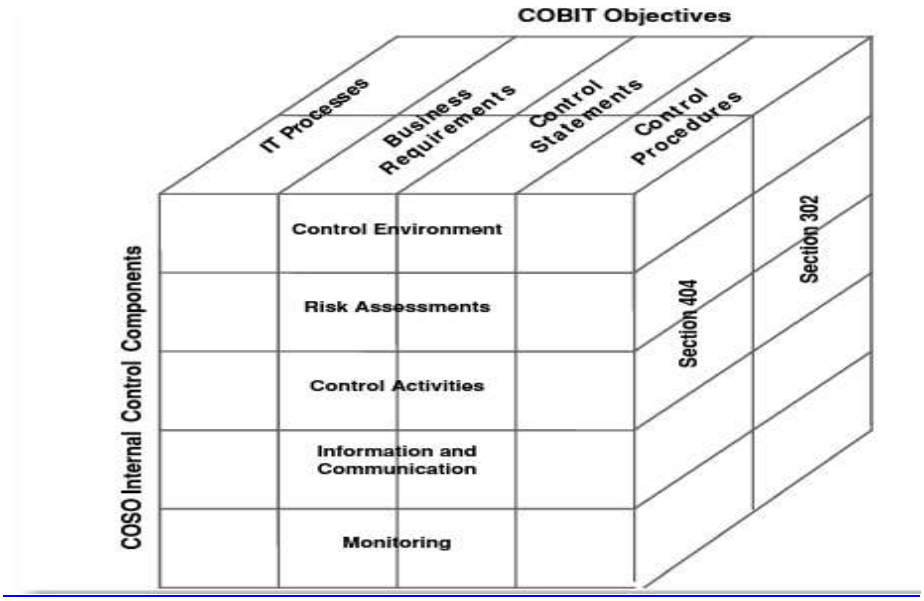
Ha perciò permesso lo sviluppo e la diffusione del framework COBIT a livello globale, permettendo un suo continuo rinnovo fino all'edizione 5.0. Se un'azienda è molto digitalizzata, la definizione, attuazione e valutazione di controlli interni sulle componenti IT sono una chiave per raggiungere la conformità SOX.

L'immagine riportata di seguito mostra la relazione che c'è tra le componenti di controllo dei due *framework* e le sezioni 302 e 404 della normativa SOX.

Nella parte superiore del cubo sono riportati gli obiettivi COBIT, nella parte frontale le componenti definite dal COSO Report e nella parte laterale le sezioni 302 e 404.

Un'implementazione integrata e adeguata dei due strumenti permetterà la conformità a queste due sezioni.

Figura 2.9: Relazione tra le componenti del COSO Report e gli obiettivi COBIT



Fonte: Moeller R., *Executive's guide to governance, Improving Systems Processes with Service Management, COBIT and ITIL,* Libro, Wiley Corporate F&A, 2013, pag. 96.

COBIT è uno strumento ampiamente utilizzato dagli *IT Auditor* per valutare i controlli IT posti in essere dalle società ma dovrebbe essere utilizzato, e conosciuto, anche dalla direzione aziendale e dai revisori interni. È utile e importante per valutare i controlli interni e la governance di un ambiente più orientato all'IT, ovvero il tipo di ambiente che incontriamo maggiormente nelle società odierne.

CAPITOLO 3: IL PROCESSO DI IT AUDITING

3.1 IT Auditing e ambiente IT

Come è stato definito dal primo capitolo, i principi di revisione affrontano per la prima volta, grazie all'aggiornamento dell'ISA Italia 315, il tema dell'IT. Sono state previste, infatti, delle procedure specifiche che il revisore deve seguire per comprendere l'ambiente IT utilizzato dalle società al fine di individuare eventuali rischi di errori significativi.

L'attività di revisione dell'ambiente IT è chiamata "*IT Auditing*" e può essere definita come un processo di raccolta e valutazione di elementi probativi al fine di definire se un sistema informativo aziendale mantiene l'integrità dei dati aziendali, salvaguardia le risorse e le utilizza in modo efficiente, consentendo così di perseguire in modo efficiente gli obiettivi dell'organizzazione.

Tale attività deve essere svolta obbligatoriamente per i soggetti sottoposti alla normativa SOX in quanto, come previsto dalla sezione 404, il revisore esterno deve certificare il sistema di controllo interno delle società. *L'audit* dei sistemi IT è fondamentale al fine di valutare il sistema di controllo interno perché verificare l'ambiente IT e i relativi controlli IT posti in essere sui sistemi informativi aziendali significa valutare, di conseguenza, come sono elaborati i dati e le informazioni che confluiranno nell'informativa di bilancio.

Le componenti IT che il revisore deve tenere in considerazione sono: le applicazioni IT, l'infrastruttura IT, le operazioni IT, la governance dell'ambiente IT e il livello di sicurezza dell'IT. Deve considerare inoltre come la società implementa, sviluppa e mantiene il sistema in un'ottica di continuità aziendale.

Per comprendere al meglio il tema in esame, l'ISA 315 ci fornisce una definizione puntuale di "Ambiente IT"[119], precisando che si concretizza nell'insieme delle applicazioni, delle infrastrutture, dei processi IT e del personale che le società utilizzano a supporto delle attività operative con il fine di raggiungere gli obiettivi aziendali.

[119]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 5, punto g).

Le applicazioni IT si sostanziano nei programmi usati per rilevare, registrare, elaborare e rendicontare le informazioni e le operazioni aziendali. Esse includono i *Data Warehouse*, ovvero quei sistemi che raccolgono dati proveniente da fonti diverse in un archivio centrale e unico con l'obiettivo di supportare l'analisi di dati e la produzione di informazioni[120]; e i *Report Writers*, ovvero *«un'applicazione IT utilizzata per estrarre dati da una o più fonti (quali un data Warehouse, un database, o un'applicazione IT) e presentati in un formato specifico»[121].*

Le infrastrutture IT invece comprendono la rete, i sistemi operativi e i database, includendo sia le loro componenti *software* che le componenti *hardware*.[122] Le componenti sono:

5) la rete: è una componente fondamentale in quanto trasmette dati, informazioni, servizi e risorse all'interno dell'azienda tramite un collegamento di comunicazioni comuni;
6) il sistema operativo: è un sistema che gestisce le comunicazioni tra hardware, applicazioni e software. Alle applicazioni e ai database, infatti, si può accedere solo tramite sistema operativo;
7) Database: tradotto "base dati", per database si intende una raccolta organizzata di dati che permette a chi li utilizza di ricercare e recuperare in modo efficiente e veloce dati e informazioni. I database, infatti, archiviano i dati utilizzati dalle applicazioni IT e si concretizzano in tabelle di dati correlate tra loro. A questi dati, può avere accesso diretto solo il personale IT oppure solo l'amministratore del database. [123]

È importante sottolineare che per *hardware* si intendono tutte le componenti fisiche e tangibili di un computer e dell'intera infrastruttura IT, come ad esempio il computer, la tastiera, il router, i dispositivi elettrici e meccanici; invece, per *software* si intendono tutte le componenti logiche e intangibili di un computer e di un'infrastruttura IT, come ad esempio la rete, il sistema operativo e i programmi.

[120]Data Warehouse, IBM, https://www.ibm.com/it-it/topics/data-warehouse .
[121]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag.79, par. 4, nota a pie di pagina 77.
[122]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", punto g), pag. 5.
[123]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", app.5, par. 16, pag. 85.

Infine, i processi correlati all'IT sono molteplici e possono essere definiti come l'insieme di attività svolte dall'impresa per gestire gli accessi all'ambiente IT, i cambiamenti nell'ambiente IT e infine le operazioni IT[124].

Perciò, *l'audit* dei sistemi IT si concretizza nell'esame dei processi IT e delle risorse IT e nella valutazione di come queste due componenti si combinano tra loro al fine di soddisfare gli obiettivi aziendali garantendo l'efficacia, l'efficienza e l'economia delle risorse, nel rispetto della normativa vigente.
Tale attività può essere schematizzata dall'immagine che segue:

Figura 3.1: Il processo di IT *Auditing*: correlazione tra processi IT, risorse IT e obiettivi aziendali

Fonte: AA. VV., Manual of Information Technology Audit, Volume I, Documenti in Pubblica consultazione, Office of the Comptroller & Auditor General of India, pag. 8.

Il processo di IT *auditing* è molto ampio e include attività diverse, le quali hanno come fattore comune l'acquisizione di un'opinione relativa al grado di affidamento che può essere posto sui sistemi IT di una determinata società. Le attività sono:

1) l'attività di *audit* finanziario, con l'obiettivo di valutare la correttezza e la veridicità dell'informativa finanziaria;
2) l'attività di *audit* operativo, con l'obiettivo di valutare il sistema di controllo interno;

[124]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", punto g), pag. 5.

3) l'attività di *audit* dei sistemi informativi, ovvero l'attività focalizzata sul sistema informativo aziendale;
4) attività specializzate e specifiche, come, ad esempio, l'attività di valutazione dei servizi forniti da soggetti esterni.

Si struttura come un normale processo di *audit* e può essere riassunto in cinque fasi.

1) La fase preliminare di pianificazione. In questa fase si valuterà l'integrità e l'indipendenza del *team* di *audit* e si definirà l'entità, le tempistiche e la natura delle procedure di *audit*. Inoltre, il *team* di revisione individuerà gli aspetti IT significativi da tenere in considerazione.
2) La comprensione dell'ambiente IT: il revisore, nel comprendere l'impresa e il suo sistema di controllo interno, dovrà acquisire una comprensione anche dell'ambiente IT. L'ISA 315 definisce degli aspetti che il revisore deve considerare al fine di comprendere la governance e la gestione della componente IT.[125]
3) La fase di identificazione e valutazione dei rischi derivanti dall'uso dell'IT. In questa fase il revisore, attraverso la comprensione dell'impresa, identifica e valuta i rischi di errori significativi. Il revisore dovrà assicurarsi di aver considerato tutti i fattori significativi relativi all'ambiente IT e dovrà identificare le applicazioni IT e altri aspetti dell'ambiente IT soggetti a rischio. Dovrà successivamente valutare il rischio di controllo identificando i controlli IT che la società ha progettato e attuato al fine di contrastare i rischi precedentemente identificati.
4) Test sui controlli: il revisore deve testare, in primo luogo, la progettazione dei controlli e successivamente deve testare l'efficacia dei controlli con l'obiettivo di valutare se può fare affidamento su tali controlli nello svolgimento delle procedure di revisione.
5) La relazione di revisione: il revisore emetterà una relazione sull'attività svolta in cui evidenzierà eventuali carenze riscontrate durante il processo. [126]

Nei paragrafi seguenti del presente elaborato sono analizzate le fasi del processo di IT *auditing* nel dettaglio.

[125]L'attività di comprensione della componente IT è ampiamente analizzata nei paragrafi 3.2 e 3.3.
[126]AA. VV., *IT Audit Manual 2017*, Documenti in Pubblica Consultazione, prima edizione, Afrosai-e, 1 Novembre 2017, pag. 7.

3.2 Comprensione dell'ambiente IT attraverso la comprensione dell'impresa

Il revisore, per poter identificare e valutare i rischi di errori significativi, deve, innanzitutto, svolgere «*un'attività di comprensione dell'impresa e del contesto in cui opera, del quadro normativo sull'informativa finanziaria applicabile e del sistema di controllo interno dell'impresa.*»[127]

Il processo di comprensione è, infatti, dinamico e iterativo ed il revisore, durante tutta la revisione, sarà tenuto a raccogliere informazioni ed elementi probativi sufficienti e appropriati.

L'attività di comprensione è utile perché supporta il revisore nello sviluppo di aspettative iniziali su saldi contabili, su classi di operazioni e sull'informativa finanziaria che potrebbero essere rilevanti per la revisione. Tali aspettative formeranno una base per definire l'ampiezza necessaria delle procedure di comprensione del sistema informativo aziendale.

Nel presente elaborato, non sarà analizzata l'attività di comprensione a livello generale ma saranno evidenziati solo gli aspetti chiave che il revisore deve considerare per comprendere come le organizzazioni aziendali utilizzano la componente IT.

Le attività di comprensione dell'impresa, del contesto in cui opera e del quadro normativo supportano il revisore nell'individuare eventi rilevanti che potrebbero influenzare la probabilità che le asserzioni contengano errori significativi. Ciò aiuta il revisore nella pianificazione dell'intera attività di revisione e nell'esercizio dello scetticismo e del giudizio professionale.

Il revisore determina l'estensione e la natura delle procedure di comprensione sulla base del proprio giudizio professionale. Esse varieranno in base alle caratteristiche specifiche della singola impresa, tra cui anche la complessità dell'impresa e la complessità del suo ambiente IT. Se la complessità dell'IT fosse tanto elevata, il revisore potrebbe aver bisogno di competenze tecniche specifiche per poter acquisire l'adeguata comprensione richiesta dall'incarico; potrebbe servirsi perciò dell'aiuto di un *IT Auditor*[128].

[127]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 7.

[128]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 22-24.

L'auditor dovrà innanzitutto comprendere, in relazione alla struttura organizzativa e all'assetto proprietario e di governance, la struttura e la complessità dell'ambiente IT. A titolo esemplificativo, le società potrebbero avere un ambiente complesso derivante dall'utilizzo simultaneo di svariati sistemi IT *legacy in business*[129] poco integrati fra loro oppure derivante dall'utilizzo di fornitori di servizi IT interni oppure esterni. I servizi potrebbero riguardare, ad esempio, l'esternalizzazione a terzi *dell'hosting*[130] del sistema IT oppure l'utilizzo di un centro di servizi condiviso per la gestione centralizzata dei processi IT in un gruppo[131]. Esternalizzare un servizio IT comporterà dei rischi che il revisore dovrà considerare.

Il revisore, in secondo luogo dovrà comprendere il modello di business, ovvero la modalità in cui una determinata impresa crea valore e lo preserva per i propri *stakeholder* considerando le proprie attività operative, la propria struttura organizzativa, i propri processi, le risorse utilizzate e la normativa di riferimento.
Ogni modello è sottoposto ad un rischio, ovvero il "rischio di business", ossia il rischio che l'impresa non raggiunga i propri obiettivi e non realizzi le proprie strategie a causa di condizioni, eventi o circostanze negative e significative.[132] Infatti, tale rischio ha come diretta conseguenza il rischio di errori significativi per saldi contabili, classi di operazioni, informativa a livello di bilancio ed informativa a livello di asserzioni; ed è proprio per questo che il revisore dovrà comprenderlo.
Il modello di business comprende anche la modalità in cui l'impresa decide di usare la componente IT per interfacciarsi con clienti, fornitori e con qualsiasi altro portatore di interesse.[133]
Il revisore dovrà comprendere come la società usa l'IT, come esso è stato implementato e come esso influenza le attività operative e finanziarie aziendali. I modi in cui le società usano la componente IT sono diversi e perciò anche il rischio ad esse correlato sarà diverso. Ad esempio, se due società vendono entrambe calzature ma la prima le vende in un negozio fisico utilizzando un sistema di gestione del magazzino e delle vendite

[129]Sistemi e applicazioni definiti obsoleti.
[130]Il termine hosting è stato spiegato nel paragrafo 3.3.4.1 della presente trattazione.
[131]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. A56, pag. 24-25.
[132]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", definizione b), pag. 5.
[133]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", app. 1, par. 1-3, pag. 63.

altamente automatizzato invece la seconda le vende attraverso un canale online svolgendo tutte le operazioni in un ambiente IT, è chiaro che, nonostante sia venuto lo stesso bene, il rischio di business sarà totalmente diverso per le due società. [134]

3.3 Comprensione dell'ambiente IT attraverso la comprensione del sistema di controllo interno

Prima di comprendere come il revisore comprende il sistema di controllo interno in ottica IT dobbiamo comprendere innanzitutto perché la tecnologia è strettamente correlata al SCI.

Come definito dall'ISA 315, il revisore deve comprendere il sistema di controllo interno delle società al fine di individuare e valutare rischi di errori significativi a livello di bilancio. Il sistema di controllo, come descritto dall'ISA 315, si compone delle cinque componenti precedentemente previste dal COSO Report del 1992, ovvero:

1) *«l'ambiente di controllo;*
2) *Il processo adottato dall'impresa per la valutazione del rischio;*
3) *Il processo adottato dall'impresa per monitorare il sistema di controllo interno;*
4) *Il sistema informativo e la comunicazione;*
5) *Le attività di controllo».*[135][136]

Non sempre le componenti definite dalle società riflettono quelle definite dall'ISA 315: possono differire per terminologia o quadro di riferimento in quanto le società differiscono tra di loro per dimensione e complessità. Le società meno strutturate metteranno in atto controlli sicuramente più semplici e meno articolati.

Comprendere le varie componenti del sistema permette allo stesso tempo di comprendere come l'impresa identifica i rischi di business e come risponde ai rischi identificati. Ciò aiuta il revisore a identificare e valutare i rischi di errori significativi e gli permette di poter definire le procedure seguenti. La comprensione delle prime tre aree del sistema di controllo interno, ovvero l'ambiente di controllo, il processo adottato per la valutazione dei rischi e il processo di monitoraggio permetteranno al revisore di

[134]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. A61, pag. 25.
[135]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 6, punto m.
[136]I nomi delle componenti non rispecchiano testualmente quanto previsto dal COSO Report ma lo scopo e la funzione di ogni componente non cambia.

identificare soprattutto i rischi di errori significativi a livello di bilancio nel suo complesso. Le ultime due aree invece, ovvero il sistema informativo e delle comunicazioni e le attività di controllo permetteranno al revisore di identificare soprattutto i rischi di errori significativi a livello di asserzioni. [137]

Il sistema di controllo interno ha l'obiettivo di fornire una ragionevole sicurezza che gli obiettivi aziendali saranno raggiunti. Anche in questo caso la sicurezza fornita non è assoluta perché al SCI sono legati dei limiti intrinseci. Questi limiti sono strettamente correlati al fatto che il sistema di controllo interno è posto in essere da "persone" e nel prendere decisioni applicano il proprio giudizio, il quale può essere errato. Un errore umano può perciò provocare un malfunzionamento del sistema in quanto è possibile che un sistema sia implementato, modificato, oppure messo in atto in modo poco efficiente. A titolo esemplificativo, è possibile che la società produca dei report per testare il controllo interno ma tali informazioni vengono utilizzate in modo inefficiente perché colui che è incaricato ad esaminarle non comprende a pieno lo scopo di tali informazioni oppure non ha le capacità per comprenderle in modo adeguato. Allo stesso modo, i controlli potrebbero essere raggirati oppure forzati da parte della direzione o da parte del personale della società. Per esempio, se viene predisposta un'applicazione IT per la segnalazione di eventuali operazioni che hanno un valore superiore ad una determinata soglia, il personale IT potrebbe disabilitare questi controlli. [138]

Nell'implementarlo le società possono servirsi delle componenti IT al fine di renderlo più efficiente, attraverso controlli e risorse. Ma il suo utilizzo non è considerato obbligatorio: possono optare, infatti, per procedure manuali, procedure altamente automatizzate oppure possono utilizzare una combinazione di entrambe in base alla struttura e alla complessità dell'azienda.
L'uso di tecnologie IT condiziona, innanzitutto, il modo in cui l'azienda recepisce, elabora, archivia e comunica le informazioni aziendali rilevanti alla redazione del bilancio e di conseguenza, ciò condiziona la configurazione dell'intero sistema. Infatti,

[137]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 31-32.
[138]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 22-23-24, pag. 74.

ogni area del sistema di controllo può integrare le tecnologie IT nella misura che ritiene più ottimale per l'organizzazione aziendale.
I benefici apportati dall'IT al sistema di controllo interno sono svariati. Innanzitutto, la tecnologia consente di rendere uniformi le regole di gestione definite dalla direzione attraverso l'elaborazione di grandi volumi di dati e operazioni. In secondo luogo, consente di rendere le informazioni tempestive, accurate e disponibili a tutto il personale aziendale e inoltre ne facilita l'analisi.
L'IT è efficace anche perché supporta la direzione sia nelle attività di monitoraggio delle performance e delle direttive aziendali che nelle attività di controllo in quanto riduce il rischio di evasione dei controlli e rafforza la possibilità di separazione delle funzioni.
L'uso di elementi manuali e di elementi automatizzati influenza l'attività del revisore in quanto deve tenerne conto nell'identificare e valutare i rischi di errori significativi e nel definire le procedure conseguenti.
I controlli svolti tramite tecnologie IT potrebbero essere più efficaci e attendibili rispetto a quelli manuali in quanto si eviterebbero errori legati ai limiti umani (come, ad esempio, gli errori di distrazione) e allo stesso tempo sarebbero più difficili da forzare e ignorare. Dovrebbero essere preferiti rispetto a quelli manuali nel caso in cui il volume delle operazioni da gestire sia elevato in quanto permette di prevenire o correggere tempestivamente degli errori prevedibili e in quanto permette di configurare dei controlli in modo adeguato ed efficiente. [139]

L'IT all'interno del sistema di controllo interno è utilizzato maggiormente nella componente sistema informativo e la comunicazione e nella componente attività di controllo in quanto la prima è strettamente correlata all'elaborazione dell'informativa finanziaria, invece, la seconda comprende tutti i controlli che la società determina e attua al fine di ridurre i rischi aziendali. L'ultima componente include anche i controlli generali IT e i controlli applicativi IT, i quali hanno l'obiettivo di ridurre e contrastare i rischi IT.
Nel comprendere però ogni componente del sistema di controllo, il revisore deve considerare anche l'aspetto IT e nei paragrafi seguenti sono analizzati gli aspetti rilevanti in ottica IT di ogni componente, i quali devono essere compresi e valutati.

