UNIVERSITÀ
DI PAVIA

Dipartimento di Scienze Economiche e Aziendali

Corso di Laurea magistrale in Economia e Legislazione d'Impresa

---

PRINCIPIO DI REVISIONE ISA 315 REVISED: ASPETTI CONCETTUALI E IMPATTI OPERATIVI

Relatore:

Chiar.mo Prof. Mauro Porcelli

Tesi di Laurea
di Asia Schilhan

Matr. n.523182

Anno Accademico 2023-2024

INDICE

INTRODUZIONE

Questo elaborato si concentra sul Principio di Revisione ISA Italia 315 “L’identificazione e valutazione dei rischi di errori significativi”. Tale principio non presenta peculiarità in termini di applicazione rispetto al principio internazionale.

A partire dai bilanci del 2022, è entrato in vigore il nuovo ISA Italia 315, il quale pone un'enfasi maggiore sull'approccio basato sui rischi durante l'attività di *audit*. Il nuovo principio sostituisce la versione precedente, "L’identificazione e valutazione dei rischi di errori significativi mediante la comprensione dell’impresa e del contesto in cui opera" applicabile ai bilanci dei periodi amministrativi precedenti. Questo implica che per le aziende sottoposte a revisione diventa cruciale la presenza di un sistema di controllo interno che sia efficace ed efficiente, un ambiente IT adeguatamente strutturato e un attento monitoraggio dei rischi.

La revisione del nuovo ISA Italia 315 evidenzia l'importanza, per il revisore, di identificare e valutare i rischi di errori significativi, ponendo particolare attenzione al ruolo del sistema di controllo interno, finalizzato a mitigare la presenza di eventuali errori nei bilanci[1]. A tal fine il principio fornisce un approccio coerente nell’ambito delle procedure di identificazione e valutazione dei rischi, in questo modo tutte le società di revisione avranno delle linee guida precise su come operativamente effettuare tale analisi, portando quindi ad una applicazione omogenea del principio.

I principi di revisione richiedono al revisore di ottenere una ragionevole sicurezza che il bilancio nel suo insieme non contenga errori significativi,

[1] Ladogana S., Santovito G., *Il principio di revisione ISA Italia 315: principali impatti attesi*, in “Amministrazione & Finanza”, 2023, pag.36

siano essi causati da frode o da eventi non intenzionali[2]. Un rischio di revisione è considerato significativo quando la sua manifestazione ha un impatto tale da influenzare le decisioni economiche degli stakeholder. È fondamentale notare che il giudizio del revisore si riferisce al bilancio nel suo complesso; di conseguenza, non è responsabile per l'individuazione di errori non significativi. Gli errori che possono portate a un bilancio significativamente errato includono sia il rischio intrinseco, ovvero rischio che il bilancio possa presentare errori significativi indipendentemente dall'efficacia del sistema di controllo interno, che il rischio di controllo, ovvero il rischio che un errore potenzialmente significativo non venga prevenuto, individuato e corretto tempestivamente dal sistema di controllo interno dell'impresa. Rispetto al principio ante revisione viene indicata in maniera esplicita quale debba essere l'approccio di revisione in ambito attività di controllo a fronte dell'individuazione di determinate tipologie di rischi intrinseci. Il nuovo principio favorisce delle risposta di revisione che rispetto al passato risultano essere più mirate a fronte di processo di *risk assessment* maggiormente strutturato.

Tra i fattori che influenzano il rischio intrinseco, chiamati appunto "fattori di rischi intrinseco", si riscontrano la complessità delle operazioni che derivano dalla natura e dalla modalità di predisposizione delle informazioni, la soggettività legata a valutazioni che possono generare risultati diversi, i cambiamenti in seguito a eventi o condizioni che influenzano l'attività dell'impresa e l'incertezza presente quando le informazioni non possono essere elaborate basandosi esclusivamente su dati precisi. Rispetto al passato il principio oltre a specificare che il revisore deve considerare e analizzare i fattori di rischio intrinseco esplicita anche quali essi siano.

[2] IAASB, Principio di revisione internazionale (ISA Italia) 200, "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionali", 2020, par. 5

In merito ai controlli che la società deve implementare, siano essi manuali o automatici si elencano le autorizzazioni e approvazioni necessarie per garantire la validità delle operazioni, le riconciliazioni utili per confrontare i dati e identificare eventuali differenza, verifiche che confrontano voci diverse o una voce con una direttiva attivando così azioni correttive in caso di incoerenza, e infine controlli sui beni fisici comprendenti le adeguate misure di sicurezza adottate dall'azienda.

Affinché ogni controllo sia efficace, è essenziale che ci sia una segregazione delle funzioni, mirata a ridurre l'opportunità di perpetrare e nascondere errori involontari o frodi.

Tra le novità introdotte nel nuovo ISA Italia 315 troviamo il concetto di spettro del rischio, al fine di effettuare una corretta e precisa valutazione del rischio. Lo spetto del rischio prevede come nel precedente principio che il rischio si determini dalla combinazione della probabilità con cui si verifica l'evento e dalla rilevanza dell'impatto conseguente, ma introduce una scala di valutazione che rende maggiormente oggettiva l'identificazione dei rischi meno che remoti, remoti e più che remoti. Di conseguenza la valutazione di tale misura del rischio andrà ad impattare sull'approccio di revisione.

Un ulteriore aspetto introdotto nel nuovo principio di revisione è il concetto di scalabilità, ovvero in relazione alla valutazione del rischio le procedure di revisione variano, per le voci di bilancio che risultano essere significative l'approccio sarà maggiormente dettagliato rispetto a voci che non vengono classificate come significative.

Un elemento trattato in maniera più approfondita riguarda l'ambiente di controllo interno dell'impresa, delineato attraverso manuali di direttive e procedure. Tale sistema è attuato principalmente dalla direzione e dai responsabili della governance.

L'ambiente di controllo include diversi elementi fondamentali:

- Responsabilità della Direzione: Le modalità con cui la direzione svolge i propri compiti, offrendo un esempio di integrità e valori etici che costituiscono la base della cultura aziendale.
- Attribuzione di Poteri e Responsabilità: Come l'impresa distribuisce poteri e responsabilità per il raggiungimento degli obiettivi, assicurandosi che le direttive siano comprese e che il personale disponga degli strumenti necessari.
- Supervisione Indipendente: Le modalità di supervisione sull'operato dell'impresa, come l'organizzazione delle attività del reparto di *internal audit*, del collegio sindacale e dell'organismo di vigilanza, garantendo loro indipendenza e integrità.
- Responsabilizzazione: Come l'impresa responsabilizza il personale per il conseguimento degli obiettivi del sistema di controllo interno, attraverso sistemi incentivanti e misurazione delle performance.
- Gestione del Personale: Le modalità attraverso cui l'impresa recluta, forma e fidelizza personale competente, comprendendo politiche di assunzione e formazione.

Infine, nel nuovo principio ha particolare rilevanza l'ambiente IT. Il sistema di controllo interno di un'impresa combina elementi manuali e automatizzati, variando in base alla complessità dell'uso degli strumenti informatici. L'utilizzo dell'IT influisce su come vengono elaborate, archiviate e comunicate le informazioni necessarie per la redazione del bilancio, configurando così il sistema di controllo interno. Con l'aumentare della complessità e del volume dei dati, un ambiente IT efficace diventa sempre più importante. I revisori devono valutare i rischi legati all'ambiente IT, come l'accesso non autorizzato ai dati, privilegi eccessivi del personale IT, modifiche non autorizzate alle applicazioni e potenziali

perdite di dati. Il nuovo ISA Italia 315 dedica particolare attenzione alla comprensione e valutazione dei controlli, sottolineando l'importanza di un adeguato ambiente IT e processi automatizzati per aziende di medie e grandi dimensioni, al fine di minimizzare errori umani e omissioni nel controllo.

Nel primo capitolo verrà trattato in generale l'attività di revisione, quindi il ruolo del revisore, quali sono i suoi doveri e come si sviluppa il processo di revisione, introducendo poi il Principio di Revisione ISA Italia 315 Revised. Nel secondo capitolo invece, vengono trattati nel dettaglio tutti quegli elementi di novità presenti all'interno del nuovo principio e le varie differenze con il precedente principio. Il terzo e ultimo capitolo nasce dall'esperienza di stage effettuata presso una società di revisione, nella quale si esplicita come viene applicato tale principio nella realtà operativa del processo di revisione.

CAPITOLO 1

REVISIONE LEGALE DEI CONTI

Il Principio di Revisione 315 Revised[3] è uno standard che stabilisce linee guida e regole per il processo di revisione delle informazioni finanziarie di un'azienda da parte di un revisore. Questo principio influisce sul modo in cui il revisore affronta il processo di revisione, nello specifico nell'identificazione e valutazione dei rischi ed errori significativi, individuando i criteri sulla cui base il revisore imposta la propria attività di valutazione del rischio inerente e del rischio di controllo e, rispetto a ciò, le proprie procedure di verifica.

Il progetto di revisione dell'ISA 315 (Revised 2019) è stato avviato all'inizio del 2016 per rispondere ai risultati chiave del progetto di monitoraggio dell'implementazione degli ISA da parte dello IAASB[4]. I risultati di tale progetto hanno dimostrato che:

- Esisteva un'incoerenza nella natura e nel numero dei rischi significativi identificati nella pratica;
- La comprensione del sistema di controllo interno è di difficile applicazione nella pratica;
- I rischi legati all'Information Technology (IT) non sono stati sufficientemente trattati nello standard.

Sono state inoltre evidenziate le difficoltà di applicazione dell'ISA 315 nella revisione contabile delle piccole medie imprese (PMI).

[3] IAASB, Principio di revisione internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019

[4] I principi internazionali dello IAASB comprendono i principi internazionali di revisione contabile (ISA), i principi internazionali sugli incarichi di revisione (ISRE), i principi internazionali sugli incarichi di assurance (ISAE) e i principi internazionali sui servizi correlati (ISRS)

Nel settembre 2016, lo IAASB ha approvato una proposta di progetto per la revisione dell'ISA 315 (Revised) con i seguenti obiettivi[5]:

- Proporre una revisione dell'ISA 315 (Revised), stabilendo requisiti più solidi e indicazioni adeguatamente dettagliate per spingere i revisori a svolgere procedure di valutazione del rischio appropriate e commisurate alle dimensioni e alla natura dell'entità. È stato previsto che queste revisioni si concentrino sul miglioramento dell'approccio del revisore alla comprensione dell'entità, del suo ambiente e delle attività di valutazione del rischio alla luce dell'evoluzione del contesto;

- Determinare se e come l'ISA 315 (Revised), nella sua organizzazione e struttura, possa essere modificato per promuovere una valutazione del rischio più efficace;

- Proporre modifiche conseguenti ad altri principi che potrebbero essere necessarie a seguito delle revisioni dell'ISA 315 (Revised);

- Determinare quali linee guida e strumenti di supporto dovrebbero essere sviluppati dallo IAASB per favorire l'effettiva applicazione.

Nella riunione di Giugno 2018, lo IAASB ha approvato la proposta per l'esposizione al pubblico dell'ISA 315 Revised. Ha inoltre convenuto che la data di implementazione effettiva di tale ISA per le revisioni contabili dei bilanci che iniziano il 15 dicembre 2021 o in data successiva sarebbe appropriata, in quanto, essendo un principio fondamentale le imprese avranno bisogno di tempo per aggiornare le metodologie e gli strumenti di revisione, sviluppare il materiale formativo e formare il personale in modo

[5] IAASB, Basis for conclusions preparared by the staff of the IAASB, Internation Standard on *Audit*ing 315 (Revised 2019) Identifying and Assessing the Risks of Material Misstatement Including Conforming and consequential amendments to other international standards, October 2019

da riflettere le modifiche apportate all'ISA 315 (Revised). Un periodo di implementazione troppo breve potrebbe comportare un'implementazione affrettata o inefficace.

Per comprendere però appieno l'effetto del Principio di Revisione 315 Revised sul processo di revisione, è importante definire cosa si intende per revisione legale e quali sono le attività svolte dal revisore in questo contesto.

1.1 Il ruolo del Revisore Legale dei Conti e contesto Isa 315

A partire dal 7 aprile 2010, in Italia è obbligatoria l'attività di revisione contabile, in conformità con il Decreto Legislativo 39 del 2010[6] che recepisce la direttiva Europea 2006/43/CE2[7].

La revisione legale può essere definita come l'attività svolta da professionisti indipendenti i quali applicano statuite procedure, al fine di accertare la conformità del bilancio alla legge, tale attività conduce alla formazione e all'espressione di un giudizio professionale in merito all'attendibilità sostanziale del bilancio. A tal fine verranno applicati i Principi di Revisione *ISA* Italia, adottati con determina del Ragioniere Generale dello Stato del 23 dicembre 2014 (e successivamente modificati e integrati con diverse altre determine).

Gli ISA Italia sono una versione tradotta e leggermente modificata degli ISA Internazionali - *International Standard on Auditing* – che vengono emanati dallo IAASB - *International Auditing and Assurance Standards Board* – organo interno dell'IFAC - *International Federation of*

[6] 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.
[7] 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.

Accountants – che elabora i principi di revisione, in seguito tradotti, recepiti e integrati dai vari Stati.

Tali Principi sono un corpo di regole molto articolate che costituiscono le norme etico-professionali del revisore contabile indipendente, le norme tecniche di svolgimento della revisione in base alle quali il revisore può esercitare il proprio giudizio professionale e le norme di stesura della relazione di revisione. Agli albori della disciplina erano dei principi tecnici che indicavano solamente i test che andavano effettuati sulle voci di bilancio tralasciando tutto ciò che riguarda la valutazione del rischio.

L'ISA Italia 250 individua come responsabilità del revisore quella 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*"[8]. Per fare ciò, il revisore deve condurre la revisione in modo professionale, utilizzando le tecniche e gli strumenti appropriati per poter esprimere un parere professionale sul bilancio, secondo criteri di ragionevole sicurezza. Invece, il principio di revisione ISA Italia 200 tratta degli obiettivi generali del revisore nello svolgimento della revisione contabile del bilancio, inclusa l'acquisizione di elementi probativi sufficienti e appropriati per ridurre il rischio di revisione ad un livello accettabilmente basso[9]. Il rischio di revisione dipende dai rischi di errori significativi e dal rischio di individuazione[10]. Il principio di revisione ISA Italia 200 spiega che i rischi di errori significativi possono sussistere a due livelli[11]: a livello di bilancio nel suo complesso; a livello di asserzioni per classi di operazioni, saldi contabili e informativa di bilancio.

[8] IAASB, Principio di Revisione Internazionale (ISA Italia) 250, "La considerazione di leggi e regolamenti nella revisione contabile del bilancio", 2020, par. 5

[9] IAASB, Principio di Revisione Internazionale (ISA Italia) 200, "Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionali", 2020, par. 17

[10] Ivi, par. 13 c)

[11] Ivi, par. A37

Secondo il Principio di Revisione ISA Italia 315, per poter raggiungere tale obiettivo il revisore dovrà valutare non solo il sistema di controllo interno adottato dall'impresa, ma anche la sua comprensione del contesto in cui opera e la sua capacità di valutare in modo accurato e obiettivo i rischi a cui è esposta[12]. Solo attraverso una valutazione dettagliata di questi elementi, il revisore sarà in grado di stabilire le procedure di revisione più appropriate da seguire per mitigare i rischi individuati e accertare la conformità del bilancio alla legge.

1.2 Attività di Revisione

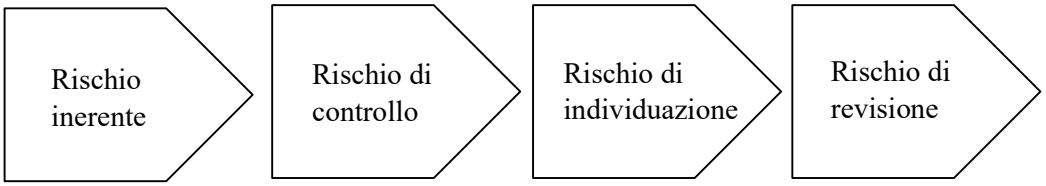
In questo paragrafo verranno illustrate le varie tipologie di rischi che caratterizzano il processo di revisione, com'è strutturata la revisione e in quali e quante fasi si divide.

Il concetto di ragionevole sicurezza implica la possibilità che il revisore non esprima un giudizio corretto. Questo rischio, definito come rischio di revisione, si presenta quando il revisore emette un giudizio favorevole su un bilancio contenente errori significativi o un giudizio negativo su un bilancio conforme alle normative vigenti. L'importanza di un'informazione contenuta in un bilancio è determinata dalla sua capacità di influenzare le decisioni di chi lo legge. In particolare, un'informazione si ritiene significativa quando la sua mancanza o inesattezza potrebbe portare a scelte errate da parte dei soggetti che si basano sul bilancio per prendere decisioni. Questo sottolinea l'importanza della completezza e dell'accuratezza delle informazioni fornite nel bilancio, al fine di garantire una corretta valutazione della situazione finanziaria di un'azienda e delle sue prospettive future.

[12] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 7

Il revisore, quindi, deve pianificare e svolgere il proprio lavoro al fine di ridurre il rischio di revisore ad un livello accettabilmente basso.

Il rischio di revisione può essere rappresentato come un susseguirsi di una serie di rischi che se non individuati e mitigati portano appunto come risultato al rischio di revisione:



Il rischio inerente (o intrinseco) e il rischio di controllo si inseriscono all'interno del Rischio di Errori Significativi in Bilancio (*Risk of Material Misstatement*).

Il concetto di Rischio Inerente si riferisce alla possibilità che ci sia un errore significativo nelle informazioni presenti nel bilancio aziendale, indipendentemente dall'efficacia del sistema di controllo interno. Si tratta di un aspetto fondamentale da valutare durante una revisione contabile, poiché può influenzare significativamente l'affidabilità dei dati finanziari.

La valutazione del rischio intrinseco, che può essere classificato come alto, moderato o basso, dipende interamente dal giudizio professionale del revisore contabile. Tale affermazione trova valore nell'ambito del processo di valutazione indipendente del rischio da parte del revisore finalizzata alla definizione della propria strategia di revisione

In sostanza, il rischio inerente rappresenta una componente essenziale nella valutazione della qualità e della veridicità delle informazioni finanziarie di un'azienda, e richiede un'attenta analisi da parte del revisore contabile per garantire la corretta rappresentazione della situazione economica, patrimoniale e finanziaria dell'ente.

Il rischio di controllo riguarda la possibilità che un errore, potenzialmente significativo, relativo a un saldo contabile o a un'informazione, non venga prevenuto o individuato e corretto tempestivamente dal sistema di controllo interno dell'impresa[13]. La valutazione di questo rischio, che può essere considerato alto, moderato o basso, dipende esclusivamente dal giudizio professionale del revisore. Come sopra citato ciò avviene nell'ambito del processo di valutazione indipendente del rischio da parte del revisore finalizzata alla definizione della propria strategia di revisione.

Il rischio intrinseco e il rischio di revisione sono strettamente collegati tra loro, poiché il primo influisce direttamente sul secondo. Pertanto, per valutare correttamente il rischio di revisione, è fondamentale considerare entrambi i tipi di rischio in modo congiunto anziché separatamente e in modo indipendente. La conoscenza del rischio risulta fondamentale per programmare la strategia generale di revisione e del piano di lavoro.

