LUISS

Corso di laurea in Strategic Management

Cattedra di REVISIONE INTERNA, COMPLIANCE E GEST.RISCHI AZ.LI

# L'INTERNAL AUDIT E IL NUOVO COMPETENCY FRAMEWORK DELLA PROFESSIONE

## L'evoluzione delle competenze della funzione per affrontare i nuovi rischi emergenti

Prof. Massimo Ferrari

RELATORE

Prof.ssa Paola Fersini

CORRELATORE

Federica Iodice

Matr. 755531

CANDIDATA

Anno accademico 2022/2023

**L'INTERNAL AUDIT E IL NUOVO COMPETENCY FRAMEWORK DELLA PROFESSIONE – L'evoluzione delle competenze della funzione per affrontare i nuovi rischi emergenti**

**INDICE**

**Introduzione**

Le aziende si trovano nel momento attuale a dover esercitare la propria attività in un contesto che è stato definito come la "*Tempesta perfetta*". L'evento meteorologico è usato come metafora per rappresentare in termini economici tutta una serie di circostanze straordinarie che si verificano e minano l'andamento dei processi aziendali. Attualmente la situazione è aggravata da diversi fattori: la pandemia da COVID-19, la guerra in Ucraina con i conseguenti effetti inflattivi su tutti i mercati e l'emergere di ulteriori nuovi rischi che si stanno progressivamente consolidando e hanno portato i governi ad accelerare lo sviluppo e l'adozione di nuove normative obbligatorie. In aggiunta a questi elementi, se si guardano con attenzione i mutamenti intervenuti contestualmente nel contesto sociale, occorre considerare la necessità di rivedere le modalità di ingresso nel mondo del lavoro della Generazione Z, che sta dimostrando di avere esigenze, competenze e obiettivi diversi dalle precedenti.
In questo contesto evolutivo, vedremo nel susseguirsi dei capitoli come l'internal audit ha dovuto cambiare ed aggiornare le proprie competenze, dovendo affrontare in prima linea i riflessi di questo mutevole contesto, dando maggiore supporto ed un tipo di consulenza più capillare all'organizzazione di cui fa parte.

L'obiettivo di questa tesi è dimostrare come in un contesto dinamico come quello in cui viviamo è necessario dover aggiornare le proprie competenze a tutti i livelli aziendali; quindi, anche il responsabile dell'IA, deve essere in grado di riconoscere i nuovi rischi, e soprattutto di avviare ed alimentare processi di valutazione e di controllo in grado di prevenirne gli impatti.

Nel primo capitolo è svolta una digressione sugli eventi che hanno portato alla nascita della figura dell'IA, dal primo intervento normativo all'attuale regolamentazione della figura in Italia. Particolare attenzione è posta sulla nascita *dell'IIA, Institute of Internal Audit,* e dell'affiliata su territorio nazionale *AIIA, Associazione Italiana Internal Audit*. Lo scopo dell'IIA è stato quello di promuovere un'evoluzione degli obiettivi e delle metodologie dell'Internal Audit verso standard internazionali che hanno portato all'affermazione della figura dell'internal auditor e del requisito di professionalità del ruolo stesso. In particolare, l'IIA oltre a fornire continuo supporto all'internal auditor, ha redatto un framework, chiamato *l'International Professional Practices Framework, IPPF,* che contiene, oltre una definizione generale del ruolo dell'IA, i principi fondamentali dell'auditor, il codice etico e gli standard che regolamentano il modo in cui svolgere la professione.

Nel secondo capitolo il focus si sposta sulle competenze che l'internal audit deve acquisire per essere al passo con il contesto mutevole, precedentemente presentato, nel quale si trova ad esercitare la propria attività. Per

questo motivo è stato introdotto il *Global Internal Audit Competency Framework,* che serve a definire le competenze necessarie a soddisfare i requisiti fissati dall'IPPF. Il framework divide le competenze in quattro ambiti, "Professionalism", "Performance", "Environment" e "Leadership&Communications", ed in base al livello di maturità delle competenze in ciascuno di questi ambiti, ogni auditor può essere classificato come un soggetto con "*General Awareness*", "*Applied Knowledge" o "Expert*". Procedendo nel capitolo si fa riferimento ad una survey dell'AIIA svolta su un panel di società nel contesto italiano, nel quale è stato valutato il livello di maturità raggiunta dalle competenze della funzione IA rispetto a quelle stabilite dal Competency framework. Infine, è affrontata l'applicazione pratica di un nuovo tool presentato a febbraio 2023 da professionisti associati all'AIIA. Questo Tool è organizzato proprio sul Competency framework e raggruppa le competenze che un IA deve possedere, e per ognuna delle competenze presentate, è effettuata una valutazione in merito alla rilevanza delle stesse ed in base alla seniority dei membri del Team.

Infine, nel terzo capitolo sono analizzati i nuovi rischi emergenti per i quali l'auditor si trova a dover garantire l'aggiornamento delle proprie competenze, facendo riferimento al rating ottenuto dal Risk in focus 2023. Il Risk in Focus è un report redatto dall'*European Confederation of Institutes of Internal Audit,* che da sette anni evidenzia le principali aree di rischio valutate dai Chief Audit Executive a livello europeo per aiutare gli internal audit a preparare il loro lavoro di valutazione indipendente del rischio, la pianificazione annuale e la definizione del campo di applicazione del piano di audit stesso. Dall'edizione del 2023 del report come principali sono emersi: *l'human capital, diversity and talent management, Cybersecurity* e tutte le *tematiche ESG*, ovvero inerenti alla responsabilità in ambito ambientale, sociale e di governance societaria. Ognuno di questi rischi è analizzato in uno specifico paragrafo, e per ognuno di questi è presentato un'analisi sulle competenze che l'internal audit deve possedere per identificarlo in azienda e valutare l'adeguatezza del sistema di controllo esistente.

# CAPITOLO 1: L'evoluzione dell'internal audit dalle origini ad oggi

## 1.1 Una prima definizione di Internal Audit

Affinché il consiglio di amministrazione possa guidare l'organizzazione in modo efficace, i membri del consiglio devono ricevere informazioni tempestive e accurate sui numerosi rischi strategici, operativi, finanziari e di conformità dell'organizzazione, nonché la garanzia che tali rischi siano gestiti in modo corretto tramite la valutazione dell'efficacia del sistema di controllo implementato, proprio per questo motivo l'*Internal audit* è una funzione cruciale all'interno di qualsiasi organizzazione. L'obiettivo principale dell'audit interno è fornire un'Assurance indipendente e oggettiva alla direzione e al consiglio di amministrazione sull'adeguatezza ed efficacia dei processi di gestione del rischio, controllo e governance dell'organizzazione.

L'IA può aiutare un'organizzazione a raggiungere i suoi obiettivi identificando aree per il miglioramento delle sue operazioni, dei suoi processi e dei suoi sistemi. Può anche assistere nello sviluppo e nell'implementazione di politiche e procedure per mitigare i rischi e migliorare le prestazioni dell'organizzazione. I professionisti dell'internal audit lavorano a stretto contatto con la direzione per valutare i sistemi di controllo interni dell'organizzazione, identificare aree di rischio e raccomandare strategie per gestire i rischi emersi dalle analisi precedentemente svolte.

L'implementazione e costante aggiornamento della funzione all'interno dell'azienda svolge un ruolo critico nel mantenere l'integrità e l'affidabilità della rendicontazione finanziaria della stessa. Inoltre, aiuta a garantire che i bilanci siano accurati e conformi agli standard contabili e ai regolamenti pertinenti. L'IA svolge anche un ruolo vitale nella prevenzione e nella rilevazione di frodi e altre irregolarità finanziarie.

La definizione del ruolo fornita da "*The Institute of internal auditors" (The IIA)* permette di delineare alcune caratteristiche richieste nello svolgimento di tale funzione.

*"L'internal audit è un'attività di garanzia e consulenza indipendente e obiettiva, finalizzata ad aggiungere valore e a migliorare le operazioni di un'organizzazione. Aiuta un'organizzazione a raggiungere i propri obiettivi attraverso un approccio sistematico e disciplinato per valutare e migliorare l'efficacia dei processi di gestione del rischio, di controllo e di governance."*

Prima di tutto l'attività a cui si fa riferimento non è una funzione aziendale strutturale, ma si tratta di servizi *Assurance e consulenza* all'organo di governo o ai comitati al suo interno, nella definizione delle funzioni

organizzative e relative al personale e delle attività da loro messe in essere, in quanto la responsabilità ultima delle operazioni rimane comunque in capo alla direzione.

*Assurance e consulenza* emergono quindi come i due capisaldi intorno ai quali gira l'intero operato della funzione di Internal Audit. Per *Assurance* si intende l'esaminazione delle evidenze emerse dallo svolgimento dell'attività aziendale, per ottenere una valutazione indipendente del processo di gestione o di governance, e per evidenziare eventuali processi inadatti, dannevoli per l'impresa. Invece l'attività di *consulenza* si articola principalmente in servizi di supporto e assistenza finalizzati a fornire suggerimenti per il miglioramento dello stesso processo di gestione e delle attività di governance, risk management e controllo. È evidente come le due attività siano sequenziali, ed in un processo svolto correttamente possano portare all'evoluzione ed alla crescita dell'azienda.

Emerge come caratteristica essenziale della figura l'*indipendenza.* Il responsabile IA deve essere "Super partes", cioè privo di restrizioni che potrebbero limitare in modo significativo la portata e l'efficacia di qualsiasi processo ed attività di internal audit o la successiva comunicazione dei risultati e delle conclusioni che ne derivano. Resta comunque necessaria empatia ed accettazione degli obiettivi generali degli enti partecipanti per evitare che gli interessi dell'IA siano differenti o opposti a quelli dell'organizzazione. L'indipendenza è anche organizzativa, ovvero le attività devono essere libere da qualsiasi interferenza esterna sia per la definizione dell'ambito in cui esercitare la propria attività, le metodologie di esecuzione del lavoro e la comunicazione del risultato.

Dalla definizione è infine richiesto di generare valore aggiunto nello svolgimento delle attività sopracitate. Il valore aggiunto è meramente inteso come superamento dei benefici generati dallo svolgimento di attività rispetto ai costi sostenuti per la stessa. Bisogna tenere a mente che le attività di verifica vengono spesso definite antieconomiche, in quanto consistono nel sostenimento di un costo per delle analisi su un evento che potrebbe anche non verificarsi, ma non sempre questo corrisponde alla realtà, semplicemente è necessario verificare se l'onere in questione per svolgere le attività di verifica è maggiore del danno evitabile. Generalmente l'attività viene svolta con maggiore frequenza nelle aree a rischio più elevato che possono variare da un campo d'azione di un'impresa ad un'altra, ma a priori l'internal audit deve esercitare la propria attività di controllo sull'operato di tutte le funzioni aziendali.

Entrando nello specifico in quella che è l'attività di internal audit, la stessa non va confusa con l'attività del revisore contabile, è necessario specificare a questo punto la distinzione tra le due.

La *revisione contabile* è svolta da revisioni legali esterni all'azienda ed ha come principale obbiettivo il rilascio di una certificazione del bilancio che per alcune categorie di aziende, come quelle quotate, è obbligatoria. Il principale obiettivo della *funzione di IA* invece è quello di valutare e monitorare il sistema di Controllo Interno ed emettere reports per uso interno. Inoltre, l'attività dei revisori è un'attività principalmente basata su delle analisi svolte a verificare azioni già concluse dall'azienda, definibile come attività di backward-looking, mentre l'IA svolge oltre questo tipo di analisi anche attività di forward-looking, dando quindi suggerimenti o raccomandazioni sulle future azioni correttive o migliorative da compiere.
L'attività di internal audit può variare notevolmente a seconda delle dimensioni e del settore dell'organizzazione. Alcuni dipartimenti hanno decine di membri del personale che lavorano in tutto il mondo. Altri hanno solo uno o due esperti di internal audit, mentre altre organizzazioni ancora esternalizzano o co-subappaltano la funzione di revisione interna.
A seconda della struttura, della maturità e delle risorse della funzione, gli auditor interni possono svolgere alcuni o tutti i seguenti compiti.
Esiste *l'Operational Audit* che ha come finalità quello di valutare ed accertare l'efficacia e l'efficienza dello svolgimento dei processi ed il corretto presidio dei rischi insisti nell'attività.
In alcuni casi, l'esperienza, la conoscenza dei controlli e l'ampia prospettiva dell'organizzazione fanno degli internal auditor i candidati ideali per fornire la consulenza ed insight su un progetto, al fine di garantire che i rischi siano presi in considerazione e che i controlli siano integrati in un processo nella fase iniziale come ad esempio, fusioni e acquisizioni, implementazione di una nuova tecnologia.
Gli internal auditor possono offrire una visione dei rischi strategici e una consulenza, anche se la direzione deve mantenere la responsabilità finale dei processi nella propria area.
I rischi sono ovunque, gli esempi da fare sarebbero infiniti, ma tra i tanti c'è la possibilità di perdita di fornitori chiave, danni alla reputazione, operazioni inefficienti, frodi, cause legali, violazioni delle politiche, conformità alle normative, furti, ecc. Il compito dell'IA è quello di valutare l'importanza dei numerosi rischi dell'organizzazione e l'efficacia degli sforzi di gestione del rischio, comunicarli alla direzione e al consiglio di amministrazione e sviluppare raccomandazioni per migliorare la gestione del rischio.

Poi c'è il *Financial Audit*, che è l'attività più simile alla revisione legale, che è volta ad accertare il sistema di controlli interni su processi prettamente amministrativo-contabili o che hanno ad oggetto l'analisi di poste di bilancio identificate, sulle quali il Management vuole un Assurance interna.
Un ulteriore attività è quella *dell'Audit di Compliance*, che consiste nella verifica dell'osservanza delle norme interne ed esterne applicabili al contesto delle strutture organizzative e delle operazioni prese in esame, in pratica si va a verificare la conformità.

Esistono anche attività di *Fraud Audit* mirate all'identificazione delle cause e delle responsabilità afferenti a specifici eventi, incidenti o comportamenti giudicati inadeguati nei confronti dell'azienda, come ad esempio casi accertati di frode o di infedeltà. I beni materiali, le risorse umane e la proprietà intellettuale dell'organizzazione sono preziosi e devono essere protetti da potenziali danni. Gli internal auditor valutano le procedure utilizzate per salvaguardare i beni da furti, incendi, attività illegali o altri tipi di perdite. Portano alla luce le carenze e formulano raccomandazioni per migliorare la protezione.
Poiché le frodi possono colpire qualsiasi livello dell'organizzazione, è importante che il consiglio di amministrazione conceda alla funzione di revisione interna l'accesso a tutti i documenti e l'autorità di condurre audit e indagare su possibili comportamenti fraudolenti in tutta l'organizzazione.

Negli ultimi anni la necessità di intercettare e gestire rischi diversi richiede che la funzione di Internal Audit abbia delle competenze sempre più specifiche. Se l'organizzazione non è grande abbastanza per far si che la funzione di IA abbia le competenze necessarie ad affrontare questi rischi, l'alternativa più efficace per soddisfare le aspettative degli stakeholder risulta l'esternalizzazione delle attività. La maggior parte delle organizzazioni, come risulta da un analisi condotta nel 2018 da PWC, optano per il 72% a soluzioni interne, la restante parte delle organizzazioni che decide, con la pratica chiamata *outsourcing,* di ricercare all'esterno le competenze che mancano si interfaccia tipicamente con società di consulenza, revisione o professionisti esterni. Tra le principali motivazioni che spingono le impresse ad esternalizzare ci sono valutazioni di maggior efficienza in termini di costi e competenze, ragioni di ottimizzazione delle risorse, indisponibilità all'interno della società di risorse e competenze adeguate, necessità di garantire indipendenza, autonomia e professionalità. *Nel secondo capitolo verrà presentato un caso pratico di applicazione di questa pratica è che chiamata Co-sourcing*.

**1.2 L'evoluzione del controllo interno e la nascita della funzione dell'IA**

Come anticipato nel precedente paragrafo l'internal audit non è da confondere con la revisione contabile, in quanto la prima è una funzione indipendente all'interno dell'azienda che monitora, per conto della *governance*, la gestione del rischio di un'impresa ed i processi di controllo interno ad ampio spettro, mente il revisore è una figura esterna che ha come principale obiettivo quello di esprimere un giudizio sul bilancio dell'azienda. Bisogna aspettare il 1934, con l'intervento della SEC, per avere una prima istituzione della figura dell'internal audit, prima di allora si parla semplicemente di revisione contabile.

I primi cenni di revisione hanno delle radici che risalgo addirittura all'era dei Babilonesi, ma solo nel periodo intercorrente tra *il XVII ed il XVIII secolo*, la revisione contabile assume una maggiore rilevanza a livello sociale, dovuta alla necessità di controllare le gestioni pubbliche e le attività delle compagnie internazionali. Dagli editti di Luigi XV emergono le prime forme di regole "salvaguardia" che disciplinavano l'obbligo contabile, facevano seguito all'editto una *"declaration"* di richiamo dall'osservanza dell'obbligo di vidimazione preventiva dei libri di commercio alle Corti di giustizia del regno.

Nel *XIX secolo* si assiste ad una evoluzione significativa nel controllo contabile, il sempre crescente numero delle imprese di assicurazione e bancarie, la costruzione delle ferrovie, l'affermazione delle Società per Azioni, fanno sì che l'attività di revisione contabile e la figura del revisore diventino attori di primo piano sulla scena economica.

Nel frattempo, il panorama economico italiano dei primi anni del nuovo Regno era connotato da avventurieri e da avventate manovre di borsa. Venivano create fittizie società in Italia che immettevano capitali verso l'estero e potenti società straniere che entravano in vari tipi rapporti con la nuova amministrazione italiana.

*Alla fine del secolo XIX* la revisione contabile in tutto l'Occidente diviene obbligatoria; tra il 1849 ed il 1913 in Gran Bretagna e negli Stati Uniti d'America nascono così le prime importanti società di revisione, si affermano le prime teorie su basi scientifiche, nel campo della revisione contabile. In questo periodo lo Stato interviene nel campo della revisione contabile, con l'emanazione dei primi provvedimenti che rendono obbligatoria la revisione del bilancio di esercizio destinato a pubblicazione affidata ad esperti esterni all'ente da verificare o con il ricorso alla stessa revisione contabile per la tutela degli interessi dei terzi, sia attraverso il controllo con suoi funzionari sulle società anonime, sia attraverso l'obbligo giuridicamente imposto di organi collegiali di controllo. La ragione dell'obbligo della revisione contabile riposa nell'inadeguatezza degli strumenti aziendali di controllo e nel dilagare di comportamenti contabili non corretti, delle frodi, della corruzione e, pertanto, nella necessità di meglio tutelare l'interesse dei soci e dei terzi.