[139]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 1-2, pag. 78.

3.3.1 Ambiente di controllo: comprensione e valutazione in ottica IT

L'ambiente di controllo deve essere visto come il comportamento e la consapevolezza dei responsabili della direzione e dell'attività di governance rispetto al sistema di controllo interno. Ha un ruolo fondamentale perché costituisce la base per l'interno sistema: se l'ambiente di controllo è ben strutturato è più probabile che anche le altre componenti operino in modo efficiente e siano ben strutturate.

È un controllo indiretto, ovvero non ha come obiettivo principale quello di identificare, correggere o prevenire errori significativi ma sostiene gli altri controlli messi in atto da altre componenti del sistema di controllo interno; pertanto, influisce indirettamente sulla probabilità che un errore sia identificato e corretto tempestivamente. [140]

Ciò che il revisore deve comprendere è rappresentato dal modo in cui la direzione aziendale crea e mantiene la propria cultura aziendale all'interno della società e il modo in cui si impegna nel rispettare valori etici e di integrità. Al centro dell'ambiente, perciò, ci sono i responsabili dell'attività di governance, i quali al fine di garantirne l'efficacia devono:

- essere indipendenti dalla direzione aziendale e devono essere capaci di valutare in modo obiettivo le loro azioni;
- conoscere adeguatamente l'attività svolta dalla società e avere le competenze necessarie per svolgere le mansioni assegnate;
- valutare la conformità del bilancio alla normativa nazionale.

L'ambiente di controllo è fondamentale perché definisce che atteggiamento ha l'organizzazione rispetto ai controlli, ovvero se trasmette la giusta consapevolezza all'intero personale in relazione all'importanza dei controlli. [141]

In relazione all'uso dell'IT, il revisore dovrà valutare la gestione e la struttura dell'IT. Il revisore, infatti, valuterà se la componente IT è gestita in modo adeguato in relazione alla natura e alla complessità dell'azienda, tenendo conto anche della complessità della piattaforma aziendale utilizzata e di quanto la società faccia affidamento sulle applicazioni IT per la predisposizione dell'informativa di bilancio.

[140]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. A96, pag. 32.
[141]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", app. 3, par. 5, pag. 69.

Valuterà anche com'è strutturato l'IT e come sono gestite le risorse IT. In tal senso, valuterà, ad esempio, l'appropriatezza dell'ambiente IT su cui la società ha investito e del *software* utilizzato dalla società, valutando inoltre se sono necessari dei miglioramenti. La società, infatti, può utilizzare un *software* commerciale oppure non commerciale, senza modifiche concesse oppure con modifiche limitate e il tipo di *software* utilizzato influisce sulle considerazioni che dovrà svolgere il revisore. In relazione alle risorse IT, il revisore esaminerà anche se il personale IT è competente e dal punto di vista numerico appropriato.

La comprensione avviene attraverso procedure di valutazione del rischio, precisamente attraverso indagini presso la direzione aziendale oppure presso fonti esterne all'azienda. Il revisore sarà interessato alla cultura aziendale diffusa in azienda, perciò, esaminerà come la direzione comunica ai dipendenti le regole di comportamento e i comportamenti considerati eticamente corretti ed esaminerà il codice di comportamento predisposto dalla direzione e i comportamenti adottati per farlo rispettare in azienda.[142]

La valutazione di questa componente è molto importante in quanto sostiene il revisore nella valutazione e nell'individuazione di eventuali carenze in altre componenti del controllo. Allo stesso tempo, aiuta il revisore a comprendere i rischi a cui è sottoposta l'impresa e di conseguenza ad individuare i rischi di errori significativi a livello di bilancio e a livello di asserzioni. [143]

3.3.2 Il processo di valutazione del rischio: comprensione e valutazione in ottica IT

In linea generale, con il processo di valutazione del rischio la direzione aziendale identifica e analizza i rischi che ostacolano il raggiungimento degli obiettivi aziendali con il fine ultimo di determinare una strategia per gestirli.

Nello specifico, in relazione all'informativa di bilancio, la direzione è interessata ad individuare i rischi correlati alla redazione del bilancio, il quale deve essere redatto in conformità al quadro normativo vigente. Dopo averli individuati infatti, è importante che la direzione ne stimi la rilevanza e ne valuti la probabilità di insorgenza per deliberare le

[142]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", paragrafo A101-102, pag. 33.

[143]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par A103, pag. 34.

azioni necessarie per affrontarli e controllarli. La società deve, infatti, stabilire dei piani d'azione specifici in relazione ai rischi, oppure, se ciò risulta troppo costoso, accetterà di sottoporsi al rischio.
Per rischio rilevante, si intende una circostanza o un evento che influenza in modo negativo la rilevazione e la contabilizzazione delle informazioni economico-finanziarie, la quale deve essere conforme alle asserzioni di bilancio.
Il revisore, perciò, deve comprendere tale processo al fine di valutarne l'appropriatezza, tenendo conto della natura e della complessità dell'azienda, sulla base del proprio giudizio professionale.

I fattori di rischio sono svariati ma in relazione all'ambiente IT, il revisore deve considerare quelli strettamente correlati alle informazioni aziendali e alla tecnologia, i quali possono essere legati, ad esempio, all'introduzione di nuove tecnologie nel sistema informativo o nel sistema di produzione. Di conseguenza anche l'aggiornamento del sistema informativo oppure l'acquisizione di un nuovo sistema sono dei fattori da considerare in quanto dei cambiamenti repentini e sostanziali potrebbero essere molto rischiosi.
In relazione all'utilizzo dell'IT invece, i rischi sono correlati:

1) all'elaborazione delle informazioni e al mantenimento dei dati integri;
2) a possibili malfunzionamenti dell'ambiente IT;
3) alle competenze non adeguate del personale aziendale nell'utilizzare i sistemi informatici;
4) a carenze legate alla struttura IT implementata nella società;
5) ai rischi di business nel caso in cui la strategia IT non sia stata definita e messa in atto in modo adeguato ed efficiente.[144]

[144]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 7-9, pag. 71.

3.3.3 Il processo di monitoraggio: comprensione e valutazione in ottica IT

Le attività adottate dall'impresa per il monitoraggio del SCI hanno l'obiettivo di esaminare l'adeguatezza del sistema di controllo per poter definire e mettere in pratica tempestivamente delle azioni correttive qualora fossero necessarie.

Queste attività possono essere: continuative, spesso legate alle attività ordinarie di un'impresa; periodiche oppure una combinazione delle precedenti. Sia la cadenza che la portata di queste attività dipendono da come una società valuta i rischi ai quali è sottoposta.

I controlli svolti per mezzo del processo di monitoraggio vengono effettuati sulle attività svolte dalla società, le quali possono essere automatizzate oppure manuali. Allo stesso modo, in base alla modalità con cui vengono predisposte, possono essere: automatizzate, manuali oppure una combinazione delle due.

Nello svolgere questo processo, la società deve considerare anche le informazioni che provengono da soggetti esterni le quali potrebbero portare alla luce degli errori che non erano stati considerati inizialmente. Tra questi soggetti ci sono i clienti, che tramite eventuali contestazioni potrebbero evidenziare problemi che prima non erano conosciuti; gli organi di vigilanza che valutano costantemente l'operatività del SCI; e infine anche i revisori esterni, che tramite le procedure di revisione comprendono il sistema nel suo complesso. [145]

Tale processo è volto anche a monitorare i controlli relativi all'elaborazione delle informazioni mediante l'uso dell'IT. In tal senso, il revisore dovrebbe comprendere:

1) i controlli messi in atto per monitorare gli ambienti IT complessi: valuta la configurazione e l'operatività dei controlli relativi all'elaborazione delle informazioni e valuta come la società li modifica in seguito a cambiamenti necessari;
2) i controlli che verificano le autorizzazioni sui controlli automatizzati, i quali hanno l'obiettivo di garantire la separazione delle funzioni;
3) i controlli che verificano come gli errori e le carenze nei controlli relativi all'automazione utilizzata per la produzione delle informazioni sono individuati e affrontati.

[145]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 71-72.

Il revisore deve perciò comprendere prima di tutto come sono state configurate e svolte le attività di monitoraggio, tenendo conto anche della frequenza dei controlli. In secondo luogo, deve comprendere come la società valuta i risultati ottenuti da tale attività, considerando anche come identifica, affronta e comunica eventuali carenze nei controlli.

Il revisore deve inoltre comprendere la funzione di revisione interna, se presente, al fine di comprendere l'attività svolta e le responsabilità ad essa assegnate. Infine, deve comprendere da dove derivano le informazioni utilizzate per l'attività di monitoraggio al fine di valutarne l'attendibilità e l'adeguatezza allo scopo.
La comprensione deve essere attuata al fine di valutare l'appropriatezza del processo. La valutazione di questa componente aiuta il revisore a comprendere anche l'efficacia delle altre componenti e perciò a comprendere l'intero sistema di controllo interno. Allo stresso tempo aiuta il revisore a individuare e a valutare i rischi di errori significativi a livello di bilancio e a livello di asserzioni. [146]

3.3.4 Il sistema informativo e la comunicazione: comprensione e valutazione

Nel sistema informativo rientrano tutte quelle attività strettamente correlate alla produzione delle informazioni aziendali che confluiranno nel bilancio d'esercizio.
Le attività di competenza di tale sistema sono le seguenti:

1) le attività di rilevazione, contabilizzazione ed elaborazione delle operazioni aziendali che saranno esposte nel bilancio d'esercizio e la rilevazione di eventi diversi dalle operazioni che sono rilevanti per l'informativa di bilancio (tra questi eventi vi sono, ad esempio, gli ammortamenti relativi alle immobilizzazioni);
2) la risoluzione tempestiva di errori legati all'elaborazione delle operazioni aziendali;
3) l'elaborazione e la documentazione di eventuali forzature sui sistemi ed eventuali evasioni dei controlli;

[146]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pagina 36-37.

4) le attività di incorporazione di informazioni che provengono dalla contabilità generale (ad esempio, nel caso di trasferimento di operazioni che provengono dalla contabilità sezionale[147]);
5) l'assicurazione che le informazioni siano state raccolte, contabilizzate ed elaborate in conformità con il quadro normativo sull'informativa finanziaria.

Le operazioni contabilizzate e formalizzate dai sistemi informativi derivano dalle attività derivanti dai processi di business di una società. Per processi si intendono innanzitutto quelli legati al core business della società, ovvero tutte le attività di acquisto, produzione, distruzione di un prodotto ed erogazione di un servizio. Si intendono anche tutti i processi volti ad assicurare l'adeguatezza delle operazioni aziendali alle leggi e ai regolamenti. Infine, si intendono anche tutte quelle attività di registrazione delle informazioni contabili e finanziarie.

Dai processi, perciò, derivano delle operazioni che sono registrate dal sistema informativo.

Per comunicazione invece si intende tutto quello che concerne il trasferimento di informazioni riguardanti il sistema di controllo interno da una persona all'altra all'interno di una società. Può avvenire in diverse forme: verbale, elettronica, tra soggetti dello stesso grado oppure attraverso comunicazioni da parte della direzione. Quest'ultima, infatti, può comunicare attraverso comunicazioni interne e dirette, ma anche attraverso comunicazioni indirette come, ad esempio, manuali di direttive e di responsabilità oppure manuali contabili e sull'informativa finanziaria. [148]

L'attività di comprensione può essere svolta attraverso indagini presso il personale competente in materia di rilevazione contabile e di predisposizione dell'informativa finanziaria oppure attraverso ispezioni delle direttive, dei manuali o dei documenti relativi al sistema informativo.

Inoltre, il revisore può osservare direttamente il personale aziendale nell'applicazione delle direttive e nello svolgimento delle procedure oppure potrebbe effettuare verifiche "*walk-through*", ovvero un test di dettaglio che permette di ripercorrere passo dopo

[147]La contabilità sezionale è quella contabilità relativa a singole operazioni, oppure relativa a specifici elementi patrimoniali oppure relativa a singole funzioni aziendali. Essa può essere più o meno integrata o collegata con la contabilità generale.

[148]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 72-73.

passo dal punto di vista contabile dall'inizio alla fine una specifica operazione o transazione scelta casualmente. [149]

Questa componente del sistema di controllo interno è quella maggiormente strettamente correlata alla componente IT e nel paragrafo seguente sarà analizzata nel dettaglio questa correlazione.

3.3.4.1 Comprensione del sistema informativo in ottica IT

Il sistema informativo, in quanto strettamente correlato alle informazioni aziendali, può prevedere l'uso di tecnologie informatiche per la rilevazione, contabilizzazione ed elaborazione delle informazioni legate alle operazioni aziendali. Anche l'archiviazione delle informazioni può avvenire in modo automatizzato tramite archivi digitali che integrano quelli cartacei. Le società, infatti, utilizzano apposite applicazioni IT che rafforzano il sistema informativo aziendale se implementate in modo efficiente.

In relazione al sistema informativo, il revisore deve comprendere l'ambiente IT in correlazione con le informazioni rilevanti per il sistema informativo e, per farlo, dovrà raccogliere informazioni legate alle applicazioni IT, alle infrastrutture IT di supporto e all'ambiente IT in generale.

L'ISA 315 ci fornisce molti esempi indicativi relativi ad aspetti che il revisore può considerare al fine di comprendere al meglio l'ambiente IT, tenendo conto anche del grado di complessità dell'ambiente IT che stiamo osservando. [150]

L'ambiente IT di una società può svilupparsi, infatti, intorno ad un *software* commerciale non complesso, intorno ad un *software* commerciale di medie dimensioni e di media complessità oppure intorno ad applicazioni IT di grandi dimensioni, in questo ultimo caso si fa riferimento anche a sistemi ERP.

Gli aspetti che il revisore deve comprendere in relazione al livello di automazione e all'uso dei dati sono elencati di seguito.

[149]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 40, par. A136.

[150]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 3-4, pag. 78.

1) Il livello di estensione e la complessità dei processi automatizzati per la predisposizione delle informazioni. L'estensione e la complessità dell'automatizzazione sarà maggiore per le applicazioni IT più grandi e complesse.
2) Il livello di affidamento che fa l'azienda sui report prodotti dal sistema per l'elaborazione delle informazioni aziendali. In questo caso i *software* non complessi o di media complessità utilizzano logiche più semplici di generazione dei report automatici invece le applicazioni IT più complesse utilizzano logiche complesse e talvolta anche sistemi di reportistica specifica (utilizzando anche i *Report Writer*).
3) Il modo in cui sono inseriti i dati all'interno del sistema informativo. I dati infatti possono essere inseriti manualmente dal personale aziendale, da clienti e da fornitori oppure attraverso il caricamento diretto di file. Nel caso in cui l'impresa utilizza *software* commerciali non complessi, i dati sono inseriti unicamente manualmente, nel caso di *software* commerciali di medie dimensioni i dati inseriti sono limitati e le interfacce[151] sono semplici; invece, nel caso siano utilizzate applicazioni IT complesse i dati inseriti sono molti e le interfacce sono complesse.
4) Il modo in cui l'uso dell'IT semplifica l'interazione tra applicazioni, *database* e le altre componenti dell'ambiente IT attraverso le interfacce del sistema informativo. L'interazione sarà maggiore e più complessa nei sistemi più complessi invece sarà minore, o nulla, nei *software* non complessi.
5) La quantità e la complessità dei dati elaborati dal *software*, considerando anche come i dati sono archiviati dal sistema. Nel caso di *software* non complessi o mediamente complessi, il volume di dati è esiguo, i dati sono semplici e sono disponibili a livello locale. Al contrario, nel caso invece di *software* molto complessi, la difficoltà di comprensione aumenta: il volume di dati è elevato, i dati sono complessi, sono utilizzati i *datawarehouse* e la società potrebbe servirsi di fornitori esterni di servizi IT per l'archiviazione dei dati.

Il revisore deve comprendere anche alcuni aspetti relativi alle applicazioni e all'infrastruttura IT, ovvero:

[151]In informatica, per interfaccia si intende un collegamento tra due sistemi che permette loro di interagire attraverso lo scambio di informazioni.