Il rischio di individuazione è il rischio che le procedure messe in atto dall'*audit*or per ridurre il rischio di revisione ad un livello accettabilmente basso non rilevino un errore che potrebbe avere un impatto significativo, sia singolarmente che in combinazione con altri errori. Questo rischio è gestito dal revisore il quale deve affrontarlo durante l'attività di revisione eseguendo le procedure appropriate come test di validità o sostanza e procedure di conformità. In altre parole, l'obiettivo è garantire che ogni errore rilevante venga individuato dalle procedure poste in essere dal revisore e corretto dalla società oggetto di revisione per garantire l'affidabilità e l'accuratezza dei report finanziari.

Ne consegue che tanto più è elevato il rischio di errori significativi in bilancio, tanto più numerose saranno le procedure di revisione da

[13] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 4

effettuare per poter ottenere adeguate evidenze sulla correttezza o non correttezza del bilancio.

Per poter stabilire con precisione il tipo e l'entità delle procedure di revisione da svolgere, è necessario valutare preventivamente il rischio di errore significativo per ciascuna asserzione di bilancio, il principio di revisione ISA 315 definisce le asserzioni 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. Le asserzioni sono utilizzate dal revisore per prendere in considerazione le diverse tipologie di errori potenziali che possono verificarsi quando identifica e valuta i rischi di errori significativi e definisce le relative risposte di revisione*"[14]. Questa valutazione permetterà di pianificare in modo adeguato le attività di revisione e di concentrare le risorse dove c'è maggiore probabilità di errore. La corretta valutazione del rischio permette di identificare le aree a maggior rischio e di effettuare un lavoro di revisione più mirato ed efficace.

L'approccio del revisore può essere un approccio orientato alla valutazione del rischio di controllo oppure un approccio di sostanza. L'approccio di controllo si basa sulla valutazione da parte del revisore dell'adeguatezza del sistema di controllo interno in termini di presidio del rischio inerente sotteso. L'analisi e il testing del sistema di controllo interno risultano essere fondamentali nelle società di maggiori dimensioni e per tutti quei settori che presentano un numero significativo e ricorrente di transazioni (es. società telefoniche, banche, assicurazioni). Questo approccio permette di comprendere al meglio le modalità di svolgimento delle operazioni

[14] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par 12 a)

aziendali, con impatto su tutte le transazioni svolte, riuscendo così a migliorare il livello di comfort ottenuto dalle attività svolte e riducendo, conseguentemente, le attività di dettaglio. Invece, l'approccio di sostanza si basa prevalentemente sull'effettuazione di procedure di revisione sui singoli saldi di bilancio. Viene utilizzato quando il sistema di controllo non risulta essere affidabile, oppure nonostante l'affidabilità del sistema di controllo la natura del rischio sotteso richiede comunque di svolgere attività di sostanza, quando le transazioni non sono particolarmente numerose e sulle stime di bilancio.

Per quanto riguarda le fasi del processo di revisione vengono suddivise nel seguente modo:

- Accettazione e mantenimento dell'incarico;
- Pianificazione "*Planning";*
- Svolgimento delle procedure di revisione "*Execution";*
- Espressione del giudizio professionale.

Accettazione e mantenimento incarico

Il revisore deve considerare sia aspetti qualitativi che quantitativi al fine di valutare se accettare un incarico, quali:

- Reputazione del cliente;
- Rapporto con revisore esterno;
- Attività svolta dall'azienda;
- Indipendenza;
- Etica professionale;
- Indicatori patrimoniali;
- Indicatori economici;
- Indicatori finanziati etc

I termini dell'incarico andranno poi concordati in un documento chiamato Lettera di incarico dove risulta:

- Obiettivo e natura dell'incarico;
- Responsabilità del revisore e della direzione;
- Identificazione quadro normativo di riferimento;
- Relazione da emettere;
- Tempi e corrispettivi.

Planning

Alla fase di pianificazione è dedicato un intero principio, l'ISA Italia 300 "Pianificazione della revisione contabile del bilancio".

"L'obiettivo del revisore è di pianificare la revisione contabile affinché sia svolta in modo efficace"[15].

La pianificazione della revisione richiede la definizione della strategia generale di revisione per l'incarico e la predisposizione di un piano di revisione. La strategia generale di revisione permette di identificare le caratteristiche dell'incarico che ne definiscano la portata, determinare gli obiettivi dell'incarico in termini di emissione di relazioni per pianificare la tempistica delle attività da svolgere, considerare fattori significativi nell'indirizzare l'attività di revisione, determinare la natura, la tempistica e l'entità delle risorse necessario per lo svolgimento dell'incarico[16].

Il revisore deve poi elaborare un piano di revisione che includa una descrizione della natura, tempistica ed estensione delle procedure di valutazione del rischio pianificate, delle procedure di revisione in risposta ai rischi identificati e valutati[17].

[15] IAASB, Principio di Revisione Internazionale (ISA Italia) 300, "Pianificazione della revisione contabile del bilancio", 2020, par. 4
[16] Ivi, par. 8
[17] IAASB, Principio di Revisione Internazionale (ISA Italia) 330, "Le risposte del revisore ai rischi identificati e valutati", 2020, par. 6

Execution

Durante la fase di esecuzione dell'incarico di revisione, vengono svolte attività relative allo svolgimento delle procedure di revisione previste dal programma di lavoro, tra le quali possono includersi:

- Procedure di conformità: test e valutazione del sistema di controllo interno. Vengono svolte per ottenere elementi probativi sull'esistenza e sull'efficacia dei controlli aziendali e per verificare che tali controlli vengano svolti durante tutto l'arco dell'anno.
- Procedure di validità: test dei saldi di bilancio

Espressione del Giudizio

Nella fase conclusiva il revisore effettuerà un riesame dell'attività svolta, valutazione delle evidenze raccolte e degli eventi successivi, otterrà la lettere di attestazione. Al termine di questa fase, il revisore attraverso il rilascio della relazione di revisione, esprime il proprio giudizio professionale in merito alla conformità del bilancio, in tutti gli aspetti significativi, al quadro normativo di riferimento.

1.3 Introduzione a ISA 315 (Revised), Identificazione e Valutazione dei rischi di errori significativi

Il principio ISA 315 Revised è in vigore dal 15 dicembre 2021 e quindi applicabile per le revisioni contabili dei bilanci relativi ai periodi amministrativi che iniziano dal 1° Gennaio 2022, questa rivisitazione si è resa necessaria al fine di ottenere una più solida identificazione e valutazione dei rischi, promuovendo così risposte più adatte ai rischi identificati. Al fine di garantire chiarezza e coerenza di applicazione, i requisiti rivisitati esplicitano cosa deve fare il revisore e vanno a migliorare, modernizzare e riorganizzare il materiale applicativo per descrivere il "perché" e il "come" le procedure devono essere intraprese;

quindi, supportare i revisori che utilizzano il principio incorporando materiale di guida che riconosca l'evoluzione dell'ambiente, anche in relazione ai sistemi IT.

I cambiamenti principali che sono stati apportati riguardano[18]:

- Rafforzamento relativo all'esercizio dello scetticismo professionale. Risultava essere di interessa pubblico migliorare l'applicazione dello scetticismo professionale nelle revisioni contabili. Gli enti regolatori di revisione hanno evidenziato notevole preoccupazioni sul modo in cui i revisori, in alcuni casi, eseguono procedure di valutazione del rischio in cui lo scetticismo professionale non sembra essere applicato in modo appropriato. Il feedback dalle consultazioni dello IAASB ha dimostrato che i revisori trovano più difficile applicare un adeguato scetticismo professionale senza una chiara comprensione dell'entità che stanno analizzando e del contesto in cui opera. Di conseguenza lo IAASB è intervenuto introducendo l'obbligo di pianificare e svolgere procedure di valutazione del rischi in modo tale da consentire al revisore di esaminare in modo imparziale le prove senza essere influenzato dall'obiettivo di confermare i rischi esistenti. Questo atteggiamento aiuta il revisore a evitare di escludere elementi probativi che potrebbero contrastare con le conclusioni desiderate. Il giudizio professionale del revisore si basa su questo scetticismo e determina se le prove disponibili sono sufficienti per la valutazione del rischio.
- Chiarimenti sul fatto che il processo di valutazione dei rischi costituisce la base per l'identificazione e la valutazione dei rischi di errore significativo e per la definizione di ulteriori procedure di revisione. Una solida valutazione del rischio è fondamentale per il

[18] IAASB, Introduction to ISA 315, 2019

revisore nel definire una strategia e un approccio di revisione che rispondano ai rischi di errori significativi identificati e valutati. Per via dei cambiamenti del contesto in cui opera l'impresa, come per esempio una maggiore complessità dei quadri di riferimento per l'informativa finanziaria, del maggior utilizzo della tecnologia e una maggiore complessità della struttura di governance è necessaria una valutazione e identificazione dei rischi più rigorosa e complessa. Per lo IAASB risulta quindi, essere importante rafforzare una maggiore comprensione del quadro normativo di riferimento, aumentare in modo significativo le considerazione del revisore in relazione all'utilizzo dell'informatica da parte dell'impresa e il suo impatto sulla revisione, migliorare la comprensione del revisore della struttura organizzativa dell'impresa, dell'assetto proprietario e della governance, infine migliorare la comprensione dell'ambiente di controllo e di come questo costituisce una base per tutti gli altri elementi del sistema di controllo interno.

- Distinguere la natura e chiarire la portata del lavoro necessario per i controlli indiretti e diretti nel sistema di controllo interno. Sono state identificate delle difficoltà relative alla comprensione del controllo interno e delle attività di controllo che risultano rilevanti ai fini della revisione contabile in particolar modo in merito alla natura e alla portata delle del lavoro da svolgere per dimostrare di aver compreso quanto richiesto, di conseguenza venivano effettuate interpretazioni diverse e venivano applicate prassi incoerenti. Lo IAASB ha cercato di chiarire la natura e l'estensione del lavoro da svolgere per ottenere una comprensione di ciascun elemento del sistema di controllo interno, ha introdotto il concetto di spettro del rischio intrinseco, ha chiarito la definizione di rischio significativo e come l'identificazione e valutazione dei rischi significativi sia poi

legato alla pianificazione delle risposte da mettere in pratica per fronteggiare tali rischi.

- Chiarire quali controlli devono essere identificati per valutare la struttura di un controllo e determinare se il controllo è stato implementato.
- Scalabilità: il materiale applicativo evidenza le considerazioni sulla proporzionalità e sulla scalabilità in una voce separata, illustrando l'aumento di scala per le situazioni che risultano essere più complesse e la riduzione per le situazioni meno complesse.
- Uso della tecnologia a supporto dell'*audit*: gli strumenti e le tecniche automatizzate vengono sempre più applicate per la valutazione del rischio da parte del revisore, ma gli ISA precedenti non trattavano in modo specifico i potenziali benefici e anche le implicazioni dell'utilizzo di queste. Il paragrafo A21 del principio di revisione ISA 315 cita "Utilizzando strumenti e tecniche automatizzate il revisore può svolgere procedure di valutazione del rischio su grandi volumi di dati inclusi analisi, ricalcoli, riesecuzioni o riconciliazioni"[19], questi strumenti -riprendendo il paragrafo A57- possono essere utilizzati "per comprendere i flussi delle operazioni e la loro elaborazione, tali procedure possono consentirgli di acquisire informazioni sulla struttura organizzativa dell'impresa o sulle sue controparti nei rapporti di affare"[20].

[19] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. A21
[20] IAASB, Principio di Revisione Internazionale (ISA Italia) 315 "Identificazione e valutazione dei rischi di errori significativi", 2019, par. A57

CAPITOLO 2

IMPATTO SULL'OPERATIVITA' DEL REVISORE: NOVITA' E APPROFONDIMENTI INTRODOTTI NELL'ISA 315 REVISED RISPETTO ALL'ISA 315

Il principio ISA 315 Revised, rinnovato dallo IAASB, al fine di includere un'identificazione e valutazione del rischio più robusta e coerente, che incoraggia una valutazione dei rischi di revisione tenendo conto dell'ambiente operativo delle società. Tuttavia, la revisione del nuovo ISA Italia 315 enfatizza l'importanza della capacità del revisore di identificare e valutare i rischi di errori significativi, considerando anche il ruolo del sistema di controllo interno nel mitigare la presenza di errori materiali in bilancio.

Il nuovo ISA 315 è caratterizzato da un maggior dettaglio rispetto al precedente, con l'introduzione di nuove definizioni e terminologie e la presenza di sei importanti appendici. Si è resa necessaria la revisione dello standard in considerazione di alcuni dubbi interpretativi che il vecchio principio lasciava aperti, quali l'esistenza di un'incoerenza nella natura e nel numero dei rischi significativi identificati nella pratica, la comprensione del sistema di controllo interno risultava era di difficile applicazione nella pratica e i rischi legati al IT non erano sufficientemente trattati, di conseguenza l'applicazione del precedente principio da parte dei revisori non risultava idonea. Questa versione sottolinea l'importanza della valutazione accurata del rischio, ponendo l'attenzione sul concetto dello spettro del rischio. In pratica, come nel precedente ISA 315 il rischio dipenderà dalla combinazione tra la probabilità che un evento accada e l'entità dell'impatto ovvero la sua magnitudo, l'ISA 315 Revised però, fornisce una scala di valutazione che rende maggiormente oggettiva l'identificazione di rischi meno che remoti, più che remoti e significativi.

La valutazione di tale misura del rischio andrà poi ad impattare sull'approccio di revisione scelto. È fondamentale quindi monitorare i rischi considerati più probabili o quelli con un impatto significativo, anche se la probabilità dovesse essere bassa. Il tema "spettro del rischio" verrà trattato in maniera più approfondito nel paragrafo *2.4.3 Identificazione e valutazione dei rischi di errori significativi - Rischi di errori significativi a livello di asserzioni*. Altre novità contenute nel nuovo ISA 315 riguardano l'ambiente di controllo interno all'impresa, in particolare riguardo all'ambiente IT. Il sistema di controllo interno di un'impresa combina elementi manuali ed automatizzati, la combinazione tra i due varia a seconda della complessità dell'utilizzo degli strumenti informatici. L'utilizzo dell'IT da parte dell'impresa influisce sul modo in cui le informazioni per il bilancio sono gestite, archiviate e comunicate, influenzando quindi anche la configurazione e l'implementazione del sistema di controllo interno. Il nuovo ISA Italia 315 dedica una maggiore attenzione alla comprensione e valutazione dei controlli, con due appendici che evidenziano questa importanza rispetto al passato. Il controllo interno dell'impresa è gestito mediante direttive e procedure, riflessi nei sistemi e nella modulistica, e viene attuato dalla direzione, dai responsabili della governance e dal personale chiave. Gli elementi dell'ambiente di controllo includono le responsabilità della direzione, la supervisione indipendente, l'attribuzione di poteri e responsabilità, la gestione del personale, e l'incoraggiamento degli obiettivi aziendali. In linea con quanto già definito dall'ISA 315 ante revisione, anche il nuovo ISA si focalizza sulla valutazione del rischio, fornendo linee guida per la comprensione della struttura del sistema di controllo interno e la valutazione dei rischi che potrebbero influenzare la corretta predisposizione del bilancio, quindi il revisore deve pianificare la propria attività focalizzandosi sulle aree di bilancio più rischiose. Il principio fornisce linee guida e regole per mettere in pratica le procedure di

revisione. La revisione del sistema di controllo interno viene effettuata attraverso indagini, analisi comparativa, osservazioni e ispezioni, al fine di valutare i rischi e garantire la corretta preparazione del bilancio aziendale. Questo processo implica la condivisione di informazioni con l'*internal audit* e la raccolta di documentazione per valutare l'efficacia dei controlli svolti e individuare rischi significativi. Le procedure di analisi comparativa, incluse informazioni finanziarie e non finanziarie, possono essere automatizzate con il *data analytics*. Se le procedure aziendali non sono documentate o se l'azienda ha controlli meno formalizzati, il principio stabilisce che il revisore ha comunque la possibilità di acquisire alcuni elementi probativi per identificare e valutare i rischi di errori significativi[21].

L'analisi svolta in questo capitolo vuole mettere in evidenza le varie differenze tra i due principi e riportare nel dettaglio le novità appena introdotte che caratterizzano il principio di revisione ISA 315 Revised.

La struttura di tale capitolo segue la struttura presentata nell'indice del documento Principio di Revisione ISA 315 "Identificazione e valutazione dei rischi di errori significativi". Per maggiore comodità mi riferirò al Principio di Revisione ISA 315 "L'identificazione e la valutazione dei rischi di errori Significativi mediante la comprensione dell'impresa e del Contesto in cui opera" entrato in vigore nel Gennaio 2020 come "ISA 315", mentre, al Principio di Revisione "Identificazione e valutazione dei rischi di errori significativi" entrato in vigore nel Gennaio 2022 come "ISA 315 Revised".

[21] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. A33

2.1 Introduzione

In entrambi i principi è presente l'oggetto trattato nel principio, che varia tra ISA 315 e ISA 315 Revised.

Nel primo caso "Il presente principio di revisione tratta della responsabilità del revisore nell'identificare e valutare i rischi di errori significativi nel bilancio, mediante la comprensione dell'impresa e del contesto in cui opera, incluso il suo controllo interno."[22], invece nel secondo caso "Il presente principio di revisione tratta della responsabilità del revisore nell'identificare e valutare i rischi di errori significativi nel bilancio."[23]

Il principio Isa 315 Revised rispetto al principio Isa 315 esplicita sia i concetti chiave relativi al principio e introduce il concetto di Scalabilità[24].

In merito ai concetti chiave vengono spiegati quali siano gli obiettivi generali del revisore, trattati anche nel principio di revisione 200, quindi acquisire sufficienti elementi probativi al fine di ridurre il rischio di revisione ad un livello accettabilmente basso. Come detto precedentemente, il rischio di revisione dipende dal rischio di errore significativo e dal rischio di individuazione; il rischio di errore significativo può essere a livello di bilancio nel suo complesso o a livello di asserzioni per classi di operazioni, saldi contabili e informativa di bilancio. I rischi a livello di asserzioni comprendono due componenti: il rischio inerente e il rischio di controllo, la combinazione delle due tipologie di rischio, spiegate precedentemente, costituisce il rischio di errore significativo. Questo principio prevede una valutazione separata

[22] IAASB, Principio Di Revisione Internazionale (Isa Italia) 315 "L'identificazione E La Valutazione Dei Rischi Di Errori Significativi Mediante La Comprensione Dell'impresa E Del Contesto In Cui Opera", par. 1
[23] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 1
[24] IAASB, Principio di Revisione Internazionale (ISA Italia) 315 "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 9

del rischio intrinseco e del rischio di controllo. Per definire il livello di rischio intrinseco viene introdotta una scala di variazione denominata "*spettro del rischio intrinseco*"[25] tema trattato nel sottoparagrafo *2.4.3 Identificazione e valutazione dei rischi di errori significativi - Rischi di errori significativi a livello di asserzioni*.

La corretta comprensione da parte del revisore dell'azienda, del contesto in cui opera, delle normative sull'informazione finanziaria e del sistema di controllo interno dell'azienda è fondamentale per identificare e valutare i rischi di errori significativi durante la revisione. Il principio di revisione internazionale (ISA Italia) n.330 richiede al revisore di definire e implementare risposte generali di revisione per affrontare i rischi di errori significativi identificati e valutati nel bilancio. Inoltre, il principio sottolinea che la valutazione dei rischi e le risposte sono influenzate dalla comprensione dell'ambiente di controllo da parte del revisore. Sempre tra i concetti chiave viene chiesto al revisore di esercitare il proprio giudizio professionale nella pianificazione e svolgimento dell'attività mantenendo lo scetticismo professionale.