Nel *XX secolo*, in Gran Bretagna, con il Companies Act del 1908 si delinea l'autonomia del compito del revisore, si fissano le modalità del suo compenso e si indicano formalità minime di svolgimento del lavoro. Negli Stati Uniti si consolidano i primi trattati in tema di "auditing", da queste opere scaturisce una copiosa produzione dottrinaria, che a poco a poco va ad influenzare i comportamenti pragmatici dei revisori contabili e ad indirizzare le iniziative professionali individuali e delle autorità di vigilanza, anche grazie alla lingua inglese che, gradatamente, diviene quella principale dei commerci e dei contratti internazionali, lingua che in parte soppianta in Europa le altre lingue. A questo si deve aggiungere l'influenza della, sempre possente economia statunitense, tenuto conto dei fenomeni migratori verso di essa e dei flussi finanziari di supporto alle economie.

In Italia con minore impatto sulle attività ragionieristiche, iniziano le prime trattazioni in tema di revisione contabile nel 1882 a seguito della disciplina dettata nel Codice di commercio. Negli anni 20 del Novecento nascono a Milano e Roma "*l'Istituto fiduciario"* ed il *"Primo istituto di revisione aziendale",* che segnano il definitivo cambiamento e l'affermazione della disciplina in merito alla revisione contabile.

Fino ai primi anni del XXI secolo la disciplina è stata trattata in Italia in modo sommario e definibile insoddisfacente; infatti, solo a partire dalla seconda metà del 900' ci sono state delle riforme che hanno portato a regolamentazioni più stringenti non solo in termini di revisione contabile ma anche proprio di Internal Audit. *Il tema sarà meglio approfondito nel terzo paragrafo "La regolamentazione dell'IA in Italia".*

Nonostante le sue antiche radici l'internal audit non è stato riconosciuto come un processo importante da molte imprese e dai loro revisori esterni fino agli anni Trenta. Questo riconoscimento è dovuto molto probabilmente all'istituzione della Securities and Exchange Commission (SEC) statunitense nel 1934 e all'evoluzione degli obiettivi e delle tecniche di revisione esterna in quel periodo. Gli Stati Uniti e il resto del mondo avevano appena attraversato una grave depressione economica. Come azione legislativa correttiva, la SEC richiese che tutte le imprese registrate presso di essa dovessero fornire bilanci certificati da revisori indipendenti. Questo requisito ha spinto le aziende a creare dipartimenti di revisione interna, ma con l'obiettivo principale di assistere i revisori indipendenti. A quel tempo, i revisori finanziari esterni si concentravano sull'espressione di un parere sulla correttezza dei bilanci di un'impresa piuttosto che sull'individuazione di debolezze del controllo interno o addirittura di errori materiali. All'epoca, i revisori interni si occupavano principalmente di controllare le registrazioni contabili e di rilevare errori e irregolarità finanziarie e spesso erano poco più che ombre o assistenti dei revisori esterni indipendenti. Ancora oggi la SEC riconosce l'importanza della figura dell'internal auditor nel quadro generale dei controlli interni di un'impresa. Un esempio è il comunicato della Commissione che autorizza le imprese a diventare Consolidated Supervised Entities (CSE) al fine di utilizzare moduli matematici interni per calcolare il capitale regolamentare richiesto.

Nel 1942, venne fondato "*The institute Of Internal Auditor",* l'IIA, da persone che avevano ricevuto il titolo di revisore interno dalle loro aziende e che volevano condividere le loro esperienze e acquisire conoscenze con altri in questo nuovo campo professionale. Al tempo le imprese non avevano bisogno di computer, fino a quando queste macchine non hanno iniziato a diventare utili per la tenuta dei registri e per altre funzioni di calcolo e contabilità, come invece lo sono oggi. La realtà delle imprese nei primi anni Quaranta era di connessioni telefoniche molto rudimentali, in cui i centralinisti smistavano tutte le chiamate in entrata a un numero limitato di telefoni.

In Italia nasce come affiliata dell'IIA, l'associazione Italiana Internal Auditors (AIIA). Dalla sua costituzione a oggi, è il **punto di riferimento in Italia** per le tematiche di **Controllo Interno**, di **Corporate Governance**, di **Compliance** e di **Risk Management** e conta numerosi professionisti associati, in rappresentanza di gruppi e imprese operanti nel settore **Finanziario, Assicurativo, Manifatturiero, Servizi** e **Settore Pubblico**.
L'AIIA oltre ad essere stata parte fondamentale dell'evoluzione del governo societario verso standard internazionali ha portato all'affermazione dell'internal auditor e del requisito di professionalità del ruolo stesso.
Offrendo ai propri associati la possibilità di partecipare a numerosi eventi di formazione e networking, come seminari, conferenze, corsi di formazione e workshop, volti a sviluppare le competenze e le conoscenze degli internal auditor italiani ed offrendo un'ampia gamma di risorse e strumenti online, tra cui pubblicazioni, video formativi, webinar e comunità virtuali di discussione, l'associazione non smette di fornire nuovi spunti agli auditor per crescere ed essere in costantemente aggiornamenti con le nuove necessità emergenti a livello globale.

L'AIIA è inoltre impegnata nella promozione della professione dell'internal audit in Italia, collaborando con organizzazioni del settore, istituzioni accademiche e organi di governo per migliorare la consapevolezza della funzione di audit interno e dell'importanza della gestione dei rischi nelle organizzazioni.

Da una survey condotta nel 2018 da Pwc chiamata *"State of the Internal Audit Profession Study"*, è emersa la tendenza dell'evoluzione della figura dell'IA da una "Assurance Provider" ad una "Trusted Adviser".

Oggi, il ruolo dell'internal audit sembra essere concentrato non più unicamente sull'analisi dei dati, ma nel riuscire a capire come essere riconosciuto come partner strategico. Il soggetto responsabile di tale funzione deve supportare l'alta direzione e fornire garanzia e consigliare sugli aspetti di mitigazione del rischio, circa la semplice esistenza, o il concreto funzionamento, di un processo efficace ed efficiente e sul sistema di governo nella sua interezza. Inoltre, la funzione è chiamata a supportare l'organizzazione stando al passo

con il ritmo dell'innovazione e soprattutto considerando l'impatto dirompente dei cambiamenti del contesto di riferimento in cui opera l'azienda ed adeguandosi di conseguenza.
I rischi organizzativi e le opportunità che perseguono cambiano e, di conseguenza, cambiano le competenze necessarie per comprendere, analizzare e valutare tali rischi.

A questo proposito, l'impatto dirompente della tecnologia, oltre che fonte indiscutibile di opportunità, espone contemporaneamente le organizzazioni a nuovi e significativi rischi, che devono essere ben compresi e gestiti con strumenti efficaci. *Tale tema sarà analizzato nel terzo capitolo.*

**1.3 Regolamentazione dell'IA in Italia**

In Italia, una primissima regolamentazione dell'audit può essere indentificata, per la prima volta nel 1974, nella legge sulla revisione contabile obbligatoria. La legge stabiliva che tutte le società per azioni quotate in borsa dovevano effettuare una revisione contabile obbligatoria, che comprendeva anche un'analisi del sistema di controllo interno e delle procedure di gestione dei rischi. L'obiettivo della legge era quello di garantire la corretta gestione delle società quotate, evitando frodi e irregolarità.
L'audit interno ha però subito un'evoluzione significativa a livello nazionale a partire dagli anni '90, quando il governo italiano ha iniziato ad adottare regolamentazioni più stringenti per migliorare la trasparenza e l'efficacia delle attività di audit interno all'interno delle organizzazioni.

Una delle prime misure adottate è stata la legge n. 262 del 1991, che ha introdotto l'obbligo per le società quotate di avere un comitato di controllo interno composto da membri del consiglio di amministrazione e da un rappresentante dei revisori dei conti. Questo comitato ha il compito di monitorare il processo di audit interno e di assicurare l'indipendenza del revisore interno.

La vera svolta normativa però per il sistema di controllo interno ed implicitamente per l'introduzione dell'internal audit si ha nell'1998 con l'entrata in vigore del "Testo Unico della Finanza - TUF" (D.lgs. n. 58 del 24 febbraio 1998, noto anche come "legge Draghi") che formalizza l'importanza del Sistema di Controllo Interno, introducendo per la prima volta nella legislazione italiana tale espressione. Prima di questo momento erano stati elaborati diversi documenti ma mai nessun intervento legislativo era stato messo in atto. Tra i primi documenti che facevano riferimento allo SCI ( *"Sistema di controllo interno")* nel 1996 il Consiglio Nazionale dei Dottori Commercialisti e dei Ragionieri ha emanato i "Principi di comportamento del Collegio Sindacale" contenenti una norma specifica sulla valutazione del sistema di controllo interno e dell'organizzazione contabile della società e seguendo l'iniziativa del parlamento europeo che esegui un'indagine sulla Corporate

governace all'interno del libro "Libro Verde", venne portato a termine nel 1997 il "Progetto Corporate Governance per l'Italia" che fece giungere alla pubblicazione del risultato delle ricerche su come ridefinire e rendere applicabili in Italia i principi per un buon SCI e un buon governo dell'impresa previsti nel *CoSO Report*. Il CoSo Report è il lavoro chiamato "Internal Control- Integrated Framework" portato a termine dal Committe of Sponsoring Organizations of the Treadways Commission. Il report è stato pubblicato nel 1992 negli US per delineare un concetto unico di controllo interno e per creare un unico modello di riferimento per la delineazione di un sistema di controllo da parte del Management e della società stessa.

Successivamente, il Decreto Legislativo n. 231/2001 ha istituito il reato di "responsabilità amministrativa delle società" e ha reso obbligatorio per le società adottare un modello di organizzazione e gestione che preveda il controllo interno e l'audit interno. Questo ha ulteriormente rafforzato l'importanza dell'audit interno e ha incentivato le organizzazioni a investire in questa funzione in quanto con il corretto sistema di controllo interno ed un adeguato *("Taylor made"*) modello organizzativo l'azienda può essere assolta da responsabilità amministrativa nella commissione di reati societari.

Nel 2003, la Banca d'Italia ha emanato una serie di disposizioni in materia di revisione interna e controllo interno per le banche, che hanno stabilito requisiti specifici per la funzione di audit interno all'interno delle banche. Queste disposizioni hanno fornito indicazioni sulle responsabilità e sulle attività della funzione di audit interno e hanno incentivato le banche a migliorare la loro funzione di audit interno.

Nel 2005, il Decreto Legislativo n. 38/2005 ha istituito il reato di "falso in bilancio" e ha ulteriormente rafforzato la necessità di una funzione di audit interno efficace all'interno delle organizzazioni. Questo decreto ha stabilito sanzioni penali per chiunque falsifichi i documenti contabili o renda dichiarazioni false riguardanti la situazione patrimoniale dell'organizzazione.

Nel 2007, l'Organismo Italiano di Contabilità ha emesso il principio contabile n. 10, che ha stabilito i principi contabili per le società quotate, tra cui le regole per l'audit interno e la valutazione dei rischi. Questo principio ha ulteriormente rafforzato la regolamentazione dell'audit interno per le società quotate.

Infine, nel 2011, il Decreto Legislativo n. 39/2010 ha recepito la Direttiva Europea 2006/43/CE, che ha stabilito le regole per la revisione legale dei conti. Questa direttiva ha previsto un ampliamento dei compiti dell'audit interno e ha introdotto l'obbligo per le società quotate di effettuare una rotazione degli auditor ogni 9 anni.

Nel 2013, l'Organismo Italiano di Contabilità ha emanato il principio contabile n. 13, che ha definito gli standard per l'audit interno e ha stabilito le linee guida per la sua implementazione. Questo principio ha fornito alle organizzazioni un quadro di riferimento chiaro e dettagliato per la gestione dell'audit interno.

Negli ultimi anni, l'audit interno in Italia ha subito ulteriori cambiamenti a causa della crescente digitalizzazione delle organizzazioni e dell'aumento delle minacce informatiche. In risposta a questi cambiamenti, il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili ha emanato il documento "Linee guida per l'audit informatico", che fornisce indicazioni specifiche per la gestione dei rischi informatici e la valutazione della sicurezza informatica durante l'audit interno.

Attualmente uno standard setter per la definizione del ruolo e dell'attività dell'IA è il *Codice di Corporate Governance* delle società quotate, il quale è, inoltre, il principale punto di riferimento nazionale in tema di corporate governance e si rivolge a tutte le società con azioni quotate sul mercato. Esso è stato redatto da un comitato di Borsa Italiana S.p.A. e pubblicato, nella prima versione, nel 1999 per poi essere aggiornato fino alla più recente versione del 2020. Ciascun articolo del Codice è suddiviso in principi che definiscono gli obiettivi di una buona governance, e in raccomandazioni, che indicano i comportamenti che il Codice reputa adeguati a realizzare gli obiettivi indicati nei principi. È importante sottolineare che il codice si basa su un modello di *"Comply or Explain",* ciò vuol dire che le società non sono obbligate ad implementare il modello, ma se dovessero differire dallo stesso dovrebbero motivare la loro scelta nella relazione annuale sul governo societario.

Ogni società che aderisce al Codice fornisce nella relazione sul governo societario informazioni accurate, di agevole comprensione ed esaustive, se pur concise, sulle modalità di applicazione del Codice.

Dal *codice di corporate governance* emerge che il soggetto incaricato della funzione non è responsabile di alcuna area operativa ma dipende direttamente dal CDA, avendo acceso diretto a tutte le informazioni necessarie per lo svolgimento dell'incarico.

Il responsabile della funzione di *internal audit*:

1. verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli *standard* internazionali, l'operatività e l'idoneità del sistema di controllo interno e di gestione dei rischi, attraverso un piano di *audit* approvato dall'organo di amministrazione, basato su un processo strutturato di analisi e prioritizzatine dei principali rischi;

2. predispone relazioni periodiche contenenti adeguate informazioni sulla propria attività, sulle modalità con cui viene condotta la gestione dei rischi nonché sul rispetto dei piani definiti per il loro contenimento. Le relazioni periodiche contengono una valutazione sull'idoneità del sistema di controllo interno e di gestione dei rischi;
3. anche su richiesta dell'organo di controllo, predispone tempestivamente relazioni su eventi di particolare rilevanza;
4. trasmette le relazioni di cui alle lettere b) e c) ai presidenti dell'organo di controllo, del comitato controllo e rischi e dell'organo di amministrazione, nonché al *chief executive officer*, salvo i casi in cui l'oggetto di tali relazioni riguardi specificamente l'attività di tali soggetti;
5. verifica, nell'ambito del piano di *audit*, l'affidabilità dei sistemi informativi inclusi i sistemi di rilevazione contabile.

In Italia, sebbene gli emittenti di titoli quotati siano tenuti a dotarsi di una struttura di controllo interno a seguito dell'adozione delle disposizioni del Codice di Autodisciplina, la legge attualmente non prevede una struttura di controllo interno, se non in alcuni settori regolamentati come quello finanziario e assicurativo, anche se progressivamente si sta proliferando anche nelle piccole aziende del manifatturiero e del terziario. Per le società non quotate, la crescente frammentazione del ruolo del preposto al controllo interno è spesso attribuita all'adozione del decreto n. 231/2001.
Come prevedibile il settore delle società quotate è regolamentato da un apposito organismo, quale Banca d'Italia, Consob o IVASS, per banche e finanza, società pubbliche ed emittenti di un'ampia gamma di titoli, e rispettivamente le compagnie di assicurazione, sono quelle società che hanno storicamente avuto tradizioni e capacità più antiche in complessi sistemi di controllo interno, in modo che esista un'adeguata struttura di audit interno. Per ovvie ragioni, l'importante ruolo che questi enti svolgono nell'equilibrio dell'economia nazionale e nella tutela del risparmio pubblico richiede un maggior grado di sicurezza rispetto agli enti più semplici.

Allo stesso modo, l'ordine in materia è passato da un grado di previsione opportunistica (anche se fortemente sostenuto attraverso lo sviluppo di norme di autoregolamentazione) a previsione regolamentare obbligatoria a tutti i livelli. Si va dalle norme fissate dagli enti regolatori, spesso derivate anche da lettere paga, manuali, circolari, norme e regolamenti, alle norme vere e proprie.

In Italia, quindi l'operato dell'internal audit è strettamente regolato dalla Consob, la Commissione Nazionale per le Società e la Borsa.

La Consob ha il compito di garantire la trasparenza e l'efficacia delle attività di controllo interno all'interno delle società quotate in borsa, nonché la tutela degli interessi degli investitori e la corretta informazione del mercato. In questo contesto, l'internal audit svolge un ruolo cruciale, poiché fornisce una valutazione indipendente e obiettiva delle attività di controllo interno e dei rischi connessi alle attività delle società quotate. L'organismo ha emesso diverse normative e linee guida per regolare l'operato dell'internal audit all'interno delle società quotate in borsa. Tra le principali normative figura il Regolamento Emittenti, che stabilisce l'obbligo per le società quotate di istituire una funzione di audit interno e definisce i compiti e le responsabilità dell'internal audit. La Consob ha anche emanato il documento "Linee guida per l'audit interno nelle società quotate", che fornisce indicazioni specifiche per la gestione dell'internal audit e la valutazione dei rischi all'interno delle società quotate. Questo documento stabilisce, ad esempio, che l'internal audit deve essere guidato da un responsabile con adeguata competenza e indipendenza e che deve essere svolto in modo sistematico e continuativo.

Inoltre, la Consob ha previsto l'obbligo per le società quotate di comunicare al mercato le informazioni relative alla funzione di audit interno, tra cui la struttura organizzativa, le modalità di svolgimento dell'attività di audit e le principali conclusioni e raccomandazioni emerse dall'audit interno.

Inoltre, la regolamentazione dell'internal audit è stata influenzata anche dalle normative internazionali, in particolare dagli standard internazionali per la pratica dell'internal audit definiti dall'IIA (Institute of Internal Auditors), l'organizzazione internazionale di riferimento per la professione dell'internal audit. Gli standard IIA sono stati adottati anche in Italia, e costituiscono un punto di riferimento per gli internal auditor italiani.
Tra questi standard alcuni ricalcano quelle che in precedenza abbiamo definito come caratteristiche che un Internal auditors deve possedere. Gli stessi saranno esposti ed analizzati nel prossimo paragrafo.

### 1.4 Ruolo dell'IIA e dell'AIIA

L'Institute of Internal auditors (The IIA) come presentato nei paragrafi precedenti, nasce nel 1942 e fonda le basi per lo sviluppo della figura dell'internal auditor a livello Globale.

L'AIIA (Institute of Internal Auditors Italy) è l'associazione italiana dei professionisti dell'internal audit, ed è affiliata all'IIA Global (Institute of Internal Auditors Global), la più grande organizzazione internazionale degli internal auditor.

L’associazione rappresenta un punto di riferimento per la formazione e la promozione della professione dell'internal audit in Italia, e si impegna a promuovere la diffusione della cultura dell'audit interno nelle organizzazioni italiane.