1) la tipologia di applicazioni IT utilizzate. Le applicazioni, infatti, possono essere commerciali con la possibilità di personalizzazione limitata o assente (questo è il caso di *software* commerciali non complessi). Le applicazioni IT di media complessità invece utilizzano applicazioni *legacy*, (ovvero applicazioni considerate obsolete in quanto sono al di sotto degli standard attuali), oppure applicazioni ERP di basso livello con possibilità di personalizzazione assente o limitata. Le applicazioni IT più complesse prevedono l'utilizzo di sistemi ERP molto complessi e personalizzabili, spesso prodotti internamente alla società;
2) il livello di complessità delle applicazioni IT e delle infrastrutture sottostanti.
   Se le società utilizzano *software* non complessi, l'infrastruttura IT sarà semplice e sarò composta da computer portatili oppure da infrastrutture semplici di *"Client – Server"*. Per *"Client – Server"* si intende un'architettura di rete in cui un computer, definito *client*, si connette attraverso la rete internet ad un *server* per fruire un servizio, comunicando anche con altri *client*. Per *server* si intende un gestore virtuale di informazioni, il quale le distribuisce a chi ne fa richiesta.
   Le società che invece utilizzano applicazioni IT complesse utilizzeranno sistemi di *"client-server"* di grandi dimensioni, *mainframe* complessi, applicazioni "*web-facing"* e *cloud* di tipo "*infrastructure as a service"*. Di seguito saranno analizzati questi concetti.
   Innanzitutto, il *mainframe* è un computer di grandi dimensioni, con alte prestazioni e con una grande quantità di memoria che elabora sistematicamente dati e informazioni. È una componente importante in quanto contiene e governa i *database* e le applicazioni aziendali. I *mainframe* sono progettati per garantire la sicurezza e l'affidabilità dei dati che governano.
   Per applicazioni *"web-facing"*, invece, si intendono applicazioni a cui si può accedere interamente o parzialmente tramite internet. Sono diventati fondamentali perché permettono di lavorare da remoto e di comunicare con clienti e fornitori in modo agevole. Un difetto di tali applicazioni è il fatto che espongono maggiormente le aziende a rischi legati alla cybersicurezza.
   Infine, per *cloud* di tipo "*infrastructure as a service"* si intende l'acquisto da parte dell'azienda di servizi *cloud*, i quali includono spazi di archiviazione, servizi di rete, server e calcolatori. Questo servizio permette di utilizzare da remoto delle risorse IT fondamentali come se fossero delle risorse su internet. In questo modo

diminuiranno i costi per le aziende: sia i costi di acquisto dell'infrastruttura IT che quelli di installazione e manutenzione, in quanto gestiti dal soggetto che offre il servizio;

3) la presenza di un *hosting* presso terzi o di un servizio di *outsourcing* dell'IT.
   Per *hosting* si intende un servizio offerto alle aziende che consente di pubblicare un sito internet o una pagina web su internet. *L'hosting* è pertanto un'organizzazione che fornisce i servizi e le tecnologie necessarie per pubblicare il sito o la pagina web, in quanto permette di "ospitare" (dall'inglese *to host)* in uno spazio internet tale pagina.
   Per *outsourcing* dell'IT, invece, si intende la strategia aziendale per la quale determinati processi IT vengono esternalizzati a fornitori di servizi o ad altri soggetti esterni all'azienda. Ciò avviene soprattutto nei casi in cui le aziende non hanno il tempo, il denaro e le competenze necessarie per coprire l'intero campo dell'IT e, pertanto, si affidano a soggetti esterni maggiormente competenti;
4) l'uso di tecnologie emergenti per la predisposizione dell'informativa finanziaria. Esempi di tecnologie emergenti sono quelli trattate nel paragrafo 2.1.1 ovvero, le *blockchain*, la robotica e l'Intelligenza Artificiale. Sono utilizzate soprattutto da società molto grandi che utilizzano applicazioni IT molto complesse perché apportano numerosi vantaggi in termini di efficienza operativa e migliore informativa finanziaria. Le tecnologie emergenti potrebbero apparire più sofisticate, e perciò più precise, ma il revisore deve comunque svolgere le procedure necessarie per comprenderle e valutarle. [152]

Gli aspetti che il revisore deve comprendere in relazione ai processi IT sono i seguenti:

1) i soggetti in azienda che si occupano dell'ambiente IT. Il revisore deve comprendere se il numero di soggetti e il loro grado di specializzazione è adeguato al fine di garantire la sicurezza dell'ambiente IT.
   Nelle aziende con *software* commerciali non complessi, il personale IT è di norma esiguo con poche competenze specifiche. Al contrario, nelle aziende con applicazioni IT molto complesse esiste solitamente un dipartimento IT con personale qualificato;

[152]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 81, par. 5.

2) la complessità dei processi al fine di gestire gli accessi. Nelle aziende con *software* non complessi o mediamente complessi, gli accessi sono gestiti solitamente da uno o più soggetti in qualità di amministratori. Nei casi di complessità maggiore invece, gli accessi sono gestiti attraverso processi complessi definiti e gestiti dal dipartimento IT;
3) il livello di sicurezza dell'ambiente IT, in termini di vulnerabilità ai rischi *cyber* soprattutto nei casi in cui l'azienda operi con interfacce esterne oppure attraverso il web;
4) i cambiamenti apportati ai *software* e alle applicazioni IT. Solitamente, le società che utilizzano *software* commerciali non complessi non sono a conoscenza del codice sorgente per poterli modificare invece le società che utilizzano *software* complessi apportano spesso cambiamenti nuovi e complessi al fine di migliorare il processo esistente;
5) i cambiamenti apportati all'ambiente IT e la loro portata. Si intendono le modifiche e gli aggiornamenti apportati alle applicazioni e all'infrastruttura IT. Anche in questo caso, al crescere della complessità dell'applicazione IT utilizzata aumenterà anche la portata delle modifiche e degli aggiornamenti;
6) le attività di conversione dei dati: il revisore valuta se avvengono con regolarità e in che modo vengono svolte. Nelle società con *software* commerciali non complessi solitamente gli aggiornamenti dei *software* sono rilasciati dai fornitori e non sono richieste conversioni di dati. Nelle società con *software* mediamente complessi, gli aggiornamenti sono solitamente minori e sono possibili conversioni di dati poco complesse. Infine, per le società che utilizzano *software* complessi si verificano spesso aggiornamenti significativi, nuove *release*[153] oppure cambi di piattaforme. [154]

[153] Per *release* (traducibile anche con il termine "versione") si intende l'uscita in commercio di una nuova versione di un *software* commerciale, di un programma o di un'applicazione.
[154] Principio di revisione internazionale (ISA Italia) 315: "Identificazione e valutazione dei rischi di errori significativi", pag. 84-85, tabella.

3.3.4.2 Scalabilità del sistema informativo in relazione al software utilizzato

Come è stato ampiamente descritto nel paragrafo precedente, i *software* e l'utilizzo dell'IT varia a seconda delle caratteristiche specifiche di ogni società e perciò l'attività del revisore nel comprendere i processi IT e dei controlli IT varierà in relazione alla complessità dell'ambiente IT.

Le imprese meno complesse e strutturate utilizzano *software* commerciali non complessi e non possiedono il codice sorgente per poter apportare modifiche al programma. Solitamente non hanno del personale IT qualificato ma hanno un soggetto, con il ruolo di amministratore, che installa i programmi al personale aziendale, installa gli aggiornamenti delle applicazioni IT forniti dal fornitore e garantisce l'accesso ai dipendenti.

Nella maggior parte dei casi, questo tipo di aziende utilizzano come unica applicazione IT un *software* commerciale di contabilità. In questo caso il revisore potrebbe considerare:

- se il *software* è consolidato nel mercato ed è affidabile;
- se l'azienda riesce a modificare il codice sorgente per effettuare modifiche o aggiornamenti a tale *software*;
- la natura e la portata delle modifiche apportate al *software*. Infatti, anche se la società non riesce a modificare il codice può comunque configurarlo. In tal senso, il revisore deve valutare come la società configura il *software* e che effetto ha la configurazione sulla completezza e sull'accuratezza delle informazioni aziendali elaborate dal sistema;
- il volume dei dati aziendali e l'accesso ad essi per la redazione del bilancio. Se il volume di dati è elevato, sarà necessario per l'impresa mettere in atto dei controlli IT al fine di mantenere l'integrità dei dati. I controlli dovrebbero essere definiti soprattutto al fine di verificare gli accessi ai dati e per gestire le modifiche degli stessi.

Al contrario, le aziende più grandi e struttura si serviranno di un ambiente IT complesso mediante l'utilizzo di applicazioni complesse, altamente personalizzate e integrate con altre applicazioni o processi. Proprio per queste caratteristiche è richiesto al revisore uno sforzo maggiore per comprenderlo. Un esempio di integrazione si verifica quando le applicazioni IT usate nello svolgimento delle attività operative dell'azienda si integrano

con le applicazioni IT che si occupano di elaborare le informazioni aziendali: entrambe, ma soprattutto, la loro integrazione sarà utile per la redazione del bilancio. La complessità di tali ambienti IT richiede la definizione di un dipartimento IT che si occupi di mantenere e sviluppare l'ambiente IT. La società potrebbe servirsi anche di fornitori esterni per gestire aspetti determinanti relativi alla componente IT, come ad esempio potrebbe utilizzare *hosting* presso terzi.
Se la complessità è elevata può essere necessario l'intervento di soggetti del *team* di revisione con competenze professionali specifiche in ambito IT al fine di comprendere al meglio i processi IT, l'ambiente IT e i rischi derivanti dall'utilizzo dell'IT. [155]

3.3.5 Le attività di controllo: identificazione e valutazione dei controlli IT

L'attività di controllo comprende tutti quei controlli, automatizzati o manuali, messi in atto sull'attività di predisposizione delle informazioni e tali controlli comprendono anche i controlli IT. Infatti, più le informazioni vengono prodotte tramite procedure automatizzate, più saranno necessari dei controlli generali IT per verificare il continuo funzionamento dei processi automatizzati.
Il revisore deve identificare e comprendere prima di tutto i controlli definiti dalla società per contrastare i rischi di errori significativi a livello di asserzioni. Tali controlli comprendono: i controlli messi in atto per contrastare i rischi di errori significativi identificati; i controlli sulle scritture contabili e sulle scritture non standard; i controlli identificati che permettono al revisore di definire la natura, la tempistica e l'estensione delle procedure di validità e infine i controlli che il revisore ritiene appropriati al fine di raggiungere il proprio obiettivo di revisione.
Il revisore deve comprendere anche i controlli posti in essere per fronteggiare i rischi connessi all'utilizzo dell'IT e i controlli generali IT posti in essere per fronteggiare i rischi IT generali.
Per ogni controllo identificato e compreso, il revisore deve valutare se è stato configurato in modo efficace al fine di fronteggiare il rischio per il quale è stato definito e successivamente valuta se il controllo è stato messo in atto. Se il revisore definirà il

[155]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. A171, pag. 48.

controllo inefficace non potrà fare affidamento su tale controllo e perciò dovrà svolgere ulteriori procedure. [156]

Il revisore, perciò, deve identificare e comprendere i controlli generali IT per le componenti dell'ambiente IT che ritiene sottoposte ad un rischio strettamente correlato all'uso della tecnologia.

I controlli generali IT hanno l'obiettivo di supportare il continuo ed efficace funzionamento dei controlli generali sulla predisposizione dell'informativa finanziaria. Le società devono mettere in atto più controlli generali IT in quanto solamente uno non basterà a fronteggiare il rischio IT. [157]

In questo paragrafo saranno analizzati i controlli generali IT tenendo conto degli esempi forniti dall'ISA 315 nell'Appendice 6, i quali guidano il revisore nell'individuarli, comprenderli e valutarli tenendo conto anche della complessità delle applicazioni IT utilizzate.

Possono essere suddivisi innanzitutto in base alla componente dell'IT che controllano: applicazione, *database*, sistema operativo e rete.

1) A livello di applicazioni IT, i controlli generali IT potrebbero essere connessi alla funzione di ogni applicazione e alle condizioni di accesso ad essa. A titolo esemplificativo, sono necessari maggiori controlli per le applicazioni molto integrate che adottano sistemi di sicurezza complessi rispetto che per le applicazioni IT legacy che utilizzano un numero ridotto di dati a cui si accede solo mediante transazioni.
2) A livello di *database* invece, i controlli generali IT dovrebbero contrastare principalmente i rischi relativi ad aggiornamenti senza autorizzazioni di *database* contenenti dati importanti per l'informativa di bilancio attraverso accessi diretti oppure attraverso l'uso di un programma o di uno script. [158]
3) A livello di sistema operativo, i controlli generali IT dovrebbero contrastare principalmente i rischi strettamente correlati agli accessi avvenuti attraverso la posizione di amministratore del sistema operativo. In questa situazione, potrebbe essersi verificata una forzatura che potrebbe aver agevolato l'elusione

[156]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 26, pag.10.
[157]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 42, par. A150.
[158]Per "script" si intende un particolare programma scritto in un linguaggio di programmazione.

di altri controlli. In questa situazione, è possibile che sia avvenuto il caricamento di virus nel sistema, l'esecuzione di programmi non autorizzati, l'immissione di soggetti non autorizzati nel sistema oppure l'eliminazione delle credenziali di soggetti autorizzati.

4) A livello di rete i controlli generali IT dovrebbero contrastare i rischi relativi all'accesso alla rete, all'accesso da remoto, all'autenticazione e alla segmentazione di rete[159]. Tali controlli sono utili soprattutto quando l'impresa ha rapporti con soggetti esterni oppure esternalizza servizi a terzi, i quali accedono da remoto e contribuiscono alla trasmissione di dati all'impresa. [160]

I controlli generali IT possono essere anche definiti ed organizzati per processo IT. I processi sono principalmente tre, ovvero: il processo di gestione dell'accesso, il processo di gestione delle modifiche a programmi oppure ad altre componenti dell'ambiente IT e infine il processo di gestione delle operazioni IT.

Il primo processo, ovvero quello che si occupa di gestire gli accessi, comprende tutte quelle azioni messe in atto per verificare gli accessi e per garantire che l'accesso sia concesso solo a chi è effettivamente autorizzato. Le azioni rilevanti che rientrano in questo processo sono diverse:

1) Autenticazione: tali controlli hanno l'obiettivo di assicurare che gli utenti che accedono all'ambiente IT utilizzano le proprie credenziali per accedere e non quelle di altri soggetti;
2) Autorizzazione: tali controlli hanno l'obiettivo di assicurare che gli utenti abbiano a disposizione solo le informazioni che gli consentono di svolgere la propria mansione al fine garantire la separazione delle funzioni;
3) *Provisioning*: tali controlli hanno l'obiettivo di gestire gli accessi, permettono ovvero di modificare l'accesso ad utenti esistenti oppure di autorizzare l'accesso a nuovi utenti;

[159]Per segmentazione si intende un metodo di sicurezza digitale che implica la suddivisione della rete principale in sottoreti, per ognuna delle quali vengono posti dei controlli di sicurezza unici e indipendenti. È un metodo utilizzato per aumentare il livello di sicurezza digitale.
[160]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 1, pag. 87.

4) *Deprovisioning*: tali controlli hanno l'obiettivo di rimuovere l'accesso degli utenti nei casi di cessazione del rapporto di lavoro oppure di trasferimento in un'altra sede lavorativa;
5) Accesso privilegiato: tali controlli hanno come oggetto l'accesso di soggetti che si trovano in una posizione privilegiata rispetto agli altri utenti, ovvero l'amministratore di sistema oppure altri utenti con privilegi elevati;
6) Riesame degli accessi: tali controlli sono attuati per valutare l'accesso degli utenti nel tempo;
7) Controlli di configurazione sulla sicurezza: ogni tecnologia ha una propria chiave di accesso per limitare gli accessi alle componenti IT;
8) Accesso fisico: tali controlli hanno come obiettivo la verifica degli accessi fisici al centro dati oppure all'*hardware*. Tali accessi potrebbero essere rischiosi in quanto potrebbero essere utilizzati per aggirare i controlli.[161]

I rischi relativi agli accessi sono connessi a due componenti: gli utenti e i dati.

Per quanto riguarda la prima componente, il rischio è connesso ai privilegi di accesso che hanno alcuni utenti. È possibile, infatti, che alcuni utenti abbiano dei privilegi di accesso superiori rispetto a quelli necessari per adempiere alle loro mansioni, generando così un'errata separazione delle funzioni.

I controlli generali IT che la società potrebbe mettere in atto dal punto di vista pratico sono molti. Innanzitutto, la direzione potrebbe approvare gli accessi per i nuovi utenti, le modifiche agli accessi già esistenti e le transazioni significative critiche relative all'informativa di bilancio.

In secondo luogo, l'accesso di un utente cessato oppure trasferito deve essere disattivato oppure modificato prontamente e gli accessi dovrebbero essere riesaminati e monitorati ciclicamente. In questo caso, le applicazioni IT non complesse di norma non applicano entrambe le verifiche ma un controllo sostituisce l'altro invece le applicazioni IT più complesse le attuano entrambe.

Una verifica ulteriore riguarda il monitoraggio della separazione delle funzioni, disabilitando eventuali accessi in conflitto se necessario. Nei *software* commerciali non complessi tale separazione non è possibile ma lo è invece per le applicazioni IT complesse.

[161]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 2, punto a), pag. 87.

Infine, un ulteriore controllo prevede l'autorizzazione, e l'eventuale limitazione, degli accessi privilegiati. Nei *software* commerciali non complessi tali controlli sono posti solo a livello delle applicazioni IT invece nelle applicazioni IT molto complesse tali controlli sono posti a tutti i livelli dell'infrastruttura IT.

In relazione ai dati aziendali invece, il rischio è connesso al fatto che è possibile che siano apportate modifiche inappropriate e non autorizzate ai dati rilevanti per l'informativa finanziaria.

Il controllo che può essere definito è quello di concedere l'accesso ai dati contenuti nei database solo a determinati soggetti sulla base della mansione che devono svolgere e delle loro responsabilità. È importante evidenziare che solo le applicazioni IT complesse e mediamente complesse permettono tale controllo.

Un ulteriore rischio è legato alla configurazione del sistema IT: è possibile che i sistemi non siano configurati e aggiornati in modo adeguato al fine di gestire correttamente gli accessi degli utenti.

Un controllo può essere posto attraverso l'utilizzo di ID utente e *password* univoci posseduti da ogni utente per verificare l'autorizzazione degli utenti che vogliono accedere al sistema. Le *password* devono rispettare parametri specifici definiti dalla società oppure dal settore di appartenenza: devono avere, ad esempio, una lunghezza minima, lettere minuscole e maiuscole, numeri, caratteri speciali, una data di scadenza e una possibilità di blocco dell'account in determinate situazioni.

Un ulteriore controllo può riguardare la configurazione appropriata del sistema di sicurezza nell'azienda. Esiste una configurazione tecnica e di sicurezza soprattutto nelle applicazioni IT di media e di grande complessità. [162]

Il processo di gestione delle modifiche a programmi oppure ad altre componenti dell'ambiente IT comprende azioni come:

1) Modifiche nel processo di gestione: tali controlli sono relativi alla definizione, programmazione, verifica e migrazione delle modifiche considerando l'utente finale del processo;

[162]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 89-90.

2) Separazione delle funzioni sulla migrazione delle modifiche: tali controlli permettono di separare gli accessi per effettuare e migrare le modifiche verso l'utente finale;
3) Sviluppo, acquisizione o implementazione di sistemi: tali controlli sono attuati nel momento di sviluppo e di configurazione di un nuovo sistema;
4) Conversione di dati: tali controlli sono relativi alla conversione di dati che si verifica durante le attività di sviluppo, implementazione e aggiornamento di un sistema IT. [163]

I rischi derivanti da questo processo di modifica dell'ambiente IT sono svariati.

Se le modifiche riguardano le applicazioni, il rischio riguarda il fatto che le modifiche apportate non siano adeguate ai sistemi e ai programmi contenenti controlli automatizzati oppure logiche di *report*. Le società potrebbero definire due tipi di controlli generali IT: potrebbero verificare e approvare le modifiche prima che esse siano trasferite nell'ambiente di produzione e potrebbero limitare l'accesso per attuare le modifiche nell'ambiente applicativo di produzione dall'ambiente di sviluppo. Ciò può essere messo in pratica nelle applicazioni IT ma non nei *software* commerciali.