In merito alla scalabilità il seguente principio viene applicato a tutte le imprese, indipendentemente dalla loro dimensione e complessità, ne consegue che le linee guida includono considerazioni specifiche per le imprese meno complesse e per le imprese più complesse, tema trattato nel sottoparagrafo *2.4.1 Procedure di valutazione del rischio e attività correlate - Scalabilità*.

2.2 Obiettivo e Definizioni

L'obiettivo del principio di revisione ISA 315 Revised risulta essere quello di "identificare e valutare i rischi di errori significativi, siano essi dovuti a

[25] IAASB, Principio di Revisione Internazionale (ISA Italia) 315 "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 5

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"[26]. il principio di revisione ISA 315 in aggiunta presenta come mezzo per il raggiungimento di tale obiettivo "la comprensione dell'impresa e del contesto in cui opera, incluso il suo controllo interno"[27].

Le definizioni risultano essere più complete e dettagliate nel principio di revisione ISA 315 Revised[28], non tutte le definizioni presenti nel ISA 315 Revised sono contenute anche nel ISA 315[29], nello specifico:

DEFINIZIONI COMUNI	
ISA 315 REVISED[30]	ISA 315
Asserzioni 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 e redatto in conformità al quadro normativo sull'informazione finanziaria applicabile. Le asserzioni sono utilizzate dal revisore per prendere in considerazione le diverse tipologie di errori potenziali che possono verificarsi	**Asserzioni** Attestazioni della direzione, esplicite e non, contenute nel bilancio, utilizzate dal revisore per prendere in considerazione le diverse tipologie di errori potenziali che possono verificarsi.

[26] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 11
[27] IAASB, Principio Di Revisione Internazionale (Isa Italia) 315, "L'identificazione E La Valutazione Dei Rischi Di Errori Significativi Mediante La Comprensione Dell'impresa E Del Contesto In Cui Opera", par. 3
[28] IAASB, Principio di Revisione Internazionale (ISA Italia) 315 "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 12
[29] IAASB, Principio Di Revisione Internazionale (Isa Italia) 315, "L'identificazione E La Valutazione Dei Rischi Di Errori Significativi Mediante La Comprensione Dell'impresa E Del Contesto In Cui Opera", par. 4
[30] Le differenze rispetto al principio precedente in merito alla definizioni sono state evidenziate in grigio

quando identifica e valuta i rischi di errori significativi e definisce le relative risposte di revisione.	
Rischio di business Un rischio derivante da condizioni, eventi, circostanze, azioni o inattività significative che potrebbero influire negativamente sulla capacità dell'impresa di raggiungere i propri obiettivi e di realizzare le proprie strategie, ovvero un rischio derivante dalla definizione di obiettivi e strategie non appropriati.	**Rischi connessi all'attività** Un rischio derivante da condizioni, eventi, circostanze, azioni o inattività significative che potrebbero incidere sfavorevolmente sulla capacita dell'impresa di raggiungere i propri obiettivi e di realizzare le proprie strategie, ovvero un rischio derivante dalla definizione di obiettivi e strategie non appropriati.
Sistema di controllo interno Il 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. Ai fini dei principi di revisione internazionali, il sistema di controllo interno e costituito da cinque componenti correlate: i. L'ambiente di controllo; ii. Il processo adottato dall'impresa per la valutazione del rischio; iii. Il processo adottato dall'impresa per monitorare il sistema di controllo interno;	**Controllo interno** Il 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. Il termine "controlli" si riferisce a qualsiasi aspetto di una o più componenti del controllo interno

iv. Il sistema informativo e la comunicazione; v. Le attività di controllo.	
Procedure di valutazione del rischio Le procedure di revisione 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.	**Procedure di valutazione del rischio** Le procedure di revisione svolte per acquisire una comprensione dell'impresa e del contesto in cui opera, incluso il suo controllo interno, al fine di valutare i rischi di errori significativi, dovuti a frodi o a comportamenti o eventi non intenzionali, a livello di bilancio e di asserzioni.
Rischio Significativo Un rischio di errore significativo identificato: i. per il quale la valutazione del rischio intrinseco è prossima all'estremità superiore dello spettro del rischio intrinseco a causa della misura in cui i fattori di rischio intrinseco influenzano la combinazione della probabilità che un errore si verifichi e dell'entità del potenziale errore qualora questo dovesse verificarsi; ovvero ii. che deve essere trattato come un rischio significativo in conformità alle regole di altri principi di revisione internazionali.	**Rischio significativo** Un rischio di errore significativo identificato e valutato che, a giudizio del revisore, richiede una speciale considerazione nella revisione.

DEFINIZIONI INTRODOTTE ISA 315 REVISED
Controlli Direttive o procedure che un'impresa definisce per conseguire gli obiettivi di controllo della direzione o dei responsabili delle attività di governance. In questo contesto:

i. Le direttive indicano ciò che dovrebbe, o non dovrebbe, essere fatto nell'ambito dell'impresa per attuare i controlli. Tali indicazioni possono essere documentate, riportate esplicitamente all'interno di comunicazioni, o implicite nelle azioni e decisioni. ii. Le procedure sono attività finalizzate ad implementare le direttive.
Controlli generali IT Controlli sui processi IT dell'impresa che supportano il continuo e corretto funzionamento dell'ambiente IT, inclusi il continuo ed efficace funzionamento dei controlli sulle elaborazioni delle informazioni e sull' integrità delle stesse (ossia la loro completezza, accuratezza e validità) nel sistema informativo dell'impresa.
Controlli sulle elaborazioni delle informazioni Controlli relativi all'elaborazione delle informazioni nelle applicazioni IT o nelle procedure manuali, presenti nel sistema informativo dell'impresa, che fronteggiano direttamente i rischi per l'integrità delle informazioni (ossia, la completezza, accuratezza e validità delle operazioni e delle altre informazioni).
Fattori di rischio intrinseco Caratteristiche di eventi o condizioni che influenzano la possibilità che un'asserzione relativa ad una classe di operazioni, un saldo contabile o un'informativa, contenga errori, dovuti a frodi o a comportamenti o eventi non intenzionali, prima della considerazione dei controlli. Tali fattori possono avere natura qualitativa o quantitativa e includono la complessità, la soggettività, i cambiamenti, l'incertezza o 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.
Ambiente IT Le applicazioni IT e l'infrastruttura IT di supporto, cosi come i processi IT e il personale addetto a tali processi, che l'impresa utilizza a supporto delle proprie attività operative e per la realizzazione delle proprie strategie. Ai fini del presente principio di revisione: i. Un'applicazione IT e un programma o una serie di programmi utilizzati nella rilevazione, registrazione, elaborazione e rendicontazione delle operazioni o delle informazioni. Le applicazioni IT includono data warehouse e report writers. ii. L'infrastruttura IT include la rete, i sistemi operativi e i database con i relativi hardware e software. iii. I processi IT sono i processi dell'impresa per gestire l'accesso all'ambiente IT, gestire i cambiamenti nei programmi o nell'ambiente IT e gestire le operazioni IT.

Asserzioni rilevanti Un'asserzione relativa ad una classe di operazioni, un saldo contabile o un'informativa e rilevante quando presenta un rischio di errori significativi identificato. La determinazione della rilevanza di un' asserzione avviene prima della considerazione dei relativi controlli.
Rischi derivanti dall'utilizzo dell'IT Possibilità che i controlli sulle elaborazioni delle informazioni siano configurati o operino in modo inefficace, o rischi per l'integrità delle informazioni (ossia, la completezza, l'accuratezza e la validità delle operazioni e delle altre informazioni) nel sistema informativo dell' impresa, dovuti ad una configurazione inefficace dei controlli o alla loro inefficacia operativa nei processi IT dell'impresa.
Classi di operazioni, saldi contabili o informativa rilevanti per la revisione Una classe di operazioni, un saldo contabile o un' informativa per i quali esistono una o più asserzioni rilevanti.

2.3 Regole

Le regole in entrambi i principi si suddividono in quattro sottoparagrafi che vengono in alcuni casi sviluppati diversamente.

2.3.1 Procedure di valutazione del rischio e attività correlate

Le regole stabilite per le procedure di valutazione del rischio e le attività correlate sono sviluppate e trattate in egual maniera nei due principi. Il revisore deve quindi svolgere procedure di valutazione del rischio al fine di raccogliere elementi probativi che possano supportare in modo adeguato l'identificazione e la valutazione dei rischi di errori significativi, che possano derivare da frodi, comportamenti involontari o eventi a livello di bilancio e di asserzioni. La procedura di valutazione del rischio include:

- Indagini presso la direzione, le persone appropriate nell'ambito della funzione di revisione interna e altri soggetti che il revisore possa ritenere essere in possesso di informazioni che potrebbero aiutarlo nell'identificazione di rischi di errori significativi;

- Procedure di analisi comparativa;
- Osservazioni e ispezioni.

Nel processo di acquisizione di elementi probativi, il revisore può prendere in considerazione informazioni ottenute durante le procedure di accettazione e/o mantenimento dell'incarico, e in alcuni casi anche da altri incarichi svolti per l'azienda dal responsabile dell'incarico. Nel caso in cui il revisore desideri utilizzare informazioni provenienti da incarichi precedenti presso l'impresa, è necessario valutare attentamente se tali informazioni sono rilevanti e affidabili come elementi probativi.

Il responsabile dell'incarico e i membri del team di revisione devono analizzare attentamente l'applicazione del quadro normativo sull'informazione finanziaria di riferimento al fine di identificare eventuali discrepanze o omissioni nonché la presenza di errori significativi nel bilancio dell'impresa.

2.3.2 Acquisire una comprensione dell'impresa e del contesto in cui opera, del quadro normativo sull'informazione finanziaria applicabile e del sistema di controllo interno dell'impresa

In merito alla comprensione dell'imprese e del contesto in cui opera e del quadro normativo sull'informazione finanziaria applicabile l'ISA 315 Revised aggiunge gli elementi riguardanti l'utilizzo dell'IT e la comprensione delle modalità e della misura con cui i fattori di rischio intrinseco influenzano la possibilità che le asserzioni contengano errori.

Quindi, il revisore deve acquisire una comprensione approfondita della struttura organizzativa, dell'assetto proprietario, della governance e del modello di business dell'impresa, inclusa l'integrazione dell'IT. Deve considerare anche il settore in cui opera l'impresa, la regolamentazione e altri fattori esterni. È importante comprendere le misurazioni utilizzate per

valutare la performance economico-finanziaria, sia interne che esterne, e avere conoscenza del quadro normativo sull'informazione finanziaria, dei principi contabili adottati e dei motivi di eventuali cambiamenti.

Per quanto riguarda la comprensione del sistema di controllo interno dell'azienda analizziamo ogni singola componente.

Ambiente di controllo

In entrambi i principi viene spiegato come il revisore debba acquisire una comprensione dell'ambiente di controllo, svolgendo procedure di valutazione del rischio. A tal fine, il revisore deve valutare se la direzione, con la supervisione dei responsabili delle attività di governance, abbia instaurato e mantenuto una cultura aziendale ispirata al valore dell'onestà ed a comportamenti eticamente corretti; l'ambiente di controllo fornisca un fondamento appropriato per le altre componenti del sistema di controllo interno dell'impresa; le carenze identificate nell'ambiente di controllo compromettano le altre componenti del sistema di controllo interno.

Il principio di revisione ISA 315 Revised, aggiunge, inoltre, che il revisore deve comprendere l'assetto organizzativo dei processi e dei controlli che riguardano diversi aspetti, quali:

- Le modalità con cui la direzione adempie alle proprie responsabilità di supervisione e la cultura aziendale, inclusi l'impegno all'integrità e al rispetto dei valori etici;
- L'indipendenza dei responsabili delle attività di governance rispetto alla direzione e la supervisione del sistema di controllo interno;
- Il reclutamento, la formazione e il coinvolgimento di personale competente;
- La responsabilizzazione del personale nel raggiungimento degli obiettivi del controllo interno.

Valutazione del rischio

Le regole riguardanti la valutazione del rischio dell'impresa rimangono invariate tra ISA 315 e ISA 315 Revised.

Il revisore deve comprendere il processo dell'impresa per identificare i rischi di business che possono influenzare l'informativa finanziaria, valutando la loro significatività e probabilità di verificarsi, e affrontandoli adeguatamente. Inoltre, il Principio di Revisione ISA 315 Revised puntualizza che il revisore ha il dovere di valutare l'appropriatezza del processo di valutazione del rischio adottato dall'impresa in relazione alla sua natura e complessità.

Quando il revisore individua rischi di errori significativi che non sono stati identificati dalla direzione, è importante valutare se tali rischi necessitavano di essere riconosciuti e identificati nel processo di valutazione del rischio adottato dall'impresa. In caso affermativo, il revisore deve acquisire una comprensione approfondita sulla mancata individuazione di tali rischi.

Monitoraggio del sistema di controllo

Anche in questo caso le regole riguardanti il monitoraggio del sistema di controllo dell'impresa non variano tra i due principi.

Il revisore deve effettuare valutazioni continue e separate per monitorare l'efficacia dei controlli e identificare eventuali carenze, adottando azioni correttive adeguate. Deve inoltre esaminare la funzione di revisione interna, se presente, comprendendone natura, responsabilità e attività. È importante che il revisore sia a conoscenza delle fonti di informazione utilizzate dall'impresa per monitorare il sistema di controllo interno e comprendere le ragioni per cui la direzione ritiene affidabili le informazioni provenienti da tali fonti. Inoltre, il principio di revisione ISA 315 Revised puntualizza il dovere del revisore di valutare l'appropriatezza

del processo di monitoraggio adottato dall'impresa in relazione alla sua natura e complessità.

Sistema informativo e Comunicazione

La disposizione delle regole in termini di sistema informativo e comunicazione è il medesimo in entrambi i principi.

Il revisore deve approfondire la comprensione del sistema informativo per l'informativa finanziaria, comprendendo in che modo le operazioni vengono rilevate, registrate, elaborate, corrette se necessario e trasferite nella contabilità per essere infine riportate nel bilancio. Deve inoltre analizzare come le informazioni su eventi e condizioni vengono acquisite e presentate nella documentazione contabile.

Deve comprendere il processo che l'impresa utilizza per predisporre l'informativa finanziaria e redigere il bilancio. Deve verificare se il sistema informativo dell'impresa è adeguato e se la comunicazione all'interno dell'azienda supporta in modo efficace la redazione del bilancio in conformità alle normative vigenti.

In aggiunta, è importante che il revisore abbia una conoscenza approfondita del sistema informativo dell'impresa, comprese le risorse disponibili e l'ambiente IT in cui opera. È essenziale che il revisore sia in grado di comprendere come l'impresa comunica i ruoli, le responsabilità e gli elementi cruciali legati alla preparazione delle informazioni finanziarie.

Attività di controllo

L'attività di controllo viene sviluppata più nel dettaglio nell'ISA 315 Revised rispetto all'ISA 315 in quanto spiega quali sono quei controlli che

vanno identificati al fine delle comprensione della componente attività di controllo. Tali controlli sono[31]:

- I controlli che affrontano specifici rischi considerati significativi;
- I controlli sulle registrazioni contabili per operazioni non ricorrenti o inusuali;
- I controlli per i quali il revisore prevede di valutare l'efficacia operativa, considerando tempistiche, natura ed estensione delle procedure di validità. Questi controlli includono quelli che affrontano rischi che non possono essere adeguatamente valutati attraverso le sole procedure di validità;
- I controlli che il revisore ritiene essere appropriati per raggiungere i propri obiettivi, basandosi sul proprio giudizio professionale.

Precisa poi che vanno identificati, sulla base dei controlli sopra citati, le applicazioni IT e gli altri aspetti dell'ambiente IT che sono soggetti a rischi derivanti dall'utilizzo dell'IT, quindi identificazione dei rischi connessi derivanti dall'utilizzo dell'IT e i controlli generali IT che l'impresa pone in essere per fronteggiare tali rischi. Nel processo di identificazione dei rischi legati all'uso dell'IT, il revisore deve prendere in considerazione la natura delle applicazioni IT identificate e altri elementi del contesto informatico. È importante comprendere le ragioni per cui questi aspetti possono essere esposti a potenziali rischi. Per determinate applicazioni IT o componenti dell'ambiente IT, il revisore potrebbe rilevare rischi specifici, come gli accessi non autorizzati o modifiche non autorizzate ai programmi, nonché rischi connessi a modifiche inadeguate dei dati. I rischi informatici tendono a essere più elevati quando il volume o la complessità dei controlli automatizzati relativi alle applicazioni e più elevato e la direzione sta facendo maggiore affidamento su tali controlli

[31] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 26

per l'efficace elaborazione di operazioni o l'efficace mantenimento dell'integrità delle informazioni sottostanti.

Dopo aver valutato attentamente ciascun elemento del sistema di controllo interno, il revisore deve determinare se siano emerse delle lacune nei controlli identificati.

2.3.3 Identificazione e valutazione dei rischi di errori significativi

Entrambi i principi stabiliscono che il revisore deve individuare i rischi di errori significativi e valutare se tali rischi sussistono a livello di bilancio o di asserzioni per classi di operazioni, saldi contabili e informativa. La differenza risiede nella valutazione dei rischi di errori significativi a livello di asserzioni in quanto viene introdotta la valutazione del rischio intrinseco. Il revisore deve valutare il rischio intrinseco considerando la probabilità e l'entità dell'errore. Deve prendere in considerazione i fattori di rischio intrinseco che possono influenzare la presenza di errori nelle asserzioni rilevanti, così come i rischi di errori significativi a livello di bilancio che possono influire sulla valutazione del rischio intrinseco per i rischi di errori significativi a livello di asserzioni. Tramite l'introduzione del concetto "fattore di rischio intrinseco", il nuovo principio espone in maniera esplicita quali fattori di rischio è opportuno considerare per arrivare a definire una misura di rischio intrinseco. Nel principio ISA 315 un approccio analogo era già presente ma non venivano esplicitati i fattori di rischio. Questo permette di facilitare una maggiore omogeneità e comparabilità.

Rispetto al principio di revisione ISA 315 viene indicata in maniera molto più esplicita quale debba essere l'approccio di revisione in ambito controlli a fronte della individuazione di determinate tipologie di rischi intrinseci o di operatività riferita a determinati ambiti, come per esempio alle scritture

contabili. Inoltre, il nuovo principio precisa che il revisore se pianifica di verificare l'efficacia operativa dei controlli deve valutare il rischio di controllo[32]. Se il revisore decidesse di non esaminare l'efficacia operativa dei controlli, è comunque necessario che la sua valutazione del rischio di controllo sia tale da garantire che la valutazione del rischio di errori significativi corrisponda alla valutazione del rischio intrinseco, in quanto nella definizione di rischio di errore significativo adottato nel caso specifico non sarebbe disponibile una misura del rischio di controllo per cui il valore del rischio di errore significativo non potrebbe che coincidere con la misura del rischio inerente identificato, misurato e valutato.