L'associazione svolge una serie di attività per supportare i propri associati nella loro attività professionale, tra cui la formazione, l'aggiornamento professionale e lo sviluppo di reti di contatti e collaborazioni tra i professionisti dell'internal audit. Inoltre, promuove l'adozione di standard di riferimento per l'internal audit, tra cui lo standard internazionale per la pratica dell'internal audit definito dall'IIA.
L’Institute of Internal Auditors definisce la mission dell’IA come quella volta a *“Arricchire e proteggere il valore dell’organizzazione, provvedendo con attività di Assurance, consulenza e strategiche basate sul rischio ed oggettive”.*
Per facilitare il raggiungimento di questo obiettivo è stato creato *l’International Professional Practices Framework (IPPF),* il quale racchiude le indicazioni per comprendere le linee guida dell’IIA, in modo che siano accessibili a tutti e di conseguenza rendendole dei *global standard setter*. Il framework è costituito da regole obbligatorie e raccomandazioni. Per operare correttamente come Internal auditor è necessario rispettare la parte obbligatoria del framework che comprende: *I principi fondamentali per la pratica professionale dell’Internal Audit; La definizione dell’IA; Il Codice Etico e gli Standard*.

### 1.4.1 I principi fondamentali

I *Principi fondamentali* sono la base dell'efficacia dell'audit interno. La funzione di internal audit è efficace se tutti i principi sono rispettati ed applicati efficacemente. I principi fondamentali sono i seguenti:

a) "Dimostrare integrità";
b) “Dimostrare competenza e la dovuta attenzione professionale”;
c) “Essere obbiettivo e libero da influenze indebite (indipendente)”;
d) “Essere allineato con le strategie, gli obiettivi e i rischi dell'organizzazione”;
e) “Essere posizionato in modo appropriato e dispone di risorse adeguate”;
f) “Dimostrare qualità e miglioramento continuo”;
g) “Comunicare in modo efficace”;
h) “Fornire garanzie basate sul rischio”;
i) “Essere perspicace, proattivo e orientato al futuro”;
j) “Promuovere il miglioramento organizzativo".

### 1.4.2 Il codice di condotta etico

Il codice etico per le imprese è un documento che prevede una serie di regole comportamentali a cui i dipendenti e collaboratori di un'azienda sono invitati ad attenersi.

Lo scopo principale di *un codice di condotta etica* per un'organizzazione professionale è quello di promuovere una cultura etica tra i professionisti al servizio degli altri. Allo stesso modo altre funzioni svolte dal codice sono quella di comunicare i valori accettabili dall'organizzazione a tutti i membri della stessa, stabilire standard oggettivi con i quali è possibile misurare le proprie prestazioni e comunicare ai soggetti terzi sterni all'azienda i valori della stessa.

Nello specifico lo scopo del Codice etico dell'Istituto è quello di promuovere una cultura etica nella professione dell'internal auditing.

Un codice etico è necessario ed appropriato per la professione dell'internal auditing, fondata proprio sulla fiducia riposta nella sua garanzia oggettiva di governance, gestione del rischio e controllo.

Il Codice etico dell'Istituto va oltre la definizione e comprende due componenti essenziali, cioè i principi rilevanti per la professione e la pratica dell'IA e le regole di condotta che descrivono le norme di comportamento attese. Queste regole sono un ausilio per l'interpretazione dei principi in applicazioni pratiche e hanno lo scopo di guidare la condotta etica degli internal auditor.

I quattro elementi all'interno del codice etico dell'IIA che ne costituiscono i principi fondamentali sono: Integrità; Obiettività; Riservatezza e Competenza.

Per *integrità* si intende il rifiuto di compromettere i valori professionali per un guadagno personale. Un altro aspetto dell'integrità è l'adempimento dei doveri professionali in conformità alle leggi vigenti.

Con *obiettività* si va a sottolineare l'impegno a fornire alle parti interessate informazioni imparziale e soprattutto a garantire l'impegno dell'individuo all'indipendenza da conflitti di interesse economico o professionale.

La *riservatezza* consiste nel rifiuto di utilizzare le informazioni organizzative per scopi privati ed infine la *competenza* risiedere nell'impegno ad acquisire e mantenere un livello adeguato di conoscenza e di abilità, e di essere sempre aggiornati e sapersi adeguare alle nuove emergiti necessità e skill richieste per svolgere l'attività di internal audit.

### 1.4.3 Gli standard

Parte fondamentale del Framework sono gli *standard,* i quali sono vitali per praticare la funzione dell'IA.

Gli obiettivi principali per i quali sono stati creati gli standard sono:

1. Guidare l'adesione agli elementi obbligatori dell'IPPF;

2. Fornire un quadro di riferimento per l'esecuzione e la promozione di un'ampia gamma di servizi di internal audit a valore aggiunto;
3. Stabilire le basi per la valutazione delle prestazioni dell'audit interno;
4. Promuovere il miglioramento dei processi organizzativi e delle operazioni.

Gli Standard sono stessi sono articolati in *Attribute Standard*, che sono quelli che regolano le responsabilità, l'attitudine e le azioni dell'attività di Internal Audit; I *Performance Standard* che governano la natura dell'IA e forniscono validi criteri per valutare l'operato degli stessi; L'IIA fornisce anche le *Interpretations* che servono a chiare le tipologie di standard precedenti; infine gli *Implementation Standard* che per ogni standard di Attribute o performance forniscono i requisiti applicabili ai servizi di Assurance e/o di consulenza.

Lo *standard 1110* stabilisce che l'auditor deve essere indipendente ed oggettivo. Quest'indipendenza fa riferimenti a tutte le situazioni che potrebbero limitare la libertà di esprimere un'opinione all'auditor e soprattutto che potrebbero addirittura condizionarne un giudizio. Inoltre, lo standard fa riferimento all'indipendenza a livello organizzativo, che comporta l'obbligo dell'auditor di dover riferire al CdA sul proprio operato e soprattutto di dover dichiarare allo stesso la propria indipendenza.

L'oggettività richiesta dal ruolo è poi ripresa anche *dallo standard 1120*, nel quale si fa riferimento alla capacità dell'auditor di essere imparziale e privo di bias per evitare di creare dei conflitti d'interesse. Questi vengono definiti come le situazioni in cui entrano in contrapposizione l'interesse personale dell'auditor e quello dettato dalla competenza professionale. È importante specificare che i conflitti d'interesse non esistono solo a seguito di azioni non etiche o improprie o illecite.

Lo *standard 1130* dispone che in caso vengano a mancare l''indipendenza e l'oggettività richiesta in precedenza si ritiene necessario svolgere una Disclosure tra le parti per verificare l'impairment di dette caratteristiche. La Disclosure varierà a seconda del tipo di conflitto. In generale l'obbiettivo è quello di limitare la creazione di "Scope limitation", ovvero azioni che precludono l'internal auditor a svolgere i propri piani e raggiungere i propri scopi.
Questi standard facevano riferimento alla "*Indipendence of the internal Auditor*", ma altrettanta importanza hanno quelli che fanno riferimento al *"Auditor proficiency*", nello specifico lo standard 1200 e 1210.

*Lo standard 1200* definisce che l'attività di audit deve essere svolta con le competenze e la dovuta attenzione professionale. Per competenze lo *standard 1210* definisce tutte le attività che complessivamente l'auditor deve

possedere o ottenere come conoscenza generale, skills ed altre necessarie per performare al meglio il proprio ruolo.

L'IPPF contiene delle attività definite raccomandate, che si articolano in azioni di implementazione e supplemento della parte obbligatoria, descrivendo nel dettaglio le pratiche per assicurare la corretta applicabilità dei principi, del codice etico e degli standard sopracitati.

Da oltre una generazione, gli standards dell'Institute of Internal Auditors (IIA) guidano i professionisti nel fornire garanzie e consulenze di revisione interna che siano indipendenti, obiettive, efficaci, efficienti, etiche e della massima qualità. In questo momento storico però gli standard sono in processo di revisione in quanto il futuro richiede servizi di internal audit che siano tempestivi, pertinenti e d'impatto, ciò implica standard perspicaci, preveggenti, chiari e diretti. Per rispondere a questa esigenza, l'IIA ha pubblicato un documento che cambia radicalmente il modo in cui gli standard, ed altri elementi dell'IPPF, vengono rappresentati e spiegati.
Gli standard e la guida all'implementazione saranno riorganizzati in cinque domini, ognuno dei quali affronterà aspetti chiave della professione.

- Il dominio I *"Scopo dell'Internal Auditing":* Questo dominio unificherà le descrizioni della professione precedentemente diffuse in vari elementi dell'IPPF;
- Il dominio II *"Etica e professionalità":* Verranno incorporati il Codice etico e gli standard relativi alla condotta dei professionisti e sarà arricchito dall'inclusione di standard relativi alla dovuta attenzione professionale.;
- Il dominio III *"Governo della funzione di revisione interna"*: il dominio proverà a chiarire il ruolo del consiglio di amministrazione. Questa modifica delinea per la prima volta le importanti responsabilità del CdA a sostegno di un'efficace revisione contabile interna e tratta il modo in cui il Chief Audit executive (CAE) può supportare lo stesso nello svolgimento delle sue responsabilità;
- Il dominio IV "*Gestione della funzione di revisione interna":* Verrà specificato il ruolo del CAE e date indicazioni sulla gestione della funzione di revisione interna;
- Il dominio V *"Esecuzione dei servizi di revisione interna":* Verranno esplicitati ulteriori requisiti e pratiche per fornire servizi di revisione interna efficaci e quotidiani.

Il principale obbiettivo della ridefinizione degli standard è quello di chiarire ed implementare il concetto di qualità, in quanto la semplice conformazione all'IPPF non è sufficiente, ma risulta necessario dover migliorare continuamente la performance per poter portare alla creazione del valore aggiunto ricercato.

A partire da 2022, l'IIA ha avviato una profonda revisione degli standard della professione con l'obiettivo di evidenziare e promuovere il ruolo strategico dell'Internal Audit all'interno delle organizzazioni aziendali. La pubblicazione dei nuovi standard è prevista entro la fine del 2023 e, ad oggi, sono state coinvolte tutte le Associazioni nazionali, inclusa AIIA, al fine di raccogliere commenti e suggerimenti per la declinazione finale dei nuovi standard. Un elemento molto importante di questo aggiornamento, tra gli altri, è la conferma della rilevanza dei principi di indipendenza, integrità e obiettività della funzione nello svolgimento delle proprie attività, avendo sempre come obiettivo il mantenimento della competenza professionale. Come già premesso, la conoscenza dei rischi a cui è esposta l'organizzazione, inclusi quelli nuovi e quelli emergenti, e la conoscenza dei processi aziendali permangono tra i principali pilastri alla base di una corretta valutazione del sistema di controllo esistente e di adeguate raccomandazioni volte al miglioramento aziendale.

# CAPITOLO 2: Il Competency Framework

## 2.1 La struttura del Global Internal Audit Competency Framework

Quando si parla di competenze si fa riferimento non soltanto alla necessità che un individuo abbia delle conoscenze teoriche, ma che lo stesso le sappia applicare concretamente, l'abilità di un individuo di portare a termine un lavoro in modo consono con un set definito di conoscenze, skills e comportamenti. Le competenze per un internal auditor devono essere tali da portare alla creazione di valore aggiunto svolgendo una determinata attività combinando le conoscenze, definibili "general knowledge", con le abilità e capacità personali intrinseche all'individuo stesso.
Ovviamente ogni ruolo, ogni funzione aziendale necessità di competenze diverse per far si che l'attività sia svolta correttamente e nel miglior modo possibile.

*"Proteggere ed accrescere il valore dell'organizzazione, fornendo Assurance obiettiva e risk based, consulenza e competenza*"

Così l'IIA definisce la mission dell'internal audit, andando a chiarire subito il ruolo imprescindibile delle competenze nell'esercizio della professione.

Inoltre, tra i principi fondamentali la competenza è una caratteristica fondamentale dell'auditor in quanto nell'esercitare il proprio ruolo lo stesso deve utilizzare un bagaglio appropriato di conoscenze, esperienze e saper dare la dovuta assistenza professionale. Anche gli standard promuovono le competenze dell'internal audit come una prerogativa necessaria per esercitare la professione.

Per spiegare al meglio la relazione tra l'IA ed il Competency Framework è necessario fare riferimento allo standard 1210, di cui si è parlato nel precedente capitolo, il quale stabilisce proprio quelle che sono le competenze necessarie per svolgere la professione di internal auditor e per costruire e mantenere dette competenze è necessario fare un *"assessment"* delle stesse basato proprio sul Framework.

Infatti, lo *standard 1210* dice che "*Gli internal auditor devono possedere le conoscenze, capacità e altre competenze necessarie all'adempimento delle loro responsabilità individuali. L'attività di internal audit nel suo insieme deve possedere o dotarsi delle conoscenze, capacità e altre competenze necessarie all'esercizio delle proprie responsabilità."*

L'Interpretazione dello Standard definisce la competenza come un termine collettivo che si riferisce alle conoscenze, alle abilità e alle altre competenze richieste all'IA, per svolgere efficacemente le loro responsabilità professionali. Inoltre, comprende anche la considerazione delle attività in corso, delle tendenze e delle questioni emergenti, al fine di fornire consigli e raccomandazioni pertinenti.

Sono stati emanati degli standard di implementazione del 1210, in relazione alla valutazione di determinati rischi. Per il rischio di frode è stato integrato lo *standard 1210.A2*, per il quale gli internal audit devono avere conoscenze sufficienti per valutare il rischio di frode e il modo in cui viene gestito dall'organizzazione; volto a mitigare i rischi informatici è stata l'emanazione dello *standard 1210.A3*, per il quale l'IA deve avere una conoscenza sufficiente dei principali rischi e controlli informatici e delle tecniche di audit basate sulla tecnologia disponibili per svolgere il lavoro loro assegnato. Queste implementazioni non presuppongono che l'internal audit sia un esperto nel campo, ma che sia capace di riconoscere questi rischi nella verifica dei controlli per prevenirli. Infine, è stato redatto lo *standard 1210.C1,* che stabilisce che il responsabile IA deve rifiutare l'incarico di consulenza o di ottenere una consulenza e fornire un'assistenza competente se non ha le conoscenze, le capacità o altre competenze necessarie per svolgere tutto o parte dell'incarico.

In questo contesto nasce "The *IIA's Global Internal Audit Competency Framework",* che è definito dall'IIA stesso come uno strumento che definisce le competenze necessarie a soddisfare i requisiti fissati dall'IPPF per il raggiungimento del successo della professione dell'Internal Audit.

Lo strumento sviluppato dall'IIA fornisce una guida chiara per la formazione, lo sviluppo e la valutazione delle competenze degli internal auditor in tutto il mondo. Allo stesso modo il framework è flessibile e può essere adattato alle specifiche esigenze e alle diverse fasi di carriera degli IA, questo perché non esiste una "One best way" per svolgere l'attività di auditor, ma ogni azienda è una realtà a sé stante e può richiedere caratteristiche e competenze diverse.
Il Competency Framework è composto da due dimensioni principali: competenze professionali e competenze personali. Le competenze professionali si riferiscono alle conoscenze tecniche e alle abilità specifiche richieste per l'internal audit, mentre le competenze personali riguardano le caratteristiche personali e le abilità trasversali necessarie per avere successo nella professione.

Le competenze professionali identificate nel framework dell'IIA comprendono la conoscenza degli standard dell'internal audit e delle procedure operative, la comprensione dei processi di business e dei rischi associati, la capacità di identificare e valutare i controlli interni, nonché la conoscenza delle normative e delle leggi

applicabili. Inoltre, il framework include competenze nel campo della gestione del rischio, della tecnologia dell'informazione, della conformità e dell'etica professionale.

Le competenze personali sono altrettanto importanti per gli internal auditor. Queste competenze riguardano la comunicazione efficace, la leadership, la capacità di pensiero critico, l'orientamento al risultato, l'etica e l'integrità, nonché la capacità di lavorare in modo collaborativo e di gestire il cambiamento. Le competenze personali sono fondamentali per stabilire una buona relazione con gli stakeholder, gestire situazioni complesse e influenzare positivamente il processo decisionale.

Dopo aver fatto la distinzione tra competenze professionali e personali, è necessario riportare quelle che sono le dieci competenze principali riportate dall'IIA, che risultano interdipendenti fra loro:

1. *Professional Ethics*: Il responsabile dell'IA deve promuovere ed applicare l'etica professionale, seguendo i principi del codice etico, anch'esso emesso dall'IIA;
2. *Internal audit Management:* È necessario sviluppare e gestire la funzione di revisione interna non trascurando quelli che sono gli interessi dell'azienda e gli obblighi conseguenti il ruolo che si ricopre;
3. *IPPF:* Come già anticipato bisogna svolgere la funzione in modo da applicare l'International Professional Practices Framework (IPPF);
4. *Governance, risk and control:* Applicare una comprensione approfondita della governance, del rischio e del controllo appropriati all'organizzazione;
5. *Bussiness Acumen*: Mantenere la conoscenza dell'ambiente di business, delle pratiche di settore e dei fattori organizzativi specifici;
6. *Communication:* È necessario saper comunicare con impatto, per far si che l'attività svolta sia compresa ed accettata nel modo corretto;
7. *Persuasion and Collaboration:* Bisogna persuadere e motivare gli altri all'interno dell'organizzazione attraverso la collaborazione e la cooperazione.
8. *Critical Thinking:* Non sono richieste sole competenze teoriche, ma è auspicabile che il responsabile della funzione di IA sappia applicare tecniche di analisi dei processi, di business intelligence e di problem solving;
9. *Internal Audit Delivery:* Non bisogna dimenticare che la funzione di internal audit ha degli output bene definiti che devono essere correttamente consegnati all'organismo di controllo;
10. *Improvement and Innovation*: Risulta fondamentale in un panorama aziendale così mutevole accogliere il cambiamento e guidare l'azienda verso il miglioramento e l'innovazione.

L’organizzazione del Competency Framework può essere descritta e compresa in modo più chiaro con la figura 2.1.