Se le modifiche riguardano invece i *database*, il rischio è che le modifiche non siano appropriate considerando l'organizzazione del *database* e la relazione tra i dati inseriti. Anche in questo caso, un esempio di controllo generale IT può essere costituito da una serie di verifiche e di approvazioni delle modifiche prima che esse siano trasferite nell'ambiente di produzione, al fine di valutarne l'appropriatezza. Anche in questo caso può essere messo in pratica nelle applicazioni IT ma non nei *software* commerciali.

Le modifiche relative al *software* di sistema possono essere rischiose se non sono appropriate. Per *software* di sistema si intende, ad esempio, la rete, il sistema operativo, il *software* per gli accessi e per il loro controllo e infine il *software* per la gestione delle modifiche. Come per il *database* e per le applicazioni, il controllo IT deve consistere nella verifica dell'appropriatezza e dell'approvazione della modifica prima che essa sia trasferita nell'ambiente di produzione, i quali però possono essere applicati solo nelle applicazioni IT.

Per quanto riguarda la conversione dei dati aziendali, i rischi possono essere maggiori nel caso in cui si convertano dati da sistemi *legacy* oppure da versioni di *software* non

[163]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 2, punto b), pag. 87-88,

aggiornate in quanto aumenta la probabilità di errori. I dati, infatti, potrebbero essere incompleti, inaccurati, obsoleti oppure ripetuti. Per assicurare una corretta conversione, un controllo generale IT potrebbe consistere nel far approvare alla direzione aziendale i risultati della conversione e nel monitorare che la conversione venga attuata in conformità alle direttive e alle procedute definite in precedenza. Ad esempio, la direzione potrebbe verificare il pareggio dei saldi di bilancio e delle riconciliazioni prima e dopo la conversione. Nei *software* commerciali non complessi questi controlli sono generalmente manuali. [164]

Il processo di gestione delle operazioni IT comprende azioni come:

1) la programmazione dei job: tali controlli hanno l'obiettivo di verificare gli accessi nel caso di avvio o programmazione di un nuovo programma o job relativo all'informativa di bilancio;
2) il monitoraggio dei job: tali controlli hanno l'obiettivo di monitorare i programmi e i job relativi all'informativa di bilancio;
3) il *backup* e il ripristino: tali controlli hanno l'obiettivo di assicurare che i *backup* dei dati siano attuati in modo adeguato e che siano svolti regolarmente al fine di rendere i dati disponibili e accessibili nei casi di *blackout* oppure di incidenti informatici;
4) l'individuazione di intrusioni: tali controlli hanno l'obiettivo di monitorare la sicurezza dell'ambiente IT.[165]

I rischi legati ai processi delle operazioni IT possono essere innanzitutto strettamente correlati alla rete nei casi in cui essa non prevenga adeguatamente gli accessi non autorizzati. Un controllo generale IT potrebbe prevedere l'utilizzo di ID e password per gli utenti, come visto in precedenza.

Un altro controllo IT prevede la progettazione della rete al fine di segmentare le applicazioni *webfacing* dalla rete interna. Nel caso di *software* non complessi e commerciali non avvengono segmentazioni di rete invece nel caso di applicazioni IT complesse e mediamente complesse bisogna valutare caso per caso se tale controllo può essere applicabile.

---

[164]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 90-91, pag. 87.

[165]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. 2, punto c), pag. 88.

Un ulteriore controllo prevede l'esame periodico della vulnerabilità della rete perimetrale da parte dei responsabili della gestione della rete. Essi dovrebbero anche svolgere indagini periodiche in merito alle minacce di intrusione ai sistemi.
I controlli di rete dovrebbero anche essere predisposti per verificare gli accessi alla Virtual Private Network (VPN),[166] i quali devono avvenire solo da parte di utenti autorizzati. Anche in questi casi, nel caso di *software* non complessi e commerciali non sarà possibile effettuare tale controllo invece nel caso di applicazioni IT complesse e mediamente complesse si valuterà caso per caso.
I rischi legati invece al *backup* e al ripristino dei dati sono connessi ad eventuali perdite di dati finanziari e all'impossibilità di recuperarli. Un controllo generale IT potrebbe prevedere l'effettuazione periodica di un *backup* dei dati finanziari. Di norma nelle società che utilizzano *software* commerciali non complessi, i *backup* vengono effettuati manualmente dai responsabili dei dati finanziari invece nei casi di maggior complessità vengono svolti in modo automatizzato.
Infine, i rischi possono essere correlati anche alla produzione dei *job* in quanto essi potrebbero elaborare i dati in modo inaccurato, incompleto e non autorizzato. I controlli in questo caso potrebbero prevedere la possibilità di aggiornare i *job* e i programmi solo per mezzo di utenti autorizzati. Per un controllo ulteriore, i *job* e i programmi devono essere monitorati per correggere eventuali errori riscontrati. Tali controlli sono previsti solo per applicazioni IT altamente e mediamente complesse. [167]

3.3.5.1 Importanza della comprensione dei controlli generali IT

Il revisore deve identificare le applicazioni IT, le componenti dell'ambiente IT e i controlli generali IT al fine di identificare i rischi derivanti dall'uso dell'IT.
L'attività di comprensione dei rischi e dei relativi controlli aiuta il revisore a prendere delle decisioni conseguenti. Il revisore, dopo aver individuato i controlli, dovrà decidere se fare affidamento su tali controlli. Per poterlo fare però dovrà determinare se tali controlli sono stati progettati e messi in atto correttamente attraverso dei test.

[166]La VPN, ossia Virtual Private Network, è una tecnica che protegge la connessione ad Internet. Utilizzandola si crea un canale protetto in cui si traferiscono i dati nascondendo l'identità di chi ne fa uso, nascondendo l'indirizzo IP e permettendo di poter utilizzare le reti WiFi pubbliche in totale sicurezza,
[167]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 92-93.

Il revisore può decidere anche di non testare i controlli e perciò di non farci affidamento, dovendo di conseguenza svolgere ulteriori procedure di revisione. Ad esempio, se i controlli generali IT non sono stati delineati in modo efficace oppure non sono stati attuati adeguatamente al fine di fronteggiare i rischi IT, il revisore potrebbe decidere di non fare affidamento su tali controlli e svolgerà delle procedure di revisioni conseguenti. L'attività di comprensione dei controlli IT ha molti effetti sulla revisione:

1) aiuta il revisore nel valutare il rischio di controllo a livello di asserzioni.
   Ad esempio, i controlli relativi all'elaborazione delle informazioni possono dipendere dai controlli sulle applicazioni IT utilizzate per predisporre l'informativa, pertanto, l'efficacia operativa dei controlli IT influenzerà il rischio di controllo: il rischio sale se il revisore ritiene che i controlli generali IT sono inefficaci oppure se il revisore sceglie di non verificarli;
2) condiziona la definizione della strategia che il revisore utilizza per verificare la relazione tra informazioni aziendali e applicazioni IT. Se il revisore, infatti, utilizza le informazioni aziendali prodotte dalla società attraverso le applicazioni IT come elementi probativi, dovrà verificare l'efficacia operativa dei controlli su tali applicazioni, i quali potrebbero assicurare un loro corretto funzionamento;
3) aiuta il revisore a valutare il rischio intrinseco a livello di asserzioni.
   Infatti, come abbiamo visto nel primo capitolo, alcuni fattori di rischio intrinseco sono legati all'IT: cambiamenti nell'ambiente IT e l'istallazione di nuovi sistemi IT sono fattori che influenzano la percezione del rischio intrinseco da parte del revisore. In presenza di queste situazioni, perciò, aumenterà il rischio intrinseco a livello di asserzioni;
4) influenza il revisore nel definire le procedure di revisione conseguenti.
   Nel caso in cui l'elaborazione delle informazioni dipenda dall'IT, anche i controlli sulle informazioni dipenderanno dai controlli IT. In questo caso il revisore può valutare l'efficacia operativa dei controlli attraverso test sui controlli. Nel caso in cui il revisore decida di non valutarle l'efficacia oppure nel caso in cui i controlli non siano efficaci, dovrà definire delle procedure di validità per fronteggiare i rischi identificati. Se però le procedure di validità svolte non fornissero elementi

probativi sufficienti e appropriati, il revisore dovrò tenerne conto nella definizione del giudizio di bilancio.[168]

3.4 Identificazione delle applicazioni IT e altri aspetti dell'ambiente IT soggette a rischi derivanti dall'utilizzo dell'IT e scalabilità

Comprendere l'ambiente IT di un'impresa, aiuta il revisore a identificare le applicazioni IT che l'impresa utilizza per produrre accuratamente le informazioni aziendali e per garantire l'integrità delle stesse.

Come abbiamo già visto nei paragrafi precedenti, le applicazioni IT possono essere soggette a rischi derivanti dall'uso dell'IT e perciò, nell'identificarle, il revisore deve comprendere i controlli che la società ha definito e messo in atto per fronteggiare tali rischi. I controlli in questo caso sono spesso automatizzati, come ad esempio controlli su calcoli automatici, controlli sui dati input, controlli sull'elaborazione dei dati e sulle informazioni output prodotte (ad esempio, un controllo triplice può avere per oggetto l'ordine di acquisto, il documento di trasporto e la fattura di vendita al fine di valutare se combaciano).

Se il revisore identifica un'applicazione IT che la società usa e identifica un controllo automatizzato su cui tale applicazione fa affidamento, è probabile che il revisore consideri quell'applicazione come un'applicazione soggetta a rischio IT.

Nell'identificare queste applicazioni, sarà utile per il revisore comprendere se la società ha accesso al codice sorgente dell'applicazione, ovvero un codice che permette alla direzione di modificare le applicazioni e i controlli. Il revisore dovrà porre, infatti, anche la giusta attenzione in merito alla misura in cui le società modificano i programmi e le applicazioni IT, alla misura in cui tali modifiche sono formalizzate e al rischio di accessi non autorizzati. [169]

I *report* prodotti dalle applicazioni IT potrebbero essere usati dal revisore come elementi probativi (come, ad esempio, un report relativo alle scadenze dei crediti oppure relativo al valore delle rimanenze) ma, per poter essere utilizzati, il revisore

[168]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", par. A166, pag. 47.

[169]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", Appendice 5, pag. 82-83.

dovrà testare la loro completezza e accuratezza. Può farlo attraverso procedure di validità sulle informazioni input e sugli output prodotti dal report oppure verificando l'efficacia operativa dei controlli messi in atto per la predisposizione di quel determinato report. Allo stesso tempo il revisore potrebbe testare l'efficacia operativa dei controlli generali IT che affrontano i rischi relativi alle modifiche inadatte e non autorizzate alle applicazioni che generano i *report* e ai dati input dei *report*.
È possibile che le applicazioni IT abbiano al loro interno la funzione di *report-writing*; invece, alcune applicazioni IT si servono di applicazioni esterne che producono i *report*.
È importante per il revisore stabilire quali sono le fonti dei report generati dal sistema al fine di definire le applicazioni soggette a rischio IT. Per fonte si intendono l'applicazione alla base che esegue il report e i dati utilizzati da tale applicazione. I dati infatti possono provenire da *database* oppure da *datawarehouse*. Nel primo caso, si può accedere ai dati mediante applicazioni IT oppure tramite l'accesso dell'amministratore del *database*, nel secondo caso invece si sta facendo riferimento ad una vera e propria applicazione IT soggetta a rischio derivante dall'uso dell'IT. [170]

Gli elementi probativi utilizzati dal revisore possono essere anche gli output prodotti dal sistema IT, i quali sono poi utilizzati dall'utente finale (ovvero il dipende dell'azienda) mediante uno strumento informatico diverso dall'applicazione IT. Per strumento informatico si intende ad esempio un foglio elettronico Excel oppure un database non complesso.
Predisporre e attuare dei controlli sugli strumenti informatici utilizzati dagli utenti finali non è facile in quanto non siamo nell'area dei controlli generali IT. In questo caso il revisore potrebbe individuare e comprendere la combinazione di controlli relativi all'elaborazione delle informazioni messi in atto dalla società, prendendo in considerazione il fine e la complessità dello strumento informativo utilizzato. I controlli combinati possono riguardare, ad esempio, i dati di partenza su cui si basa l'elaborazione delle informazioni, i quali comprendono anche i controlli automatizzati relativi al *database* oppure *datawarehouse* da cui sono estratti.
Altri controlli invece possono verificare che il processo di estrazione dei dati avvenga correttamente ovvero, verificando che i dati dei report siano riconciliati con i dati di

[170]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", Appendice 5, par. 10-11-12, pag. 83.

derivazione comparando i dati del report con la fonte del dato e verificando l'applicazione corretta delle formule.
Infine, un altro tipo di controllo potrebbe prevedere l'uso di *software* per valutare la correttezza e l'integrità dei fogli elettronici, verificando sistematicamente le formule utilizzate.

Oltre alle applicazioni IT, ci sono altri aspetti dell'ambiente IT che possono essere soggetti a rischi derivanti dall'utilizzo dell'IT. Tra questi aspetti ci sono la rete, i *database*, il sistema operativo e le integrazioni tra applicazioni IT.
È bene ricordare che nel caso in cui non venissero identificate dal revisore applicazioni con rischi derivanti dall'uso dell'IT, non sarebbero identificati neanche altri aspetti dell'ambiente IT. Nel caso contrario invece, essi sarebbero identificati perché essi supportano e interagiscono con le applicazioni.
Di noma, nei casi in cui sono state individuate applicazioni IT soggette a rischi sono, di conseguenza, individuati i *database* nei quali sono archiviati i dati utilizzati da tali applicazioni. Per lo stesso principio, le applicazioni IT operano attraverso i sistemi operativi, i quali saranno di conseguenza soggetti a rischi.
La rete invece è individuata e valutata dal revisore nel caso in cui sia un punto di accesso centrale per l'applicazione IT e per il *database* soggetto a rischio IT, nel caso in cui l'applicazione sia utilizzata anche da fornitori oppure da soggetti esterni all'azienda attraverso internet oppure nel caso in cui l'impresa utilizzi applicazioni IT *webfacing*.

L'attività di comprensione dei processi IT, delle applicazioni IT e dei controlli generali IT che il revisore deve svolgere non è un'attività standard ma varia a seconda della complessità e della struttura dell'ambiente IT della società di riferimento e soprattutto sulla base dei controlli che il revisore ha identificato.
Le applicazioni IT utilizzate dalla società possono essere soggette a rischi IT oppure no e ciò dipende da svariati fattori. L'impresa, infatti, ha come obiettivo quello di mantenere efficienti i processi di archiviazione e di elaborazione delle informazioni aziendali all'interno del sistema informativo aziendale; ciò però è influenzato dalla complessità e dalla quantità di operazioni e informazioni aziendali. Infatti, al crescere della complessità e della quantità di operazioni, diminuirà la possibilità che l'impresa mantenga integre le informazioni solo attraverso i controlli sull'elaborazione delle

informazioni, come ad esempio i controlli sugli input oppure sugli output. In queste situazioni, sarà difficile per il revisore acquisire elementi probativi sufficienti e appropriati sulla completezza e sull'accuratezza delle informazioni solo attraverso procedure di validità.
Nel caso in cui invece la quantità e la complessità delle operazioni aziendali sia minore, i soli controlli sull'elaborazione delle informazioni saranno sufficienti al fine di verificarne l'accuratezza e la completezza. È possibile in questo caso, ad esempio, riconciliare gli ordini di vendita elaborati con i documenti cartacei; ciò diventerebbe impossibile nel caso in cui l'azienda gestisce un volume elevato di operazioni.

Se l'impresa mette in atto controlli generali IT con l'obiettivo di garantire l'integrità delle informazioni usate dalle applicazioni IT, il revisore converrà che tali applicazioni sono soggette a rischi derivanti dall'uso dell'IT. Le applicazioni possono essere suddivise in due categorie:

1) applicazioni che non sono soggette a rischi derivante dall'IT, ovvero se si presentano le seguenti caratteristiche: è un'applicazione autonoma, non è complessa, il volume di dati sottostante non è significativo e ogni operazione è sostenuta dal proprio documento cartaceo originale. Non è soggetta a rischi innanzitutto perché, dato il volume esiguo di dati, la società non ha definito dei controlli generali IT.

   Se l'applicazione fornisce dei report che la direzione usa come controllo, prima di farci affidamento, il revisore dovrà riconciliare i dati del report con la documentazione cartacea;
2) applicazioni soggette a rischi derivanti dall'uso IT, ovvero se si presentano le seguenti caratteristiche: è interfacciata e interconnessa, il volume di dati sottostante è significativo ed è complessa, in quanto utilizza processi automatizzati e calcoli complessi connessi per permettere l'automazione. Il rischio è presente in quanto la direzione fa affidamento su un'applicazione che elabora e archivia i dati in quanto il loro volume è troppo elevato per poterlo fare manualmente. Inoltre, la direzione fa affidamento sui controlli automatizzati svolti dall'applicazione, i quali sono identificati dal revisore[171].

[171]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", Appendice 5, par. 14-17, pagina 84.

3.5 Risk assesment e individuazione dei controlli

Grazie all'attività di comprensione dell'ambiente IT e dei controlli IT, il revisore può identificare e valutare i rischi aziendali derivanti dall'utilizzo dell'IT in conformità all'ISA Italia 315 mediante procedure di valutazione del rischio. Il revisore dovrà stimare la significatività dei rischi e la loro probabilità di avvenimento al fine di determinare le azioni da intraprendere per affrontare tali rischi.

Nel valutare il rischio IT, il revisore deve considerare:

- gli esiti prodotti da precedenti incarichi di revisione;
- il processo di valutazione del rischio globale dell'impresa;
- la probabilità che un determinato rischio accada;
- l'effetto prodotto da un determinato rischio in termini monetari nell'eventualità che accada.

L'obiettivo di tale valutazione è quello di ridurre il rischio di errori significativi ad un livello accettabilmente basso, il quale, come abbiamo visto nei capitoli precedenti, è composto dal rischio intrinseco e dal rischio di controllo.

Dopo aver identificato il rischio intrinseco, infatti, il revisore dovrà identificare i controlli posti in essere dalla società al fine di individuare il rischio di controllo.

Come accennato in precedenza, le imprese devono progettare e mettere in atto dei controlli generali IT per individuare, prevenire e correggere eventuali errori che potrebbero verificarsi dovuti all'utilizzo dell'IT. Essi, infatti, hanno l'obiettivo di supportare il corretto funzionamento dell'ambiente IT e, allo stesso tempo, monitorano il funzionamento dei controlli sull'elaborazione delle informazioni, ovvero quei controlli relativi alle applicazioni IT utilizzate nei sistemi informativi aziendali messi in atto per fronteggiare i rischi legati all'integrità delle informazioni. [172]

Il revisore, dopo aver individuato i rischi di errori significativi, dovrà identificare quali controlli sono stati definiti e attuati dalla società e, se deciderà di fare affidamento su tali controlli, dovrà testarli al fine di valutarne l'efficacia.

L'obiettivo del revisore è infatti quello di determinare se i controlli IT sono stati disegnati in modo adeguato, se sono efficaci e se la separazione dei compiti e delle responsabilità avviene in modo efficace.

[172]Principio di revisione internazionale (ISA 315): "Identificazione e valutazione dei rischi di errori significativi", pag. 5, punto d e punto e.