Rispetto al precedente principio viene anche esplicitato che il revisore deve valutare se gli elementi probativi ottenuti dalle procedure di valutazione del rischio sono sufficienti per identificare e valutare correttamente i rischi di errori significativi. Se i risultati non sono sufficienti, il revisore deve eseguire ulteriori procedure per ottenere elementi probativi necessari per identificare in modo adeguato tali rischi.

Il revisore deve valutare se le classi di operazioni, saldi contabili o l'informativa che non sono stati ritenuti rilevanti inizialmente potrebbero diventare significativi durante la revisione e quindi essere necessario esaminarli attentamente.

2.3.4 Documentazione

Le regole sulla documentazione restano invariate da ISA 315 a ISA 315 Revised.

[32] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 34

2.4 Linee guida e altro materiale applicativo

Entrambi i principi suddividono questo paragrafo in sottoparagrafi che andremo ad analizzare uno alla volta.

2.4.1 Procedure di valutazione del rischio e attività correlate

In questo sottoparagrafo il principio di revisione ISA 315 Revised tratta temi come lo scetticismo professionale, la scalabilità, informazioni da altre fonti, strumenti e tecniche automatizzate che invece non risultano essere presenti nel principio di revisione ISA 315.

Tale principio stila un elenco di ulteriori principi che nel dettaglio forniscono linee guida per l'identificazione e valutazione di errori significativi:

- ISA Italia 240 relativamente a frodi;
- ISA Italia 540 relativamente alle stime contabili;
- ISA Italia 550 relativamente ai rapporti e alle operazioni con parti correlate;
- ISA Italia 570 relativamente alla continuità aziendale;
- ISA Italia 600 relativamente al bilancio di gruppo.

In merito allo scetticismo professionale è necessario per una valutazione critica dei dati raccolti durante le procedure di valutazione del rischio, poiché aiuta il revisore a rimanere obiettivo e a non essere influenzato nel cercare conferma dei rischi, escludendo invece prove che possano andare in senso contrario. Lo scetticismo professionale è un elemento fondamentale della professione di revisore e deve essere costantemente applicato per garantire l'integrità e l'efficacia del processo di valutazione del rischio. Il concetto di scetticismo professionale implica:

- la necessità di porre domande sulle informazioni contraddittorie e sull'affidabilità dei documenti;

- di valutare le risposte alle indagini e altre informazioni fornite dalla direzione e dai responsabili della governance;
- di essere vigili riguardo a possibili errori causati da frodi o eventi non intenzionali;
- di verificare se le prove raccolte sostengano l'identificazione e la valutazione dei rischi di errori significativi da parte dell'*audit*or.

Per acquisire elementi probativi, il revisore può utilizzare fonti interne ed esterne all'impresa. Tuttavia, non è tenuto a eseguire una ricerca approfondita per identificare tutte le potenziali fonti di prove. Le fonti di informazioni per valutare i rischi includono le interazioni con la direzione, i responsabili della governance, i revisori interni e parti esterne come le autorità di vigilanza. È possibile considerare anche informazioni disponibili al pubblico, come comunicati stampa o report da parte di analisti.

Scalabilità

Come sopra citato, l'ISA 315 Revised tratta della scalabilità, ovvero la natura e l'estensione delle procedure di valutazione del rischio variano in base alla natura e alle circostanze dell'impresa. Il revisore utilizzerà il proprio giudizio professionale per determinare natura e estensione delle procedure. Il principio specifica che anche in assenza di una formalizzazione strutturata delle direttive e dei processi, il revisore è tenuto a valutare il controllo interno e il rischio di errori significativi. Questa valutazione può avvenire tramite osservazione e indagini, anche se non vi è una documentazione dettagliata prodotta dall'impresa in termini di policy e procedure o piuttosto di evidenze di controllo prodotte. In generale lo svolgimento di osservazioni e ispezione possono supportare, confermare o contraddire le indagini condotte presso direzione e altri soggetti, fornendo informazioni sull'impresa e sul contesto in cui opera. Inoltre, il principio sottolinea che la natura e l'estensione delle procedure

di valutazione del rischio da svolgere possono essere più ampie in caso di primo incarico rispetto a un incarico ricorrente, negli anni successivi al primo incarico il revisore può focalizzarsi sui cambiamenti avvenuti rispetto l'anno precedente.

Attraverso l'impiego di strumenti e tecniche automatizzate, il revisore è in grado di effettuare una valutazione del rischio su vasti quantitativi di dati attraverso analisi, ricalcoli, riesecuzioni e riconciliazioni.

Le indagini presso la direzione, i responsabili dell'informativa finanziaria e altri soggetti all'interno dell'impresa offrono al revisore una varietà di prospettive utili per individuare e valutare potenziali rischi di errori significativi. Se un'impresa ha una funzione di revisione intera lo svolgimento di indagini presso le persone appropriate nell'ambito di tale funzione può aiutare il revisore, sempre mantenendo un profilo indipendente, a comprendere l'impresa e il contesto in cui opera e il suo sistema di controllo interno, ai fini dell'identificazione e della valutazione dei rischi[33].

Considerazione per la comprensione della funzione di revisione interna di un'impresa

La funzione di revisione interna ha il compito di svolgere procedure e valutare i risultati per garantire alla direzione e ai responsabili dell'azienda un' *assurance* sulla configurazione e l'efficacia dei processi di gestione del rischio, del sistema di controllo interno e della governance. Questo ruolo è importante nel monitorare il sistema di controllo interno dell'azienda. Tuttavia, la revisione interna potrebbe anche concentrarsi sull'analisi dell'economicità, dell'efficienza e dell'efficacia delle attività operative, senza essere direttamente legata all'informativa finanziaria dell'azienda.

[33] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. A25

La funzione di revisione interna, nel corso del proprio lavoro, acquisisce una conoscenza dettagliata delle attività dell'impresa e dei rischi ad esse collegati. Questa conoscenza può fornire al revisore informazioni utili per comprendere meglio l'impresa, il contesto in cui opera, il quadro normativo e il sistema di controllo interno. Anche se il revisore non prevede di utilizzare il lavoro della funzione di revisione interna per modificare le proprie attività di revisione, è comunque importante svolgere indagini per valutare il rischio e garantire la corretta esecuzione delle procedure di revisione. Il revisore potrebbe decidere di consultare le relazioni della funzione di revisione interna se ritiene che possano fornire informazioni significative per l'informativa finanziaria dell'impresa e per la revisione contabile del bilancio. Queste relazioni potrebbero riguardare la strategia e la pianificazione della funzione di revisione interna, nonché i risultati delle verifiche condotte dalla stessa per la direzione o i responsabili delle attività di governance. Il revisore, nell'analizzare l'ambiente di controllo, valuta come la direzione ha gestito le criticità segnalate dalla revisione interna riguardanti i controlli rilevanti per la redazione del bilancio. In particolare, verifica se le risposte della direzione sono state implementate e in seguito valutate dalla funzione di revisione interna. Se la funzione di revisione interna è in grado di svolgere attività di assurance legate all'informativa finanziaria dell'impresa, il revisore esterno potrebbe basarsi sul lavoro svolto da essa per adeguare le proprie procedure di revisione, riducendo il carico di lavoro e migliorando l'efficienza. Questo è più probabile quando la funzione di revisione interna dispone di risorse adeguate e riporta direttamente ai responsabili delle attività di governance, in base all'esperienza del revisore e alla valutazione del rischio svolta[34].

[34] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, Appendice 4

Il principio ISA 315 Revised tratta dell'utilizzo di procedure di analisi comparativa come procedure di valutazione del rischio, il principio ISA Italia 520 che tratta dell'utilizzo delle procedure di analisi comparativa può essere utilizzato come linea guida qualora il revisore volesse appunto utilizzare procedure di analisi comparativa come procedura di valutazione del rischio. Queste procedure di analisi comparativa possono essere svolte utilizzando strumenti automatizzati.

In merito alle informazioni da altre fonti, possono essere rilevanti in quanto forniscono indicazioni in merito alla natura dell'impresa, i rischi di business, i cambiamenti rispetto ai periodi amministrativi precedenti, ai valori etici della direzione e dei responsabili dell'attività di governance, al quadro normativo sull'informazione finanziaria applicabile. Il revisore può utilizzare informazioni provenienti da:

- Analisti o agenzie di credito;
- Autorità fiscali;
- Autorità di vigilanza;
- Sindacati;
- Finanziatori.

2.4.2 Acquisire una comprensione dell'impresa e del contesto in cui opera, del quadro normativo sull'informazione finanziaria applicabile e del sistema di controllo interno dell'impresa

Il principio di revisione ISA 315 Revised rispetto al principio di revisione ISA 315 spiega quali sono le motivazioni per cui è necessaria una comprensione dell'impresa e del contesto in cui opera, il quadro normativo sull'informazione finanziaria applicabile e il sistema di controllo interno. Risulta essere importante in quanto permette al revisore di comprende gli eventi e le condizioni rilevanti per l'impresa e identificare le modalità

tramite cui i fattori di rischio intrinseco influenzano la possibilità che le asserzioni contengano errori. Tale comprensione aiuta il revisore a pianificare la revisione ed esprimere il proprio giudizio professionale, lo aiutano a sviluppare un' aspettativa da utilizzare nello svolgimento delle procedure di analisi comparativa, a definire e svolgere conseguenti procedure per acquisire elementi probativi sufficienti ed appropriati.

Le procedure di valutazione del rischio sono soggette a scalabilità, possono essere adattate in base alle dimensione e alla complessità delle imprese coinvolte, ovvero una valutazione del rischio può essere semplificata e più rapida per le imprese di dimensioni minori e una valutazione del rischio più dettagliata e approfondita per imprese di dimensioni maggiori. In alcuni contesti normativi, le imprese di dimensioni minori sono autorizzate a semplificare la loro informativa finanziaria, tuttavia ciò non esonera il revisore dall'obbligo di acquisire una conoscenza dell'impresa e del contesto in cui opera.

La comprensione della governance dell'impresa può permettere al revisore di comprendere le capacità dell'impresa di effettuare supervisione adeguata al proprio sistema di controllo interno, questa comprensione può mettere anche in rilievo le carenze e quindi consapevolezza di una maggiore probabilità che ci siano errori significativi a livello di bilancio. La comprensione del modello di business aiuta il revisore a comprendere la strategia e i rischi di business dell'impresa che possono dare origine a rischi di errori significativi, se il modello di business utilizza l'IT è necessario comprendere i rischi che ne derivano. Il revisore, però, non ha il dovere di comprendere tutti i rischi di business in quanto non tutti danno origine a rischi di errori significativi.

Il modello di business è la descrizione del modo in cui un'impresa organizza le proprie attività operative e considera aspetti come la struttura organizzativa, i clienti, i concorrenti, i processi, le opportunità di crescita,

la globalizzazione, le normative, le tecnologie e come integra l'utilizzo dell'IT. Questo modello indica come l'impresa crea e preserva valore finanziario o valore in senso più ampio per i suoi stakeholders. La direzione d'impresa mette in atto una strategia al fine di raggiungere gli obiettivi prefissati, includendo tutte quelle operazioni volte a fronteggiare i rischi sottesi a tali obiettivi e cogliere le opportunità. Un rischio di business può influenzare il rischio di errori significativi per classi di operazioni, saldi contabili ed informativa a livello di asserzioni o di bilancio. Per esempio, il rischio di business derivante da una flessione significativa dei valori del mercato immobiliare può aumentare il rischio di errori significativi associati alla asserzione della valutazione per un'impresa che eroga prestiti a medio termine garantiti da immobili Tuttavia, lo stesso rischio, in particolare in combinazione con una grave recessione economica che contemporaneamente aumenta il rischio sottostante di perdite sui crediti per l'intera durata dei presiti, può anche avere una conseguenza a più lungo termine. In questo caso, ciò potrebbe avere implicazioni per le conclusioni della direzione e del revisore in merito all'appropriatezza dell'utilizzo del presupposto della continuità aziendale da parte dell'impresa e per stabilire se esista un'incertezza significativa[35].

In merito alla comprensione del quadro normativo sull'informazione finanziaria il revisore può considerare le prassi relative al processo di predisposizione dell'informativa finanziaria dell'impresa, la comprensione della scelta e applicazione dei principi contabili con annesse le ragioni di eventuali cambiamenti.

In merito alla comprensione del sistema di controllo interno dell'impresa fornisce al revisore una comprensione preliminare delle modalità con cui

[35] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, Appendice 1

l’impresa identifica i rischi di business e li fronteggia, include anche gli aspetti relativi agli obiettivi di reporting dell’impresa, alle attività d’impresa e ad obiettivi di conformità quando questi aspetti sono importanti ai fini dell’informazione finanziaria. Tale comprensione influirà sull’identificazione e valutazione dei rischi di errori significativi da parte del revisore, permettendogli così di definire le procedure di revisione più adatte da applicare.

Ambiente di controllo

La valutazione dell'ambiente di controllo permette al revisore di comprendere l'integrità e il rispetto dei valori etici all'interno dell'impresa in quanto è definito dalle attività di governance e di direzione dell’azienda e dagli atteggiamenti, dalla consapevolezza e dalle azioni dei responsabili nei confronti del controllo interno. L’ambiente di controllo influenza la percezione e l’importanza che i dirigenti e i responsabili delle attività di governance attribuiscono al sistema di controllo interno all’interno dell’organizzazione. Tale atteggiamento generale fornisce il fondamento su cui si basano le altre componenti del sistema di controllo interno. Questa valutazione permette al revisore di identificare eventuali lacune o problemi che potrebbero compromettere il sistema di controllo interno e di conseguenza influenzare la corretta redazione dei bilanci e delle asserzioni dell'impresa. L'ambiente di controllo comprende:

- la modalità con cui la direzione adempie le proprie responsabilità, come la creazione e il mantenimento della cultura aziendale e l'impegno per l'integrità e il rispetto dei valori etici. L'integrità e il comportamento eticamente corretto dipendono dai principi etici e di comportamento dell'impresa, dai codici di comportamento e dal modo in cui vengono comunicati e messi in pratica. La comunicazione di tali direttive può avvenire attraverso la

divulgazione delle politiche e dei codici di comportamento aziendali.

- Nel caso in cui vi sia separazione tra i responsabili delle attività di governance e la direzione dell'impresa, come dimostrano indipendenza dalla direzione e supervisione sul sistema di controllo interno. È importante valutare se ci sono abbastanza persone indipendenti dalla direzione e se sono obiettive nelle valutazioni e nelle decisioni. Le responsabilità dei dirigenti per le attività di governance sono riconosciute nei codici di comportamento e nelle leggi e regolamenti.
- Delega dei poteri e delle responsabilità all'interno dell'impresa per perseguire i propri obiettivi, con particolare attenzione alle aree chiave di poteri e responsabilità, la formazione e le risorse fornite al personale, la comunicazione degli obiettivi aziendali e la responsabilità individuale.
- L'impresa deve attrarre, formare e fidelizzare personale competente in linea con gli obiettivi, garantendo che abbiano le capacità necessarie attraverso standard di assunzione, politiche di formazione e promozioni basate su valutazioni di performance.
- Le modalità con cui le persone vengono responsabilizzate nel raggiungimento degli obiettivi del sistema di controllo interno. Ciò può avvenire attraverso meccanismi di comunicazione e richiesta di assunzione di responsabilità, nonché attraverso l'implementazione di azioni correttive quando necessario. Inoltre, l'impresa può stabilire misurazioni di performance, incentivi e premi per i responsabili del sistema di controllo interno, valutando continuamente la loro rilevanza e prevedendo provvedimenti disciplinari quando necessario per garantire la corretta gestione del controllo interno dell'impresa.

La valutazione dell'ambiente di controllo da parte del revisore in merito all'utilizzo dell'IT da parte dell'impresa è un processo complesso che può includere diversi aspetti rilevanti. In particolare, il revisore potrebbe esaminare se la gestione dell'IT all'interno dell'impresa è proporzionata alla natura e complessità delle attività dell'azienda che sono rese possibili grazie all'IT. Questo potrebbe includere la valutazione della complessità o della maturità della piattaforma o dell'architettura tecnologica dell'impresa e anche il grado di affidabilità delle applicazioni IT utilizzate per supportare l'informativa finanziaria. Inoltre, il revisore potrebbe analizzare la struttura organizzativa dell'IT all'interno dell'impresa e le risorse assegnate a questa funzione. Ad esempio, potrebbe valutare se l'impresa ha investito in un ambiente IT appropriato e se siano stati effettuati i necessari miglioramenti. Potrebbe anche considerare se l'azienda abbia assunto un numero sufficiente di persone con le competenze adeguate per gestire in modo efficace l'IT, includendo la valutazione sull'utilizzo di software commerciale. La valutazione dell'ambiente di controllo in relazione all'utilizzo dell'IT da parte dell'impresa è fondamentale per garantire che l'azienda abbia i controlli necessari per gestire in modo efficiente e sicuro i processi IT e proteggere l'integrità dei dati e delle informazioni finanziarie.

Processo di valutazione del rischio

Risulta essere importante comprendere il processo adottato dall'impresa per la valutazione del rischio, tale processo risulta essere un ciclo continuo di identificazione e analisi dei rischi, mirati al raggiungimento degli obiettivi aziendali, e fornisce le informazioni necessarie alla direzione o ai responsabili delle attività di governance per determinare quali rischi affrontare e gestire. Non tutti i rischi di business comportano rischi di errori significativi pertanto, è importante che la direzione e i responsabili delle attività di governance identifichino i rischi di business rilevanti per

la redazione del bilancio in conformità al quadro normativo sull'informazione finanziaria applicabile, ne valutino la probabilità di manifestazione e adottino le azioni necessarie per affrontarli. Il revisore può valutare diversi aspetti in questo processo, tra cui la chiara definizione degli obiettivi dell'impresa, l'identificazione e l'analisi dei rischi legati al raggiungimento di tali obiettivi, nonché la considerazione della possibilità di frode in relazione a tali rischi. Valutato questo processo di valutazione del rischio implementato dall'impresa, il revisore dovrà procedere con una sua valutazione indipendente del rischio che potrebbe anche condurre a risultati differenti rispetto a quelli raggiunti dall'impresa a seguito del processo di valutazione del rischio. I rischi possono manifestarsi o evolversi a causa di vari fattori quali cambiamenti nell'ambiente operativo, personale neoassunto o nuovo nella funzione, sistema informativo nuovo o aggiornato, rapida espansione dell'impresa, nuova tecnologia, nuovi modelli di business o nuovi prodotti/attività, ristrutturazioni aziendali, incremento delle attività estere, nuovi principi contabili e utilizzo dell'IT i cui rischi connessi riguardano il mantenimento dell'integrità dei dati e elaborazione delle informazioni, ai rischi relativi alla strategia aziendale se non supportata in modo efficace dalla strategia IT dell'impresa.

Monitoraggio del sistema di controllo interno

Il revisore deve comprendere anche il processo adottato dall'impresa per monitorare il sistema di controllo interno. È importante considerare vari aspetti per comprendere in che modo l'impresa gestisce il monitoraggio del proprio sistema di controllo interno.

In primo luogo, il revisore dovrebbe valutare la configurazione delle attività di monitoraggio adottate dall'impresa. Ad esempio, è importante capire se il monitoraggio viene effettuato in modo periodico o continuativo, oppure una combinazione delle stesse. Inoltre, è importante

valutare lo svolgimento e la frequenza delle attività di monitoraggio. Un monitoraggio regolare e costante può consentire all'impresa di individuare tempestivamente eventuali anomalie e agire prontamente per correggerle. Altro aspetto da considerare è la valutazione tempestiva dei risultati delle attività di monitoraggio. È importante capire se i controlli implementati sono effettivamente efficaci nel prevenire errori o frodi. In caso di carenze identificate, è essenziale capire come queste siano affrontate mediante azioni correttive adeguate. Inoltre, la comunicazione tempestiva di tali carenze a chi ha la responsabilità di intraprendere le azioni correttive è fondamentale per garantire un sistema di controllo interno efficiente e funzionante.