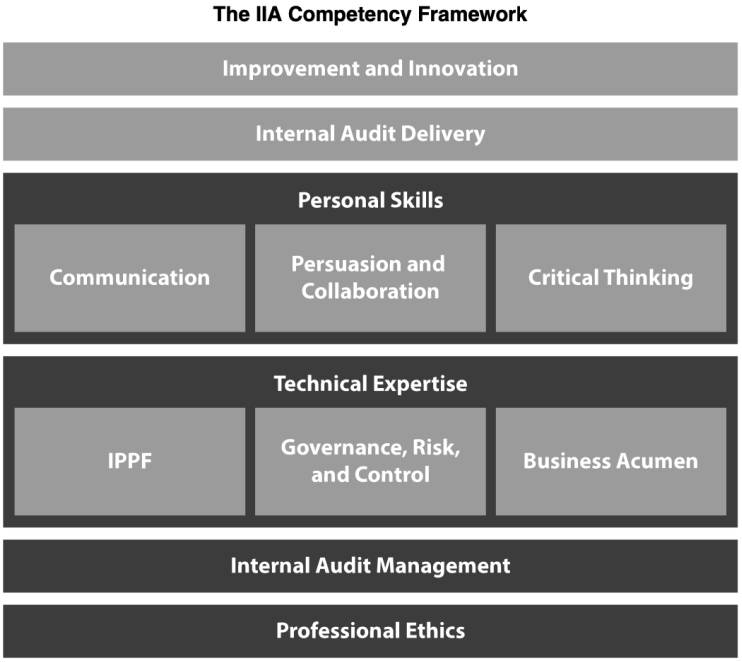


*Figura 2.1, The IIA Competency Framework, CIA 2019*

È da sottolineare come l’etica professionale e l’IA Management siano la base per riuscire a raggiungere la padronanza di tutte le competenze richieste dal Framework, e come l’utilizzo di tutte le competenze porti a fornire il deliverable auspicato e il miglioramento e l’innovazione dell’organizzazione stessa.

Nello specifico il Framework raggruppa le competenze in quattro ambiti inerenti all’attività di Internal Audit, ovvero *“Professionalism”, “Performance”, “Environment” e “Leadership & Communications”.*
Per ognuno di queste aree ci sono delle diverse aree di conoscenza, ed in base alle caratteristiche e competenze individuali , per ogni area il responsabile della funzione di IA può essere definito come un soggetto che ha “General Awareness”, quindi un livello di conoscenza base, non molto specifico; “Applied Knowledge” , ovvero ha non solo una conoscenza più elevato , ma è anche in grado di applicarlo correttamente; ed infine “Expert”, quando non solo ha le competenze adeguate e le sa applicare, ma è anche in grado di portare valore aggiunto all’organizzazione nella sua interezza.
Nell’ambito del Professionalism, si vanno a definire i connotati dell’Auditor, partendo dai principi etici alla base del suo operato arrivando alle competenze professionali necessarie a svolgere al meglio la funzione essendo autorevoli ed ispirando fiducia degli altri membri dell’organizzazione. Le principali aree di

“Knowledge” sono la Mission ed il mandato dell’IA, l’indipendenza organizzativa, l’obiettività individuale, il comportamento etico, la dovuta cura professionale e lo sviluppo professionale stesso.

La parte del Framework inerente alla Performance descrive le modalità operative per eseguire il mandato di IA, per pianificare tutta l’attività in conformità con quanto dettato dagli Standard. Le aree oggetto di valutazione sono la prestazione ed il governo operativo, il modo in cui è disposto il sistema di controllo interno e gestione del rischio, ed il modo in cui vengono riconosciute, valutate e prevenute le frodi. Inoltre, viene valutato l’engagement sotto diversi punti di vista, ad esempio si valuta il piano di lavoro, il risk assessment, le risorse a disposizione, i metodi di analisi in generale partendo dalla raccolta delle informazioni, passando per il sampling ed i tools utilizzati, arrivando alle evidenze riscontrate ed alle review analitiche.

Il Framework poi valuta anche l’Environment, cioè dove viene creato il valore. Questo ambito ricopre sia aspetti professionali che tecnici per identificare, monitorare, affrontare ed in alcuni casi prevenire, i rischi specifici dell’ambiente in cui opera un’organizzazione. Vista la vastità della risonanza che il rischio ambientale può avere su un’impresa, l’area della valutazione del Competency Framework è abbastanza vasta. Riguarda si aspetti di organizzazione dal punto di vista di management e planning strategico, quindi dalla struttura alla leadership, le tematiche dei processi aziendali comuni e della responsabilità ESG, e per finire le aree riguardanti l’IT e contabilità e finanza.

Ultimo ambito analizzato è quello della Leadership & Communications. In questo caso si va ad analizzare a chi va offerto il servizio, serve per dare una guida e per rafforzare le relazioni sia con il team che con gli Stakeholder. Lo svolgimento dell'attività di internal audit nel suo insieme richiede competenze trasversali e la capacità di definire un adeguato approccio strategico, cioè comunicare in modo efficace e coltivare relazioni produttive con gli stakeholder, sia interni che esterni, nonché la capacità di gestire efficacemente persone e processi. Le aree in cui viene valutato questo aspetto sono tutti quelli di pianificazione, quindi quella strategica e di gestione dell’internal audit, quella di coordinamento degli sforzi dell’audit e dell’Assurance ed inoltre vengono valutati, se esistenti, i programmi di garanzia e miglioramento della qualità. Importantissima per la comunicazione la valutazione delle relazioni e l’”advocacy”, cioè la capacità di mantenere ed implementare i rapporti con gli Stakeholders, il ruolo delle soft skills e dell’innovazione, ed infine anche il modo in cui viene effettuato il reporting.
Il Competency framework però non è stato progettato solo per aiutare gli Internal auditor a sviluppare le competenze necessarie a raggiungere gli obiettivi di carriera individuali, o a svolgere la propria attività correttamente, ma può essere anche d’aiuto ad altre figure interne o esterne la realtà aziendale.

Ad esempio, può essere utilizzato dagli sviluppatori di corsi e gruppi di certificazione all'interno della professione per garantire che i corsi e le certificazioni sviluppino e valutino adeguatamente le competenze richieste dalla professione. Anche la comunità accademica deve fornire un elenco di competenze professionali critiche da considerare nello sviluppo dei corsi per preparare gli studenti all'ingresso nella professione di revisore interno. Di conseguenza lo strumento è anche utilizzato dagli studenti per comprendere le competenze che devono dimostrare per diventare Internal Auditor di successo, e che servono ad assisterli nella valutazione dei loro piani individuali di sviluppo professionale.
Il framework può essere utilizzato dai datori di lavoro o da altri professionisti in generale come punto di riferimento per il confronto ed il benchmarking con i propri quadri di competenza, ed anche per ottenere una visione chiara e dettagliata dei livelli di competenza richiesti dagli Internal Auditor.
Di conseguenza sarebbe auspicabile che il Competency Framework venisse utilizzato anche dai selezionatori e dai professionisti delle risorse umane per sviluppare descrizioni delle mansioni appropriate e reclutare personale adeguatamente qualificato rispetto le competenze delineate dal Framework stesso.

**2.2 Attuale livello di maturità delle competenze della Funzione IA**

Nel 2022 è stato organizzato un webinar dall'Associazione Italiana Internal Auditors, durante il quale si è discusso del livello della maturità raggiunta delle competenze della Funzione di IA rispetto a quelle stabilite dal Competency Framework.
È stata condotta una survey su circa 50 società facenti appartenenti a diversi settori industriali, per rilevare il livello di maturità prima citato. L'analisi è stata condotta sui raggruppamenti delle competenze effettuati dal competency Framework e sulla base dei livelli di conoscenza citati nel precedente paragrafo, ovvero del "General Awareness", quindi un livello di conoscenza base, non molto specifico; "Applied Knowledge"; ed infine "Expert", quando non solo ha le competenze adeguate e le sa applicare, ma è anche in grado di portare valore aggiunto all'organizzazione nella sua interezza.

Il sampling è composto da un numero limitato di società e quindi non fornisce una rappresentazione esaustiva delle competenze dei professionisti dell'IA, ma riesce comunque ad essere la base per delle riflessioni circa l'andamento generale dello sviluppo delle competenze.
La survey risulta meritevole di analisi in quanto fornisce degli spunti su cui andare a lavorare per migliorare la condizione dell'IA rispetto alla continua implementazione ed integrazione del Competency Framework.
I partecipanti alla survey sono principalmente aziende quotate, appartenenti ai settori: Assicurativo, Finanziario, dei Servizi, Manifatturiero ed al Pubblico. Le soglie di fatturato sono per il 21% del sampling

superiori ai € 5.000 ml, del 35 % sono soglie tra i €1.000 ml ed i €3.000 ml, per il 23% sono tra i €500 ml ed i 1.000 ml, e la restante parte del sampling ha un fatturato inferiore ai €500 ml.
L'analisi prosegue con delle distribuzioni delle competenze per ogni ambito del Competency Framework in base alla media AS-IS e quella TO-BE.
I modelli AS-IS e TO-BE sono utilizzati per descrivere lo stato attuale di un sistema o di un'organizzazione (AS-IS) e lo stato futuro desiderato (TO-BE). Questi modelli vengono spesso utilizzati nell'ambito della gestione dei processi aziendali o dell'analisi degli stessi per promuovere implementazioni o migliorie.

Il modello AS-IS rappresenta lo stato corrente delle attività, dei processi, dei sistemi e delle strutture organizzative di un'azienda. È una rappresentazione dettagliata di come le cose funzionano attualmente. Il modello AS-IS viene solitamente creato attraverso interviste, osservazioni e analisi delle informazioni disponibili. Può aiutare a identificare i punti di forza, le inefficienze e le aree problematiche all'interno dell'organizzazione.

Il modello TO-BE, d'altra parte, rappresenta il futuro desiderato o lo stato obiettivo dell'organizzazione. Rappresenta come l'organizzazione vorrebbe che le cose funzionassero una volta che i cambiamenti o le migliorie sono stati implementati. Il modello TO-BE viene creato sulla base delle informazioni raccolte durante l'analisi AS-IS, ma con l'aggiunta di nuove idee, miglioramenti e soluzioni per affrontare i problemi identificati. Questo modello può aiutare a visualizzare il modo in cui i processi aziendali potrebbero essere ottimizzati, come i ruoli e le responsabilità potrebbero essere ridefiniti o come i sistemi informatici potrebbero essere migliorati.

Ritornando ai risultati della survey, dal punto di vista dell'ambito della professionalità, il divario più grande tra la media AS-IS e quella TO-BE è sul *comportamento etico*. La maggior parte ha un livello di competenze fermo sulla conoscenza applicata, cioè dimostrano la conformità al codice etico, ma una minore proattività nella promozione degli standard etici. Per sopperire questo gap tra la realtà e la prospettiva sono stati forniti diversi spunti di riflessione, che sono delle attività che concretamente possono essere attuate per ottenere dei miglioramenti. Prima fra tutti gli auditors dovrebbero dichiarare e sottoscrivere un'assenza di conflitto di interesse, dopo di che nel momento dell'assegnazione degli incarichi agli stessi devono essere comunicati i principi del Codice Etico IIA. Come ulteriore spunto di analisi, risulta produttivo ed efficace promuovere nell'ambito della "peer to peer" uno scambio di feedback inerenti alla corretta applicazione degli standard IA. Dai sondaggi tra gli auditors risulta poi necessario promuovere formazione sia esterna, che in house, che on the job per il raggiungimento del livello "EXPERT" nell'ambito della professionalità.

Nell'ambito della performance le principali differenze del modello AS-IS e TO-BE sono relative ai temi delle Frodi, del Risk Assessment e all'Analisi dei dati.

*Il tema delle frodi* è nelle competenze per esattamente il 50% del sampling fermo su un livello di conoscenza applicata, che consiste in una valutazione delle frodi e nell'istituzione di determinati controlli per prevenire la realizzazione delle stesse, ed invece un 34% fermo su un livello di conoscenza generale.
Sebbene per il 64% del sampling il modello TO-BE è improntato sul raggiungimento del livello "Expert", sono presentati diversi spunti di riflessione sul raggiungimento di tale obiettivo. Prima di tutto sarebbe opportuno definire degli indicatori di frode, definiti "red flag", e di conseguenza creare una Fraud Library, cioè degli schemi di frode. Risulta necessario segnalare repentinamente al CdA e adottare un approccio di continuos auditing, per questo motivo sarebbe altrettanto ulite sviluppare delle sinergie con il canale di Whistleblowing. Un ulteriore intervento, che andrebbe a creare un cambiamento definitivo nel mondo dell'audit, potrebbe essere quello di integrare i fraud risk nell'impianto degli audit operativi, di creare ed implementare la cosiddetta "Fraud Prevention".

*Il Risk Assessment in sede di pianificazione* è invece è un tema che posiziona la maggior parte delle aziende del sampling su un livello "Expert", tranne per quasi la totalità delle aziende del settore Pubblico ed Assicurativo. La principale differenza tra i diversi livelli di competenza in questo ambito è relativa alla capacità di riuscire a valutare il rischio durante il periodo dell'incarico dell'audit e non successivamente nel caso in cui il rischio, che doveva essere prevenuto, si è effettivamente verificato.
I principali punti di miglioramento riguardano l'adozione di tecniche di dynamic risk assessment, soprattutto se la funzione IA è "connessa" con tutti gli altri player dell'organizzazione e con le diverse linee di business attraverso un processo di Enterprise risk Management, cioè di gestione del rischio operativo a tutti i livelli aziendali, non solo accentrato ai vertici. Inoltre, per poter migliorare la modalità di operato dell'auditor sarebbe auspicabile consentirgli la possibilità di accedere indipendentemente ai sistemi di riferimento per monitorare indicatori di rischio nel corso dell'anno.

Sempre nell'ambito della performance si è riscontrata particolare carenza *sul tema dell'analisi dei dati*, in quanto nel sampling dalla media AS-IS risulta che il 52% sia fermo su un livello di conoscenza generale, cioè attestati su una mera descrizione dell'analisi dei dati e l'applicazione di metodi di analisi ai fini solo dell'incarico audit. Gli spunti di riflessione in merito all'analisi dei dati sono basate principalmente sul cogliere le opportunità di digitalizzare tali processi, sulla possibilità di specializzare determinate figure ed individuare idonei strumenti di data robotics in vista di un piano di continuous audit.

Attualmente, le competenze legate alla knowledge area dell'"Environment" sono giudicate complessivamente a livello di "conoscenza applicata", se non fosse per il tema della misura delle performance. Questo aspetto può essere ricollegato anche all'analisi dei dati presentata precedentemente, in quanto le competenze legate alla misura della performance sono strettamente connesse ai data analytics. La necessità per avvicinarsi ad un livello "Expert" di questa competenza è quella di trovare degli indicatori più specifici possibili in base alla tipologia di performance da dover valutare e vista l'importanza che i target ESG stanno assumendo negli ultimi anni, di inserirli all'interno del pano di audit di verifica dell'attività.

Infine, l'analisi si sofferma sull'ambito della Leadership&Comunication su due temi in particolare, ovvero quello del coordinamento degli sforzi di Assurance, che vede la distribuzione la maggior parte delle aziende del sampling o fissa su un livello di conoscenza generale o su un livello "Expert"; e sul tema delle Soft skill ed innovazione, che è principalmente fisso su un livello di conoscenza applicata.

L'azione principale da intraprendere per migliorare il coordinamento delle funzioni di Assurance è quella di comunicare il piano di audit integrato, promuovendo l'adozione di uno stesso approccio per le funzioni di secondo livello, inoltre armonizzando i template di reporting dei risultati e le metriche di valutazione. Un'ulteriore forma di miglioramento potrebbe essere, soprattutto nelle realtà più sviluppate ed articolate, la previsione della creazione un comitato di Audit & Assurance Integration.

Per quanto riguarda il tema delle soft skill ed innovation, per far sì che si riesca a raggiugere un livello di competenze "Expert", è necessario fare molta formazione sulle soft skill, valutando il tutoring o mentoring o coaching delle risorse senior. Sarebbe opportuno poi promuovere la partecipazione a progetti innovati e che la stessa funzione di audit abbia degli approcci innovativi come la produzione di indicatori e l'implementazione delle dashboard di monitoraggio.

In conclusione, da questa survey è stato possibile capire come il mondo dell'audit stia approcciando nei diversi settori all'evoluzione verso lo sviluppo delle competenze richieste dall'IIA, ma che la strada per essere considerati degli esperti nello svolgimento della professione dell'IA è ancoro lunga e soprattutto costantemente improntata sull'implementazione continua dei diversi processi per tenere il passo con le mutevoli condizioni del mercato e conseguentemente delle attività delle aziende.

### 2.3 Il futuro della funzione di Internal Audit

L'AIIA è un'associazione professionale ed ha come primo obiettivo quello di seguire ed anticipare i bisogni dei soci, in termini di crescita professionale, di training e di conoscenze generali. Per raggiungere il proprio obiettivo l'associazione mette al centro di ogni analisi i rischi che impattano sullo svolgimento della

professione, che continuano a crescere in quanto sono emergenti da un contesto dinamico che si complica continuamente.

Il cambiamento dell'organizzazione aziendale è condizione necessaria per adeguarsi al mondo post pandemia, con l'ingresso lavorativo delle nuove generazioni, considerando l'impatto dell'utilizzo delle nuove tecnologie e tutta la complessità generata dalle *tematiche ESG*. L'acronimo corrisponde alla responsabilità ambientale, sociale e di governo societario che le aziende hanno e devono rispettare nell'esercitare la propria attività. Attualmente questo è un rischio che coinvolge i diversi livelli aziendali, anche la funzione di internal audit, e *per questo motivo è approfondito nel capitolo terzo.*

Tre anni di crisi sia per la pandemia che per la guerra, hanno creato una sorta di tempesta perfetta, nella quale bisogna imparare a convivere con i rischi che sono molto interconnessi fra di loro, tra quelli definibili noti e quelli ancora emergenti.

Tutto ciò porta alla creazione di tematiche importanti in relazione alla business continuity delle aziende, rischi di liquidità e di solvenza. In aggiunta, occorre considerare anche altri impatti sul mondo del lavoro, primo fra tutti proprio il modo di lavorare. Viene sempre di più richiesta l'integrazione del lavoro in presenza con lo smart working, questo anche perché le persone iniziano a trasferirsi dalle città in quanto il costo della vita è estremamente elevato, ed inoltre si afferma il concetto della *"Work life balance"*, cioè puntare ad una qualità di vita diversa con miglior equilibrio tra vita privata a lavoro. Puntare ad ottenere maggior equilibrio comporta delle problematiche per l'internal audit perché diventa difficile riuscire a soddisfare le necessità dei singoli dipendenti, correndo il rischio di perdere persone competenti nel caso in cui le stesse non sentano di avere un giusto equilibrio tra vita privata e vita lavorativa. Come affermato da uno studio di Microsoft nel 2022, analizzando i dati del Work Trend Index, i lavoratori chiedono condizioni di lavoro sempre più flessibili, ma sebbene 7 manager su 10 siano disposte a concederle, il 53% delle organizzazioni non presta attenzione ai propri lavoratori.

Tutto ciò è accompagnato dal fenomeno della *Great resignation*, fenomeno americano, che ormai si sta espandendo in tutto il mondo, che consiste nella fuga di talenti o di persone con skill cruciali, che portano con sé la grande difficoltà di sostituire i talenti che vanno via, con nuove leve equamente skillate.