I controlli sono normalmente suddivisi dai revisori esterni in due categorie:

1) ITGC (*IT General Controls*), ovvero i controlli manuali messi in atto dalla società per valutare le componenti dell'ambiente IT a livello generale. Sono progettati al fine di garantire alla società di poter fare affidamento sulle informazioni finanziarie prodotte dal sistema informativo aziendale. Tali controlli sono stati definiti e ampiamente descritti nel paragrafo 3.3.5 e possono essere raggruppati in tre categorie:
   a) controlli relativi all'accesso a dati, *software*, programmi e all'infrastruttura IT: il loro obiettivo è quello di garantire che accedano alle componenti IT solo coloro che sono autorizzati a farlo;
   b) controlli relativi alle modifiche e allo sviluppo di programmi: il loro obiettivo è quello di garantire che i programmi siano sviluppati e implementati correttamente e che le modifiche ai programmi siano autorizzate, testate, documentate e approvate;
   c) controlli relativi alle operazioni IT: il loro obiettivo è quello di garantire che le operazioni siano autorizzate e che qualsiasi deviazione dai comportamenti correttamente riconosciuti sia identificata, investigata e risolta.

   Sono dei controlli fondamentali in quanto permettono di poter fare affidamento sui dati aziendali, sui report prodotti, sui controlli automatizzati e sui processi;
2) ITAC (*IT Application Controls*), ovvero i controlli applicativi che monitorano una particolare applicazione o programma che supporta un processo specifico. Tali controlli sono automatici e verificati attraverso procedure di revisione definite CAAT's (*Computer Assisted Audit Techniques*) che prevedono l'utilizzo di tecniche di revisione sofisticate e automatizzate.[173]

   Tali controlli sono incorporati ai *software* e alle applicazioni e hanno l'obiettivo di prevenire eventuali processi non autorizzati oppure consentono l'elaborazione di processi previa autorizzazione.

   I controlli applicativi si combinano ai controlli generali al fine di assicurare la completezza, l'accuratezza, l'autorizzazione e la validità dei processi elaborati. Comprendono ad esempio:

[173]Nel paragrafo 3.7 della presente trattazione sono analizzate nello specifico le procedure CAAT's.

a) Attività di controllo dei dati, ovvero controlli che rilevano errori di immissioni di dati attraverso riconciliazioni tra i dati inseriti (sia manualmente che in modo automatizzato) con un totale di controllo.
b) Controlli attraverso database predefiniti, ovvero il controllo permette che gli utenti abbiano accesso solo a database che contengono solo i dati che gli sono stati autorizzati di utilizzare;
c) Controlli di autorizzazione, ovvero controlli che permettono la registrazione di determinate operazioni significative rilevanti per l'informativa di bilancio solo previa autorizzazione (questo tipo di controllo può riguardare ad esempio operazioni con un importo superiore ad un determinata soglia). [174]

Le due categorie di controllo sono strettamente correlate in quanto la definizione e l'attuazione dei controlli generali IT ha un impatto sull'efficacia dei controlli applicativi: i controlli generali forniscono alle applicazioni le risorse necessarie per poter operare e assicurano che le modifiche e le autorizzazioni di accesso avvengano in modo corretto.
Allo stesso tempo, i controlli applicativi si occupano dei singoli dati e delle singole transazioni al fine di assicurare che i dati siano immessi, elaborati ed emessi correttamente dal sistema.
Questi due livelli di controllo, se messi insieme, dovrebbero ridurre il rischio che il bilancio contenga errori significativi dovuti al rischio di controllo informatico.

3.6 Test sui controlli

Dopo aver individuato i controlli IT il revisore dovrà valutare innanzitutto la corretta progettazione del controllo e in secondo luogo l'efficacia del controllo.

Al fine di valutare l'efficacia relativa alla progettazione dei controlli (tali test sono tecnicamente definiti "*Test of Design Effectiveness*"), il revisore dovrà raccogliere elementi probativi al fine di valutare se i controlli sono costruiti in modo adeguato al fine di perseguire gli obiettivi di controllo. Il revisore dovrà comprendere per ogni controllo, infatti:

[174] AA. VV., *Taking Control, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 200, Documento in Pubblica Consultazione*, Deloitte, 2004, pag. 21.

1) chi è il titolare del controllo, ovvero chi è il soggetto responsabile del controllo;
2) come opera il processo, ovvero dovrà comprendere attraverso una spiegazione dettagliata come il processo di controllo è stato definito e attuato;
3) se il controllo è stato progettato e costruito correttamente e se il controllo permetterà di raggiungere l'obiettivo per il quale è stato progettato;
4) se sussistono eventuali carenze e quali sono;
5) come la società corregge eventuali carenze riscontrate.

Il metodo di valutazione utilizzato dal revisore dipenderà da diversi aspetti come ad esempio: la tipologia di controllo, le competenze dei soggetti responsabili, la frequenza del controllo, l'uso di fornitori esterni per il servizio di controllo e il quadro normativo di riferimento.

In secondo luogo, il revisore dovrà testare l'efficacia operativa dei controlli (tecnicamente definito *"Test of Effectiveness*"). Tale attività, come abbiamo visto nel paragrafo 2.6, è resa obbligatoria dalla sezione 404 della legge SOX, in quanto il revisore deve attestare quanto dichiarato dal management e per poterlo fare dovrà testare l'efficacia dei controlli.

I controlli da testare sono gli stessi valutati nella fase precedente e le tecniche che il revisore utilizza sono diverse, le quali sono utilizzate spesso in combinazione tra loro:

1) inchieste, ovvero interviste dettagliate per ottenere prove sull'efficacia dei controlli. Possono essere interviste dirette, ovvero svolte al personale aziendale che esegue direttamente il controllo sottoposto al test, oppure interviste indirette, ovvero svolte a soggetti che non svolgono direttamente il controllo ma ne sono a conoscenza e possono giudicane l'efficacia;
2) osservazione di un determinato controllo: questa tecnica fornisce prove sostanziali relative all'efficacia di un controllo. Se il revisore vuole testare, ad esempio, i controlli su un inventario può osservare direttamente come i dipendenti lo eseguono e come mettono in pratica i controlli. Questa prova non è sufficiente e dovrà essere supportata da ulteriori prove perché se i dipendenti sanno di essere osservati svolgeranno le proprie attività più accuratamente;
3) esame della documentazione, nel caso in cui un controllo sia documentato e il revisore possa ottenere tale documentazione, sia in formato elettronico che

scritto manualmente. Il grado di affidabilità a tale documentazione dipenderà dalla natura del controllo;

4) ri-esecuzione del controllo: ovvero la ripetizione di un controllo. Questo test è meno efficace per i controlli manuali: se il controllo supera positivamente il test ciò non ci fornisce comunque la sicurezza assoluta che in passato il controllo sia stato eseguito in modo corretto. È più efficace per i controlli automatizzati in quanto i test sono elaborati sistematicamente dai computer.

   Ad esempio, è possibile che un'applicazione abbia un controllo che rigetta eventuali transazioni errate: per verificare tale controllo il revisore può inserire transazioni errate per verificarne l'effettivo funzionamento del test.[175]

Oltre a tali procedure, il revisore può utilizzare tecniche computerizzate e più sofisticate definite *CAATs*, ovvero *Computer Assisted Audit Techniques*.

Il revisore deve documentare questi test, descrivendo: il test svolto, il risultato ottenuto, le conclusioni sull'efficacia di ogni controllo testato e le eventuali carenze di controllo riscontrate.

Se il revisore evidenzia eventuali carenze sia nell'attività di progettazione del controllo e sia nell'efficacie del controllo, dovrà definire se è presente:

1) Carenza nei controlli, ovvero nei casi in cui:
   a) il controllo sia stato progettato e attuato ma non consente di prevenire eventuali rischi di errori significativi;
   b) non è stato configurato un controllo necessario per prevenire un eventuale rischio di errori significativi;
2) Carenza significativa nei controlli, ovvero quando una carenza nei controlli è significativa da dover essere riportata alla direzione aziendale [176]

Al fine di valutare la carenza, il revisore deve considerare innanzitutto la probabilità che una carenza di controllo comporti un errore per l'informativa di bilancio e in secondo luogo l'entità dell'errore potenziale derivante da tale carenza.

Se il revisore definisce i controlli carenti, alla luce dei rischi identificati dovranno essere svolte ulteriori procedure per fronteggiare i rischi di errori significativi per determinare:

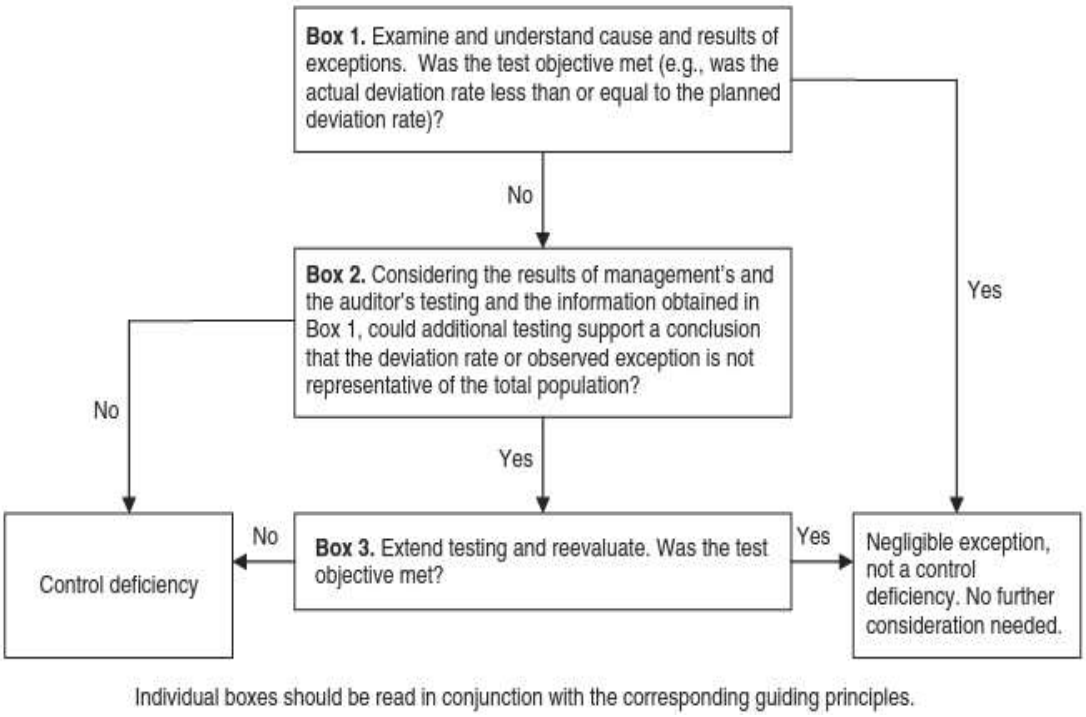
---

[175]AA. VV., *Taking Control, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 200, Documento in Pubblica Consultazione*, Deloitte, 2004, pag. 20-26

[176]Principio di revisione internazionale (ISA Italia) 265: "Comunicazione delle carenze nel controllo interno ai responsabili delle attività di governance ed alla direzione", par. 6, pag, 2-3.

1) se si sono verificati i rischi derivanti dall'uso dell'IT precedentemente identificati. Ad esempio, il revisore identifica che un utente ha il libero accesso ad un'applicazione alla quale non dovrebbe essere autorizzato e perciò ha la possibilità di accedervi e di effettuare modifiche. Il revisore dovrà verificare se l'utente ha usato impropriamente l'accesso per valutare il rischio identificato.
2) se, per quel determinato rischio IT, esistono ulteriori controlli IT non identificati in precedenza. Il revisore dovrà identificarli, valutarne la progettazione e infine l'efficacia. Ad esempio, nel caso in cui il revisore definisca come carente il controllo relativo agli accessi degli utenti ma allo stesso tempo la società effettua un controllo manuale periodico degli accessi tramite un report prodotto dal sistema: tale controllo dovrà essere valutato dal revisore prima di poter esprimere un giudizio.

Figura 3.1: Come esaminare i controlli



Fonte: Graham L., *Internal control audit and compliance, Documentation and Testing under the New COSO Framework*, Wiley Corporate F&A, 2015, pag. 268.

3.7 CAAT's (Computer Assisted Audit Techniques)

Oltre alle procedure precedentemente descritte per testare l'efficacia dei controlli, il revisore può usare tecniche computerizzate definite comunemente *CAATs* (*Computer Assisted Audit Techniques),* ovvero tecniche che utilizzano il computer come uno strumento di *audit.*

Queste procedure hanno lo scopo di migliorare le procedure di *audit* in quanto consentono di fornire degli elementi probativi relativi all'efficacia dei controlli nel caso in cui non ci siano dati input, non ci siano controlli visibili oppure nel caso in cui la dimensione dei campioni selezionati sia molto grandi, e perciò difficile da analizzare manualmente.[177]Nel caso di quantità elevate di dati, tali procedure permettono di analizzare l'intera popolazione senza dover svolgere campionamenti.

Tali procedure sono utili, infatti, in ambienti complessi in quanto permettono di verificare un numero elevato di operazioni registrate in formato elettronico oppure contenute in archivi contabili elettronici.[178]

Gli strumenti CAAT si dividono in due categorie: quelli utilizzati per verificare e convalidare programmi e quelli utilizzati per verificare e convalidare i dati. Per le procedure svolte sui programmi sono richieste al revisore competenze specifiche informatiche e deve conoscere le componenti IT e la struttura informatica della società che sta analizzando; sono perciò molto complesse da svolgere. Le seconde procedure invece si concentrano sui dati e non sul programma che genera i dati.

Tali tecniche possono essere utilizzate nelle seguenti procedure di *audit*

1) test di dettaglio su transazioni e saldi contabili, come per esempio, l'uso di *software* per svolgere ricalcoli oppure per l'estrazione di fatture dai registri informatici delle società con importi superiori un determinato valore soglia;
2) procedure analitiche, come ad esempio l'individuazione e l'analisi di scostamenti significativi relativi ai saldi contabili;
3) procedure di campionamento per l'estrazione di dati utili per i test di *audit*;
4) l'esecuzione di ricalcoli;
5) test dei controlli generali IT, per testare ad esempio il sistema operativo oppure gli accessi ai database;

[177]The International Auditing Practices Committee, CAATs, 2001, par. 1, pag. 2.
[178]Principio di revisione internazionale (ISA 315) 330: "Le risposte del revisore ai rischi identificati e valutati", par. A16, pag. 11.

6) test dei controlli applicativi, per testare ad esempio il funzionamento di un particolare controllo relativo ad una applicazione IT.[179]

I dati analizzati mediante tali procedure non provengono solo dal sistema contabile della società. È questo il caso soprattutto nel caso dei test sui controlli generali IT in quanto i dati sono solitamente sotto forma di testo e possono provenire dalle applicazioni IT. [180]

Durante la pianificazione dell'attività di *audit*, il revisore deciderà come combinare tecniche di revisione manuali e computerizzate e per farlo terrà in considerazione i seguenti fattori:

1) le competenze informatiche e l'esperienza del *team* di *audit*. Il *team*, infatti, deve avere le competenze adeguate al fine di svolgere tali procedure e il grado di conoscenza dipenderà dalla complessità delle procedure e dalla complessità dell'ambiente IT della società di riferimento;
2) la disponibilità di strumenti informatici adeguati al fine di svolgere procedure CAATs. Il revisore deve valutare se dispone di strutture informatiche e di sistemi informatici adeguati: è possibile, infatti, che gli strumenti del revisore siano incompatibili con gli strumenti e il formato dei dati fornito dalla società;
3) l'impossibilità di svolgere procedure manuali. Ciò avviene quando è necessario svolgere calcoli ed elaborazioni di dati complesse oppure quando la quantità di dati da processare sia troppo elevata. Dato il livello di automazione in costante crescita, le prove cartacee non sono più disponibili e perciò non è possibile svolgere verifiche manuali, come ad esempio:

- quando le operazioni delle aziende sono tutte gestite in formato elettronico e alcune operazioni potrebbe essere automaticamente gestite dal sistema (come, ad esempio, l'applicazione di sconti oppure il calcolo di interessi);
- quando i controlli non sono visibili ma gestiti dal sistema informatico (come, ad esempio, quando un programma associa in automatico l'ordine d'acquisto e la fattura di vendita);
- quando i report sono prodotti da un sistema sulla base dei propri dati di supporto;

[179]The International Auditing Practices Committee, CAATs, 2001, par. 4-5, pag. 2.
[180]The International Auditing Practices Committee, CAATs, 2001, par. 6, pag. 3.

4) l'efficacia e l'efficienza. L'uso di CAATs può aumentare l'efficacia e l'efficienza delle procedure di revisione soprattutto nel caso di un ambiente IT complesso e nel caso in cui il numero di transazioni sia elevato.

Prima di utilizzare tali procedure però, il revisore deve individuare i controlli generali IT e applicativi per valutare se sia possibile applicare le procedure computerizzate e se sia conveniente applicarle.

Se il revisore utilizza tali procedure, deve documentarle, descriverle, documentare i controlli sulle procedure che ne garantiscono l'appropriatezza e infine deve documentare i risultati.

3.8 Relazione di revisione

Al termine dell'attività di IT *Auditing*, il revisore dovrà emettere una relazione relativa al sistema di controllo interno in ottica IT sulla base delle evidenze raccolte durante tutto il processo di revisione. Per poterla emettere, il revisore deve aver raccolto elementi probativi sufficienti e appropriati a sostegno del proprio giudizio.

L'ISA di riferimento per redigere la relazione di revisione da parte di un IT *Auditor* è l'ISAE (*International Standard on Assurance Engagements)* 3400[181] ovvero lo standard di riferimento per gli incarichi di *Assurance* diversi dalla revisione finanziaria. L'ISACA ci fornisce delle indicazioni ulteriori utili per la redazione del report nel suo *framework* "*IT Audit Framework*"[182].

Nonostante la natura tecnica di un *audit* IT, i revisori IT devono garantire che il report sia pienamente comprensibile alla direzione aziendale, agli *stakeholder* e al pubblico in generale.

La relazione deve contenere i seguenti punti:

1) il titolo;
2) il destinatario dell'attività svolta dai revisori. L'attività può avere come oggetto una società, una parte di essa, un processo aziendale, un sistema informativo oppure una particolare tecnologia aziendale;

[181]Principio internazionale sugli incarichi di Assurance (ISAE) 3400: "L'esame dell'informativa finanziaria prospettica".

[182]AA. VV., IT Audit Framework (ITAF™) "A Professional practices Framework for IT Auditor", 4th edition, Documento in Pubblica consultazione, ISACA, 2020.

3) gli standard utilizzati: i principi di revisione internazionale oppure gli standard di *best practice* riconosciuti a livello globale comunemente utilizzati (come, ad esempio, gli standard emessi dall'ISACA o dall'AIEA, ovvero Associazione Italiana IS *Auditor*);
4) un'attestazione di responsabilità svolta della direzione aziendale con la quale dichiara l'efficacia delle procedure di controllo IT messe in atto e con la quale si ritiene responsabile delle procedure e del mantenimento del controllo all'interno della società;
5) la finalità della relazione e l'eventuale divieto di divulgazione se espressamente richiesto dalla direzione aziendale;
6) una sintesi sulle procedure di revisione svolte per ottenere ragionevole sicurezza che gli elementi probativi acquisiti siano sufficienti e appropriati al fine di poter emettere un giudizio;
7) giudizio su quanto revisionato, ovvero deve esprimere un giudizio in merito all'efficacia, sotto tutti gli aspetti rilevanti, della progettazione e/o del funzionamento dei controlli IT messi in atto dalla società. Il giudizio sarà:

- positivo: se il revisore sostiene che i controlli IT sono stati progettati adeguatamente per fronteggiare i rischi oppure se tali controlli operano in modo efficace per tutto il periodo specificato. I controlli verificati saranno quelli utili a fornire una ragionevole sicurezza che gli obiettivi di controllo saranno raggiungi;
- con modifiche: se il revisore sostiene che i controlli IT non sono stati progettati adeguatamente per fronteggiare i rischi riscontrati oppure se tali controlli non operano in modo efficace. Tale giudizio deve essere dato anche nel caso in cui il revisore non riesca ad acquisire elementi probativi sufficienti e appropriati a sostegno del proprio giudizio.