Il revisore deve valutare come l'impresa monitora il sistema di controllo interno riguardante l'utilizzo dell'IT per elaborare le informazioni. Questo può includere:

- Monitoraggio costante dell'efficacia dei controlli sull'elaborazione delle informazioni in ambienti IT complessi, e adattamento dei controlli in base ai cambiamenti nelle condizioni;
- Valutazione dell'efficacia operativa dei controlli sull'elaborazione delle informazioni;
- Monitoraggio delle autorizzazioni per i controlli automatizzati sull'elaborazione delle informazioni, garantendo la separazione delle funzioni;
- Monitoraggio e gestione degli errori o delle carenze nei controlli relativi all'automazione dell'informativa finanziaria.

Questi controlli sono essenziali per garantire che le informazioni elaborate tramite l'IT siano affidabili e accurate, e che le possibili minacce alla sicurezza siano individuate e gestite in modo efficace.

La valutazione da parte del revisore sulle modalità con le quali l'impresa effettua valutazioni continue e separate per monitorare l'efficacia dei controlli permette di comprendere se il sistema di controllo interno dell'impresa funzioni correttamente. Questo processo permette al revisore di identificare eventuali lacune o punti deboli nel sistema di controllo interno e di valutarne l'efficacia complessiva. Inoltre, consente al revisore di individuare e valutare i rischi di errori significativi a livello di bilancio e di asserzioni.

Processo di monitoraggio del proprio sistema di controllo interno da parte dell'impresa

Le funzioni di revisione interna sono responsabili di valutare e monitorare l'efficacia del sistema di controllo interno dell'impresa. Ciò include attività come l'esame delle riconciliazioni bancarie, la valutazione dei venditori sul rispetto delle direttive aziendali e la supervisione dell'ufficio legale sull'osservanza delle direttive aziendali in tema di etica e prassi operative. Il monitoraggio è importante per garantire che i controlli continuino ad operare efficacemente nel tempo, evitando interruzioni nel processo come nel caso delle riconciliazioni bancarie. I controlli necessari per il monitoraggio del sistema di controllo interno di un'impresa possono essere automatizzati, manuali o una combinazione di entrambi. È importante distinguere tra un'attività di monitoraggio e un controllo connesso al sistema informativo, considerando i dettagli specifici dell'attività e il livello di supervisione coinvolto. La supervisione non equivale automaticamente a un'attività di monitoraggio. Ad esempio, un controllo mensile di completezza mira a individuare e correggere gli errori, mentre un'attività di monitoraggio si concentra sul motivo per cui gli errori sono stati commessi e attribuisce la responsabilità alla direzione per correggere il processo e prevenire errori futuri. In sostanza, un controllo connesso al sistema informativo affronta un rischio specifico, mentre un'attività di

monitoraggio valuta se i controlli nelle cinque componenti del sistema di controllo interno stiano funzionando correttamente[36].

I controlli relativi al "sistema informativo e comunicazione" e "attività di controllo" sono per la maggior parte controlli diretti, ovvero controlli che sono indirizzati a prevenire, individuare e correggere errori a livello di asserzioni.

Sistema informativo e comunicazione

Il revisore ha il compito di analizzare e comprendere come il sistema informativo e di comunicazione dell'impresa influenzi la redazione del bilancio. Questo significa capire le direttive dell'impresa riguardo ai flussi delle operazioni e ad altri aspetti relativi all'elaborazione delle informazioni contabili. La valutazione di questa componente è essenziale per determinare se supporta in modo adeguato la preparazione del bilancio e per identificare eventuali rischi di errori significativi.

La comprensione e l'analisi della componente "sistema informativo e comunicazione" possono aiutare il revisore a individuare possibili rischi di errori a livello di asserzioni contabili. Se i risultati delle procedure di revisione contabile non sono coerenti con le aspettative basate sul sistema di controllo interno dell'impresa, potrebbero emergere rischi di errori significativi a livello di bilancio. Il revisore deve avere una conoscenza approfondita delle direttive che regolano i flussi di informazioni all'interno del sistema informativo dell'impresa. Questo include la comprensione delle operazioni, dei saldi contabili e delle informazioni cruciali per la revisione. Inoltre, è importante che il revisore comprenda anche altri aspetti correlati all'elaborazione delle informazioni dell'impresa. Le informazioni ottenute dalla valutazione del sistema informativo possono

[36] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, Appendice 3

confermare o modificare le aspettative iniziali del revisore riguardo alle operazioni, ai saldi contabili e alle informazioni rilevanti per la revisione.

Nella valutazione del sistema informativo, il revisore esamina come l'impresa rileva le operazioni e raccoglie le informazioni necessarie per la preparazione del bilancio. Questo include l'analisi dei sistemi aziendali e delle direttive adottate per raggiungere gli obiettivi di gestione e di conformità. Alcune imprese possono avere sistemi così integrati che i controlli sono progettati per soddisfare contemporaneamente obiettivi finanziari, di conformità e di gestione. La comprensione del sistema informativo dell'impresa include anche la valutazione delle risorse umane coinvolte nelle attività di elaborazione delle informazioni. È importante considerare la competenza delle persone coinvolte nel lavoro, la disponibilità di risorse adeguate e l'adeguata separazione delle funzioni per garantire l'integrità del sistema informativo. Il revisore, nel comprendere le direttive che definiscono i flussi delle informazioni all'interno del sistema informativo e comunicazione, può considerare diversi aspetti. In particolare, può esaminare la natura dei dati o delle informazioni relative alle operazioni, agli eventi e alle condizioni da elaborare. Inoltre, può valutare le modalità con cui queste informazioni vengono elaborate per mantenere l'integrità dei dati stessi. Infine, può analizzare i processi informativi, il personale e le altre risorse utilizzate nel processo di elaborazione delle informazioni.

Il revisore ha la possibilità di utilizzare strumenti automatizzati per accedere direttamente ai database dell'impresa contenenti le registrazioni contabili. Questi strumenti consentono di verificare come le operazioni vengono registrate nel sistema informativo, tracciando le scritture contabili o altre registrazioni digitali relative alle operazioni. Analizzando popolazioni complete di operazioni, il revisore può individuare variazioni rispetto ai processi normali o attesi, che potrebbero indicare la presenza di

errori significativi. Inoltre, l'uso di tecniche automatizzate consente al revisore di confermare la corretta comprensione delle operazioni e dei processi aziendali.

Il revisore deve quindi avere una conoscenza approfondita dell'ambiente IT dell'impresa, comprese le specifiche applicazioni e altri aspetti rilevanti per i flussi di operazioni e l'elaborazione di informazioni nel sistema informativo. È importante comprendere come il modello di business dell'impresa integri l'utilizzo dell'IT per poter valutare i rischi derivanti dall'uso di queste tecnologie. Inoltre, il revisore deve essere in grado di identificare e comprendere le eventuali modifiche ai programmi delle applicazioni IT o ai dati contenuti nei database che potrebbero influenzare il flusso delle operazioni o delle informazioni nel sistema informativo. È fondamentale per il revisore acquisire una conoscenza dettagliata delle applicazioni IT e dell'infrastruttura di supporto, in modo da comprendere come le informazioni pertinenti per la revisione vengano elaborate e trasmesse all'interno del sistema informativo dell'impresa.

Attività di controllo

Il revisore, nell'esercizio della sua attività, ha il compito di individuare con precisione i controlli specifici inerenti all'attività di controllo all'interno dell'entità sottoposta a revisione. Deve valutare la configurazione di tali controlli e verificare se essi sono stati implementati correttamente. Questo processo permette al revisore di comprendere l'approccio adottato dalla direzione per gestire i rischi e fornisce una base per pianificare e eseguire le procedure di revisione necessarie per affrontare tali rischi, come richiesto dai principi internazionali di revisione.

In presenza di rischi elevati, definiti tali tramite lo spettro di rischio intrinseco, all'interno dell'entità controllata è fondamentale che il revisore disponga di elementi probativi solidi e persuasivi. Anche se il revisore non

ha l'intenzione di testare l'efficacia operativa dei controlli individuati, la sua comprensione degli stessi può influenzare la natura, la tempistica e l'estensione delle procedure di *audit* volte ad accertare la validità delle informazioni finanziarie e a mitigare i rischi di errori significativi.

Il processo di identificazione e valutazione dei controlli relativi alla componente “attività di controllo” si concentra principalmente sui controlli delle scritture contabili e sui controlli che il revisore intende verificare per garantire l'efficacia operativa. Questa valutazione è fondamentale per determinare quali procedure di validità adottare e per definire la natura, la tempistica e l'estensione di tali procedure.

La valutazione del rischio intrinseco da parte del revisore può influenzare significativamente l'identificazione dei controlli relativi alla componente "attività di controllo". Il revisore può identificare i controlli relativi ai rischi significativi solo dopo aver valutato il rischio intrinseco a livello di asserzioni. Inoltre, i controlli che affrontano i rischi per i quali le sole procedure di validità non forniscono prove sufficienti e adeguate possono essere identificati solo dopo che il revisore ha valutato il rischio intrinseco.

L'identificazione e la valutazione dei rischi di errori significativi a livello di asserzioni sono influenzate dalla comprensione delle direttive adottate dall'impresa per le attività di elaborazione delle informazioni all'interno della componente "sistema informativo e comunicazione", così come dall'identificazione e valutazione dei controlli relativi alla componente "attività di controllo".

La componente "attività di controllo" all'interno del sistema di controllo interno di un'impresa comprende i controlli che garantiscono l'applicazione corretta delle direttive in tutte le altre componenti del sistema. Questi controlli possono essere diretti o indiretti e sono cruciali per assicurare l'integrità delle informazioni nel sistema informativo

dell'azienda. Il revisore si concentra principalmente sui controlli relativi alle elaborazioni delle informazioni, che sono fondamentali per garantire la completezza, accuratezza e validità delle operazioni e delle informazioni. Non è necessario che il revisore identifichi e valuti tutti i controlli relativi alle direttive dell'impresa che definiscono i flussi delle operazioni e altri aspetti delle attività di elaborazione delle informazioni per le classi di operazioni, saldi contabili e informativa rilevanti per la revisione. Tuttavia, è importante considerare anche i controlli diretti presenti nell'ambiente di controllo, nel processo di valutazione del rischio e nel monitoraggio del sistema di controllo interno. È importante riconoscere che i controlli indiretti possono essere meno efficaci nel prevenire o individuare errori rispetto ai controlli diretti. Pertanto, è fondamentale che l'impresa implementi un sistema di controllo interno completo e ben strutturato per garantire l'efficacia dei controlli e la corretta gestione dei rischi.

Il revisore è tenuto a identificare e valutare una serie di controlli per garantire che le procedure di revisione siano condotte in conformità con gli standard professionali. Questi controlli includono:

- Controlli per verificare l'efficacia operativa nel determinare la natura, la tempistica e l'estensione delle procedure di validità, al fine di stabilire le procedure di conformità richieste dal principio di revisione internazionale n. 330;
- Controlli che affrontano i rischi significativi e i controlli sulle scritture contabili, che influenzano la comprensione dei rischi di errori significativi e determinano la natura, la tempistica ed estensione delle procedure di validità in risposta ai rischi identificati;

- Altri controlli ritenuti appropriati dal revisore per raggiungere gli obiettivi della revisione con riferimento ai rischi a livello di asserzioni, basati sul suo giudizio professionale.

Esempi di controlli nella componente “attività di controllo” includono le seguenti azioni:

- Autorizzazioni e approvazioni: garantire che tutte le transazioni siano autorizzate da personale competente e che le transazioni significative siano approvate da un livello gerarchico della direzione più elevato;
- Riconciliazioni: confrontare e conciliare regolarmente i dati finanziari e contabili per assicurare che siano corretti e completi. Se vengono identificate delle differenze viene messa in atto un’azione per raccordare i dati;
- Verifiche automatizzate: utilizzare sistemi informatici per controllare e verificare la correttezza dei dati inseriti e dei calcoli effettuati;
- Separazione delle funzioni: dividere i compiti e le responsabilità in modo da evitare conflitti di interesse e ridurre il rischio di frodi;
- Controlli fisici e logici: implementare misure di sicurezza fisiche e informatiche per garantire la protezione dei beni dell'azienda e dei dati sensibili;
- Controlli sulla conformità normativa: assicurare che l'informativa finanziaria sia redatta in conformità alle normative contabili e finanziarie applicabili, incluso l'*audit* del bilancio e delle informazioni non provenienti dalla contabilità generale.

I controlli che dovrebbero essere identificati e valutati in tutte le revisioni contabili per fronteggiare i rischi di errori significativi a livello di asserzioni sono i controlli sulle scritture contabili. Le imprese utilizzano

le scritture contabili per registrare le informazioni nella contabilità generale, che possono essere standard o non standard, automatizzate o manuali. La presenza di altri controlli può variare a seconda della natura dell'impresa e dell'approccio alle procedure di revisione adottato dal revisore.

Altri controlli che il revisore potrebbe ritenere appropriato identificare includono:

- Controlli che affrontano rischi valutati come significativi ma che potrebbero non essere stati identificati come tali in precedenza;
- Controlli che riguardano la conciliazione tra registrazioni di dettaglio e contabilità generale;
- Controlli aggiuntivi che l'impresa utilizzatrice potrebbe implementare se esternalizza determinate attività attraverso fornitori di servizi.

Nella valutazione di un controllo identificato, il revisore deve considerare se sia effettivamente in grado di prevenire, individuare e correggere errori significativi. Il revisore verificherà che il controllo effettivamente esiste, che l'impresa lo utilizzi e la configurazione dello stesso; un controllo configurato in modo improprio può creare una carenza nei controlli.

Al fine della valutazione dei controlli implementati e identificare eventuali criticità o punti deboli che possono influenzare la gestione del rischio è necessario effettuare indagini presso il personale dell'impresa, osservazioni dell'applicazione di controllo specifici e ispezioni di documenti e report. Al fine di acquisire elementi probativi non è sufficiente effettuare solo e unicamente indagini presso il personale dell'impresa.

Valutare la configurazione e controlli identificati nella componente "attività di controllo" non è sufficiente per verificare l'efficacia operativa.

Nel caso dei controlli automatizzati, il revisore può pianificare di verificare l'efficacia operativa testando il controllo automatico su una sola istanza, rispetto a tutti gli attributi rilevanti, e, al fine di garantire uniformità nell'operatività del controllo oggetto di test in periodi diversi dal momento in cui lo stesso test è stato svolto, fare affidamento sui controlli generali IT ove ne sussistano le condizioni. L'acquisizione di elementi probativi sulla messa in atto di un controllo manuale in un momento specifico non garantisce l'efficacia operativa del controllo in altri momenti durante il periodo di revisione. Le verifiche sull'efficacia operativa dei controlli, comprese quelle dei controlli indiretti, sono descritte in dettaglio nel principio di revisione internazionale n. 330.

Ambiente IT

La comprensione dei rischi derivanti dall'utilizzo dell'IT e dei controlli generali IT messi in atto dall'impresa può influenzare diversi aspetti della revisione contabile.

Innanzitutto, la decisione del revisore se verificare o meno l'efficacia operativa dei controlli per fronteggiare i rischi di errori significativi a livello di asserzioni dipenderà dalla configurazione e dall'efficacia dei controlli generali IT. Se i controlli generali non sono adeguati a prevenire o individuare correttamente modifiche non autorizzate ai programmi o accessi non autorizzati alle applicazioni IT, il revisore potrebbe decidere di non fare affidamento sui controlli automatizzati delle applicazioni coinvolte.

In secondo luogo, la valutazione del rischio di controllo a livello di asserzioni da parte del revisore potrebbe essere influenzata dall'efficacia operativa dei controlli generali IT. Ad esempio, se un controllo sulle elaborazioni delle informazioni dipende da controlli generali IT che prevengono modifiche non autorizzate ai programmi, la valutazione del

rischio di controllo sarà influenzata dalla presenza o dall'assenza di tali controlli generali.

La strategia del revisore per la verifica delle informazioni prodotte dall'impresa che coinvolgono applicazioni IT sarà influenzata dalla presenza o dall'efficacia dei controlli generali IT. Il revisore può decidere di verificare i controlli sui report generati dal sistema quando le informazioni prodotte dall'impresa da utilizzare come elementi probativi sono generate da applicazioni IT. Ciò include la verifica dei controlli generali IT che proteggono contro modifiche non appropriate o non autorizzate nei programmi, così come contro cambiamenti diretti ai dati contenuti nei report.

Inoltre, la valutazione del rischio intrinseco a livello di asserzioni potrebbe essere influenzata da significative modifiche nei programmi relativi alle applicazioni IT. Queste modifiche potrebbero essere indicative della complessità delle nuove disposizioni o aggiornamenti normativi, e potrebbero aumentare i rischi derivanti dall'utilizzo dell'IT.

Infine, la definizione delle procedure di revisione conseguenti potrebbe variare in base all'efficacia dei controlli generali IT. Se i controlli sulle elaborazioni delle informazioni dipendono dai controlli generali IT, il revisore potrebbe decidere di verificare l'efficacia operativa di tali controlli e definire procedure di conformità. Tuttavia, se si prevede che i controlli generali IT siano inefficaci, potrebbero essere necessarie procedure di validità per fronteggiare i rischi derivanti dall'utilizzo dell'IT o rendersi necessario un test di affidabilità delle informazioni generate da sistema per ciascuna istanza delle stesse su cui il revisore intenda fare affidamento. In alcuni casi, le sole procedure di validità non risultano essere sufficienti per ottenere adeguati e sufficienti elementi probativi, il revisore quindi dovrà considerare tali implicazioni per la formazione del giudizio del bilancio.

Per comprendere quali rischi derivanti dall'utilizzo dell'IT sono soggette le applicazioni IT dell'impresa, il revisore identifica le voci di bilancio significative, identifica i processi di business e le filiere informative che alimentano quelle voci di bilancio, identifica le *IT Dependencies* rilevanti (es. report, controlli automatici, ecc.), identifica i sistemi applicativi che supportano tali filiere informative e implementano tali *IT Dependencies*, comprende quali siano le infrastrutture IT che supportano tali sistemi applicativi, comprende quali sono i processi IT che governano tali infrastrutture, identifica i controlli che presidiano i rischi inerenti di processo IT. Il revisore si concentra sui controlli automatizzati che sono stati identificati, specialmente quelli che affrontano rischi che le sole procedure di validità non riescono a coprire adeguatamente. Inoltre, il revisore valuta come le informazioni necessarie per la revisione sono archiviate ed elaborate nel sistema informativo, e se la direzione si affida ai controlli generali IT per garantire l'integrità di tali informazioni. I controlli rilevati dal revisore possono dipendere da report generati dal sistema, in questo caso le applicazioni IT utilizzate per la generazione dei report possono essere soggette a rischi IT.

Qualora l'impresa presentasse un ambiente IT complesso è necessario coinvolgere all'interno del team di revisione membri con competenze specifiche nell'IT, al fine di contribuire all'identificazione, insieme al *core audit team*, delle applicazioni IT, dei controlli IT e dei relativi rischi derivanti da tale utilizzo.