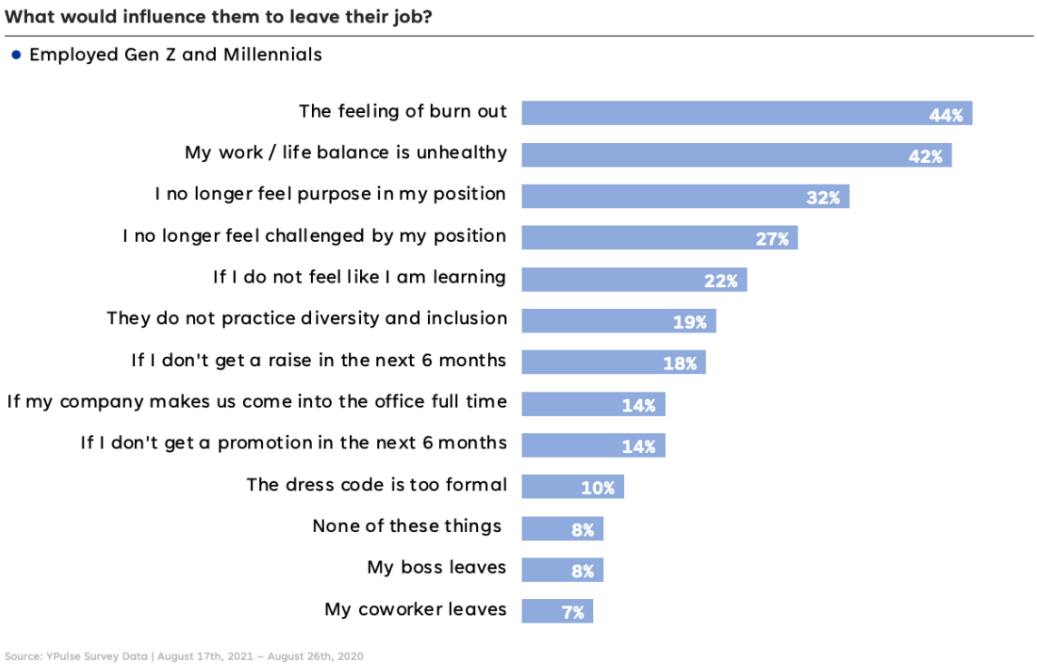


*Figura 2.2, Ypulse Survey Data, August 2021*

Come dimostra la figura 2.2 le dimissioni volontarie sono in aumento perché i giovani prediligono sempre di più condizioni di lavoro migliori e retribuzione più alte, mentre la popolazione di lavoratori più grande cerca maggiore equilibrio. Cambiamento di attitudine, le giovani generazioni sono maggiormente interessate a lavorare in organizzazioni in cui lo scopo sociale e la sensazione di «fit-for purporse» è più alto ed è maggiormente allineato alle loro convinzioni, risulta quindi necessario fronteggiare la nuova challenge dell'allineamento valoriale. L'85% degli executive e managers ritengono che lo scopo delle organizzazioni per cui lavorano sia tangibile. Solo il 15% degli impiegati concorda con questa affermazione.
Nel 2020 è stata fatta una lista delle skills for the future, le principali sono quasi tutte soft skills come la curiosità, il saper lavorare in team, coraggio e volontà al cambiamento, Problem-solving, proattività, capacità di comunicazione, la capacità di ascoltare e l'intuizione.
Esiste uno standard emanato dall'IIA, il 2030 sul resource management, il quale stabilisce che i CAE (Chief Audit Executive) devono assicurarsi che le risorse di internal audit siano appropriate, sufficienti ed effettivamente abilitate a raggiugere il piano approvato.

Emerge quindi che non c'è nulla di costante tranne il cambiamento. La figura dell'IA deve adattarsi a questi cambiamenti per soddisfare le necessità degli stakeholders. Oggi il cambiamento è l'elefante nella stanza, non può non essere visto.

Il punto di partenza è la consapevolezza che nell'attuale contesto le aziende si trovano a dover gestire una serie di sfide: rischi emergenti, cambiamenti organizzativi e tecnologici, nuove regolamentazioni ESG, ecc.

Cambiano le aziende, cambiano i rischi, cambiano le aspettative sul ruolo dell'Internal Audit. Gli stakeholders chiedono valore, efficienza, velocità di azione. La vera sfida è costruire dei processi per adattarsi al cambiamento, in modo rapido ed efficace, dimostrando resilienza. I cambiamenti ci saranno sempre ed è altrettanto probabile che le competenze richieste di cui oggi potrebbero essere già obsolete tra pochi anni.

Il tema People non è più solo limitato all'area delle risorse umane, anche il team di Audit deve saper attrarre talenti e soprattutto saperli mantenere.

Da delle analisi condotte dalle società di consulenza è emerso che circa il 30% della forza lavoro presente in azienda dovrà aggiornare le proprie competenze, il cosiddetto fenomeno delle re-skilled. Andare ad aggiornarsi rispetto a quelle che sono le esigenze del contesto lavorativo attuale. Il 68% dei responsabili in ambito HR pensano che la top priority della loro funzione sia la creazione e la formazione delle figure e delle conseguenti competenze che servono per raggiungere gli obiettivi aziendali. Il 33% delle skills che oggi sono necessarie per svolgere determinati task potrebbero essere obsolete tra 2 anni. La survey non ha delle base scientifiche solide, ma sicuramente aiuta a capire che il processo di creazione delle competenze deve essere un processo continuativo, sempre aggiornato.

Per affrontare questi mutevoli cambiamenti è necessario avere due competenze ovvero il pensiero analitico ed il continuo apprendimento. Queste sono due competenze che permettono di approcciare in modo diverso in base agli interlocutori e permettono di capire il contesto e di abilitare nel comprendere i cambiamenti organizzativi, sia di processo che a livello di tecnologie.

Il problema per affrontare il cambiamento è che bisogna essere consapevoli che non si possono inseguire ed applicare tutte le nuove tecnologie. È necessario avere un processo chiaro, una strategia da seguire per abilitare al meglio le aspettative degli stakeholder che cambiano mutevolmente. Per riuscire ad ottenere la migliore soluzione possibile per creare valore per gli stakeholder ed essere sostenibili economicamente per l'azienda è necessario raggiungere un Trade-Off tra la visione d'insieme a discapito della cura di tutti i minimi dettagli, che in un contesto in continua evoluzione sarebbe impossibile da soddisfare.

**2.4 Lo sviluppo del Competency Assessment Tool**

Grazie al supporto del Competency Framework nel corso del 2022 è stato effettuato uno studio da dei professionisti dell'AIIA, volto ad identificare le competenze chiave che è auspicabile siano presenti, seppur con un diverso livello di granularità e maturità, all'interno dei Team di Internal Audit. Sono state identificate circa settanta competenze chiave ed è stato creato un tool mappato sulle quattro aree in cui il Competency framework raggruppa le competenze che un IA deve possedere, e per ognuna delle competenze esaminate, è stata effettuata una valutazione in merito alla sua rilevanza e al livello di maturità attesa in base alla seniority dei membri del Team. Quest'analisi è svolta con la consapevolezza che "No One Size Fits It All", cioè che il tool potrà essere una base di partenza per tutte le aziende, ma non è possibile creare uno strumento che corrisponda alle necessità di ognuna essendo ogni impresa una realtà a sé stante.

Il tool è uno strumento a griglia che identifica le tipologie di azioni da intraprendere in base al livello di seniority ed al grado di importanza della competenza. Nello specifico si svolgono due analisi che portano alla creazione di due griglie, che serviranno per svolgere la terza analisi cioè quella degli scostamenti tra le prime due. Nella prima griglia viene fatto un elenco delle competenze identificate per area, valutate dal gruppo di lavoro per seniority e per priorità. Invece nella seconda griglia vengono evidenziate le competenze già presenti all'interno del proprio team sempre per priorità e seniority. Infine, la terza analisi, come anticipato, verifica gli scostamenti dell'assessment svolto rispetto alle valutazioni iniziali del gruppo di lavoro.

Il livello di seniority è articolato su quattro figure: *Junior Auditor, Senior Auditor, Audit Manager e CAE.*

*Il Junior auditor* è una risorsa con limitata esperienza, operativamente coinvolta nello svolgimento degli audit e di altri task assegnati, sotto supervisione delle risorse maggiormente esperte.

Il *Senior auditor* è una risorsa con un livello di esperienza medio e relativamente autonome nello svolgimento di audit ricorrenti. Garantisce un primo livello di supervisione sulle risorse junior.

*L'audit Manager* è una risorsa con un buon livello di esperienza e autonomo nello svolgimento di audit a media o anche elevata complessità. Coordina e supervisiona risorse junior e senior, contribuendo alla loro formazione.

Il *CAE* è il responsabile di Funzione, con un elevato livello di esperienza nella gestione del Team e con una visione ampia sul Piano complessivo delle attività e delle relazioni con le altre funzioni.

Nonostante ogni team non è detto abbia tutti i diversi livelli di seniority, sicuramente potrà beneficiare di un buon mix degli stessi.

Per il grado di competenza è stato ipotizzato che gli stessi possano essere *Mandatorio, Raccomandato, Nice to Have ed Outsourced.*

Tutte le competenze mandatorie sono necessarie allo svolgimento delle attività assegnate alla risorsa e non sono derogabili ad altri. Per le risorse junior ad esempio non sono presenti, quindi devono essere sviluppate con il supporto di attività formative interne e/o esterne. Le competenze raccomandate invece sono quelle che servono per lo svolgimento efficace ed efficiente delle attività, ed eventuali gap tra le competenze effettivamente possedute dall'auditor e quelle raccomandate dovrebbero essere colmate nel medio termine. Molto spesso è consigliata la supervisione di risorse competenti. Invece le competenze Nice to have ed outsourced non sono strettamente necessarie allo svolgimento delle attività ricorrenti, ma le prime rappresentano un valore aggiunto e vanno potenzialmente monitorate in termini di rilevanza nel futuro, mentre le seconde sono richieste dallo svolgimento di alcune attività ad hoc o altamente specifiche, che richiedono all'occorrenza un continuo aggiornamento specialistico.

Dallo svolgimento di ulteriori analisi svolte sempre da professionisti associati all'AIIA, è emerso che nelle prime fasi le principali skill da imparare sono di tipo Hard, come la conoscenza degli standard e dei generali metodi di controllo, mentre con l'aumento della maturity aumenta anche la richiesta di soft skills come la capacità di gestire i conflitti ed essere un modello di comportamento. In generale poi emerge un concetto importantissimo alla base di ogni competenza, ovvero quello prima di tutto di dover imparare, sviluppare e consolidare le stesse, ma poi successivamente di diffonderle a tutte le persone di grado inferiore ed anche superiore. Sviluppare una condivisione non solo della conoscenza ma anche della competenza.

*Il competency assesstment tool* può rappresentare un utile riferimento per comprendere quali competenze sviluppare e mantenere all'interno del proprio audit team investendo prima sulle aree ritenute maggiormente critiche e successivamente su quelle meno rilevanti. Facendo un focus richiamando quelli che sono gli ambiti in cui sono state raggruppate le competenze chiave dal Competency framework dell'IIA, si possono definire per ciascun ambito delle competenze chiave.

Nell'ambito della *Leadership & Communications* la principale capacità emersa dallo studio dell'AIIA che ha portato alla creazione del tool, risulta quella di istaurare relazioni costruttive e di fiducia, gestendo eventuali situazioni conflittuali, integrando con il Business, il Top Management e gli Organi di controllo. Tra le competenze inerenti alla *Performance* invece la capacità principale è quella di comprendere e valutare processi

e l'adeguatezza dei controlli, adottando opportune metodologie di testing, evidenziando rilievi e concordando con il Management adeguati action plan. È richiesto sempre più ai membri del Team di Audit di saper comunicare ed interfacciarsi in modo adeguato, efficace e sinergico con gli stakeholders aziendali, fornendo attività che offrano valore aggiunto all'organizzazione in ottica di continuo miglioramento. Risulta invece imprescindibile per le competenze relative all'environnement la conoscenza della struttura organizzativa e dei processi aziendali, compresi framework di controllo adottati ed i sistemi informati a supporto dell'operatività. Infine, per le competenze inerenti la *Professionalità* è necessario sviluppare la capacità di condurre incarichi di Assurance e consulenza nel rispetto degli standard della professione e con resilienza e capacità di adattamento. È opportuno che i membri dei Team di Audit a tutti i livelli di seniority comprendano il contesto aziendale per svolgere efficacemente le attività di audit, mentre può essere valutata l'esternalizzazione di attività che richiedano competenze altamente specialistiche.

Inoltre, il tool si sofferma anche sulla necessità di dover andare a fronteggiare i cambiamenti del mutevole contesto, definito *"new normal"*, in cui al giorno d'oggi l'internal auditor si trova a dover lavorare, e quindi soprattutto le competenze emergenti da tale contesto. Acquisisce sempre maggior rilevanza la capacità di adattamento ai cambiamenti, di resilienza e di gestione delle situazioni nuove e conflittuali e *disruptive*, da qui la necessità di dover pianificare in modo agile gli audit, e rivalutare periodicamente le priorità. In questo contesto così mutevole, risulta un valore aggiunto possedere all'interno dei team di audit competenze specifiche non solo sui modelli del frame work di controllo tradizionale, ma anche su quelli emergenti, in ambito ESG Reporting, Cyber Security, Tax Control Framework, Health, Safety & Environment.

### 2.4.1 Esempi di applicazione concreta del nuovo Tool

Un esempio concreto di applicazione di questo strumento è avvento, grazie alle attività svolte da AIIA, in una grande società italiana quotata, appartenente al settore industriale ("la Società"). Nell'ultimo anno la Società ha iniziato un'attività di formazione collegata alla mappatura delle skill e delle competenze all'interno del gruppo di audit, un gruppo multiregionale che coinvolge più di 150 persone solo della funzione dell'IA.

Nel 2022 è stato costruito un database solo con le competenze minime attese per ciascun livello di audit, chiamato *corporate skills library*. Dopodiché su questo database è stato richiesto a ciascun auditor di dare il proprio self-assessment, in base alle proprie capacità attuali e quelle derivanti da esperienze precedenti e soprattutto focalizzandosi sulle nuove skills richieste come quella di lavorare da remoto, di analisi dei dati e di condivisione dei risultati e degli action plan.

Il risultato di questo self-assessment ha evidenziato alcuni punti di miglioramento su alcune competenze minime che ciascun auditor dovrebbe avere, sui quali sono poi statti programmati dei percorsi di formazione, e rende presente quali sono le competenze di ciascun auditor in base agli obiettivi di crescita del gruppo e stimolare la crescita di ciascun auditor nel breve periodo, creando così un bacino per i nuovi manager del futuro.

Si prospetta di agire nel seguente modo: il o i responsabile/i della funzione di Internal Audit e Compliance (IA&C) creano una matrice delle skill, che viene poi integrata nei Tool del team HR. Segue un processo di assessment da parte del team di IA&C ed i risultati vengono consolidati, e ci si muove per le nuove skill da ottener attraverso la creazione di appositi training plan.

L'esempio portato della Società è specifico sulle competenze di performance e consiste in attività concrete sviluppate per accelerare il processo di acquisizione di dette competenze.

Tra queste ci sono diverse competenze di tipo prettamente tecnico ed una invece più di tipo interpersonali che coinvolge le soft skills. La competenza principale che risulta più difficile da ottenere è la capacità di organizzare e guidare un team, anche a livello internazionale, composto da culture diverse. Come risultato dell'assessment è apparso opportuno, oltre la classica introduzione di piattaforme online per lo studio delle lingue, lo sviluppato dall'area IA&C in collaborazione con il team HR, la predisposizione di un'ulteriore assessment per capire il posizionamento del singolo rispetto a tematiche di "Diversity and inclusion", andando ad individuare punti di forza e di debolezza, e per i punti di debolezza sono presenti delle risorse online per implementare ed approfondire la conoscenza di altre culture. Azioni che coinvolgono direttamente la funzione di Internal Audit sono invece l'istituzione di "Coffee Break", cioè degli incontri di 30 minuti ogni 2 mesi, che coinvolgono dalle quattro alle cinque persone appartenenti all'area IA&C di paesi diversi che ancora non hanno mai lavorato insieme. Sono istituti anche dei Coffee con il Chief Audit Executive, i quali sono svolti con lo stesso modus operandi dei Coffe Break, solo che inoltre c'è la possibilità di avere un incontro diretto proprio con il responsabile CAE per far si di essere aggiornati con l'evoluzione della funzione all'interno di tutta la diramazione dell'azienda.

Per l'ottenimento di competenze più tecniche, come la conoscenza del Manuale della funzione IA e la capacità di determinare lo scopo e l'ambito di un engagement, è stato preposto un "Welcome Kit", sia online che in presenza, in cui viene presentata la struttura dell'internal audit, la vision e la mission, e tutti i passaggi del processo di audit, che comprende anche i vari tool utilizzati. Questo kit è assegnato a chiunque sia in contatto con la funzione di audit.

Infine, La società ha condotto anche le azioni volte ad implementare le competenze sempre tecniche ma dal punto di vista delle metodologie applicate nello svolgimento dell'attività di audit, quindi le tecniche di campionamento, di risk assessment, di definizione di un work program e la non banale attività di valutazione della pertinenza, sufficienza, utilità ed affidabilità delle evidenze ottenute. Tali interventi si concretizzano in quattro gruppi di attività. Il primo intervento è chiamato *"Testing and working paper training"* che impronta una formazione su base regionale con sessioni di due ore, sia per junior auditors che per persone che vogliono approfondire determinate competenze. Un ulteriore intervento più innovativo è quello della *"Peer to Peer review"*, che ha cadenza trimestrale ed è a cura del dipartimento di Metodologia e Qualità, nella quale degli esperti in Internal Audit rianalizzano cartelle di lavoro per dare un giudizio sull'operato. È sottolineato che queste persone non hanno avuto nessun tipo di ruolo nella realizzazione delle carte che analizzano, per evitare qualsiasi tipo di conflitto di interesse. Nel caso in cui vengano riscontrate delle anomalie ricorrenti, viene predisposto un action plan per provare a correggere tali anomalie. Poi l'intervento successivo, la *"Methodology Huddles"* session, è collegato con il precedente in quanto, sempre trimestralmente, e sempre a cura del dipartimento di Metodologia e Qualità, vengono istituite delle sessioni con focus o sulle problematiche emerse dalla Peer to Peer Review, o per divulgare gli aggiornamenti su report e valutazioni oppure per il monitoraggio delle azioni correttive. Infine, l'ultimo intervento previsto è l'istituzione di una *"Lesson Learn"* a cadenza semestrale a livello di Senior Manager, a cascata per livelli di team regionali, per condividere i risultati dei "salienti auditis" e le varie criticità trasversali emerse.