8) osservazioni, risultati, raccomandazioni e conclusioni. Il revisore descriverà i test e le procedure messe in atto per poter esprimere un'opinione e comunicherà alla società eventuali carenze riscontrate. In questo caso dovrà proporre delle azioni correttive che la società potrebbe implementare per colmare le carenze;
9) una data della relazione, la quale deve essere coincidente oppure posteriore alla data di termine delle procedure di revisione svolte;
10) la sede del revisore oppure della società di revisione;

11) la firma del revisore.[183]

Il revisore esprimerà un giudizio con modifiche nel caso in cui non sia ragionevole esprimere un giudizio positivo. Potrà in questo caso esprimere un giudizio negativo oppure potrà recedere dall'incarico a seconda della situazione.
Se il revisore ha riscontrato carenze significative nei controlli IT il revisore dovrà esprimere un giudizio negativo. Se invece si trova nell'impossibilità di svolgere procedure necessarie per esprimere un giudizio o se non ha acquisito elementi probativi sufficienti e appropriati, il revisore dovrà recedere dall'incarico di revisione oppure dichiarerà l'impossibilità di esprimere un giudizio. In questo caso dovrà descrivere le limitazioni riscontrate durante lo svolgimento dell'incarico. [184]

Se il revisore IT lavora all'interno di incarichi di *audit* finanziario, dovrà sempre comunicare i risultati ottenuti dalle procedure svolte ai revisori legali che controllano l'informativa di bilancio in quanto eventuali debolezze relative ai sistemi di produzioni dei dati avranno effetto anche sull'informativa bilancio; pertanto, le carenze dovranno essere discusse congiuntamente. Nel comunicare tali informazioni, il revisore IT dovrà usare un gergo comprensibile al revisore finanziario.
In questo caso, perciò, i risultati dell'IT *auditor* saranno incorporati nella relazione di revisione svolta dai revisori legali sul bilancio d'esercizio.

[183]AA. VV., IT Audit Framework (ITAF™) "A Professional practices Framework for IT Auditor", 4th edition, Documento in Pubblica consultazione, ISACA, 2020, pag. 89-93.
[184]Principio internazionale sugli incarichi di Assurance (ISAE) 3400 "L'esame dell'informativa finanziaria prospettica", par. 30-31-31, pag.7.

CAPITOLO 4: IL RUOLO DELL'IT AUDITOR NELLA PRATICA: APPROFONDIMENTO ATTRAVERSO UN'INTERVISTA

4.1 La figura dell'IT Auditor

Come è stato definito nei capitoli precedenti, con il crescere dell'automazione dei processi amministrativi e contabili, è aumentata la necessità di avere maggior sicurezza nei dati e nel bilancio aziendale. Per comprendere tali processi però, le sole competenze economiche non sono sufficienti in quanto sono necessarie sempre più competenze in ambito informatico: nasce così la figura dell'IT *Auditor*.

L'IT *Auditor* è quel revisore che si occupa di verificare la corretta governance dei sistemi IT, valuta l'uso della tecnologia per la produzione dell'informativa di bilancio e valuta i controlli interni IT messi in atto per fronteggiare i rischi IT. Nel momento in cui il revisore identifica un problema o una carenza, comunica quanto rilevato alla direzione aziendale e propone delle soluzioni.

L'*IT Auditor* può essere sia un revisore interno che esterno.

Se è un revisore interno, lavorerà direttamente per la società e si occuperà di analizzare e valutare l'efficacia e l'efficienza dei sistemi IT e dei processi IT. Valuterà inoltre i controlli IT messi in atto per contrastare i rischi IT con l'obiettivo di identificare e correggere eventuali carenze riscontrate.

Se invece è un revisore esterno, sarà un soggetto indipendente alla società revisionata e si occuperà di valutare e certificare i sistemi IT e i controlli generali IT messi in atto dalla società, i quali garantiscono la correttezza dell'informativa di bilancio.

L'*IT Auditor* esterno può lavorare singolarmente oppure può lavorare con il revisore finanziario.

Nel primo caso, gli sarà conferito un mandato specifico per svolgere tale funzione e dovrà verificare come le componenti IT e i sistemi IT sono utilizzati dalla società per raggiungere gli obiettivi aziendali. In questa situazione il revisore dovrebbe avere anche l'accesso libero e diretto alla documentazione aziendale, sia cartacea che elettronica, per poter adempiere al mandato ricevuto.

Nel secondo caso, il conferimento del mandato di *audit* finanziario sarà sufficiente al fine di svolgere l'attività di IT *auditing* senza il bisogno di un mandato aggiuntivo. Infatti,

come definito dall'ISA 315, il revisore deve comprendere l'impresa, il suo sistema di controllo interno considerando anche la componente informatica al fine di identificare errori significativi nel bilancio. Se l'ambiente è automatizzato, sarà necessario l'intervento di un IT *auditor* che comprenda i sistemi IT e i controlli IT relativi alla produzione dell'informativa di bilancio.
L'attività dei due soggetti è perciò strettamente correlata: il revisore finanziario verifica che il bilancio dia una rappresentazione veritiera e corretta della realtà aziendale, invece, il revisore IT valuterà come le informazioni e i dati sono registrati, elaborati e come essi confluiscono nel bilancio. Allo stesso tempo il revisore valuterà e testerà i controlli IT su cui il revisore finanziario potrà fare affidamento, solo se tali controlli sono progettati e implementati in modo adeguato.
I risultati ottenuti dal revisore IT saranno poi comunicati al revisore finanziario che ne terrà conto nello svolgimento della propria attività.

L'IT *Auditor* ha competenze prettamente informatiche che derivano da una formazione superiore oppure da una laurea in campo informatico, come ad esempio una laurea in sistemi informativi informatici oppure una laurea in tecnologia dell'informazione. Deve avere infatti competenze specifiche relative a sistemi IT, applicazioni IT e infrastrutture IT, le quali poi sono applicate in ambito economico e aziendale.
Il revisore, infatti, deve saper valutare e progettare nuovi sistemi IT, valutare il livello di sicurezza informatica dell'azienda di riferimento, saper modificare i programmi e le applicazioni IT e saper garantire la sicurezza dei dati aziendali.
Per svolgere tale professione, esistono diverse certificazioni, tra cui:

- la certificazione CIA (*Certified Internal Audit*), la quale attesta e permette di acquisire le competenze necessarie per poter svolgere il ruolo di *auditor* interno alle aziende;
- la certificazione CISA (*Certified Information Systems Auditor*), la quale è rilasciata a cura dell'ISACA. Tale certificazione permette di acquisire le competenze necessarie in termini di: IT *Governance*, *Audit* dei sistemi IT e processi IT, implementazione e sviluppo di sistemi informatici e cybersicurezza.
  Per poterla conseguire però è necessarie che il soggetto abbia un'esperienza lavorativa comprovata nel campo del controllo dei sistemi IT di almeno 5 anni;

- ➔ la certificazione CISSP (*Certified Information Systems Security Professional*), relativa alla sicurezza digitale. Il soggetto che la acquisisce sarà in grado di implementare e sviluppare un sistema di sicurezza digitale ottimale. Anche per questa certificazione è necessaria un'esperienza lavorativa comprovata in campo di sicurezza dei sistemi informatici di almeno di 5 anni;
- ➔ la certificazione COBIT, la quale consente di acquisire ed attestare le conoscenze relative al *framework* COBIT e perciò competenze relative all'IT Governance e Management.

Le *soft skills* che dovrebbe avere un IT *Auditor* invece sono diverse:

1. attenzione ai dettagli: il revisore IT è tenuto ad analizzare un grande ammontare di dati al fine individuare eventuali malfunzionamenti e carenze. Proprio per questo, il revisore deve essere capace di valutare i dettagli per poter definire una strategia adeguata e per individuare le carenze e le relative soluzioni in modo efficace;
2. pensiero critico: è fondamentale per poter analizzare e valutare obiettivamente le informazioni possedute dal revisore. Questa caratteristica è importante nell'individuazione dei rischi, dei controlli, delle carenze e delle relative soluzioni;
3. capacità di lavorare in *team*: i revisori IT, e in generale i revisori, devono avere una forte capacità di leadership per poter interagire e lavorare in un team di revisione. Tale capacità è importante anche nell'interazione con i *team* che svolgono *audit* finanziario;
4. abilità comunicative: la comunicazione è fondamentale per diversi aspetti. Innanzitutto, come detto nel punto precedente, l'IT *auditor* lavora in gruppo e la comunicazione all'interno del *team* è fondamentale. All'interno del *team*, infatti, i revisori si comunicano i risultati ottenuti dai test svolti e traggono insieme delle conclusioni. Allo stesso tempo, la comunicazione è fondamentale nel trasmettere, sia verbalmente che in forma scritta, i risultati ottenuti alla direzione aziendale e ai revisori finanziari: in questi casi il revisore IT deve utilizzare dei termini comprensibili a chi non ha competenze informatiche.[185]

[185]Rotich R., What is an IT Auditor? (with Duties, Skills and Salary), Indeed, 28 Dicembre 2022, https://www.indeed.com/career-advice/finding-a-job/what-is-it-auditor

4.2 Intervista al revisore IT: domande

Per concludere la presente trattazione, è stato intervistato un IT *auditor* con l'obiettivo di comprendere al meglio e dal punto di vista pratico il suo lavoro. Questa intervista, infatti, ha permesso di approfondire il tema trattato nell'elaborato grazie all'aiuto di un esperto del settore e ha permesso di capire più precisamente come si struttura il suo lavoro, quali sono le normative a cui fa riferimento e quali sono i principali rischi IT che si trova ad affrontare un revisore IT.

Sono state sottoposte all'IT *Auditor* svariate domande (per la precisione 17 domande) con l'obiettivo di chiarire dei temi che era fondamentale approfondire e, allo stesso tempo, per vedere la reale applicazione dei concetti che sono stati trattati e analizzati ampiamenti durante la trattazione.

Le domande sono state selezionate sulla base dei temi che sono stati trattati nei precedenti capitoli; di seguito sono riportate le domande nel dettaglio.

Per strutturare la prima parte dell'intervista gli obiettivi che si volevano raggiungere erano: quello di comprendere quale percorso formativo e quali certificazioni avesse conseguito il revisore per essere qualificato quale revisore IT; comprendere dal punto di vista pratico come si struttura un'attività di *IT auditing* e come si svolge tale attività all'interno del *team* di *audit*; comprendere come si rapporta la figura del revisore IT con altri soggetti quali il revisore finanziario in primis e successivamente con tutto il corpo aziendale; infine comprendere anche quali fossero le principali procedure e attività svolte dal revisore e quali procedure CAAT's sono utilizzate maggiormente nel campo.

Le domande definite riguardo questi temi sono le seguenti:

1. Qual è stato il suo percorso formativo per essere IT *Auditor*? Ha svolto qualche certificazione?
2. Lei lavora in tutti i *job* oppure solo nei *job* in cui sono richieste competenze specifiche in tema IT?
3. Lavora in *team* oppure singolarmente? E come si rapporta con il *team* di *audit*?
4. Quali sono i soggetti con cui si interfaccia all'interno della società?
5. Può descrivermi come si strutturano nell'arco dell'anno il processo di revisore da lei svolto in tema IT?
6. Quali sono le principali procedure CAAT's da lei utilizzate? Qual è l'area in cui sono più utili da utilizzare?

7. Quali sono le competenze che dovrebbe avere un IT *auditor*?

La seconda parte verteva sull'ISA 315. L'interesse era rivolto a conoscere l'opinione del revisore IT, data la sua grande esperienza nel campo, sull'aggiornamento dell'ISA 315 e, nello specifico, era interessante comprendere se secondo lui tale aggiornamento fosse effettivamente utile e facilmente applicabile o se avesse riscontrato delle carenze.
Le domande predisposte a riguardo sono state:

1. Da un Report sull'applicazione dell'ISA 315 svolto dallo IAASB risulta che molti revisori ritengono che l'ISA non rifletta a sufficienza la complessità dei sistemi informativi utilizzati dalle grandi imprese e che i rischi IT non siano enfatizzati a sufficienza. Ritiene che l'aggiornamento dell'ISA 315 tratti sufficientemente il tema dell'IT e dei rischi connessi all'utilizzo dell'IT?
2. Gli esempi pratici forniti dall'ISA 315 relativi agli aspetti da comprendere relativi all'infrastruttura IT e ai processi IT sono utili e facilmente utilizzabili?
3. In relazione ai controlli generali IT, gli esempi forniti dall'Appendice 6 riguardo i processi per gestire gli accessi, i processi per gestire le modifiche ai programmi e i processi di gestione IT sono utili?
4. Prima che dell'aggiornamento dell'ISA 315, a che normativa faceva riferimento?

L'ultima parte dell'intervista voleva trattare domande relative ai rischi IT al fine di comprendere se le società fossero a conoscenza dei principali rischi IT e se fossero consapevoli dell'importanza di avere un sistema IT ben strutturato per contrastare tali rischi. Riguardo questi aspetti, è stato affrontato il tema del COBIT al fine di comprendere se fosse conosciuto e applicato dalle aziende.
Infine, l'intervista voleva ottenere un'opinione di un revisore IT riguardo il tema dei rischi *cyber*, in particolare il fenomeno del *phishing*, in quanto è un argomento importante da affrontare data la sua diffusione.
Le domande in merito a quest'ultima parte sono:

1. All'interno delle società, la direzione comprende quanto sia importante implementare un sistema IT ben strutturato e organizzato?
2. Dalla sua esperienza, quali sono i rischi IT più frequenti che ha riscontrato?

3. Io ritengo che per prevenire i rischi IT in una società sia importante che tutto il personale sia formato e sia a conoscenza di tali rischi al fine di prevenirli e ridurli. Quanto secondo lei questo è importante e quanto ciò avviene nelle aziende?
4. Svolge delle procedure specifiche per verificare come le società prevengono gli attacchi di *phishing*?
5. La complessità di un sistema IT è strettamente correlata alla grandezza di una società? Ed è correlata alla complessità di una società?
6. Le società conoscono, comprendono e utilizzando il framework COBIT per implementare in modo efficiente e integrato la componente informatica?

4.3 Intervista al revisore IT: risposte

In questo paragrafo sono analizzate le risposte alle domande che sono state sottoposte al revisore IT. L'intervista è avvenuta il giorno 18 maggio 2023 in via telematica.

Il soggetto intervistato è stato il Dottor Iannucci Sandro, IT *Auditor* Partner della società di revisione Crowe Bompani Spa presso la sede di Roma. Il Dottor Iannucci è un IT *Auditor* che ha svolto svariate attività lavorative in campo IT. Ha lavorato per la società Enidata come programmatore IT e, successivamente, ha ricoperto il ruolo di analista e programmatore IT nella società Agip Petroli. Ha lavorato per il gruppo Finsiel come responsabile IT. A seguire è passato al settore della consulenza e ha lavorato presso la società di revisione Ernst & Young per più di dieci anni.

In seguito, è tornato a lavorare in azienda lavorando per la società B-V tech, un'azienda di sviluppo *software* che voleva implementare il settore della consulenza.

Attualmente, è socio del gruppo Crowe Bompani Spa e ricopre il ruolo di capo del dipartimento IT e dell'attività di consulenza sulla qualità della *privacy* da circa cinque anni.

Il Dottor Iannucci ha lavorato inoltre nei gruppi di lavoro relativi al COBIT 3 per poterlo implementare.

Dal punto di vista didattico, si è laureato all'università di Roma ma ha avuto una formazione prettamente tecnica.

L'intervista al revisore IT è iniziata con una breve introduzione sui lavori da lui svolti per poi citare le certificazioni che ha conseguito.

In ambito IT, le certificazioni sono svariate e sono molto importanti in quanto consolidano le conoscenze di chi le consegue, fatto confermato anche dalla risposta del revisore, il quale sostiene che le certificazioni in questo campo sono molte, ma che alcune siano più utili di altre.

L'intervistato ha conseguito la certificazione BS 7799 (in vigore dal 2002), ovvero l'attuale certificazione ISO 27001 (in vigore dal 2005), e la certificazione ISO 19011.

Come è stato trattato dal paragrafo 2.2.2, la certificazione ISO 27001 consente di acquisire le competenze per poter implementare all'interno delle società sistemi di gestione alla sicurezza efficaci ed efficienti. Il revisore IT, infatti, deve conoscere tali regole e procedure per poterle mettere in pratica nelle aziende.

La certificazione ISO 19011 invece attesta la conoscenza delle tecniche di *audit*. Svolgendo tale certificazione, il soggetto acquisisce le competenze per poter condurre e gestire un incarico di *audit*; fornisce inoltre linee guida specifiche per *l'audit* dei sistemi di gestione.

Allo stesso tempo, oltre alle certificazioni, l'intervistato ha sostenuto, durante l'intervista, che è bene fare parte di associazioni IT, ovvero associazioni *ad* hoc in campo IT che permettono di essere sempre aggiornati e allineati a livello di *best practice*. Tali associazioni studiano ed emettono costantemente delle nuove metodologie utili per i revisori IT nello svolgimento del proprio lavoro.

Lui infatti è iscritto all'AIEA, ovvero Associazione Italiana IS *Auditor*, la quale aderisce all'ISACA. L'ISACA è una delle associazioni più attive e famose in campo IT in quanto fornisce aggiornamenti, *best practice* e metodi di analisi e valutazione sempre aggiornati relativi ad *Audit/ Assurance, Security, Risk, Governance, Cybersecurity* e tecnologie emergenti. Come è stato trattato visto nei capitoli precedenti, l'ISACA ha prodotto il *framework* COBIT.

La prima parte dell'intervista ha riguardato il lavoro del revisore IT.

Il soggetto intervistato ha confermato che il lavoro di IT *auditing*, come quello di *auditing* finanziario si svolge in *team*. Afferma infatti che lui stesso crea il *team*, essendo partner della società di revisione in cui lavora, e comunica lo scopo e il *timing* dell'attività ai membri incaricati; questo aiuta i suoi sottoposti a capire quali sono le aree critiche e qual è il perimetro delle loro attività. Ogni qual volta in cui un membro del *team* ha delle incertezze o rileva elementi significativi dovrà interfacciarsi con lui.