Altri elementi dell'ambiente IT che possono presentare rischi derivanti da tale utilizzo comprendono la rete, i sistemi operativi, i database e le interfacce tra applicazioni IT. Questi aspetti vengono presi in considerazione quando il revisore identifica applicazioni IT soggette a rischi derivanti dall'uso dell'IT.

I rischi derivanti dall'utilizzo dell'IT variano in base alla natura e alle caratteristiche delle applicazioni IT e degli altri aspetti dell'ambiente IT. Possono sorgere rischi quando si utilizzano fornitori interni o esterni di servizi IT, ad esempio esternalizzando l'hosting del proprio ambiente IT a terzi o utilizzando un centro servizi condiviso. È più probabile che i rischi siano maggiori quando ci sono controlli automatizzati più complessi e l'azienda fa maggiore affidamento su di essi per garantire operazioni efficaci e l'integrità delle informazioni.

Comprensione dell'utilizzo dell'IT da parte dell'impresa nelle componenti del proprio sistema di controllo interno

Il sistema di controllo interno di un'impresa comprende sia elementi manuali che automatizzati, che vengono utilizzati per garantire la corretta gestione e monitoraggio delle attività dell'impresa. La combinazione di elementi manuali e automatizzati varia in base alla natura e alla complessità dell'utilizzo dell'IT da parte dell'impresa. L'IT influisce sul modo in cui le informazioni rilevanti per la redazione del bilancio vengono elaborate, archiviate e comunicate, influenzando quindi la configurazione e l'attuazione del sistema di controllo interno.

L'utilizzo dell'IT nel sistema di controllo interno permette anche di automatizzare processi ripetitivi applicando in maniera uniforme regole di gestione predefinite, riducendo il rischio di errori umani e aumentando l'efficienza complessiva dell'impresa. Inoltre, l'IT consente il miglioramento nella tempestività, disponibilità e accuratezza delle informazioni facilitandone l'analisi. Infine, l'IT permette di migliorare il monitoraggio delle attività dell'impresa e delle relative direttive e procedure, ridurre il rischio di elusione dei controlli e implementare controlli di sicurezza per garantire una separazione efficace delle funzioni in relazione alle applicazioni IT, database e sistemi operativi. I controlli automatizzati possono essere più affidabili dei controlli manuali perché

non possono essere elusi o ignorati facilmente e sono meno soggetti a errori umani. Possono essere più efficaci rispetto a controllo manuali in situazioni di elevato volume di operazioni ripetitive o prevedibili, che possono essere gestite e corrette in modo più efficiente attraverso l'automazione. Inoltre, i controlli il cui processo può essere configurato e automatizzato in modo appropriato possono trarre maggior beneficio dall'automazione.

Per un'impresa meno complessa che utilizza un software commerciale e non ha accesso al codice sorgente, acquisire una comprensione dell'ambiente IT può essere più semplice. Questo tipo di impresa potrebbe non avere risorse IT dedicate ma potrebbe avere un amministratore che si occupa dell'accesso ai dipendenti e degli aggiornamenti delle applicazioni forniti dal fornitore. Il revisore potrebbe considerare diversi aspetti per capire meglio il software utilizzato, come la sua affidabilità, la possibilità di apportare modifiche al codice sorgente o effettuare configurazioni, l'accesso ai dati per la redazione del bilancio e i controlli necessari per garantire l'integrità dei dati, specialmente in presenza di un grande volume di dati. Invece, gli ambienti IT complessi possono comprendere applicazioni altamente personalizzate o integrate, rendendo necessario un maggiore sforzo per comprenderli. I processi e le applicazioni IT per la preparazione dell'informazione finanziaria possono essere integrati con altre applicazioni utilizzate nelle attività operative dell'impresa. Questa integrazione coinvolge anche le applicazioni rilevanti per i flussi operativi e informativi dell'azienda. In tali contesti, alcune delle applicazioni utilizzate per le attività operative potrebbero essere importanti anche per la redazione del bilancio. Gli ambienti IT complessi possono richiedere dipartimenti IT dedicati con processi strutturati e personale competente. Alcune imprese potrebbero invece affidarsi a fornitori esterni per gestire parti del proprio ambiente IT, come ad esempio il servizio di hosting.

Attraverso la comprensione dell'ambiente IT dell'impresa, il revisore può determinare su quali applicazioni IT l'impresa si basa per elaborare in modo accurato le informazioni finanziarie e garantirne l'integrità. L'identificazione delle applicazioni IT su cui un'impresa fa affidamento è un fattore determinante per il revisore nella decisione di verificare i controlli automatizzati all'interno di tali sistemi. L'identificazione delle applicazioni IT utilizzate dall'impresa può influenzare la decisione del revisore di verificare i controlli automatizzati in esse implementati. Se l'impresa fa affidamento su un'applicazione IT, è probabile che i controlli automatizzati fronteggino i rischi identificati e siano verificati con successo. Al contrario, se l'impresa non fa affidamento su un'applicazione IT, i controlli automatizzati in essa implementati potrebbero non essere appropriati o sufficientemente precisi per essere verificati efficacemente. Ad esempio, i controlli automatizzati possono includere calcoli automatici o controlli sugli input, sull'elaborazione e sull'output come il triplice abbinamento di ordine di acquisto, documento di spedizione del fornitore e fattura. Quando il revisore identifica e capisce i controlli automatizzati e riconosce che l'impresa si affida all'applicazione IT che li contiene, potrebbe essere più probabile che identifichi tale applicazione come soggetta a rischi legati all'uso dell'IT.

Nel considerare se le applicazioni IT per le quali il revisore ha identificato controlli automatizzati siano soggette a rischi derivati dall'utilizzo dell'IT, il revisore terrà conto della possibilità che l'impresa abbia accesso al codice sorgente per apportare modifiche ai programmi sottostanti, valutando anche la frequenza e la formalizzazione delle modifiche effettuate. Inoltre, il revisore esaminerà il rischio di accesso non autorizzato o di manipolazione dei dati all'interno delle applicazioni IT.

I report generati dal sistema possono essere utilizzati come elementi probativi per il revisore. Questi report possono includere informazioni

come scadenze dei crediti commerciali o valutazione delle rimanenze di magazzino. Il revisore acquisisce elementi probativi sulla completezza e accuratezza dei report attraverso procedure di validità sugli input e output del report. Inoltre, il revisore può verificare l'efficacia dei controlli sulle procedure di generazione e mantenimento del report, esponendosi a rischi legati all'utilizzo dell'IT in quanto l'applicazione IT che genera il report potrebbe essere soggetta a tali rischi. È importante per il revisore verificare anche l'efficacia dei controlli generali IT per prevenire modifiche inappropriate o non autorizzate nei programmi che generano i report e nei dati contenuti all'interno di essi.

Un'applicazione IT è probabile che sia esposta a rischi derivanti dall'IT se le applicazioni sono interfacciate, il volume dei dati risulta essere elevato, la funzionalità dell'applicazione si dimostra complessa in quanto l'applicazione individua le operazioni automaticamente e risulta essere presente una molteplicità di calcoli complessi sottostanti gli inserimenti automatici; inoltre, è probabile che l'applicazione IT sia soggetta a rischi derivanti dall'IT quando la direzione si affida a un sistema applicativo per gestire l'elaborazione e la memorizzazione dei dati, in quanto il loro volume è considerevole[37].

Comprensione dei controlli generali IT

I controlli generali IT vengono implementati per gestire i rischi legati all'utilizzo dell'IT. Il revisore utilizza la sua comprensione delle applicazioni e dell'ambiente IT, così come dei relativi rischi, per identificare i controlli IT. Quando un'azienda utilizza processi IT comuni, è possibile identificare rischi e controlli generali comuni.

[37] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, Appendice 5

I controlli generali IT per ciascuno degli aspetti dell'ambiente IT sono essenziali per garantire la sicurezza e l'integrità dei dati. Per le applicazioni IT, i controlli dipenderanno dalla complessità e dalla portata delle funzionalità, così come dalle modalità di accesso consentite. Ad esempio, le applicazioni altamente integrate e complesse richiederanno maggiori controlli rispetto alle applicazioni legacy con funzionalità limitate.

Per quanto riguarda i database, i controlli generali IT sono volti a prevenire aggiornamenti non autorizzati alle informazioni finanziarie cruciali, che potrebbero avvenire attraverso accessi diretti, script o programmi non autorizzati. Per i sistemi operativi, i controlli mirano a prevenire l'accesso non autorizzato come amministratore di sistema, che potrebbe compromettere le credenziali degli utenti, aggiungere nuovi utenti non autorizzati, caricare virus o l'esecuzione di programmi non autorizzata.

I controlli di rete sono fondamentali per gestire i rischi legati alla trasmissione dei dati, all'accesso remoto e all'autenticazione. Sono particolarmente importanti per le aziende che hanno relazioni commerciali significative con terzi, aumentano la necessità di un accesso remoto sicuro.

I controlli generali IT organizzati per processo IT includono:

- Gestione dell'accesso: controlli per garantire che solo gli utenti autorizzati abbiano accesso alle informazioni necessarie per svolgere le proprie responsabilità, che tali utenti stiano utilizzano le proprie credenziali
- Gestione delle modifiche: controlli per gestire in modo controllato e sicuro le modifiche ai programmi o all'ambiente IT.
- Gestione delle operazioni IT: controlli per garantire il corretto funzionamento delle operazioni quotidiane, monitorare i job critici

e garantire la disponibilità dei dati in caso di emergenza tramite backup[38].

2.4.3 Identificazione e valutazione dei rischi di errori significativi

Le informazioni raccolte durante le procedure di valutazione del rischio sono essenziali per l'identificazione e la valutazione dei potenziali rischi di errore significativo. Ad esempio, gli elementi probativi ottenuti nel valutare la configurazione dei controlli identificati e nel determinare se siano stati effettivamente messi in atto vengono utilizzati per supportare la valutazione del rischio. Questi elementi probativi vengono utilizzati dal revisore per definire le risposte generali di revisione per affrontare i rischi di errori significativi a individuati e valutati a livello di bilancio; inoltre, tali elementi probativi aiutano il revisore a stabilire e adattare le procedure di revisione successive in modo da affrontare specificamente i rischi rilevanti a livello di asserzioni contabili.

Rischi di errori significativi a livello di bilancio

Il revisore ha il compito di individuare i rischi di errori significativi a livello di bilancio per determinare se i rischi abbiano un effetto pervasivo sul bilancio. Inoltre, individuare i rischi di errori significativi a livello di bilancio aiuta il revisore a valutare i rischi di errori significativi a livello di asserzioni, in quanto i rischi a livello di bilancio possono appunto influenzare le singole asserzioni, e definire le procedure di revisione successive in relazione agli stessi.

L'identificazione di tali rischi possono essere influenzate dalla comprensione da parte del revisore del sistema di controllo interno dell'impresa, nello specifico dall'ambiente di controllo, i processi adottati

[38] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, Appendice 6

dall'impresa per la valutazione del rischio e per il monitoraggio del sistema di controllo. In particolare, i rischi a livello di bilancio possono originarsi da problemi nel sistema di controllo interno dell'azienda o da fattori esterni come l'andamento economico negativo.

Rischi di errori significativi a livello di asserzioni

Il revisore valuta attentamente la probabilità e l'entità degli errori potenziali correlati ai rischi individuati, dal momento che il grado di rischio intrinseco associato dipende dalla combinazione di questi due fattori. È fondamentale determinare il punto preciso in cui si colloca il rischio individuato all'interno dello spettro del rischio, in modo da poter elaborare procedure di revisione specifiche ed efficaci per affrontare tale rischio in maniera adeguata.

La valutazione del rischio intrinseco riguardante un particolare rischio di errori significativi a livello delle asserzioni richiede un giudizio professionale che tiene conto dell'intervallo di rischio intrinseco, che va dall'estremità inferiore a quella superiore dello spettro del rischio. Questo giudizio riguardante il punto in cui il rischio si inserisce all'interno dello spettro dipende dalla natura, dalle dimensioni e dalla complessità dell'azienda, e tiene conto della valutazione della probabilità e dell'entità degli errori, nonché dei fattori di rischio intrinseco.

Fattori di rischi intrinseco

I fattori di rischio intrinseco sono caratteristiche di eventi o condizioni che influenzano la possibilità che un'asserzione relativa ad una classe di operazioni, un saldo contabile o un'informativa contenga errori, dovuti a frodi o comportamenti non intenzionali. Tra fattori di rischio intrinseco relativi alla predisposizione delle informazioni richieste dal quadro normativo sull'informazione finanziaria applicabile, si posso individuare:

- La complessità - La complessità deriva sia dalla natura delle informazioni che dalle modalità con cui sono predisposte. Ad esempio, quando vengono utilizzate molte fonti di dati con caratteristiche diverse e l'elaborazione dei dati richiede molte fasi correlate, si verifica una maggiore difficoltà nell'identificazione, acquisizione, accesso, comprensione ed elaborazione dei dati.
- La soggettività - La soggettività è determinata dalla limitata capacità di predisporre obiettivamente le informazioni richieste, a causa dei limiti nella conoscenza disponibile. Questo porta la direzione a fare scelte soggettive sull'approccio da adottare e sulle informazioni da includere nel bilancio. All'aumentare dei limiti nelle conoscenze o nei dati, aumenta anche la soggettività nelle valutazioni che potrebbero essere effettuate da individui informati e indipendenti, portando a una maggiore diversità nei risultati possibili.
- I cambiamenti - I cambiamenti nelle imprese sono causati da eventi o condizioni che nel tempo influenzano diversi aspetti dell'attività aziendale, come quelli di natura economica, contabile, regolamentare, di settore o altri aspetti del contesto in cui l'impresa opera. Questi cambiamenti possono avere un impatto sulle decisioni e valutazioni della direzione, compresa la scelta dei principi contabili, le modalità con cui vengono effettuate le stime contabili e l'informazione correlata.
- L’incertezza - L'incertezza si presenta quando le informazioni richieste non possono essere garantite solo attraverso dati precisi, completi e verificabili tramite osservazione diretta. In questi casi, potrebbe essere necessario utilizzare le conoscenze disponibili per predisporre le informazioni utilizzando dati osservabili accurati e completi, se disponibili, oppure assumere ipotesi ragionevoli supportate dai dati più appropriati disponibili.

- La possibilità di errori dovuti a ingerenze da parte della direzione- La possibilità di ingerenze da parte della direzione può derivare da condizioni che mettono a rischio la neutralità della direzione nel predisporre le informazioni. Queste ingerenze possono essere intenzionali o involontarie e portare a errori significativi nelle informazioni, potenzialmente anche fraudolenti. Alcuni indicatori di possibili ingerenze da parte della direzione includono incentivi o pressioni che influenzano il rischio e l'opportunità di mantenere la neutralità nella valutazione delle informazioni[39].

Il revisore utilizza la significatività della combinazione tra la probabilità e l'entità di un possibile errore per stabilire il punto dello spettro del rischio intrinseco in cui è valutato il rischio intrinseco. Quanto più alta è la combinazione tra probabilità e entità, tanto più alta sarà la valutazione del rischio intrinseco; quanto più bassa è la combinazione tra probabilità e entità, tanto più bassa sarà la valutazione del rischio intrinseco. Non necessariamente un rischio valutato elevato nello spettro del rischio intrinseco si traduce in una probabilità e un'entità dell'errore elevata. La posizione all'interno dello spettro dipende dall'intersezione dei due elementi, per esempio potrei avere un rischio valutato elevato dovuto ad una combinazione tra probabilità valutata bassa e entità valutata molto alta. In base alla valutazione dei rischi, il revisore può creare delle categorie di rischi di errore significativo all'interno dello spettro del rischio intrinseco con il fine di pianificare strategie adeguate in risposta ai rischi di errori significativi. La prossimità all'estremità superiore dello spettro del rischio intrinseco varia da impresa a impresa, e può anche variare da periodo amministrativo nella medesima impresa.

[39] IAASB, Principio di Revisione Internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, Appendice 2

Se nel valutare i rischi di errori significativi a livello di asserzioni il revisore si dovesse rendere conto che alcuni di questi rischi si riferiscono in modo più pervasivo al bilancio nel suo complesso e quindi interessare più asserzioni può modificare e aggiornare l'identificazione di rischi di errori significativi a livello di bilancio.

È importante stabilire quali rischi siano significativi in quanto permette al revisore di focalizzarsi principalmente su quei rischi che si trovano nell'estremità superiore dello spettro del rischio intrinseco per poi mettere in atto risposte adeguate.

In primo luogo, è necessario identificare i controlli che fronteggiano i rischi significativi e valutare se tali controlli siano stati configurati in modo efficace e siano stati messi in atto. Inoltre, è richiesto che i controlli che fronteggiano tali rischi siano verificati nel periodo di amministrazione soggetto a revisione e che vengano pianificate e svolte procedure di validità in risposta ai rischi identificati.

Altro elemento da considerare, il revisore deve acquisire elementi persuasivi tanto più pertinenti e persuasivi quanto più è elevata la posizione del rischio significativo all'interno dello spettro di rischio intrinseco.

Inoltre, il revisore deve comunicare alla direzione e ai responsabili dell'attività di governance i rischi identificati.

Infine, un riesame tempestivo della documentazione contabile da parte del responsabile dell'incarico durante tutte le fasi della revisione è fondamentale per affrontare rapidamente e in modo efficace gli aspetti critici, compresi i rischi rilevanti, entro la data della relazione di revisione o prima di essa.

Tra le situazioni che possono aumentare il rischio intrinseco ci sono le operazioni contabili che ammettono diversi trattamenti e che quindi

richiedono un giudizio soggettivo, le stime contabili soggette a elevata incertezza o basate su modelli complessi, la complessità nella raccolta e nell'elaborazione dei dati contabili, i saldi contabili che richiedono calcoli complessi, i principi contabili che possono essere interpretati in modi diversi e i cambiamenti nel business dell'azienda che comportano modifiche nei principi contabili, come ad esempio fusioni e acquisizioni.

CAPITOLO 3
COME SI INSERISCE l'ISA 315 R NEL PROCESSO DI REVISIONE

Dal mese di gennaio fino aprile 2024 ho avuto l'opportunità di svolgere uno stage nell'ambito dell'Audit Risk Financial Services presso una delle Big4. Con questo capitolo vorrei appunto mostrare come si inserisce il principio di revisione ISA 315 R all'interno del processo stesso; quindi, quali sono nella pratica gli step eseguiti da un team di revisione. Questo in quanto il nuovo principio ha chiarito alcuni aspetti che avevano portato a problemi interpretativi su come applicare operativamente il principio, siccome la precedente versione aveva generato delle difformità di applicazione del principio da parte delle varie società di revisione. Lo IASSB a tal fine ha mantenuto sostanzialmente invariata la struttura generale del principio ante revisione ma ha esplicitato maggiormente una serie di aspetti che presentano una ricaduta operativa; quindi, fornisce una serie di linee guida operative per l'applicazione del principio.