Un altro esempio portato da un ulteriore società quotata è il caso di Co-sourcing, che come già anticipato nel *primo capitolo,* è la situazione in cui alcune delle competenze richieste dall'incarico sono esterne al team di audit e risulta necessario effettuare una collaborazione con altri team interni oppure con specialisti esterni, per specifici progetti. Questa attività oltre ad avere come output quella di ottenere un deliverable, può essere vista come un'opportunità formativa per le risorse interne.

Nel caso specifico della società quotata hanno svolto co-sourcing sia interno che esterno.

Per il co-sourcing esterno, ci si rivolge ad un consulente esterno. La figura interna avrà sicuramente maggiori competenze dal punto di vista dell'ambito dell'environment, quindi della conoscenza della struttura organizzativa e sui processi della società, dei sistemi aziendali e del mercato, del prodotto e delle normative del settore. Dalla figura esterna ci si aspettano invece maggiori competenze nell'ambito del Profesionalism, cioè capacità come la gestione efficace sia dei tempi che delle risorse, di condurre incarichi di Assurance e consulenza, ma soprattutto di predisporre Work program efficaci. L'affiancamento alla figura esterna comporta per quella interna una possibilità di apprendimento di tipo Learning on the job e dell'acquisizione

di cultura e metodo. Inoltre, lavorare in questa tipologia di progetti comporta maggiore engagement da parte della risorsa e della creazione di maggiore fiducia nelle proprie capacità.

Invece, il co-sourcing interno consiste nel far ricorso a persone interne alla società ma non appratenti alla funzione di Audit. Un esempio può essere la richiesta di affiancamento delle unità tecniche per la creazione di un programma ad hoc. Si interfacciano in questo caso la risorsa interna di audit che porta competenze nell'ambito dell'environnement e la risorsa sempre interna ma di un'altra area che porta competenze nell'ambito del Professionalism. L'obiettivo formativo raggiungibile con l'affiancamento di risorse Expert al team di audit è primo fra tutti sicuramente quello di consentire al team di ridurre il tempo necessario alla comprensione del processo oggetto di audit e soprattutto migliora la capacità dell'audit di gestire team eterogenei, addirittura con una limitata conoscenza del processo di audit stesso. Inoltre, è possibile per l'auditor anche sviluppare nuove competenze diverse da quelle classiche dell'attività di audit che potrebbero essere riutilizzate in attività successive.

Molto spesso può capitare che il co-sourcing interno, in società abbastanza strutturate, si evolva diventando un elemento strutturato all'interno del percorso di crescita di alcune risorse, cioè coinvolgendo persone di funzioni diverse ad un percorso di formazione in un'altra area aziendale, nello specifica quella in cui è avvenuto il co-sourcing, per accrescere le competenze individuali ed anche la rete relazionale, ed soprattutto si la possibilità  di comprendere al meglio alcuni processi aziendali.

## CAPITOLO 3: La professione e i rischi emergenti nel mercato

Il rischio è un concetto probabilistico, che implica la probabilità che un certo evento possa causare danni a persone o cose, o innescare altri fattori. Il rischio economico si basa sulla probabilità che un determinato avvenimento possa cambiare gli scenari in cui l'azienda opera e di conseguenza comportare dei cambiamenti nell'azienda stessa. Ogni anno *l'EIRG, European Institutes Research Group*, che opera sotto la guida de*ll'ECIIA, European Confederation of Institutes of Internal Audit,* aggiorna un report chiamato *Risk In Focus,* che presenta i principali rischi di mercato sui quali è necessario orientare la professione di Internal Audit.

L'affiorare di nuovi rischi sul mercato comporta per l'IA la necessità di aggiornare le proprie competenze per affrontare rapidamente le nuove necessità delle aziende e dare supporto alle stesse in situazioni rischiose, incerte e volatili. Nel capitolo si analizzeranno le competenze necessarie per specifico rischio. Come è emerso dal report, ma anche dal Competency Tool presentato nel secondo capitolo, le principali competenze su cui l'internal audit deve concentrarsi per fronteggiare l'attuale contesto mutevole, sono le soft skills, cioè non competenze tecniche, generalmente definite Hard skills. Questo ordine di priorità non esclude la necessità di mantenere all'interno della funzione le principali conoscenze tecniche o specialistiche necessarie a comprendere il funzionamento dei processi aziendali, ma vuole sottolineare l'importanza di integrare l'approccio tradizionale dell'audit con una attenzione rinnovata verso la strategia e le tecniche di comunicazione in tutte le direzioni. Nello specifico le competenze più ricercate sono tutte quelle afferenti all'area di "Leadership & Communications" e dell'"Environment" del Competency framework. Si ricerca la capacità di conoscenza dei processi aziendali; dei modelli di controllo, come il 231, Tax Control Framework, Privacy etc; Conoscenza dei sistemi *ERP, Enterprise Resource Planning*, aziendali; Capacità di essere un modello di comportamento e dare il buon esempio al suo gruppo di lavoro; Capacità di definire obiettivi stimolanti perseguendo alti standard di eccellenza per sé ed il proprio gruppo di lavoro; Capacità di gestire, valorizzare e/o promuovere la diversità; Capacità di motivare gli altri e utilizzare una varietà di approcci per motivare i membri del team; Capacità di interazione con il Top Management e con gli organi di controllo; Capacità di esprimere in modo chiaro e organizzato idee e pensieri, nonché di discutere eventuali finding riscontrati in fase di audit con il management auditato, provvedendo a presentare la situazione rilevata, possibili implicazioni e soluzioni concordate a riguardo; Capacità di ascolto attivo ed empatico; Capacità di gestione di situazioni e dinamiche conflittuali.

Le competenze tecniche restano comunque importanti, infatti per fronteggiare e valutare ciascun rischio è richiesta almeno una conoscenza di base delle normative, ad esempio in ambito ESG o di cybersecurity, come sarà presentato nei prossimi paragrafi.

### 3.1 Risk in Focus

Negli ultimi sette anni, Risk in Focus ha cercato di evidenziare le principali aree di rischio per aiutare gli internal auditor a preparare il loro lavoro di valutazione indipendente del rischio, la pianificazione annuale e la definizione del campo di applicazione dell'audit. Il programma aiuta i Chief Audit Executive (CAE) a capire come i loro colleghi considerano l'attuale panorama dei rischi, mentre preparano i piani di audit per l'anno successivo.

Come anticipato nel capitolo precedente, nel 2022 le organizzazioni sono state colpite da una tempesta perfetta, come riportato nella figura 3.1, che ha portato con sé rischi ad alto impatto e interconnessi, gettando le aziende in uno stato di crisi prolungato. Dopo la pandemia, la guerra in Ucraina ha intensificato i problemi della catena di approvvigionamento, ha causato un'impennata dei prezzi dell'energia e ha alimentato l'inflazione. L'azienda è costantemente esposta ad attacchi cyber, all'aumento del costo della vita e l'incalzante inflazione con i conseguenti problemi di insolvenza finanziaria.

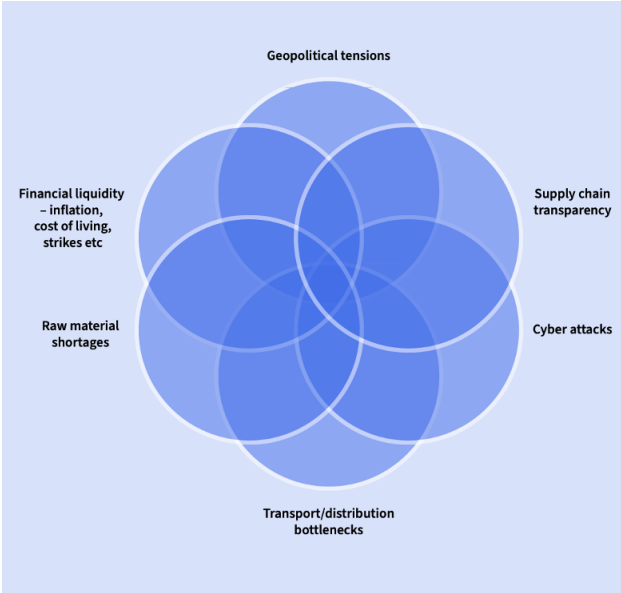


*Figura 3.1, "Venn Diagram Illustrating the Perfect Storm of High-Impact Interlocking Risks", Risk in focus 2023*

Questo ha costretto molte organizzazioni non solo a riscrivere i loro registri dei rischi, ma anche a smantellare le tassonomie dei rischi obsolete che favoriscono il vecchio stile di pensiero a blocchi. Per affrontare i rischi improvvisi e sistemici a livello di organizzazione, con ramificazioni contagiose e imprevedibili in tutta l'azienda, che non sono più visti come occasionali, ma come elementi che ormai costituiscono la realtà

aziendale, è necessario che l'analisi dei rischi e dei controlli sia prima di tutto integrata a tutti i livelli aziendali e soprattutto diventi un'attività continua. Si passa a dei sistemi *"ERP",* cioè sistemi integrati di pianificazione aziendale delle risorse, ai quali è possibile associare software per l'analisi dei dati. Viene definito un nuovo modo di fare audit, definito *Conitinuous Audit*, che permette agli IA di migliorare la qualità delle loro valutazioni grazie un approccio non più basato su revisioni di episodi con un *focus* limitato, ma incentrato su una logica più ampia e maggiormente proattiva. In questo modo diventa possibile un'allocazione delle risorse più efficiente ed un'assistenza fornita ai manager più efficace. In questa maniera, dovrebbe essere agevolata la compliance con le politiche aziendali, nonché con le procedure previste anche con le leggi ed i regolamenti vigenti, ed uno degli strumenti maggiormente diffusi, per attuare questo processo, è l'utilizzo dei *KPI*, ovvero *i Key Performance Indicator,* che stabiliscono degli obiettivi a livello aziendale legati proprio alla performance ed anche di indicatori specifici sui rischi ovvero i *KRI, Key Risk Indicator.*

Gli Internal auditors devono prendere rapidamente coscienza di questa situazione e aiutare le loro organizzazioni a navigare in tempi più rischiosi, incerti e volatili, e per far fare un passo avanti alla professione sfruttando a pieno il potenziale della situazione.

Quest'anno, Risk in Focus 2023 ha visto la collaborazione di 14 Associazioni di Internal Auditor di 15 Paesi europei, tra cui: Austria, Belgio, Bulgaria, Francia, Germania, Grecia, Italia, Lussemburgo, Paesi Bassi, Slovenia, Spagna, Svezia, Svizzera e Regno Unito e Irlanda. Questo rappresenta il numero più alto di paesi coinvolti nella storia del reporting. L'indagine ha ottenuto un numero record di 834 risposte da parte di CAE di tutta Europa e contemporaneamente, sono state organizzate quattro tavole rotonde con 39 CAE su ciascuna delle aree di rischio trattate nel rapporto.

I responsabili IA che hanno partecipato a Risk in Focus 2023 hanno evidenziato cinque rischi come prioritari: incertezza geopolitica, cambiamento climatico, cultura organizzativa, rischio informatico e dei dati, digitalizzazione e intelligenza artificiale.

È stata redatta una classifica dei rischi emergenti, come si vede dalla figura 3.2, dove sono stati evidenziati con il giallo l'incidenza dei rischi nel 2022 ed i blu l'incidenza degli stessi nel 2023. Nella figura 3.3 invece sono raffigurati i rischi dell'azienda su cui gli internal auditor concentrano la loro attività, in blu, ed invece in giallo la priorità del rischio stesso.

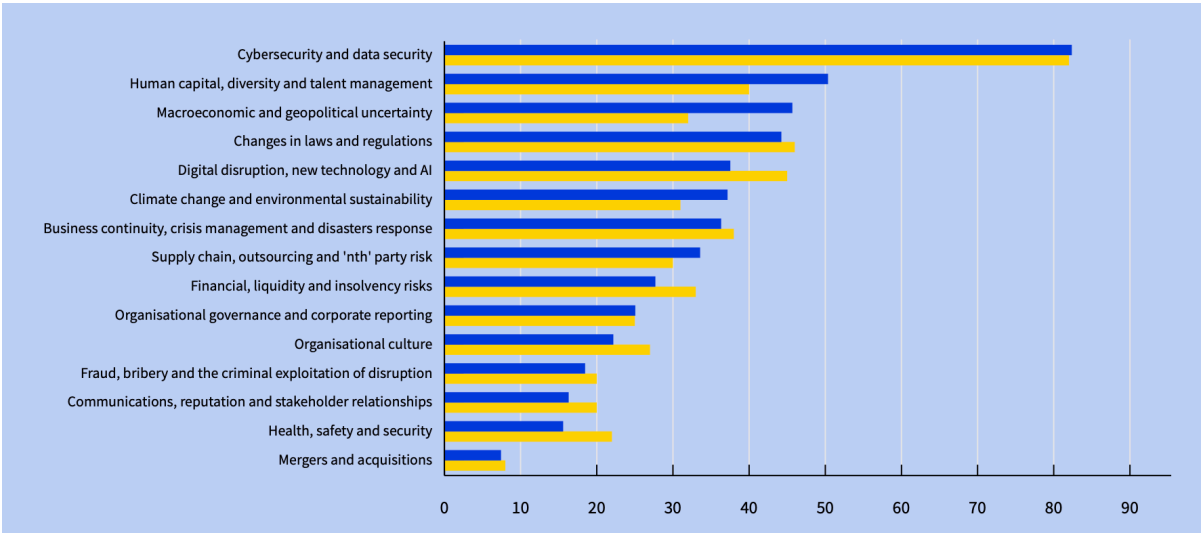


*Figura 3.2, "What are the top five risks your organization currently faces?", Risk in Focus 2023*

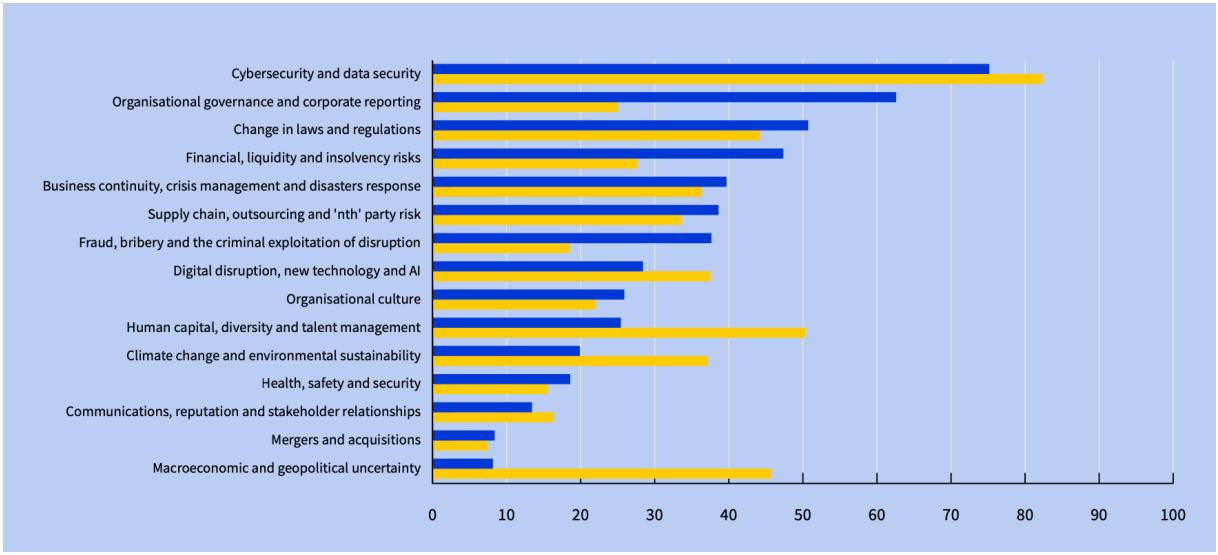


*Figura 3.3, "What are the top 5 risks on which internal audit spends most time and effort?", Risk in Focus 2023*

Dall'analisi dei due grafici è evidente come i principali rischi per la professione dell'IA, che verranno approfonditi nei prossimi paragrafi, e sui quali è necessario investire maggiormente per provare a prevenirli, sono la sicurezza dei dati e la *cybersecurity, Human capital, diversity e talent management* e diverse tematiche possono essere racchiuse nella grande tematica della *responsabilità ESG, Environmental Social Governance*, che negli ultimi anni cresce sempre di più per le imprese.

In generale come risultato di questa edizione del Risk in Focus emerge come, in primis, i board debbano concentrarsi sui rischi sistemici che creano vulnerabilità in molte parti dell'organizzazione contemporaneamente e garantire che le attività di valutazione e gestione del rischio forniscano al consiglio di amministrazione una chiara supervisione di tali rischi. Inoltre, bisogna verificare che il CdA abbia una propensione al rischio aggiornata, al fine di fornire chiarezza nel rapido processo decisionale strategico. Nello svolgere questa tipologia di valutazione dei rischi è necessario garantire che le attività di governance, gestione e controllo del rischio siano collegate e coerenti rispetto ai rischi strategici. Per questo motivo al CdA è anche chiesto di collaborare con il responsabile dell'internal audit per garantire che la funzione dedichi tutto il tempo necessario alle aree di rischio strategico e sistemico emergenti e soprattutto fornire al Chief Audit Executive il profilo, l'autorità e le risorse necessarie per supportare adeguatamente l'organizzazione nel raggiungimento dei suoi obiettivi strategici.

**3.2 Cybersecurity**

L'impatto dirompente della tecnologia e la velocità del relativo progresso, oltre che fonte indiscutibile di opportunità, espone contemporaneamente le organizzazioni a nuovi e significativi rischi, che devono essere ben compresi e gestiti con strumenti efficaci.
Pertanto, l'internal audit deve padroneggiare competenze, metodi e strumenti di lavoro diversi.
Infatti, la velocità del cambiamento tecnologico è senza dubbio una delle principali preoccupazioni delle organizzazioni. In un mondo di rivoluzione digitale, sono inevitabili nuove e diverse prospettive sul sistema dei controlli da implementare e, di conseguenza, sull'internal audit. È necessario per le imprese comprendere appieno la portata dei nuovi rischi che devono affrontare e implementare nuove, e molto spesso diverse, misure di prevenzione e controllo.
I nuovi strumenti per condurre attività analitiche sono qualcosa che l'internal audit non può permettersi di ignorare.

Gli aggiornamenti in corso sugli standard della professione mirano ad incorporare alcuni di questi cambiamenti facendo riferimento a eventuali ruoli aggiuntivi assunti dal Chief audit executive, al coordinamento con altri fornitori di servizi di assicurazione e consulenza interna e altri fornitori esterni all'organizzazione, piani di miglioramento della qualità e comunicazione e riferire al Consiglio di Amministrazione e all'Alta Direzione.
Ogni progresso tecnologico comporta un miglioramento degli strumenti attuali e la nascita di nuove applicazioni e di nuove competenze, allo stesso modo l'evoluzione tecnologica non è sfruttata solo a livello

aziendale, ma espone maggiormente le aziende stesse ad attacchi informatici che potrebbero compromettere l'intera attività produttiva.