Per quanto riguardo il rapporto con i revisori finanziari, l'intervistato afferma che c'è un costante scambio di informazioni. Come detto nei capitoli precedenti, il revisore IT lavora con il *team* di *Audit* finanziario nel caso in cui siano richieste delle competenze specifiche in ambito IT, le quali non sono in possesso dal revisore finanziario.
Come confermano le risposte ottenute durante l'intervista, l'attività di IT *auditing* supporta l'attività di *auditing* finanziario, seguendo le tempistiche e le esigenze di quest'ultima.
Le attività che svolge il revisore IT in tal senso sono svariate, e ne sono state citate un paio durante l'intervista. Il revisore IT è chiamato innanzitutto a svolgere un *assesment* IT, ovvero valuterà l'infrastruttura IT al fine di individuarne i punti di forza e le carenze. Con tale valutazione il revisore indagherà sullo stato di salute dell'ambiente IT e sul suo livello di sicurezza informatica.
Un'altra attività di competenza del revisore IT è la valutazione del livello di *compliance* della società alla GDPR, ovvero alla normativa sulla *privacy*, in quanto poi il revisore finanziario nella relazione di revisione dovrà dichiarare se la società ne è conforme.
Un'ulteriore attività si concretizza nella verifica della spesa in IT svolta dalle società revisionate. Il revisore in tal senso porta un esempio, affermando che se un'azienda dichiara di spendere un importo elevato e poi l'infrastruttura IT non combacia con tale somma questa discrepanza dovrà essere indagata. Sarà un compito del revisore IT verificare che la spesa dichiarata dalla società sia effettivamente valida. Queste attività saranno utili per il revisore finanziario nella stesura della relazione finale di revisione.
Oltre alle attività elencate in precedenza, sono state evidenziate ulteriori attività che il revisore svolge più legate all' attività di consulenza alle aziende sulle componenti IT. Nonostante queste siano attività che non coinvolgono in maniera diretta il revisore finanziario, quest'ultimo potrebbe comunque servirsene in caso di necessità.
Tra le attività di consulenza citate, c'è l'analisi della governance della componente IT, lo svolgimento di "*penetration test*" (ovvero simulazioni di attacchi al sistema informatico dell'azienda posta in oggetto), attività di *audit* sui fornitori esterni IT di un'azienda e analisi del rischio di tutto l'apparato IT che solitamente un'azienda non svolge.

Riguardo le procedure che svolge il revisore IT, sono state approfondite anche quali fossero le procedure CAAT's maggiormente utilizzate dal punto di vista pratico. Il revisore IT intervistato ha affermato che una delle cose importanti da fare è verificare e controllare i *report* prodotti dalle società, soprattutto nel caso in cui il personale abbia svolto dei calcoli attraverso fogli elettronici, in quanto queste sono le situazioni in cui una società può falsificare oppure omettere con più facilità degli importi.
Le società utilizzano sistemi SAP e tecnologie emergenti, ma secondo la sua personale esperienza l'attenzione deve essere posta soprattutto sui fogli Excel prodotti dal personale aziendale, sui quali devono essere svolti dei controlli più accurati.

Come indagato nei capitoli precedenti, oltre ai revisori finanziari, il revisore deve interfacciarsi anche con il personale aziendale. Tra i soggetti citati durante l'intervista ci sono innanzitutto l'amministratore delegato e il *compliance manager*, in quanto afferma che l'IT ha impatto su ogni attività di *compliance*. I revisori si interfacciano anche con i responsabili di IT *Audit* interno all'azienda, in quanto quest'ultimi sono interessati ad avere un'opinione esterna e indipendente relativa alla componente IT e ai livelli di sicurezza della propria azienda. Si rapportano inoltre con il responsabile IT, in quanto i revisori hanno l'interesse di capire se quest'ultimo è a conoscenza e ha sotto controllo la situazione dell'intera infrastruttura IT.
Secondo il soggetto intervistato, la figura e la funzione dell'IT *Auditor* non è sempre compresa fino in fondo in quanto viene percepita spesso come un'attività di verifica e controllo fine a sé stessa. L'IT *Auditor* invece controlla e svolge test sul sistema IT di una società al fine di individuarne carenze, le quali se riscontrate, saranno comunicate al responsabile IT e il revisore potrebbe aiutare la società a colmarle. L'IT *Auditor*, infatti, dovrebbe essere visto come un valore aggiunto per una società in quanto potrebbe aiutare a strutturare un sistema IT efficiente.

Per approfondire il tema della scalabilità, trattato nel primo capitolo, l'obiettivo era quello di chiedere al revisore se ci fosse una correlazione tra complessità di un sistema IT e grandezza dell'azienda. Dalle risposte ottenute, è stato confermato quanto definito dall'ISA 200 ovvero che non c'è correlazione. L'intervistato afferma che esistono e ha revisionato aziende molto grandi con sistemi IT non complessi. È possibile che un'azienda sia grande con tante sedi diffuse ma che il suo sistema informatico sia

centralizzato in un'unica sede; in questo caso deve essere posta solo maggior attenzione nella trasmissione dei dati da un punto A, che può essere la sede, ad un punto B, che può essere la centrale.
Non esiste correlazione neanche tra complessità di un sistema IT e complessità della società, afferma l'intervistato: esistono infatti aziende molto complesse con sistemi informatici di facile gestione.
Il compito del revisore è quello di comprendere ogni entità sulla base delle caratteristiche specifiche possedute da essa senza focalizzarsi sulla grandezza dell'azienda o sulla sua complessità, ma sulla base delle caratteristiche del sistema informatico.

Nella seconda parte dell'intervista sono state rivolte delle domande relative all'ISA 315: al fine di comprendere quali fossero i punti di forza e di debolezza dell'aggiornamento avvenuto nel 2022.
Da un Report sull'applicazione dell'ISA 315 svolto dallo IAASB[186] risulta che molti revisori ritengono che l'ISA non rifletta a sufficienza la complessità dei sistemi informativi utilizzati dalle grandi imprese e che i rischi IT non siano enfatizzati a sufficienza, volevo perciò conoscere il punto di vista del revisore intervistato.
Il revisore conferma il fatto che non sono stati trattati dei temi importanti, tra cui quello della cyber sicurezza; tale concetto infatti è cambiato e si è sviluppato fortemente negli anni, facendo scoppiare un tipo di "*Cyberwar*" completamente diversa rispetto al passato. Per "*Cyberwar*", ovvero guerra cibernetica, si intendono tutti questi attacchi informatici ad impatto elevato. Tali attacchi hanno di solito come obiettivo il sistema informatico o la rete di uno Stato, oppure di una società statale strategica importante, con il fine di causare danni. Prima, infatti, le aziende avevano solo 3-4 attaccanti, ora sono molti di più e gli attacchi fanno spesso parte di strategie.
L'utilità degli esempi forniti dall'ISA 315 per comprendere i sistemi IT delle aziende è stata confermata. Tali esempi però, secondo l'intervistato, costituiscono solo una base per iniziare. Il revisore, infatti, si serve degli esempi forniti dall'ISA, ma dovrà riadattarli alla società di cui ha l'incarico. Determinati controlli non li farà oppure li farà con più attenzione in base alla situazione e all'infrastruttura IT che si troverà a revisionare.

[186]AA. VV., *Clarified International Standards on Auditing – Findings from the post-implementation Review*, Documento in Pubblica Consultazione, IFAC, Luglio 2013.

Anche dei controlli IT definiti dall'ISA 315 ne è stata confermata l'utilità. Essi però, secondo l'intervistato, sono utili ma non sono sufficienti in quanto con l'aumento costante del livello di automazione sono necessari sempre più controlli specifici.
Secondo lui, alcuni sono complessi e andrebbero alleggeriti, ma afferma che è importante ricordare che tali controlli partono dal mercato americano e che di conseguenza l'applicazione in campo europeo deve essere riadattata. Inoltre, ricorda che determinati controlli, che prima non erano di competenza IT, ora lo sono, citando come esempio i controlli sulla *privacy*.

Nell'ultima parte dell'intervista l'obiettivo era quello di conoscere dal punto di vista pratico quali fossero i rischi IT più diffusi e quale fosse il punto di vista delle aziende.
Innanzitutto, avevo l'interesse di comprendere ulteriormente come le società percepissero la componente IT e quanta attenzione ponevano a tale aspetto. Ho chiesto perciò al revisore IT, se la direzione aziendale comprende quanto sia importante implementare un sistema IT ben strutturato e organizzato. Legato a questo, ero interessata a sapere se i responsabili IT conoscono il *framework* COBIT, al fine di governare in modo efficiente il sistema IT.
Dalle risposte ottenute, è possibile affermare che prima del 2001, ovvero l'anno in cui sono state attaccate le Torri Gemelle, le società non ponevano la giusta attenzione ai temi IT, ma da quell'anno in poi hanno capito che la parte IT doveva essere ben strutturata. Ad oggi, a causa della tematica della *cybersecurity*, le società hanno compreso sempre di più l'importanza di tale concetto. Inoltre, le piccole aziende con un assetto proprietario limitato solitamente sono meno orientate ai temi IT a differenza di quelle più strutturate.
Come è stato ampiamente affermato nei capitoli precedenti, il *framework* COBIT è lo strumento ideale che aiuta le aziende e i revisori IT nell'implementare una governance efficiente dei sistemi IT. L'intervistato, in merito, sostiene che le società non conoscono abbastanza questo strumento e perciò non viene spesso messo in pratica. Afferma inoltre che il COBIT è nato dall'esigenza di banche, assicurazioni e aziende in cui era importante la gestione monetaria: per queste società avere una governance pulita, puntuale e precisa era essenziale; per questi motivi, afferma che questo strumento sarebbe molto utile da applicare a tutti i tipi di società, ma che non è ancora stato compreso a pieno.

Come trattato nel secondo capitolo, uno dei rischi maggiori a cui è sottoposta una società riguarda gli attacchi alla sicurezza digitale. L'alta diffusione e la gravità è stata confermata dalle risposte dell'intervistato, in quanto questo rischio è dovuto soprattutto alla mancata applicazione delle regole base, come per esempio la lunghezza e la complessità della password; anche non cambiare molto spesso le password degli utenti, delle applicazioni e degli apparati, mina la sicurezza di qualsiasi infrastruttura IT dalle basi.
Per quanto riguarda invece il fenomeno del *phishing*, è stato confermato che è fondamentale prevenirlo attraverso una formazione adeguata dei dipendenti. È importante che il personale sappia intercettare eventuali *e-mail* dannose, ma per riconoscere tali rischi è necessario che i dipendenti siano formati adeguatamente in merito: ad un soggetto sorge il dubbio di essere attaccato solo se è stato ben istruito precedentemente. Per questo motivo, tra le attività che deve svolgere un revisore IT, c'è anche la verifica che i dipendenti siano adeguatamente formati sotto questo aspetto.

Per concludere l'intervista, ho chiesto al revisore quali fossero le competenze e le certificazioni fondamentali che dovrebbe possedere un revisore IT per iniziare a ricoprire quel ruolo.
L'intervistato sostiene che, innanzitutto, un IT *Auditor* dovrebbe provenire dal mondo applicativo e non dal mondo della realizzazione del *software* e dalle telecomunicazioni, inoltre dovrebbe essere certificato ISO 27001, dovrebbe aver fatto un corso sul COBIT e dovrebbe avere una buona conoscenza sul tema della *privacy*.

4.4 Risultati ottenuti dall'intervista

L'intervista si poneva degli obiettivi specifici, ovvero:

1. comprendere come si struttura il lavoro del revisore nella pratica e come si rapporta il revisore con gli altri soggetti (team di revisione, revisori finanziari e società);
2. comprendere le principali procedure svolte nella pratica;
3. ottenere un'analisi critica relativa all'aggiornamento dell'ISA 315;
4. ottenere un'analisi sui rischi IT, soprattutto sui rischi legati alla cybersicurezza, e sulle attività di prevenzione svolte dalle società per contrastarli;

5. ottenere un'analisi relativa al livello di comprensione che hanno le aziende rispetto alla governance efficiente di un sistema IT.

Tali obiettivi sono stati posti per toccare la maggior parte dei temi che sono stati trattati nella presente trattazione al fine di poterli trattare e comprendere a livello pratico e non solo teorico, i temi generali sono: l'ISA Italia 315 e le procedure dettate da tale principio, il *framework* COBIT, i rischi IT, la cybersicurezza e l'implementazione dell'IT.
Le domande sono state poste al fine di ottenere un'analisi critica e delle constatazioni relative a temi diversi, le quali possono essere fornite solo da un soggetto autorevole che lavora nel campo da molti anni e che perciò possiede le competenze adeguate per poter rispondere alle domande.
Dopo aver svolto l'intervista, posso affermare che gli obiettivi dell'intervista sono stati soddisfatti dalle risposte del soggetto intervistato.

L'intervista ha evidenziato come si struttura l'attività di IT *Auditing*, la quale può essere integrata all'attività di audit finanziario o autonoma rispetto a quest'ultima.
Nel primo caso, infatti, l'IT *Auditor* può supportare il revisore finanziario svolgendo procedure specifiche sui sistemi IT, sui sistemi di gestione alla sicurezza digitale, per comprovare la conformità al regolamento GDPR e per controllare la governance dell'IT.
Nel secondo caso invece, l'IT *Auditor* può supportare le società attraverso attività di consulenza analizzando il sistema IT implementato, verificando le carenze riscontrate e definendo delle soluzioni. In questo il revisore si occuperà, ad esempio, di governance e management dell'IT, di sicurezza digitale e di analisi relativa all'implementazione di nuove tecnologie.
Il lavoro si svolge in *team* in quanto la quantità di procedure da svolgere è elevata ed è importante che le procedure siano svolte e successivamente revisionate da soggetti con competenze diverse e anni di esperienza diversi, in quanto è importante che gli aspetti relativi all'IT siano analizzati da soggetti diversi che consentono così di raccogliere punti di vista diversi. Il lavoro in *team* in questo tipo di lavoro è fondamentale perché permette un'analisi più accurata degli aspetti IT. Il *team* è formato dal partner IT che nomina i membri dei *team*, il quale deve essere composto da soggetti con competenze e esperienze professionali diverse, dal manager al dipende appena assunto, in quanto ogni soggetto apporterà un valore aggiunto all'interno del gruppo. In fase di pianificazione

dell'attività, dovrà essere definito l'obiettivo dell'attività e verrà suddiviso il lavoro. Ogni soggetto dovrà svolgere quanto richiesto per raggiungere il fine comune.

Per quanto riguarda l'ISA Italia 315, è stato confermato il fatto che l'aggiornamento è stato un punto di partenza in quanto ha cambiato totalmente il modo in cui le aziende devono considerare la componente informatica, introducendola in modo esplicito tra le procedure da svolgere al fine di comprendere l'impresa e il suo sistema di controllo interno. È vero anche che la velocità con cui si evolve il mercato della tecnologia è immane e per questo alcuni temi importanti non sono stati trattati a sufficienza, tra cui gli aspetti relativi alla cybersicurezza. Tale concetto è citato ma non ne viene data la giusta importanza: come è stato analizzato nel paragrafo 2.2.1, è un tema importante perché gli attacchi alla cybersicurezza sono pericolosi e sempre più diffusi.
Essendo l'aggiornamento originale dettato dallo IAASB nel 2019, non è stato tenuto conto degli effetti del Covid-19 relativi agli attacchi cyber. La pandemia del 2020 ha fatto comprendere alle aziende quanto fosse importante la tecnologia per il business e ha diffuso il lavoro da remoto: l'uso crescente della tecnologia e di reti remote ha aumentato la vulnerabilità dei sistemi informatici agli attacchi hacker. L'ISA Italia 315 non ha ancora definito per il revisore delle procedure specifiche in tal senso.
In ogni caso, le procedure dettate da tale principio di revisione e gli esempi forniti, sia in termini di aspetti da considerare per comprendere l'ambiente IT che in termini di controlli da valutare, sono molto utili per il revisore ma costituiscono solo una base per il lavoro che dovrà essere svolto: il revisore dovrà riadattarle sulla base delle specificità delle imprese che avrà di fronte.
Per quanto riguarda invece il tema della cybersicurezza, il rischio di *cyber* attacchi è molto pericoloso ma sale se le aziende non adottano i comportamenti giusti per contrastarlo. Tra i comportamenti consigliati dal revisore IT c'è l'attività di prevenzione per gli attacchi di *phishing* attraverso la formazione del personale dipendente e il rispetto delle regole base relative alle password degli utenti e dei dispositivi aziendali. Le regole base come la lunghezza della password, l'uso di parole non comuni per comporla e il cambio regolare della stessa sembrano aspetti banali ma sono fondamentali da rispettare.
Il revisore dovrà verificare se la società metterà in pratica queste attività.

Per concludere, era importante e interessante comprendere quale fosse la percezione e l'importanza posta dalle aziende in relazione ai temi IT. È importante, infatti, che i sistemi IT siano governati in modo efficace per contrastare i rischi IT.
Per governare adeguatamente l'ambiente IT delle società, come trattato nel paragrafo 2.5, può essere utilizzato il *framework* COBIT, ovvero lo strumento che definisce delle linee guida per implementare un sistema di governance e di management efficiente.
Tale strumento però non è compreso a sufficienza dalle aziende, le quali non lo conoscono e perciò non lo applicano. Lo conoscono per lo più le aziende strutturate con un dipartimento IT adeguatamente formato, a differenza delle aziende piccole che non hanno le risorse, sia umane che monetarie, per dedicare alla governance IT la giusta attenzione.
Anche riguardo la cybersicurezza ci sono ancora delle lacune. Con il passare del tempo le società comprendono l'importanza di implementare un sistema di gestione della sicurezza delle informazioni dato dal fatto che i possibili attacchi sono molto costosi poi da riparare.
Le imprese dovrebbero sicuramente implementare dei progetti di formazione per i dipendenti in quanto gli attacchi colpiscono il personale aziendale che riceve *e-mail* e naviga sul web soprattutto, perciò il personale amministrativo. Informare questi soggetti sulla pericolosità di questi attacchi ridurrebbe notevolmente il rischio a cui è sottoposta un'impresa.

Le domande poste al revisore IT e le risposte hanno approfondito il tema trattato in questo elaborato, portando alla luce aspetti interessanti e spunti di riflessione che potevano essere evidenziati solo grazie ad un soggetto operante nel campo.
L'intervista ha perciò soddisfatto positivamente gli obiettivi che erano stati prefissati inizialmente.

CONCLUSIONE

Come è stato ampiamente descritto in questa trattazione, l'introduzione dell'aggiornamento dell'ISA 315 ha introdotto l'obbligo esplicito rivolto al revisore di comprendere e valutare l'ambiente IT delle società sottoposte a revisione. Il revisore, infatti, non è più un soggetto che osserva esclusivamente il bilancio e le scritture contabili, ma gli è richiesta una formazione e un'esperienza professionale che gli permetta di valutare l'azienda nel suo complesso, considerando anche la componente IT. Gli sono richieste competenze sempre più trasversali al fine di individuare e valutare i rischi di errori significativi a livello di bilancio.
Proprio perché il revisore finanziario non ha sempre le competenze adatte in tema IT, nei casi di ambienti IT molto complessi interverrà il revisore IT che collaborerà con il revisore finanziario per individuare i rischi e per valutare i controlli IT implementati dalle società.
Il revisore IT supporta il revisore finanziario ogni qualvolta siano necessarie le sue competenze tecniche, ma i due soggetti hanno lo stesso obiettivo finale: riuscire ad emettere un giudizio sul bilancio d'esercizio per attestarne la correttezza e la veridicità. I due *team* collaboreranno e comunicheranno costantemente le evidenze ottenute attraverso i test e le procedure svolte al fine di individuare e valutare eventuali rischi che potrebbero incidere sul bilancio d'esercizio.
Questa collaborazione, perciò, è fondamentale per svolgere un incarico di revisione adeguato e nel rispetto del principio di revisione ISA 315.