3.1 Fase di planning

La fase di planning, come spiegato nel primo capitolo, è quella fase in cui viene pianificata l'attività di revisione affinché sia svolta in modo efficace. Il revisore come prima cosa deve identificare e valutare i rischi di errori significativi all'interno del bilancio, questo è possibile tramite la comprensione dell'impresa e del contesto in cui opera, incluso il suo sistema di controllo interno. Ciò permette al revisore di comprendere gli eventi e le condizioni rilevanti per l'impresa e identificare la modalità tramite cui i fattori di rischio intrinseco influenzano la possibilità che le asserzioni contengano errori. In questa fase, quindi, il revisore deve comprendere il business del cliente, approfondire le conoscenze

dell'ambiente IT, valutare l'affidabilità del controllo interno, definire i valori soglia ovvero la materialità e le asserzioni impattanti il bilancio.

Criteri di valutazione del rischio di errore significativo

Primo step: fattori rilevanti

Il principio prima di entrare nel merito della valutazione del rischio a livello di asserzioni fa riferimento ai "fattori rilevanti" effettuando un primo *assessment* del rischio a livello di singola voce di bilancio intesa nella sua totalità. Il revisore per ogni voce del bilancio analizza determinali fattori, quali:

- Dimensione e composizione della voce;
- Suscettibilità della voce ad errori o frodi;
- Volume di attività, complessità, omogeneità delle transazioni;
- Natura della voce, delle classi di transazioni e della relativa disclosure;
- Complessità dei criteri di contabilizzazione e reporting;
- Impatto di transazioni con parti correlate;
- Modifiche significative rispetto al periodo precedente;
- Impatto di stime o valutazioni soggettive;

Questa prima analisi fornisce al revisore già un'idea sulla suscettibilità dell'errore in relazione a quella determinata voce, quindi permette di capire se la stessa è suscettibile o meno al rischio e in quale misura. Ad esempio, una voce caratterizzata dall'applicazione di principi contabili particolarmente complessi o di prima applicazione è maggiormente suscettibile ad un errore rispetto a una voce per la quale i principi di riferimento sono meno complessi o consolidati.

Secondo step: Identificazione delle asserzioni applicabili alle singole voci

Fatta questa prima analisi delle voci tramite i *driver* di fattori rilevanti si procede all'analisi delle singole asserzioni per ogni voce. Le asserzioni si suddividono nelle seguenti categorie:

- Accuratezza (A): le attività/passività/operazioni sono state correttamente rilevate, ciò include anche la corretta classificazione degli importi, dei saldi e dell'informativa in bilancio;
- Completezza (C): Tutto ciò che dovrebbe essere registrato o formare oggetto di informativa in bilancio è stato incluso. Non vi sono attività, passività, operazioni o eventi che non siano stati registrati; non vi sono note al bilancio mancanti o incomplete;
- Cut off (CO): le operazioni e gli eventi sono stati registrati nel corretto periodo amministrativo;
- Esistenza e occorrenza (E/O): le operazioni e gli eventi che sono stati registrati si sono verificati e riguardano l'impresa;
- Presentazione e informativa (P/D): una voce/operazione è evidenziata, classificata e corredata da adeguata informativa;
- Diritti e obblighi (R/O): una attività/passività è di pertinenza dell'azienda ad una certa data;
- Valutazione (V): Le attività, le passività e le interessenze nel patrimonio netto sono registrate in bilancio per l'importo o valore corretto. Ogni rettifica di valutazione richiesta dalla loro natura o dai principi contabili applicabili è stata registrata correttamente.

Il revisore all'interno del bilancio ha una serie di voci, per ognuna di esse deve valutare quali asserzioni sono applicabili, ovvero quali sono quelle asserzioni che nel caso in cui non dovessero essere verificate possono portare alla manifestazione di un errore materiare e quindi significativo,

che può impattare su quella voce. Di conseguenza, la manifestazione dell'errore impatterebbe sulla voce su cui si applica un'asserzione specifica. Come prima cosa il revisore analizza una voce e si domanda quali sono le asserzioni *applicabili* alla stessa. Applicabile significa che, se si dovesse manifestare un rischio per il fatto che va ad impattare su quell'asserzione, può determinare un errore all'interno di quella voce di bilancio per la quale quell'asserzione risulta applicabile.

Per esempio, il revisore si domanda se l'asserzione completezza sia applicabile alla voce crediti; questa asserzione risulta essere applicabile alla voce crediti poiché vi è la possibilità di avere dei crediti sovra o sottostimati in temini di numerosità e porterebbe a una sovra o sottostima del valore dei crediti di bilancio. Al contrario, con riferimento a voci non caratterizzate da alcuna componente valutativa, l'asserzione V(Valutazione) risulterebbe essere non applicabile (c.d. inerentemente non rilevante).

Il revisore utilizza le asserzioni come driver per capire quale tipologia di rischio può essere applicabile a quella voce, nell'esempio sopra citato l'asserzione completezza crediti si riferisce al fatto che esiste una qualche probabilità tale per cui il rischio di incompletezza si può applicare a quella voce di bilancio. Il rischio, come già spiegato precedentemente, può essere misurato attraverso la combinazione probabilità e impatto, il revisore quindi deve analizzare la probabilità di manifestazione del rischio e, per fare, ciò il principio introduce il concetto di "spettro del rischio".

Terzo step: spettro del rischio

Il nuovo principio considera un rischio come rischio significativo nel momento in cui la sua probabilità di manifestazione è più che remota. Operativamente, significa stabilire una soglia al di sotto della quale il rischio risulta essere meno che remoto, a livello della soglia il rischio è

remoto, al di sopra della soglia la manifestazione del rischio è più che remota. Tutti questi rischi, la cui probabilità di manifestazione è più che remota, sono definiti rischi significativi. Quindi il rischio risulta essere significativo sulla base della sua collocazione all'interno dello spettro del rischio. L'introduzione di un concetto di "spettro", cioè di un intervallo di variabilità del rischio, consente, in termini operativi, di trattare in maniera diversa due rischi che siano classificabili entrambi come rischi significativi (misura del rischio superiore alla soglia di rischio remoto), ma che si collochino l'uno in prossimità della soglia di riferimento, l'altro in prossimità del limite superiore dell'intervallo di variazione del rischio. Ragionevolmente la probabilità di manifestazione di quest'ultimo rischio sarà maggiore e quindi relativamente più invasive potrebbero essere le procedure di revisione poste in essere dal revisore. Tutto ciò in coerenza con un approccio, proposto in maniera esplicita nel principio, di scalabilità e proporzionalità nell'approccio di revisione adottato.

Quarto step: fattori di rischio inerente

Lo IASSB per garantire un approccio di *risk assessment* quanto più possibilmente omogeneo ha inserito i fattori di rischio inerente. Tali fattori di rischio vengono utilizzati per stimare da un punto di vista operativo la probabilità di manifestazione associata al rischio. I fattori da considerare sono:

- Complessità;
- Soggettività;
- Variabilità e cambiamento;
- Incertezza;
- Suscettibilità ad errore anche in conseguenza di pregiudizio o frode.

In merito all'esempio sopra riportato la voce crediti potrebbe essere affetta da errore in quanto la gestione del credito potrebbe non essere un processo

semplice, non vengono gestiti unicamente prodotti standard, oppure l'entità potrebbe far parte di un gruppo invece che essere un'entità a sé o, in aggiunta, potrebbe avere più applicativi magari anche customizzati piuttosto che avere un unico applicativo standard.

Maggiori sono i fattori di rischio inerente impattanti le asserzioni applicabili alla specifica voce, maggiore è la probabilità che si possa manifestare un rischio che impatti la voce stessa

Rispetto al principio ante revisione il revisore è obbligato a considerare i fattori di rischio intrinseco ed esplicita quali essi siano.

Il rischio quindi, oltre che essere più che remoto, si può collocare più vicino alla soglia stabilita o molto distante da essa; quanto più il rischio si sposta nel range che va dalla soglia definita all'estremo superiore dell'intervallo, tanto maggiore è la probabilità di errore e quindi il rischio viene rilevato come rischio significativo.

Il rischio inerente può essere classificato come normale, elevato e significativo.

Da un punto di vista operativo è importante effettuare questo tipo di analisi, ovvero valutare i fattori di rischio per stimare la probabilità di manifestazione associata al rischio e considerare come la probabilità si posiziona rispetto alla soglia che definisce il rischio remoto, tale per cui la probabilità può essere al di sotto della soglia, coincidere con essa o essere al di sopra, in quanto mi permette di stabilire se l'asserzione è rilevante o meno.

Quinto step: tipologie di asserzioni

Le asserzioni possono essere classificate come:

- Asserzioni rilevanti: tutte quelle asserzioni affette da un rischio la cui probabilità di manifestazione è più che remota ed è affetta da

un rischio di errore significativo, ciò determina la classificazione della voce di bilancio come significativa;

- Asserzioni inerentemente non rilevanti: ovvero rispetto a quella voce specifica in assoluto non si applicata l'asserzione in quanto non pertinente;
- Asserzioni senza una ragionevole possibilità di errore significativo: quelle che, definita la loro applicabilità alla voce oggetto di analisi, sono caratterizzate da una probabilità di manifestazione di un errore che le può andare ad impattare remota o meno che remota.

Questa classificazione viene effettuata per tutte le asserzioni di bilancio che si applicano a quella voce di bilancio.

È importante capire se in riferimento a quella voce di bilancio ho un'asserzione rilevante perché, se una voce di bilancio ha almeno un'asserzione classificata come rilevante, allora quella voce di bilancio si classifica come voce di bilancio significativa.

Definizione della risposta di revisione in funzione dell'attività di risk assessment e di classificazione delle voci

In base a come il revisore classifica la voce di bilancio varierà l'approccio di revisione. A fronte dell'attività di valutazione del rischio voce per voce, l'esito finale di questa attività porta a classificare le voci in tre categorie[40], la differente classificazione in termini operativi comporta un approccio in termini di strategia di revisione diverso.

[40] Le voci di bilancio possono essere classificate in significative, non significative ma materiali, non significative e non materiali. Tema approfondito successivamente.

Identificazione e valutazione dei sistemi informativi rilevanti per il revisore

Primo step: driver di complessità

Una delle motivazioni che ha guidato la IAASB nella formulazione del nuovo principio è stata dettata dalla sempre più spinta centralità dei sistemi informativi nella generazione e gestione di dati e informazioni rilevanti con riferimento al processo di *financial reporting*. In tale contesto, il principio fornisce una serie di spunti operativi che dovrebbero orientare il revisore nel processo di *assessment* del rischio IT.

Il principio fornisce una serie di driver di complessità legati ai sistemi IT che permettono al revisore di desumere se l'ambiente IT risulta essere complesso, non complesso, moderatamente complesso. I driver indicati dal principio sono:

- Grado di automazione;
- Grado di affidamento da parte della società sui report generati da sistema;
- Grado di personalizzazione del sistema;
- Grado di orientamento del business model verso la digitalizzazione;
- Tasso di cambiamento;
- Utilizzo di tecnologie emergenti.

In base a come il revisore classifica i sistemi informativi cambia la strategia di revisione, operativamente può impattare sulla necessità di coinvolgere o meno specialisti in ambito IT, oppure può impattare sulla definizione delle procedure di sostanza e test di controllo.

Questa valutazione in passato veniva comunque effettuata, ma seguendo criteri che ciascun valutatore si definiva. Nell'ambito dell'ISA 315 Revised, lo IAASB ha definito dei criteri di valutazione della complessità

puntuali, il revisore deve analizzare in modo rigoroso la corretta applicazione di questi criteri. Il nuovo principio ha reso questo processo operativamente oggettivo la cui ricaduta operativa si caratterizza da una maggior complessità dell'attività, maggior impiego di tempo per l'analisi di ogni driver e la necessità di documentare l'attività anche per rendere il processo ripercorribile.

Secondo step: IT Dependencies

I processi d business e le filiere informative alimentanti le singole voci di bilancio sono supportati da sistemi applicativi, innestati su specifiche infrastrutture IT, nell'ambito delle quali sono disegnate e implementate soluzioni di carattere funzionale dipendenti dall'IT (*IT Dependencies*) che contribuiscono alla generazione e alla gestione di dati e informazioni. L'errato funzionamento di tali componenti potrebbe determinare errori che minano l'integrità dei dati e delle informazioni rilevanti con riferimento alle filiere informative alimentanti il bilancio e, quindi, potenzialmente influire sulla generazione di errori materiali impattanti le voci di bilancio alimentate.

Le *IT Dependencies* sono cinque:

- Automated controls;
- Report;
- Interfaces;
- Calculations;
- Segregation of duty.

Venivano identificate anche nel precedente principio ma mancava la correlazione stretta fra le *IT Dependencies* e i processi IT a supporto delle stesse.

Le *IT Dependencies* vengono generate all'interno di un sistema applicativo specifico, il revisore considera rilevante il sistema applicativo se nel suo processo di revisore intende fare affidamento su quella determinata *IT Dependency*. Il sistema applicativo risulta essere rilevante in quanto supporta la filiera informativa e genera per esempio il report su cui il revisore intende fare affidamento. Per poter capire se un sistema applicativo è rilevante o meno il revisore deve capire cosa genera e come processa le informazioni e come tale modalità impatta l'impostazione delle procedure di revisione. Quindi, per poter valutare una *IT Dependencies* e validarla, se su di essa il revisore intende fare affidamento, nel nostro esempio, è necessario associare il report ad un sistema applicativo specifico.

Il sistema applicativo è rilevante oltre che nei casi in cui generi report su cui il revisore o la società oggetto di revisione intendano fare affidamento anche per il fatto che gestisce flussi di dati e informazioni, in input e output, che possono risultare rilevanti per il revisore e, di conseguenza, possono impattare sulle attività di revisione. Tale impatto potrebbe riguardare la sfera dei test di dettaglio o la valutazione della struttura del controllo interno dell'entità su cui il revisore potrebbe decidere di fare affidamento.

I sistemi applicativi che generano *IT Dependencies* sono concretamente implementati su una struttura IT e quindi gestiti attraverso processi IT. Come tutti i processi, anche i processi IT, possono essere affetti da rischi di processo che potranno essere presidiati da attività di controllo che si innestano su ciascun processo IT e che prendono il nome di Controlli Generali IT (ITGCs). Non tutti i processi IT risultano essere rilevanti ai fini della revisione, in quanto se dovessi ipotizzare di verificare una serie di *IT Dependencies* che fanno riferimento ad un unico sistema applicativo che però non è sviluppato all'interno dell'entità, il processo IT di gestione

di tutte le fasi di sviluppo applicativo potrebbe non essere del tutto rilevante.

Il revisore quindi, parte dall'identificazione delle voci di bilancio; attraverso il processo di risk assessment svolto sulle voci di bilancio le classifica ed è importante perché in funzione di questa dipende l'approccio di revisione. Le voci vengono generate poiché esiste un processo che determina una filiera informativa che alimenta le voci stesse. La filiera viene gestita da sistemi applicativi a supporto, i quali sono rilevanti ma non tutti hanno la stessa importanza, la rilevanza dipende da cosa generano questi sistemi applicativi (IT Dep.) e l'utilizzo che ne viene fatto nell'ambito dell'attività di revisione, che può riguardare l'ambito della sfera dei test di dettaglio oppure la sfera del controllo interno. Tutte le volte che il revisore fa affidamento su un output di sistema, tale output deve essere validato. Il numero di *IT Dependencies* correlabile a una determinata applicazione determina, insieme ad altri fattori che il revisore può prendere in considerazione,[41] il grado di rilevanza di tale applicazione. I sistemi applicativi sono innestati su infrastrutture IT che vengono gestiti dall'entità attraverso processi IT. Quindi, i processi IT gestiscono i sistemi applicativi a cui sono correlate un numero più o meno elevato di *IT Dependencies*, i sistemi applicativi però potrebbero non impattare su tutti i processi IT ma solo su alcuni. Questa analisi permette di definire il perimetro ITGCs che varia in funzione della strategia di revisione impostata.

Una volta definito il perimetro ITGCs, i controlli generali IT su cui il revisore intende fare affidamento vanno testati; questo test genererà un esito positivo o negativo.

[41] Si pensi, a tiolo esemplificativo, ai seguenti elementi: tipologia di processo/area di bilancio supportata, grado di innovazione della tecnologia utilizzata, gradi di pervasività del sistema applicativo, ecc.

Con riferimento alla correlazione esistente fra le procedure di revisione adottate in relazione al test dei controlli generali IT e le modalità di test delle *IT Dependencies* valgono le seguenti considerazioni:

- Identificate le *IT Dependencies* rilevanti, se su di esse il revisore intenderà fare affidamento, occorrerà procedere alla loro validazione attraverso opportune attività di test
- Il revisore svolge la propria attività di test a una data definita e gli esiti di tale attività di validazione sono riferibili, a rigore, unicamente alla data in cui il test è stato effettuato o al periodo a cui è riferibile l'*IT Dependency* testata
- Ciò comporterebbe la necessità, per il revisore, di attuare un processo di test iterativo applicato a ciascuna delle istanze dell'*IT Dependency* in oggetto. Ad esempio, se il report rilevante viene generato mensilmente (12 volte in un esercizio) il revisore dovrebbe testare lo stesso report per 12 volte,
- Tuttavia, se il revisore potesse ottenere comfort in merito al fatto che la logica alla base dell'IT Dependency testata (ad esempio un report) non abbia subito modifiche nel corso dell'esercizio, allora potrebbe concludere che l'esito ottenuto a fronte del test effettuato a una data specifica e su unica istanza del report possa essere esteso all'intero periodo oggetto di audit.
- Tale comfort potrebbe derivare dal testare, con esito positivo, i controlli generali IT relativi al processo di sviluppo applicativo; ottenendo *assurance* circa il fatto che i processi IT di sviluppo applicativo e i relativi rischi inerenti siano adeguatamente governati e che, quindi, sia remota la possibilità che la logica alla base del report oggetto di test possa essere stata modificata in assenza di un robusto processo di governance IT.

Nel dettaglio il revisore parte dalla voce di bilancio, essa viene alimentata da un processo di filiera informativa, che è supportata da uno o più sistemi applicativi, le applicazioni implementano una o più *IT Dependencies*, testo le *IT Dependencies* che sono rilevanti ai fini della revisione, la validità dell'esito che il test svolto a livello di processo di business valga per l'intero esercizio è determinata dal fatto che quel sistema applicativo è supportato da una serie di processi IT i cui rischi sono indirizzati dagli ITGCs, questi controlli vengono valutati in termini di disegno e se l'esito di questo test è positivo possiamo fare affidamento su di esse.

Il revisore non deve effettuare questa attività per tutti i processi IT e i controlli dell'entità ma solo sul perimetro ITGCs che ritiene opportuni, guidato dalla selezione dei sistemi applicativi di interesse, cioè quelli che supportano sia le filiere informative sia quelli che implementano una serie di *IT Dependencies* che sono rilevanti ai fini della revisione.

Potrebbero esserci altri rischi IT che non dipendono dalle *IT Dependencies*, per esempio un rischio relativo alla sicurezza fisica; i server che fanno funzionare le applicazioni sono all'interno delle server room, se un individuo dovesse rompere tali server l'applicazione sarebbe danneggiata, il rischio che ci sia un'effrazione fisica non è legato ad un processo di business specifico anche se genera un rischio IT che va ugualmente gestito. Il revisore, pertanto, identifica controlli generali IT, relativi sia alla gestione dei rischi inerenti dei processi IT, che derivano per la maggior parte dall'analisi delle *IT Dependencies,* sia da altri rischi IT non direttamente correlabili a rischi di business afferenti le filiere informative in perimetro. A questo punto, una volta definito il perimetro ITGCs, il revisore avrà identificato una serie di controlli che devono essere testati, in termini di valutazione del disegno, di effettiva implementazione e di efficacia operativa.