Negli ultimi anni le minacce informatiche hanno assunto un ruolo di primo piano dovuto, oltre che al progresso tecnologico, ad un mix di eventi che comprendono la crisi ucraina, le persistenti minacce COVID-19 e le crescenti tensioni tra Stati Uniti e Cina. Insieme. Ad oggi, per queste variabili e altre ancora, la cybersecurity ha posto significativo tra i rischi della professione, come evidenziato dalla figura 3.2, è al primo posto nelle mappe dei rischi degli internal auditor.

L'importanza di questo rischio è legata al fatto che l'internal audit ha un ruolo fondamentale nell'aiutare le organizzazioni a gestire le minacce informatiche, sia fornendo una valutazione indipendente dei controlli esistenti e necessari, sia aiutando il comitato di audit e il consiglio di amministrazione a comprendere e affrontare i diversi rischi del mondo digitale. Nell'esercitare un ruolo di tale importanza è necessario per l'IA, come precedentemente anticipato, aggiornare le proprie competenze, ma necessariamente rappresentato in materia di cybersecurity, ma dalle conoscenze in materia di identificazione del rischio, la comunicazione del rischio e la valutazione dei controlli per affrontare il rischio. A titolo esemplificativo e a maggior chiarimento, nel successivo paragrafo si riportano i contenuti dell'intervento della SEC negli Stati Uniti, nell'ambito delle società quotate.

### 3.2.1 Come le aziende possono affrontare il tema della Cybersecurity: l'esempio dell'intervento della SEC

Secondo gli intervistati del rapporto *"North American Pulse of Internal Audit 2022"* dell'IIA, che andando oltre il benchmarking offre approfondimenti su come i CAE gestiscono le loro funzioni, la cybersecurity rappresenta in media solo il 9% dell'allocazione del piano di audit nelle organizzazioni quotate in borsa, un dato in crescita rispetto al 7% dei tre anni precedenti, ma di gran lunga inferiore al 35% allocato per il reporting finanziario. Le ragioni sono molteplici: limitazioni di budget, mancanza di risorse sufficienti, mancanza di conoscenze o di esperienza.

Il vero valore che l'internal audit può fornire, tuttavia come anticipato precedentemente, non è necessariamente la conoscenza della cybersecurity, ma la conoscenza dell'identificazione del rischio, della comunicazione del rischio e della valutazione dei controlli per affrontare il rischio.

Quello che la *Securities and Exchange Commission (SEC)* si propone di raggiungere è che le organizzazioni valutino i loro rischi di cybersecurity, che i consigli di amministrazione delle organizzazioni dispongano di strutture di governance in grado di valutare e garantire la supervisione del programma di gestione del rischio

di cybersecurity. Per questo motivo ha portato due proposte che, se integraste nei normali processi di assessment, potrebbero portare ad avere una copertura maggiore del rischio di cybersecurity.

La prima proposta si concentra sui consulenti d'investimento registrati, sulle società d'investimento registrate e sulle società o fondi di sviluppo aziendale. In base alle norme proposte, i consulenti e i fondi sarebbero tenuti ad adottare ed implementare politiche e procedure scritte di cybersecurity, successivamente segnalare alla SEC, tramite un modulo riservato, gli incidenti significativi di cybersecurity che interessano il consulente o i suoi clienti di fondi o fondi privati stessi. Inoltre, la proposta prevede di divulgare pubblicamente i rischi di cybersecurity e gli incidenti significativi di cybersecurity verificatisi negli ultimi due anni fiscali nelle brochure e nelle dichiarazioni di registrazione.

La seconda proposta, invece, consiste nel segnalare gli incidenti di cybersecurity, ed è diretta a tutte le società quotate in borsa. L'obiettivo è, come dichiarato dalla SEC, quello di *"Migliorare e standardizzare le informazioni relative a gestione del rischio di cybersecurity, la strategia, la governance e la segnalazione di incidenti di cybersecurity da parte delle società pubbliche soggette agli obblighi di rendicontazione della Securities and Exchange Commission, soggette ai requisiti di reporting del Securities Exchange Act del 1934"*.

Le nuove regole richiedono alle società pubbliche di fornire informazioni relative alle politiche ed alle procedure della società per identificare e gestire i rischi di cybersecurity, incluso il caso in cui ci si avvalga della consulenza di soggetti terzi e tutti gli storici delle azioni svolte per prevenire e per mitigare incidenti legati alla cybersecurity. Inoltre, per la proposta il management deve essere in grado di implementare le politiche e le procedure di cybersecurity, e soprattutto constatare la competenza del consiglio di amministrazione sul tema ed il ruolo che effettivamente esercita nella supervisione di tali rischi.

La proposta include poi una modifica al *Modulo 8-K*, cioè un rapporto di eventi materiali non programmati o cambiamenti aziendali in una società che potrebbero essere importanti per gli azionisti o per la Securities and Exchange Commission, che richiede alle società pubbliche di divulgare incidenti di cybersecurity entro quattro giorni lavorativi, così come sono già tenute a fare per qualsiasi altro evento materiale non programmato.

Sebbene non si tratti di una sfida da prendere alla leggera, l'internal audit fortunatamente conosce gli strumenti e le competenze necessarie per fornire garanzie su quest'area di rischio in continua evoluzione. L'IA, grazie alla sua posizione unica nell'organizzazione, deve essere incluso quando si tratta di piani di risposta agli incidenti informatici di un'organizzazione.

Per un migliore e più efficiente piano di prevenzione dei rischi di attacchi informatici risulta necessaria una sana relazione tra l'internal audit e la funzione IT. Questa unione offre inoltre molteplici vantaggi

all'organizzazione, in primo luogo nell'allineamento e nella comprensione del profilo di rischio informatico dell'organizzazione, nella presenza sia di vulnerabilità che di opportunità, e nella comprensione del livello di maturità del sistema e dello stato dei test di penetrazione.

Aiuta a fornire una comunicazione coerente e unificata alla C-suite e al consiglio di amministrazione sui rischi, le esigenze, le priorità e lo stato di salute della cybersecurity. L'indipendenza dell'internal auditor può essere tutelata con successo, se non addirittura rafforzata, quando entrambe le parti sviluppano una comprensione e un apprezzamento più profondi dei ruoli, degli approcci e dei compiti.

Un altro vantaggio intrinseco della partnership è il modo in cui entrambi i team tendono ad evolversi ed a crescere nella comprensione e nell'apprezzamento dei rispettivi approcci per raggiungere lo stesso obiettivo: mantenere l'organizzazione sicura dal punto di vista informatico. Un processo articolato in questo modo fa si che la funzione di internal audit debba essere costantemente vigile, agile, reattiva e pertinente, e che per fronteggiare al meglio ogni tipo di minaccia debba essere in grado di sviluppare competenze che vadano oltre quelle generalmente richieste, sempre più specifiche per ogni tipologia di rischio.

### 3.2.2 Una proposta di risk assessment

Uno studio di Deloitte, *"Cybersecurity and the role of internal audit An urgent call to action "*, afferma che la minaccia di attacchi cyber è significativa e in continua evoluzione. Molti comitati di revisione e consigli di amministrazione si aspettano che l'audit interno comprenda e valuti le capacità dell'organizzazione di gestire i rischi associati.

Attualmente da un'analisi condotta da Pwc, che ha portato alla pubblicazione dell'articolo chiamato *"Internal Auditing: evoluzione della professione tra obblighi di disclosure e nuovi scenari di rischio",* ha evidenziato che risultano *"Evolver",* cioè avanguardisti rispetto l'utilizzo della tecnologia solamente il 14% dei responsabili della funzione di Internal audit, mentre la maggioranza, cioè il 46%, è definito *"Follower",* poiché comprendono la strategia degli evolver ma hanno dei tassi di azione più lenti. La restante parte è definita *"Observer"*, i quali usano la tecnologia in modo molto limitato e comunque abbastanza basilare.

Le componenti di conoscenza e talento associate all'adozione di strumenti *analytics* sono ora identificate come barriere per molti; infatti, il 44% di coloro che ritengono necessaria la conoscenza delle nuove tecnologie vede le attività di analisi dei dati come le competenze tecniche che richiederanno il maggiore investimento per soddisfare le future esigenze.

Un primo passo efficace per l'IA è quello di condurre una valutazione del rischio informatico e distillare i risultati in una sintesi concisa per il comitato di revisione e il consiglio di amministrazione, che poi guiderà un piano pluriennale di audit sulla cybersecurity, basato proprio sul rischio.

Le unità aziendali e la funzione informatica (IT) integrano la gestione del rischio informatico nel processo decisionale e nelle operazioni quotidiane e costituiscono la prima linea di difesa di un'organizzazione. La seconda linea comprende i leader della gestione del rischio informatico e tecnologico che stabiliscono la governance e la supervisione, monitorano le operazioni di sicurezza e intervengono se necessario.

Sempre più spesso, molte aziende riconoscono la necessità di una terza linea di difesa informatica: la revisione indipendente delle misure di sicurezza e delle prestazioni da parte della funzione di Internal audit. L'IA dovrebbe svolgere un ruolo fondamentale nella valutazione e nell'identificazione delle opportunità di rafforzamento della sicurezza aziendale. Allo stesso tempo però l'auditor ha il dovere di informare il comitato di revisione e il consiglio di amministrazione sull'esistenza e sul corretto funzionamento dei controlli di cui è responsabile, una preoccupazione crescente in tutti i consigli di amministrazione che devono affrontare potenziali responsabilità legali e finanziarie.

È stato progettato un processo di risk assessment che il responsabile internal audit dovrebbe seguire per fornire all'azienda un nuovo livello di protezione dai rischi di cybersecurity. Questo processo viene avviato per cercare di adeguare il proprio sistema di controlli su uno dei tre livelli proposti dalla società di consulenza.

I livelli si articolano in:

- *Secure:* La maggior parte delle organizzazioni stabilisce controlli come le difese perimetrali, la gestione delle identità e la protezione dei dati per proteggersi dalle minacce note ed emergenti. I programmi incentrati sul rischio danno priorità ai controlli nelle aree che si allineano ai principali rischi aziendali;
- *Vigilant*: Le informazioni sulle minacce, il monitoraggio della sicurezza e le analisi comportamentali e dei rischi vengono utilizzati per rilevare attività dannose o non autorizzate, come modifiche alla configurazione delle applicazioni o movimenti di dati insoliti, e per aiutare l'organizzazione a rispondere al panorama mutevole delle minacce;
- *Resilient*: I protocolli di risposta agli incidenti, le analisi forensi e i piani di continuità operativa e di *disaster recovery* vengono messi in atto per recuperare il più rapidamente possibile e ridurre l'impatto.

Per adeguarsi ad un determinato livello ed avviare applicare correttamente un processo di risk assessment, sono diversi i fattori che i professionisti dell'internal audit devono considerare per arrivare ad una valutazione

corretta della cybersecurity. Prima di tutto è necessario coinvolgere persone con l'esperienza e le competenze necessarie ed adeguate; è fondamentale coinvolgere professionisti dell'audit con un adeguato livello di competenze tecniche e di conoscenza dell'ambiente di rischio attuale. Un professionista dell'IA orientato alla tecnologia e con una buona conoscenza del mondo informatico può essere una risorsa indispensabile. Successivamente è necessario valutare l'intero quadro di cybersecurity, piuttosto che selezionare solo alcuni elementi. Questa valutazione implica la comprensione dello stato attuale rispetto alla direzione che l'organizzazione sta prendendo e delle pratiche minime di cybersecurity attese nell'industria o nel settore di attività. Inoltre, la valutazione iniziale deve essere alla base di ulteriori esami più approfonditi, quindi un punto di partenza e non un punto di arrivo per contrastare tale rischio. Non si tratta di un'analisi esaustiva che richiede test approfonditi, ma piuttosto, la valutazione iniziale dovrebbe guidare ulteriori verifiche approfondite della cybersecurity basate sui rischi.

Oltre l'assessment può essere svolto, insieme o in alternativa, anche una maturity analysis che serve per fornire valore aggiuntivo al management consentendo allo stesso di avere una visuale veloce delle aree in cui è necessario agire. L'analisi si sviluppa in cinque stage:

- Il primo è quello *iniziale* nel quale viene riconosciuto il problema e viene fatta una casistica in base alla specificità dell'evento. C'è una prima definizione degli obiettivi ma non è previsto nessun training, nessuna forma di comunicazione o di standardizzazione;
- Lo stage successivo è quello della *gestione* in cui il processo viene preso in analisi, le responsabilità sono definite insieme alle procedure con le rispettive deviazioni. Viene progettato anche un primo processo di review;
- Il terzo stage è quello della *definizione*, in cui il processo prende vita e le procedure vengono comunicate. Iniziano dei processi di integrazione con le altre funzioni aziendali ed anche attività di raccolta dei dati delle prestazioni. In questa fase c'è già un controllo da parte della funzione compliance;
- Nel quarto stage, quello definito *Predittivo,* vengono definite delle soglie quantitative di prestazione ed anche dei limiti di controllo. È promosso il costante miglioramento ed implementazione del sistema, che allo stesso modo inizia ad automatizzarsi. Iniziano ad essere gestiti gli obiettivi a livello di business;
- Nell'ultimo stage, quello *dell'ottimizzazione*, c'è un continuo miglioramento non solo dei sistemi di controllo e dei processi ma anche degli obiettivi definiti. Si raggiunge un'integrazione ed una cooperazione continua tra la funzione IT e la funzione di internal audit. Da questa collaborazione risulta

più facile implementare tutto il processo di gestione dei rischi cyber e di poterlo aggiornare con le nuove ed emergenti tecnologie.

### 3.3 Human capital, diversity and talent management

Al secondo posto dei rischi che attualmente un'internal auditor si trova a dover fronteggiare, con una crescita esponenziale ogni anno che passa, c'è il tema dell'Human capital, diversity e talent management. Il principale motivo, come anticipato nel precedente capitolo, è la tempesta perfetta nella quale si sono ritrovate le aziende a dover svolgere la propria attività, che nasce da diversi fattori come l'esplosione della pandemia da COVID-19, la guerra in Ucraina, e non ultima, l'entrata nel mondo del lavoro della Generazione Z con la creazione di nuove esigenze lavorative. Nello specifico le nuove generazioni richiedono salari più elevati, con condizioni lavorative migliori, in termini di orari di lavoro, di attenzione rivolte alla crescita all'interno dell'azienda che accresce il senso di appartenenza verso la stessa e spinge i giovani a restare nell'ambiente in cui si trovano. Non indifferente è il ruolo dello smart working, che ha rivoluzionato il modo di svolgere qualsiasi tipo di attività, riuscendo a ridurre distanze territoriali e temporali, consentendo a tutti di essere connessi anche se da remoto.

Il risk in Focus ha prodotto dei dati che hanno evidenziato il tema del capitale umano ancora più sensibile di quanto lo si possa immaginare. Tra questi i più significativi sono:

- I datori di lavoro immaginano di dovere riqualificare il 70% dei propri dipendenti entro il 2025, mentre solo il 42% degli impiegati sta cogliendo le opportunità ed il supporto offerto dai superiori;
- Il 50% delle organizzazioni si aspetta di trasformare il proprio processo produttivo nei prossimi tre anni;
- Il 38% dei datori di lavoro afferma che la carenza di personale è una preoccupazione, e gli investimenti in tecnologia potrebbero aiutare ad affrontare le sfide di reclutamento che il 61% dei datori di lavoro ha dichiarato di star vivendo;
- Il 50% dei lavoratori si sta interfacciando con problemi di work-life balance mentre il 45% ha problemi familiari come la gestione dei figli;
- Il 64% dei lavoratori vogliono supporto da parte dei datori di lavori dal punto di vista finanziario, delle condizioni di vita e dell'assistenza sanitaria.

Le aziende che si aspettano che le cose tornino come prima, potrebbero perdere delle opportunità o, peggio, non riconoscere le sfide ai loro modelli di business. Gli internal audit sono nella posizione ideale per aiutare

l'azienda a distinguere tra quelle che possono essere solo tendenze cicliche e i cambiamenti più profondi e permanenti che stanno avvenendo.

### 3.3.1 Il ruolo dell'internal audit

Mentre la gestione del capitale umano, della diversità e dei talenti si è classificata al secondo posto sia nella categoria dei rischi attuali che in quella dei rischi futuri nell'indagine Risk in Focus 2023, l'argomento ha ottenuto rispettivamente solo il decimo e l'ottavo posto in termini di tempo dedicato dagli IA alla questione. In effetti, una recente ricerca della *Chartered IIA UK and Ireland* ha dimostrato che solo il 37% degli internal auditor ha integrato il tema della cultura nei propri audit standard, mentre oltre la metà ha dichiarato di non essere stata invitata dal consiglio di amministrazione o *dall'audit committee* a produrre relazioni sull'argomento, il che suggerisce che molti non prendono sul serio la questione.

Storicamente, gli internal audit fanno verifiche soprattutto su controlli procedurali di processi quasi sempre standardizzati, invece di recente l'attenzione si è concentrata maggiormente sui controlli morbidi e più specifici. Per quanto riguarda questioni come la gestione del capitale umano, è più difficile definire i controlli perché, anche laddove esistono, questi riguardano fattori non facilmente monitorabili, essendo un'attività principalmente volta a valutare le competenze adeguate a gestire il nuovo contesto digitale e l'istituzione di processi e percorsi finalizzati alla valorizzazione dei talenti.

Gli internal auditor devono quindi lavorare per definire dei controlli sul capitale umano che però siano allineati agli obiettivi strategici dell'organizzazione. Ad esempio, una ricerca condotta dagli studiosi di Google ha rilevato che la *sicurezza psicologica*, cioè la capacità di creare un ambiente in cui le persone si sentono libere di esprime senza aver paura di sbagliare, è diventato un elemento chiave per l'efficacia dei team e influisce sulla durata della permanenza del personale in azienda. I responsabili IA devono comprendere appieno quali sono i fattori che influenzano la creazione e lo sviluppo di team di successo e assicurarsi che tali questioni siano portate all'attenzione del comitato di audit o del consiglio di amministrazione per un intervento.

Concretamente un internal audit può aiutare l'organizzazione in diverse fasi. Prima di tutto deve valutare fino a che punto le strategie dell'organizzazione, in materia di risorse umane, sono allineate con la sua vision e mission. È necessario poi capire come, in questo contesto storico di scarsità e di assenza di risorse umane competenti, attrarre e trattenere i dipendenti all'interno dell'organizzazione. Bisogna valutare in che misura tali strategie vengono attuate ai diversi livelli aziendali e se le stesse vengono discusse periodicamente, anche nelle riunioni del consiglio di amministrazione. L'IA deve assicurarsi lo scopo sociale dell'azienda e la sua cultura organizzativa siano almeno in parte incorporati nei processi di acquisizione e gestione dei talenti. Inoltre, è da

tenere in considerazione che il mondo del lavoro è in continua evoluzione per questo motivo occorre essere rapidi ed efficaci a adattare le infrastrutture tecnologiche e fisiche ai cambiamenti emergenti.