L'aggiornamento relativo all'ISA 315 ha modificato sostanzialmente l'attività di revisione attraverso l'obbligo esplicito di analizzare e comprendere il sistema informativo di un'azienda, incrementando sempre di più la necessità di servirsi di un revisore IT. I numerosi esempi relativi agli aspetti da comprendere e relativi ai controlli aiutano il revisore nel proprio lavoro in quanto può utilizzarli come supporto durante la sua attività.
Le aziende però hanno tutte caratteristiche diverse che possono dipendere ad esempio dal mercato di appartenenza, dalla struttura societaria, dal prodotto/servizio venduto e

da molte altre componenti. È importante che il revisore abbia le competenze e l'esperienza per saper riadattare gli esempi alla situazione reale che si trova di fronte.
L'aggiornamento, anche se probabilmente già obsoleto a causa della velocità con cui si evolve l'informatica, è stato un punto di partenza che ha confermato l'importanza della comprensione della componente IT per l'individuazione di eventuali errori significativi.
L'uso della tecnologia all'interno delle società è diventato ormai fondamentale nello svolgimento di qualsiasi processo al fine di renderlo più efficiente ed efficace, dai processi amministrativi a quelli operativi. L'evoluzione dell'uso della tecnologia all'interno delle aziende è stata rapidissima, partendo da computer obsoleti arrivando a tecnologie emergenti come robot, *blockchain* e utilizzando l'intelligenza artificiale. La tecnologia, soprattutto quella di nuova generazione, consente alle aziende di ottenere dei benefici e dei risultati che non avrebbero mai potuto raggiungere senza.
Proprio per l'uso a 360° dell'IT, la maggior parte dei rischi IT incide anche sull'informativa di bilancio. La tecnologia infatti governa i dati, i quali, una volta elaborati, diventeranno informazioni essenziali per la società: sia per l'informativa finanziaria che per poter prendere delle decisioni. Proprio per questo motivo diventa essenziale per le società governare in modo efficace la componente informatica.
Il *framework* COBIT, il quale è stato descritto nel secondo capitolo, è uno strumento fondamentale in quanto permette di definire dei processi di governance e di management dell'ambiente IT efficiente: sulla base degli obiettivi degli *stakeholder*, i quali vengono allineati con gli obiettivi aziendali IT, sono definite le risorse IT ottimali (sia dal punto di vista tecnico che relative al capitale umano) per poter strutturare e gestire un sistema IT efficiente ed efficace. Permette infatti di raggiungere gli obiettivi prefissati attraverso una struttura tecnologica adeguata.
È uno strumento che dovrebbe essere più diffuso in quanto, come evidenziato dall'intervista svolta, non è conosciuto e compreso a sufficienza dalle società e dai propri responsabili IT, e perciò poco utilizzato. Il fatto che le aziende non comprendano l'importanza di progettare un sistema informativo efficiente potrebbe essere un problema, soprattutto alla luce dei numerosi rischi correlati all'IT.
La conoscenza di questo strumento dovrebbe essere alla base anche della formazione di un revisore IT; sia se si tratta di un revisore IT interno che esterno. Il revisore IT interno dovrebbe conoscerlo per poterlo applicare nell'azienda in cui lavora al fine di controllare e progettare un sistema informativo adeguato. Nel caso di revisore esterno

invece, la sua conoscenza è fondamentale al fine di valutare il sistema e i controlli IT delle aziende revisionate.

Governare efficacemente l'IT risulta fondamentale anche al fine di contrastare i principali rischi IT. Come abbiamo visto nei capitoli precedenti sono svariati, ma uno dei rischi che si è maggiormente diffuso negli ultimi anni, anche a seguito della pandemia da Covid-19, è il rischio di attacchi alla cybersicurezza. Questi attacchi infatti mettono a rischio i dati e le informazioni dell'azienda e dei suoi dipendenti e allo stesso tempo possono Gli attacchi sono aumentati e se le aziende non mettono in atto delle attività di formazione e di prevenzione adeguate saranno maggiormente esposte al rischio.
Come ha evidenziato l'*IT Auditor* intervistato infatti, la formazione in tal senso è fondamentare e deve essere implementata in qualsiasi tipo di società, dalle più piccole alle più grandi. Come rappresentato graficamente dalla figura 2.2.1 questa formazione, anche se svolta, spesso non risulta efficace a contrastare tali rischi in quanto i dipendenti aziendali non si sentono sicuri riguardo queste tematiche. Questa formazione, perciò, dovrebbe essere svolta in modo più consapevole al fine di ottenere dei risultati positivi e di conseguenza un'esposizione al rischio minore.
Anche l'obbligatorietà della conformità alla normativa sulla *privacy*, ovvero il regolamento GDPR, ha rafforzato e sensibilizzato le aziende riguardo il tema della cybersicurezza, anche se si tratta di sicurezza relativa ai dati personali è un punto di partenza.
La certificazione ISO 27001, anche se non obbligatoria, dovrebbe comunque essere svolta dalle società per implementare dei sistemi di gestione della sicurezza al fine di aumentare la fiducia dei soggetti che si interfacciano con l'azienda e per rendere le informazioni aziendali sicure. La sicurezza relativa ai dati è fondamentale, in quanto i dati sono un elemento essenziale per qualsiasi azienda e se essi venissero danneggiati, rubati oppure manomessi si andrebbe incontro a conseguenze monetarie e gestionali gravissime. Tali conseguenze potrebbero mettere in dubbio la continuità dell'azienda.

La disciplina relativa all'IT ha molte norme di riferimento, le quali sono state ampiamente descritte nei capitoli precedenti. Possono essere riassunte così:

- ➔ i principi di revisione, nello specifico l'ISA 315: tali principi hanno l'obiettivo di definire le regole e le procedure che deve seguire un revisore, nello specifico

anche il revisore IT, al fine di comprendere un sistema IT per individuare rischi di errori significativi a livello di bilancio e a livello di asserzioni;

- ➔ il *framework* COSO, ovvero lo strumento utilizzato per progettare un sistema di controllo interno adeguato;
- ➔ il *framework* COBIT, ovvero lo strumento utilizzato al fine di implementare un sistema di controllo interno orientato alla componente IT, il quale definisce processi di governance IT e processi di management IT efficienti sulla base degli obiettivi aziendali;
- ➔ la normativa SOX, la quale prevede l'obbligo per le aziende quotate alla borsa americana di implementare un sistema di controllo efficace, il quale dovrà essere documentato dalla società e certificato da un revisore esterno;
- ➔ ISO 27001, ovvero la certificazione che attesta l'implementazione di un sistema di gestione delle informazioni efficace;
- ➔ il regolamento europeo GDPR, che si occupa di trattamento dei dati personali.

Non esiste perciò una legge univoca che può essere seguita per comprendere e valutare un ambiente IT. Nel presente elaborato non sono state trattate tutte le normative vigenti e certificazioni possibili in tema IT, ma sono stati analizzati gli strumenti e le norme più importanti e maggiormente conosciute. Conoscere l'insieme normativo permette di avere una comprensione globale sugli aspetti rilevanti relativi ad un sistema IT in termini di governance, management, gestione e valutazione del rischio IT, sicurezza e privacy. Tale conoscenza permette di strutturare un sistema IT con processi IT e controlli adeguati al fine di contrastare i rischi IT generali e i rischi legati alla cybersicurezza con l'obiettivo di far fluire le informazioni in azienda in modo efficiente, sicuro, protetto, consapevole e responsabile in relazione alla normativa sulla *privacy*.

L'ISACA emette periodicamente nuove *best practice* che potrebbero aiutare il revisore IT nel proprio lavoro. Soprattutto alla luce della velocità con cui si espande questo campo, è importante essere sempre aggiornati e conoscere nuovi modelli di gestione e valutazione del rischio della componente IT.

BIBLIOGRAFIA

AA. VV., *Analyzing COBIT 5 IT Audit Framework Implementation using AHP Methodology Mutiara*, Documento di Ricerca, Volume 1 n. 2, JOIV: International Journal on Informatics Visualization, 2017.

AA. VV., *Assirevi Monografie – L'evoluzione della governance e dei rischi di Information Technology, Modelli di governo da considerare per un'efficace gestione dei rischi legati alla tecnologia*, Documento di Ricerca, Assirevi, 04 Maggio 2023.

AA. VV., *Basis for conclusions (october 2019) preparared by the staff of the IAASB, Internation Standard on Auditing 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement Including Conforming and consequential amendments to other international standards,* Documento in Pubblica Consultazione, IFAC, December 2019.

AA. VV., *Clarified International Standards on Auditing – Findings from the post-implementation Review*, Documento in Pubblica Consultazione, IFAC, Luglio 2013.

AA. VV., *Cobit 5 an ISACA Framework, L'infrastruttura aziendale per la governance ed il management dell'IT*, Documento di Pubblica Consultazione, traduzione italiana, ISACA, 2012.

AA. VV., General IT Control (ITGC), Risk and Impact, Documento in Pubblica Consultazione, Deloitte, Novembre 2018.

AA. VV., *Global Technology Audit Guide (GTAG) 8: Auditing Application Controls,* Documento in Pubblica Consultazione, *The Institute of Internal Auditors, 2009.*

AA. VV., *Introduzione ai Principi di Revisione Internazionali (ISA Italia) elaborati ai sensi dell'art. 11 del Decreto Legislativo 27 gennaio 2010, n. 39,* Documento in pubblica consultazione, Ministero dell'Economia e delle Finanze, 2022.

AA. VV., *ISA 315 (Revised 2019), Identifying and Assessing the Risks of Material Misstatement, First-Time Implementation Guide*, Documenti in Pubblica Consultazione, IFAC, Luglio 2022.

AA. VV., *IT Audit Framework (ITAF™) "A Professional practices Framework for IT Auditor"*, 4th edition, Documento in Pubblica Consultazione, ISACA, 2020.

AA. VV., *IT Audit Manual 2017*, Documenti in Pubblica Consultazione, prima edizione, Afrosai-e, 01 Novembre 2017.

AA. VV., *L'applicazione dei principi di revisione internazionali alle imprese di dimensioni minori*, Documento in Pubblica Consultazione, Consiglio Nazionale dei Dottori Commercialisti e degli esperti contabili, 2011.

AA. VV., Manual of Information Technology Audit, Volume I, Documenti in Pubblica consultazione, Office of the Comptroller & Auditor General of India.

AA. VV*., Normativa "protezione dei dati personali" per i casi di revisione (legale e volontaria) e incarichi disciplinati da legge o regolamenti*, Documento di Ricerca n.227, Assirevi, Febbraio 2019.

AA. VV., *Phishing defense and governance, How to Improve User Awareness, Enhance Controls and Build Process Maturity*, Documento di Pubblica Consultazione, ISACA, 2019.

AA. VV., *Regolamento generale sulla protezione dei dati (GDPR), Guida alla conformità,* Documento di Pubblica Consultazione, IT governance, Maggio 2018.

AA. VV., *Sicurezza delle informazioni e ISO 27001*, Documento di Pubblica Consultazione, IT Governance, Gennaio 2018.

AA. VV., *Strategy for 2015–2019: Fulfilling Our Public Interest Mandate in an Evolving World*, Documento in Pubblica Consultazione, IFAC, Dicembre 2014.

AA. VV., *Taking Control, A Guide to Compliance with Section 404 of the Sarbanes-Oxley Act of 200,* Documento in Pubblica Consultazione, Deloitte, 2004.

AA. VV., *Work Plan for 2015–2016: Enhancing Audit Quality and Preparing for the Future,* Documento in Pubblica Consultazione, IFAC, Dicembre 2014.

Basso A., *Revisione legale e crisi d'impresa: il caso del Gruppo Stefanel,* Università Ca' Foscari Venezia, 2022, http://hdl.handle.net/10579/22494.

Biener C., Eling M., Hendrik Wirfs J., *Insurability of Cyber Risk: An Empirical*, Vol. 40, Documento di Ricerca, Springer, Giugno 2014.

Bozzola M, Faedo I., *Sarbanes- Oxley Act, Sezione 404 (Internal control over Financial reporting)*, Documento in Pubblica Consultazione, E&Y, 22 novembre 2010.

European Investment Bank, *Digitalisation in Europe 2021-2022, Evidence from the EIB Survey,* Documento di Pubblica Consultazione, 2022.

Frigerio C., Maccaferri F., Rajola F., *ICT e società dell'informazione*, McGraw Hill, Milano, 2019.

Graham L., *Internal control audit and compliance, Documentation and Testing under the New COSO Framework*, Wiley Corporate F&A, 2015.

Lahti C., Peterson R., *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools*, Synngress, 2015.

Luciano M., *Revisione aziendale e sistemi di controllo interno*, Quarta edizione, Giuffrè Francis Lefebvre, Milano, 2019.

Ministero dell'Economia e delle Finanze, *Principi di Revisione Legale Handbook 2020, Edizione in lingua italiana,* Documento di Pubblica Consultazione, Roma, Ottobre 2020.

Moeller R., *Executive's guide to governance, Improving Systems Processes with Service Management, COBIT and ITIL*, Wiley Corporate F&A, 2013.

Pesenato A., *COSO Report I e COSO Framework SCIGR: loro applicazione nella revisione legale e nel MOGC ex D.Lgs 231/2001*, Documento di Pubblica Consultazione n. 256, Periodico "Il commercialista veneto", Associazione dei Dottori Commercialisti e degli Esperti Contabili delle Tre Venezie, 2020.

Pighin M., Marzona A., *Sistemi informativi aziendali, ERP e sistemi di data analysis, Terza edizione*, Pearson, Milano, 2018.

SITOGRAFIA – ARTICOLI

Aa. Vv.„ *Top Risks and Rewards of Moving to the Cloud, ISACA, 14 Marzo 2023* https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/top-risks-and-rewards-of-moving-to-the-cloud

Antonielli A, *Riconoscere e difendersi dai Malware: significato, esempi e tipologie più comuni*, Politecnico di Milano, 21 Gennaio 2021 https://blog.osservatori.net/it_it/malware-significato-esempi-riconoscerli

Associazione Italiana delle Società di Revisione Legale (Assirevi), https://www.assirevi.com/

Associazione Italiana IS Auditor (AIEA), https://www.aiea.it/

Coletta M., *I rischi di errori significativi per il revisore*, Documento in Pubblica Consultazione, La revisione Legale rivista online del revisore legale e del sindaco, 2020, https://www.larevisionelegale.it/2020/10/04/i-rischi-di-errori-significativi-per-il-revisore/

Delinea, *Delinea recognized as a Leader again in the 2022 Gartner Magic Quadrant for Privileged Access Management, Documento di ricerca, 19 Luglio 2022,* Message from Delinea

Deloitte&Touche S.p.A., https://www2.deloitte.com/it/it.html

Ernst&Young S.p.A., https://www.ey.com/it_it

IAASB, https://www.iaasb.org/

IBM, https://www.ibm.com/it-it

IBM, Cloud Computing, 2022, https://www.ibm.com/it-it/topics/cloud-computing

IBM, *Cos'è il Phishing?*, 2022, https://www.ibm.com/it-it/topics/phishing

Information Systems Audit and Control Association (ISACA), https://www.isaca.org/

International Federation of Accountants (IFAC), https://www.ifac.org/

Ministero dell'Economia e delle Finanze (MEF), https://www.mef.gov.it

Ordine dei Dottori commercialisti e degli Esperti Contabili di Roma, https://www.odcec.roma.it/

Revisione legale -MEF, https://www.revisionelegale.mef.gov.it/opencms/opencms/

Rigoni A., *I 3 principi chiave della sicurezza informatica: la triade CIA*, Cyberment, https://cyberment.it/sicurezza-informatica/3-principi-chiave-della-sicurezza-informatica/

Rotich R., What is an IT Auditor? (with Duties, Skills and Salary), Indeed, 28 Dicembre 2022, https://www.indeed.com/career-advice/finding-a-job/what-is-it-auditor

Sarbanes Oxley Act, Sarbanes- (SOX) Audit Requirements (sarbanes-oxley-101.com)

Symantec, *Internet Security Threat Report*, volume 23, March 2018, www.symantec.com/security-center/threat-report

TusciaFisco.it La scelta giusta in materia fiscale, https://www.tusciafisco.it/

RIFERIMENTI NORMATIVI E PRINCIPI DI REVISIONE

Codice Civile, Regio Decreto 16 marzo 1942, n. 262, pubblicato in G.U. il 4 aprile 1942, n. 79.

Decreto Legislativo 17 luglio 2016, n. 135: "Attuazione della direttiva 2014/56/UE, che modifica la direttiva 2006/43/CE concernente la revisione legale dei conti annuali e dei conti consolidati", pubblicato in G.U. il 21 luglio 2016, n. 169.

Decreto Legislativo 27 gennaio 2010, n. 39: "Attuazione della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati", che modifica le direttive 78/660/CEE e 83/349/CEE, e che abroga la direttiva 84/253/CEE, pubblicato in G.U. il 23 marzo 2010, n. 68, Supplemento Ordinario n. 58.

Direttiva 2006/43/CE del Parlamento Europeo e del Consiglio, del 17 maggio 2006, relativa alle revisioni legali dei conti annuali e dei conti consolidati, che modifica le direttive 78/660/CEE e 83/349/CEE del Consiglio e abroga la direttiva 84/253/CEE del Consiglio, pubblicata in G.U.U.E. il 9 giugno del 2006, n. L157.

Legge 28 dicembre 2005, n. 262: *Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*, pubblicato in G.U. il 28 dicembre 2005, n.301.

Regolamento (UE) n. 537/2014 del Parlamento Europeo e del Consiglio del 16 aprile 2014, relativo ai requisiti specifici della revisione legale dei conti di enti di interesse pubblico e che abroga la decisione 2005/909/CE della Commissione, pubblicato in G.U.U.E. il 27 maggio 2014, n. L158.

Regolamento (UE) n. 678/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE della Commissione (regolamento generale sulla protezione dei dati), pubblicato in G.U.U.E. il 04 maggio 2016, n. L119, applicabile dagli Stati membri dal 25 maggio 2018.

Principio di Revisione Internazionale (ISA Italia) 200: Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionali.

Principio di Revisione Internazionale (ISA Italia) 220: Controllo della qualità dell'incarico di revisione contabile del bilancio.

Principio di Revisione Internazionale (ISA Italia) 230: La documentazione della revisione contabile.

Principio di Revisione Internazionale (ISA Italia) 240: Le responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio.

Principio di Revisione Internazionale (ISA Italia) 260: Comunicazione con i responsabili delle attività di governance.

Principio di Revisione Internazionale (ISA Italia) 265: Comunicazione delle carenze nel controllo interno ai responsabili delle attività di governance ed alla direzione.

Principio di Revisione Internazionale (ISA Italia) 315: L'identificazione e la valutazione dei rischi di errori significativi.

Principio di Revisione Internazionale (ISA Italia) 320: Significatività nella pianificazione e nello svolgimento della revisione contabile.

Principio di Revisione Internazionale (ISA Italia) 330: Le risposte del revisore ai rischi identificati e valutati.

Principio di Revisione Internazionale (ISA Italia) 500: Elementi probativi.

Principio di Revisione Internazionale (ISA Italia) 540: Revisione delle stime contabili, incluse le stime contabili del fair value, e della relativa informativa.

Principio di Revisione Internazionale (ISA Italia) 610: Utilizzo del lavoro dei revisori interni.

Principio di Revisione Internazionale (ISA Italia) 701: Comunicazione degli aspetti chiave della revisione contabile nella relazione del revisore indipendente.

Principio Internazionale sugli Incarichi di Assurance (ISAE) 3400: L'esame dell'informativa finanziaria prospettica.

The International Auditing Practices Committee: CAATs.