Scalabilità

Ulteriore elemento che è stato introdotto nel nuovo principio è il concetto di scalabilità: in funzione della valutazione del rischio non necessariamente l'approccio di revisione deve essere uniforme in tutto. Operativamente, una volta che il revisore ha identificato le voci di bilancio e le ha classificate in funzione dell'esito della procedura di risk assesment, può definire la strategia di revisione per quella voce. Per l'area crediti definita come significativa in quanto almeno una delle asserzioni ad essa applicabile risulta essere rilevante adotterò una strategia diversa rispetto alla voce spese del personale che non ritengo rilevante ma materiale in quanto saldo elevato.

Questo approccio di scalabilità si può anche applicare al modo in cui il revisore va ad analizzare i processi e la filiera informativa, se la voce è significativa sarà opportuno un approccio più approfondito, se la voce non è significativa ma materiale avrò un approccio scalabile. In funzione dell'esito del processo di valutazione del rischio sono necessari degli approcci differenziali in termini di mappatura e analisi dei processi e delle filiere informative.

Approccio differenziato all'identificazione, valutazione dei controlli in funzione della natura del rischio sotteso

L'ISA chiarisce una serie di aspetti dell'attività che va svolta in termini di valutazione del disegno e di validazione con riferimento alle attività di controllo in considerazione della natura del rischio che queste attività di controllo vanno a indirizzare.

Il revisore deve acquisire una comprensione della componente attività di controllo, svolgendo procedure di valutazione del rischio[42] attraverso

[42] IAASB, Principio di revisione internazionale (ISA Italia) 315, "Identificazione e valutazione dei rischi di errori significativi", 2019, par. 26

l'identificazione dei controlli che fronteggiano i rischi di errori significativi a livello di asserzioni nel seguente modo:

- I controlli che fronteggiano un rischio ritenuto significativo. Il revisore si domanda se il controllo che sta analizzando intende presidiare un rischio inerente di processo (IPO) che risulta essere un rischio significativo, ovvero caratterizzato da una probabilità di manifestazione più che remota, se la risposta a tale domanda è positiva il controllo analizzato rientra in questa prima categoria;
- I controlli sulle scritture contabili, incluse le scritture non standard utilizzate per registrare operazioni non ricorrenti o inusuali o le scritture di rettifica;
- I controlli che non presidiano rischi significativi, che non sono a presidio di rischi riguardanti le scritture contabili ma che nella strategia di revisione si vogliono testare poiché su di essi si intende fare affidamento, in quanto si valuta che, con riferimento ad una particolare voce di bilancio, le sole procedure di dettaglio non sono sufficienti;
- Controlli residuali che il revisore, in base al proprio giudizio professionale, ritiene appropriato testare per raggiungere un maggiore comfort.

Inoltre, il principio esplicita che per tutti i controlli individuati e che rientrano in queste categorie, il revisore deve almeno svolgere un'attività di valutazione del disegno, verificare l'effettiva implementazione del controllo e fornire evidenze che non siano limitate alle sole interviste del personale. Se il revisore intende fare affidamento su quel determinato controllo deve anche testarlo in termini di efficacia operativa.

Tutte le volte che il revisore individua un controllo che presidia un rischio significativo e appartiene alle categorie sopra elencate, deve svolgere una serie di attività quali: identificare il controllo, identificare rischio sotteso

e capire se è un rischio significativo. Qualora riscontrasse una certa significatività, deve effettuare valutazione del disegno dell'implementazione, se intende far affidamento su quel controllo deve effettuare e documentare test di efficacia operativa.

Rispetto al passato il principio fornisce delle linee guida precise e descrive le attività da svolgere in maniera più schematica.

In secondo luogo, sulla base dei controlli identificati precedentemente, il revisore deve identificare le applicazioni IT e altri aspetti dell'ambiente IT dell'impresa che siano soggetti a rischi derivanti dall'utilizzo dell'IT. I controlli che ho identificato se non sono controlli puramente manuali ma hanno una componente automatica comportano una analisi delle applicazioni, delle *IT Dependencies*, e dei controlli generali IT. Per tali applicazioni IT e per gli altri aspetti dell'ambiente IT identificati è necessario identificare i rischi connessi derivanti dall'utilizzo dell'IT e i controlli generali IT dell'impresa che fronteggiano tali rischi.

Classificazioni voci di bilancio e definizione della risposta di revisione

Come accennato precedentemente, il principio prevede un approccio differenziato in base alla classificazione delle voci di bilancio. La classificazione delle voci può avvenire nel seguente modo:

- Voce di bilancio significativa: analizzando la voce nella sua interezza attraverso i fattori rilevanti il revisore può già definire una prima valutazione della rischiosità di quella voce, se da questa analisi risulta che la voce possa essere significativa il revisore è tenuto, attraverso una maggiore attività di dettaglio, che riguarda le singole asserzioni, il rischio inerente e tutto il processo descritto precedentemente, ad ottenere conferma dell'effettiva significatività della voce. Qualora riscontrasse una certa significatività vuol dire che almeno un'asserzione è affetta da un rischio significativo a

livello di bilancio; successivamente attraverso il meccanismo degli IPO (*Information Processing Objectives*), che verrà spiegato successivamente, potrà collegare l'asserzione al processo o alla filiera informativa che alimenta quella voce di bilancio. In questo modo il revisore può identificare dei rischi inerenti di processo e successivamente le attività di controllo a presidio degli stessi. Se l'attività di controllo presidia un rischio inerente significativo oltre che pianificare i test di sostanza il revisore è tenuto a determinare un *Expected Controls Reliance*;

- Voce di bilancio non significativa ma materiale: il saldo in bilancio è rilevante ma non è affetto in maniera significativa da un errore. In questo caso il revisore deve documentare la motivazione che l'ha portato a dire che quella voce effettivamente non è da considerare significativa. Quindi considerate tutte quelle asserzioni che sono applicabili a quella voce di bilancio, su queste asserzioni il revisore deve effettuare l'analisi che lo porta a determinare quali fra quelle asserzioni sono rilevanti o meno, concludendo che la voce di bilancio non possiede nessuna asserzione che sia rilevante. Rispetto al passato è fondamentale la documentazione che renda ripercorribile tutto il processo effettuato dal revisore per determinare la non rilevanza delle asserzioni. Una volta che questa analisi è stata effettuata e documentata il revisore per tali voci può limitarsi a svolgere attività di sostanza.

  Se i soli test di sostanza per il revisore non generano un comfort sufficiente potrà decidere di fare affidamento su alcuni controlli, oppure se vuole effettuare ulteriori valutazioni in termini di efficienza oltre alle procedure di dettaglio può svolgere delle attività di controllo il cui esito offre un determinato comfort ottenuto dal fatto che il revisore non ha svolto le procedure di sostanza in maniera completa sulla base di una serie di valutazioni

professionali. In questo caso ci troveremmo nella categoria descritta nel punto quattro trattato nel sottoparagrafo *Approccio differenziato all'identificazione, valutazione dei controlli in funzione della natura del rischio sotteso*, nel quale il principio richiede di valutare il disegno del controllo e l'effettiva implementazione e quindi se i controlli sono a presidio dei rischi significativi. Se il revisore intende farne affidamento su quei controlli deve anche testarne l'efficacia operativa;

- Voce di bilancio non significativa e non materiale: il revisore non è tenuto a svolgere alcun tipo di procedura di dettaglio e tanto meno procedure di controllo, tranne nel caso in cui per indirizzare rischi di frode non siano previste procedure di *unpredicatability*. Anche per questa fattispecie andranno documentate le logiche sottese che hanno condotto il revisore a tale conclusione.

Information Processing Objectives (IPO)

Come precedentemente accennato, se una voce è significativa vuol dire che almeno un'asserzione è affetta da un rischio significativo a livello di bilancio, successivamente attraverso il meccanismo degli IPO possiamo collegare l'asserzione al processo o alla filiera informativa che alimenta quella voce di bilancio. I quattro criteri degli IPO sono così suddivisi:

- Completezza: assicura che tutte le informazioni necessarie siano incluse.
- Accuratezza: garantisce l'esattezza dei dati elaborati.
- Validità: verifica che le informazioni siano rilevanti e coerenti.
- Autorizzazioni e separazione dei compiti: promuove la sicurezza attraverso la corretta gestione dei diritti di accesso e la suddivisione delle responsabilità.

Gli IPO ci permettono quindi di collegare la valutazione del rischio effettuata a livello di voci di bilancio con i rischi inerenti di processo/filiera informativa che hanno generato quell'informazione. IPO e Asserzioni sono collegati tra di loro, nella seguente tabella viene indicato in che modo.

IPO	ASSERZIONI
Completezza (C)	Completezza (C)
Accuratezza (A)	Accuratezza (A), Valutazione (V)
Validità (V)	Esistenza e occorrenza (E/O), Diritti e obblighi (R/O)
Autorizzazioni e separazione dei compiti (R)	Completezza (C), Accuratezza (A), Valutazione (V), Esistenza e occorrenza (E/O)

Di seguito la presentazione di uno schema esemplificativo per capire come nella pratica si collega un IPO ad una asserzione prendendo come esempio la Completezza: valuto se possiedo tutti i documenti a livello di processo. L'obiettivo è quello di negare l'IPO di riferimento così da ottenere il rischio di processo e il rischio inerente che può essere più o meno significativo.

Rischio di processo incompletezza	Rischio Inerente	Attività di controllo
Nego la completezza; A livello di processo valuto ciò che potrebbe accadere e quale attività mi porterebbe ad un rischio inerente a livello incompletezza nel processo	Se rilevante come viene presidiato? Valuto impatto e probabilità per capire se il disegno a presidio è adeguato	Effettuo attività di controllo per valutare se i rischi sono adeguatamente presidiati

Il "*Walk-through test*" è un'ulteriore tecnica conoscitiva che il revisore può utilizzare per comprendere, su base documentale, il modo in cui il processo è strutturato. Attività nella quale si analizza come una transazione viene avviata e segue il suo percorso all'interno del sistema contabile dell'impresa fino al suo completamento. Operativamente tuttavia, il revisore potrebbe utilizzare il *walk-through test* per approfondimenti successivi: analizza il processo ad un livello medio alto, identifica "a livello logico" dove potrebbero collocarsi i rischi inerenti lungo il processo, svolge attività di *walk-through test* per confermare che i rischi siano posizionati correttamente e comprendere come è fatto il processo, nel dettaglio, e capire quali azioni operative possono concretamente generare il rischio. Il *walk-through test* viene effettuato per ottenere un comfort sufficiente sul fatto che il processo, le attività correlate e i rischi di riferimento siano in effetti generati come viene descritto. A tal fine il revisore effettuerà interviste ai dipendenti, osserverà direttamente i dipendenti mentre gestiscono le informazioni e raccoglierà le evidenze documentali a supporto. Tramite questo test il revisore ha la possibilità di verificare l'esistenza del controllo, la sua implementazione, come sia effettivamente strutturato il processo in modo da comprendere le modalità di generazione del rischio, se produce evidenze e quali e se l'obiettivo del controllo è coerente con l'IPO di riferimento e il rischio sotteso.

3.2 Fase di Execution

In questa fase il revisore pone in essere le attività pianificate nella fase di planning e andrà a testare i controlli dell'impresa. I *Test of Controls* (ToC) o procedure di conformità vengono definite come "procedure di revisore definite per valutare l'efficacia operativa dei controlli nel prevenire od individuare e correggere errori significativi a livello di asserzioni"[43].

All'interno dei *Test of Controls* viene descritta la tipologia del controllo posta in essere dalla società, ovvero se è un controllo manuale, automatico o *IT Dependencies*, qual è l'obiettivo del controllo, la sua periodicità, ogni quanto viene svolto il controllo e la popolazione di riferimento.

Il revisore stabilisce quanti elementi testare per il test di controllo in base alla frequenza del controllo. Nella tabella sotto riportata viene indicato il numero di elementi che il revisore deve testare, in base alla frequenza del controllo, nel caso in cui volesse ottenere un livello di *assurance* elevato.

Frequenza del controllo	**Popolazione presunta dei controlli**	**Numero di elementi da testare**
Annuale	1	1
Trimestrale	4	2
Mensile	12	2
Settimanale	52	5
Giornaliero	250	20
Più volte in un giorno	+250	25

Invece, nel caso in cui il livello di *assurance* da ottenere fosse moderato:

Frequenza del controllo	**Popolazione presunta dei controlli**	**Numero di elementi da testare**
Annuale	1	1
Trimestrale	4	1
Mensile	12	2
Settimanale	52	4
Giornaliero	250	10
Più volte in un giorno	+250	15

[43] IAASB, Principio di Revisione (ISA Italia) 330, "Le risposte del revisore ai rischi identificati e valutati", 2022, par. 4 b)

I *Test of Controls* descrivono anche la procedura svolta dal team di revisione per quel determinato controllo, il disegno del test posto in essere, ovvero esplicita punto per punto cosa intende verificare di quel determinato controllo, descrive l'esecuzione dello stesso indicando gli elementi probativi ottenuti.

Le procedure utilizzate per verificare il controllo possono essere diverse a seconda dei controlli che il revisore vuole testare. Di seguito vengono riportare le procedure che normalmente vengono utilizzate:

- *Inquiry*: indagine presso la direzione, processo di richiesta di spiegazioni al cliente relativamente al processo di controllo o alle transazioni. L'indagine è un tipo di controllo che può fornire solo prove limitate. Il cliente potrebbe comunicarci delle ottime procedure di controllo descritte nei documenti, ma potrebbe non eseguire correttamente tali procedure di controllo nella pratica.
- *Observation*: l'osservazione è il processo di osservazione delle procedure eseguite dal cliente. Questo test di controllo viene eseguito sia per avere prova che il controllo esista sia per aver certezza che le procedure di svolgimento del controllo siano messe in pratica correttamente.
- *Inspection*: l'ispezione è il processo di esame dei documenti di supporto relativi alle procedure di controllo. Questo tipo di test di controllo può fornirci prove più attendibili rispetto all'indagine e all'osservazione, in quanto ispezioniamo evidenze fisiche che le procedure di controllo sono in atto e vengono eseguite dal personale del cliente
- *Reperformance*: la riesecuzione è il processo in cui il revisore riesegue le procedure di controllo eseguite dal cliente. La

riesecuzione è il tipo di controllo più affidabile e ci fornisce una maggior garanzia rispetto agli altri tipi di test di controllo.

Una volta terminata questa fase il revisore avrà ottenuto gli elementi probativi per esprimere un giudizio in merito all'affidabilità del sistema di controllo interno dell'impresa e il suo ambiente IT.

CONCLUSIONE

Alla luce di quanto presentato in questo elaborato, la revisione del principio ISA 315 ha modificato l'attività di revisione introducendo determinati obblighi e linee guida specifiche, affinché, lo svolgimento della revisione, in relazione alla identificazione e valutazione dei rischi di errori significativi potesse essere maggiormente oggettiva, comparabile e omogenea.

Questa revisione ha portato al superamento di determinati ostacoli operativi presenti nel precedente principio, quali: i rischi legati all'utilizzo dell'IT non erano sufficientemente trattati nello standard; la comprensione del sistema di controllo interno risultava essere di difficile applicazione; esisteva un'incoerenza nella natura e nel numero di rischi significativi che venivano identificati nella pratica.

Rispetto al passato, oltre ad avere una maggiore rilevanza l'identificazione e la valutazione del rischio di errore significativo, il processo risulta essere più strutturato attraverso l'introduzione di nuovi elementi che obbligatoriamente il revisore deve considerare.

Questi elementi introducono un approccio di revisione, in merito alla valutazione del rischio, diverso rispetto al principio ante revisione, considerando l'analisi di fattori rilevanti, l'introduzione del concetto di spettro del rischio, la considerazione dei fattori di rischio inerente esplicitando quali essi siano, le diverse tipologie di asserzioni e l'introduzione del concetto di scalabilità.

Attraverso tutto il processo di *risk assessment* il revisore potrà classificare le voci di bilancio e in base a tale classificazione adotterà una procedura di revisione differente.

Inoltre, l'ISA chiarisce una serie di aspetti dell'attività che va svolta in termini di valutazione del disegno e validazione con riferimento alle attività di controllo, in considerazione della natura del rischio che queste attività di controllo vanno a presidiare. Questa attività veniva svolta anche prima, ma seguendo criteri operativi che ciascun revisore si definiva. Il nuovo principio ha maggiormente oggettivato il processo di identificazione e valutazione delle attività di controllo dell'entità.

Il nuovo principio ha introdotto l'obbligo di comprendere e valutare oltre al sistema di controllo interno dell'entità sottoposta a revisione anche il suo ambiente IT. Gli innumerevoli esempi riguardanti gli aspetti da comprendere e i relativi controlli forniscono al revisore un supporto all'attività da svolgere. La revisione di tale principio ha costituito un punto di partenza fondamentale dimostrando l'importanza di comprendere l'ambiente IT e tutto ciò che ne comporta per identificare potenziali errori significativi.

BIBLIOGRAFIA

Chilla Luca, *Via alle nuove versioni dei principi di revisione, novità in tema di valutazione dei rischi*, in "Norme & Tributi Plus Diritto", 2022

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.

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.

International Auditing and Assurance Standards Board, *Basis for conclusions prepared 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*, October 2019.

International Auditing and Assurance Standards Board, *Introduction to ISA 315*, 2019.

International Auditing and Assurance Standards Board, Principio di Revisione Internazionale (ISA Italia) 200, *Obiettivi generali del revisore indipendente e svolgimento della revisione contabile in conformità ai principi di revisione internazionali*, 2020, par. 5; 17; 13 c); A 37.

International Auditing and Assurance Standards Board, Principio di Revisione Internazionale (ISA Italia) 250, *La considerazione di leggi e regolamenti nella revisione contabile del bilancio*, 2020, par. 5.

International Auditing and Assurance Standards Board, Principio di Revisione Internazionale (ISA Italia) 300, *Pianificazione della revisione contabile del bilancio*, 2020, par. 4; 8.

International Auditing and Assurance Standards Board, Principio di Revisione Internazionale (ISA Italia) 315, *Identificazione e valutazione dei rischi di errori significativi*, 2019, par. 1; 4; 5; 7; 9; 11; 12; 12 a); 26; 34; A21; A25; A33; A57, appendice 1; 2; 3; 4; 5; 6.

International Auditing and Assurance Standards Board, Principio Di Revisione Internazionale (Isa Italia) 315, *L'identificazione E La Valutazione Dei Rischi Di Errori Significativi Mediante La Comprensione Dell'impresa E Del Contesto In Cui Opera*, par. 1; 3; 4.

International Auditing and Assurance Standards Board, Principio di Revisione (ISA Italia) 330, *Le risposte del revisore ai rischi identificati e valutati*, 2022, par. 4 b).

KPMG, *ISA 315 – Key requirements,* in "Accounting and Auditing Update", 42 (2020).

Ladogana S., Santovito G., *Il principio di revisione ISA Italia 315: principali impatti attesi*, in "Amministrazione & Finanza", 2023.

Peta Monica, *Rischio di controllo e rischio di revisione: il nuovo ISA Italia 315,* in "Fisco e Tasse", 2022.

Peta Monica, *Rischio intrinseco: le valutazioni del revisore su probabilità ed entità d'errore*, in "Fisco e Tasse", 2022.