L'internal audit deve constatare che nell'applicazione delle politiche e procedure occupazionali, l'organizzazione raggiunga un giusto equilibrio tra le esigenze potenzialmente mutevoli dei dipendenti e la cultura organizzativa preferita.

Un primo passo che l'IA può compiere può è la esaminazione delle norme culturali esistenti e l'utilizzo dei risultati come catalizzatore per definire la cultura attuale dell'azienda e sviluppare una roadmap per il cambiamento. La ricerca di opinioni esterne all'azienda è fondamentale. I clienti e gli stakeholder, come i fornitori e gli appaltatori, spesso hanno una chiara visione della cultura prevalente grazie alla continua interazione con il personale. Quando i feedback sono positivi, quindi le terze parti si sentono apprezzate e rispettate e non ritengono di subire comportamenti ingiusti o dittatoriali, è un segnale indicativo che la cultura si sta muovendo nella giusta direzione.

La roadmap deve anche mostrare come i comportamenti culturali desiderati sono incorporati nei processi dell'organizzazione e sono allineati a ruoli e responsabilità chiari. Resta fondamentale il coinvolgimento dei vertici aziendali per promuovere la cultura e far si che ogni processo ne sia pregnante.

Un insieme ben compreso di attributi comportamentali desiderati può essere incluso nei programmi di formazione e gestione dei talenti, nelle procedure di selezione e di inserimento dei dipendenti, nelle descrizioni delle mansioni e persino durante i colloqui di uscita per assicurarsi che i problemi siano identificati in aree specifiche dell'azienda.

### 3.3.2 Un sistema di applicazione per ridurre il rischio

Lo studio di settore condotto dal *Word Economic Forum*, presentato nell'insight *Future of Jobs Report*, evidenzia come circa il 30% della forza lavoro attuale deve cambiare le proprie competenze in virtù del fatto che le organizzazioni evolvono, unitamente ai propri modelli di business, per adeguarsi agli innumerevoli avvenimenti del contesto in cui sono immerse, ovvero, come citato precedentemente, un contesto in cui è esplosa una tempesta perfetta.

Unica certezza di questo cambiamento è che le persone saranno sempre di più attori protagonisti del proprio sviluppo e della propria crescita. Quindi risulta necessario fornire alle persone le risorse per poter gestire il loro sviluppo all'interno di un'organizzazione, con strumenti adatti a garantire alle persone di poter dichiarare

le proprie ambizioni e portele sviluppare e dall'altro canto permettere all'organizzazione di intercettare questi talenti e combaciarli con le proprie necessità.

Per poter aiutare le persone a riconoscere il proprio potenziale, una società multinazionale nel settore farmaceutico ("La multinazionale") ha creato un meccanismo per il quale viene chiesto alle persone, secondo un processo di people development, di pensare alle proprie abilità e competenze e poi successivamente di poterne discutere con il proprio manager, in un processo di performance management, per poter impostare un possibile iter di formazione che viene poi seguito da un leadership team con la creazione di veri e propri percorsi di carriera.

Riuscire a portare le persone a capire che cosa vogliono fare e come vogliono crescere è un processo molto difficile, per questo motivo sono state create delle serie di domande, che crescono in complessità, che dovrebbero aiutare il singolo ad arrivare ad una visione potenziale di sé stesso.

Questo è un processo che viene applicato a tutti i livelli dell'organizzazione, per questo motivo anche l'internal audit deve adeguarsi e sviluppare le competenze necessarie per far si che questo processo, applicato alla gestione del capitale umano della propria funzione, porti dei risultati.

Bisogna individuare il proprio ruolo con i propri punti di forza, cosa bisogna sviluppare e soprattutto quali sono gli interessi ed i valori che non si è disposti a rinunciare, o che si vuole accrescere. Successivamente è necessario contestualizzare questo aspetto personale nel contesto aziendale, quindi cosa bisogna cambiare, cosa ci si aspetta e cosa bisogna fare per raggiungere l'obiettivo prefissato, focalizzando la direzione in cui si vuole crescere e quali sono i passi da compiere per raggiungerla.

La multinazionale ha creato un piano che è articolato in tre passaggi principali: *La fissazione dei "Goal"; L'ottenimento delle risorse; La misurazione dei risultati.*

Nella fase iniziale bisogna coinvolgere i singoli per definire gli obiettivi di crescita, combinando talento e potenziale. Il Talento è l'abilità che una persona possiede dalla nascita ed è un'attività che risulta molto semplice alla persona da mettere in pratica, molto spesso non si è neanche molto consapevoli del proprio talento, ma è una variabile osservabile. Il potenziale invece è una promessa futura, qualcosa che ancora non si può vedere. Per questo motivo rispetto al concetto di prestazione è più difficile da riconoscere ed alimentare. Dopo aver individuato gli obiettivi personali è necessario valutare anche l'impatto degli stessi sul business, sulla performance e sulla carriera, e definire i KPI (Key Performance Indicator) per misurare l'apprendimento.

La seconda fase definisce il piano di sviluppo, ricercando le risorse adatte per promuoverlo eseguendo un approccio 70-20-10 per creare un piano individuale di apprendimento. *L'approccio 70-20-10* nasce dalla consapevolezza che seguire unicamente corsi di formazione teorici non sia abbastanza formativo; infatti, secondo questa metodologia soltanto il 10% del piano di apprendimento dovrebbe essere basato sul "Formal learning", cioè e-learning, self Study e classi di training o seminari. Invece il 70% del piano dovrebbe essere basato sull'esperienza, con il metodo del "*Learning by doing*", cambiando completamente il modo di lavorare oppure esercitandosi su un nuovo ruolo. Il restante 20% dovrebbe poi essere riservato ad attività di tipo relazionale, *"Learning from others",* cioè un apprendimento correlato a dei "role models" dai quali apprendere, seguendoli ed accompagnandoli nell'esercizio di determinate attività.

L'ultima fase, che in realtà è svolta in maniera continuativa durante tutto il percorso di apprendimento, è la fase di misurazione. Attraverso i KPI, definiti all'inizio del percorso, si misura l'avanzamento del piano e si apportano delle modifiche nel caso in cui sia necessario. Nel caso in cui gli obiettivi personali cambino, oppure debbano essere implementati, queta fase comprendere la possibilità di sostituire i KPI e consolidare nuove skills.

Le principali competenze da dover apprendere per poter svolgere correttamente questo processo sono la comunicazione e la leadership, soprattutto nella fase di *"Learning from others*", ma anche nella fase del "*Learning by doing*" per poterle poi trasferire ad un'altra persona; la capacità di guidare un team e coordinarlo ed infine la capacità di avere un pensiero strategico capace di influenzare le decisioni di business.

### 3.4 Environmental, Social, Governance

Negli ultimi anni un'azienda per definirsi sostenibile deve essere qualificata da fattori sia di tipo ambientale, che sociale e di governo societario. Dal punto di vista ambientale è necessario che l'azienda sviluppi processi con minor spreco di energia e minor impatto ambientale, ponga attenzione al cambiamento climatico ed al rispetto delle biodiversità; i fattori sociali che influenzano la sostenibilità dell'impresa sono le relazioni lavorative, il tema della diversity and inclusion, il rispetto dei diritti umani ed il progressivo miglioramento del benessere della collettività, intesa come l'ecosistema aziendale ed ogni soggetto esterno che ha dei rapporti con la stessa; infine l'aspetto legato al governo societario riguarda il rispetto di politiche di diversità nella composizione degli organi di amministrazione delle imprese, la presenza di consiglieri indipendenti, la remunerazione dei dirigenti, lotta alla corruzione attiva e passiva, relazioni con i fornitori e partner commerciali, ma più in generale tutti i temi legati agli elementi che hanno un ruolo importante nell'assicurare che i fattori precedentemente elencati, sociali ed ambientali, vengano considerati nelle decisioni aziendali.

I programmi e le iniziative ESG messi in atto dalle organizzazioni sono partiti da semplici attività filantropiche e di volontariato dei dipendenti, fino ad oggi ad arrivare ad un'integrazione a tutti i livelli aziendali. Questo cambiamento è dovuto ad un maggiore riconoscimento dei rischi collegati alla responsabilità ESG insieme ad un forte incentivo normativo di leggi e regolamenti.
Nel 2016 per la prima volta il *d.lgs. 254/2016* introduce l'obbligo per gli enti di caricare informazioni di tipo non finanziario per giungere poi al 2021 in cui è stata emanata la prima *"Legge europea sul clima"*. Nello stesso anno entra in vigore il SFDR, cioè il "*Sustainable Finance Disclosure Regulation"*, che oltre ad imporre norme comuni a diverse categorie di operatori finanziari sulla divulgazione di informazioni sui temi di sostenibilità, contiene una definizione di "investimento sostenibile", che è presentato come un'attività economica che contribuisce a un obiettivo ambientale.
È stata pubblicata sulla Gazzetta Ufficiale dell'UE una nuova direttiva 2022/2464 sulla rendicontazione societaria di sostenibilità, la *CSRD*, *Corporate Sustainability Reporting Directive,* che fa riferimento a delle misure volte a migliorare il reporting di sostenibilità per convergere verso un sistema economico e finanziario pienamente sostenibile ed inclusivo.

Attualmente le aziende stanno affrontando numerose tematiche ESG in tutte le funzioni e nei rapporti con i principali stakeholder. Bisogna valutare fattori ESG in diversi processi:

- *Supply chain e fornitori*: Bisogna gestire i rapporti con i fornitori assicurandosi che siano rispettatati sia i diritti umani che le biodiversità, e che il fornitore stesso applichi delle strategie che siano attente agli impatti ambientali;
- *Comunità sociali*: È necessario che sia rispettata sia giustizia sociale che ambientale, le due devono coesistere perché le misure per il contrasto della crisi climatica, per la transizione ecologica e la sostenibilità ambientale, per la trasformazione energetica devono favorire, anche nel breve termine, le fasce più deboli e vulnerabili della popolazione;
- *Gestione della produzione*: I processi di produzione devono essere in grado di garantire un moderato impatto ambientale, sia dal punto di vista del packaging che dal punto di vista dell'energia consumata e delle emissioni. Bisogna valutare i cambiamenti climatici ed agire di conseguenza adattando i propri sistemi di produzione;
- *Clienti e consumatori*: L'azienda deve assicurare la sicurezza e la qualità dei prodotti e soprattutto la sostenibilità del prodotto, in quanto questo è un requisito richiesto dal 54% dei consumatori, affermato dall'analisi del 2022 di *Edelman Trust Barometer*, come necessario per prendere una decisione d'acquisto. Post-vendita è necessario poi garantire privacy e sicurezza dei dati acquisiti dal cliente;

- *Risorse umane*: Per le risorse umane il tema ESG è affrontato in diversi ambiti, principalmente però è necessario garantire una strategia adeguata di DEI, cioè Diversity, equity and inclusion, a tal punto che è stata creata un'apposita diramazione delle risorse umane che si occupa solo di gestire queste tematiche. Inoltre, spetta al reparto di H&R la valutazione dei sistemi di salute e sicurezza sul lavoro;

Dalla survey del 2022 di *Edelman Data & Intelligence (DxI)*, nella sua 22° edizione, il sondaggio sulla fiducia e credibilità, ha intervistato ben 36.000 persone provenienti da 28 paesi diversi, se sono emersi diversi dati relativi al tema dell'ESG.
In particolare, il 70% dei dipendenti ritiene importante per valutare la necessità di cambiare impiego, la posizione della propria azienda sulle problematiche sociali. Inoltre, ormai l'84% degli investitori istituzionali afferma che sono sottoposte sotto lo stesso scrutinio sia le telematiche ESG affrontate dalle aziende che le considerazioni di carattere finanziario e produttivo.

Le aziende che affrontano le tematiche ESG in modo responsabile – e le integrano all'interno della propria strategia e governance – possono creare e sostenere il proprio valore economico nel tempo, per tutti gli stakeholder.
Attualmente questa è una sfida che coinvolge anche la funzione internal audit, che oltre aiutare il management a definire strategie e obiettivi, deve contribuire alla sensibilizzazione e al sostegno significativo delle iniziative ambientali. Bisogna coinvolgere tutte le persone presenti in azienda e fissare obiettivi, sia dal basso che dall'alto dell'azienda, per creare un processo completo che sia guidato da persone che vogliono che il cambiamento avvenga.
Per fare questo l'internal audit si trova ancora a dover aggiornare le proprie competenze, ed in questo caso oltre alle soft skills già citate nei precedenti paragrafi, l'auditor deve essere aggiornato sulle nuove normative, deve portare innovazione creando nuovi modelli di analisi, gestione e monitoraggio del rischio.

### 3.4.1 Climate change and environmental sustainability

Con le temperature che hanno raggiunto livelli insolitamente alti in tutta Europa e i fenomeni atmosferici più gravi che sono diventanti sempre più frequenti anche in aree geografiche tradizionalmente meno esposte, tra i principali rischi, come evidenzia la figura 3.2, c'è il "Climate change and enviromental sustainability".
Sebbene gli internal audit stiano destinando maggiori risorse agli incarichi relativi al cambiamento climatico, non gli attribuiscono ancora la priorità che merita, oggi il tema si colloca solo all'undicesimo posto tra le aree in cui gli IA, figura 3.3, dichiarano di impiegare il loro tempo e i loro sforzi, tuttavia, se gli internal audit non

affrontano subito la questione, il rischio potrebbe diventare la prossima grande crisi per cui le organizzazioni saranno impreparate.

Il documento *dell'IIA Olanda*, *"Cambiamento climatico e rischio ambientale"*, consiglia di concentrare gli sforzi della funzione di IA sulla garanzia del reporting, sulla gestione del rischio degli obiettivi di sostenibilità e sulla consulenza in materia di clima, se necessaria. Inoltre, lo studio separato dell'IIA Olanda, ha rilevato che le misure adottate per affrontare il rischio di cambiamento climatico vanno dall'inclusione dell'argomento nel registro dei rischi per il 47%, all'utilizzo di KPI al 41%, ma nessuna delle iniziative è stata utilizzata da oltre la metà delle organizzazioni intervistate. Il passaggio ad un approccio più regolamentato, di conseguenza più pratico, ha sollevato delle questioni spinose, andando a dimostrare che un modello di governance di un'organizzazione possa funzionare efficacemente per integrare gli obiettivi di sostenibilità senza essere relegato a un esercizio di spunta sui requisiti normativi.
Gli internal auditor devono assicurarsi che gli sforzi di conformità di base della loro organizzazione non replichino i peggiori eccessi della cultura creata dalla legge *Sarbanes-Oxley del 2002* sui controlli relativi all'informativa finanziaria, la quale spinse molti IA a svolgere attività di conformità di basso livello, a discapito della possibilità di fornire servizi a maggior valore aggiunto, con aziende brave a comunicare il rischio di informativa finanziaria ma scarse nell'applicare azione preventive, ma soprattutto concrete.
Visti i precedenti, il Risk in Focus 2023 evidenzia come il rischio di *green-washing*, cioè un ecologismo di facciata, è in parte il risultato di un livello relativamente basso di maturità degli standard di rendicontazione finanziaria attualmente disponibili ed ancora in fase di sviluppo.

La *Conference of the Parties, COP 26,* ha stabilito nuovi obiettivi climatici che le organizzazioni potrebbero faticare a raggiungere. Tra gli obiettivi principali c'è quello di garantire le emissioni globali nette ad un livello molto contenuto entro il 2030, arrivando ad emissioni nette zero entro il 2050, per contenere il riscaldamento globale.
Il mondo ha bisogno di soluzioni energetiche più numerose e più pulite per alimentare il progresso, e questo richiede un apprendimento rapido, un processo decisionale complesso e una gestione efficace dei rischi.
Poiché le organizzazioni si trovano a diversi livelli di maturità nel loro percorso verso la sostenibilità ambientale, il ruolo dell'IA può essere difficile da definire con certezza.
I responsabili internal audit che hanno partecipato alla conferenza per la redazione del Risk in Focus 2023, hanno concordato sul fatto che, oltre ad aiutare il management a definire strategie e obiettivi, gli IA devono essere i primi a contribuire alla sensibilizzazione e a raccogliere un sostegno significativo per le iniziative ambientali, è necessario coinvolgere quante più persone possibili e fissare gli obiettivi sia dal basso che dall'alto dell'azienda per creare un processo completo a tutti i livelli.

È necessario assicurarsi che i membri del team più impegnati a contribuire ad affrontare le questioni relative al cambiamento climatico, siano responsabili di ruoli chiave negli incarichi relativi a questo tema. Proprio per questo motivo, per coloro che hanno avviato un'attività di audit ambientale, una delle maggiori sfide è stata quella di aggiornare i propri team. Questa è una difficoltà per tutti i dipartimenti, data la difficoltà di attrarre e trattenere personale di alta qualità nell'ambito dell'internal audit. Il complesso panorama normativo globale e la sua potenziale importanza per l'azienda può essere un'impresa ardua e molte imprese si rivolgono a società di revisione esterne e a consulenti globali. Un'ulteriore capacità è quella di coinvolgere ingegneri, scienziati e altri esperti per contribuire alla creazione di competenze specifiche.

I modi concreti in cui il team di internal audit può aiutare la propria organizzazione sono diversi, ma altrettanto dipendono dal livello di importanza data proprio alla funziona all'interno dell'azienda. Il Chief Audit Executive deve essere in grado di parlare con l'amministratore delegato, con il comitato di revisione, di mettere le cose all'ordine del giorno e di assicurarsi che la voce dell'audit sia effettivamente ascoltata, ma al di fuori delle grandi industrie multinazionali, i responsabili dell'internal audit non godono sempre di questo status.

In un contesto in cui però questo status sussiste, come emerge dal Risk in Focus 2023, il responsabile IA dovrebbe:

- Parlare con l'amministratore delegato o il consiglio di amministrazione per aiutare a riflettere sulla posizione dell'azienda in materia di cambiamenti climatici e su ciò che i vertici aziendali realmente vogliono ottenere rispetto alle normative, ai concorrenti e alle aspettative della società;
- Comprendere gli obiettivi e l'attuale grado di maturità dell'azienda in materia di sostenibilità climatica e valutare in che misura ciò si rifletta nei piani aziendali e d'azione a diversi livelli;
- Valutare fino a che punto il management ha considerato sia l'impatto dell'organizzazione sull'ambiente sia l'impatto dell'ambiente sull'azienda, spesso di parla di *"questione della doppia materialità"*;
- Valutare l'affidabilità dei KPI relativi al clima dell'organizzazione se esistono, nel caso non siano presenti gli stessi vanno integrati;
- Verificare la solidità dei controlli e dei processi di gestione del rischio associati a questi obiettivi e rischi;
- Constatare la capacità della seconda linea di monitorare i rischi legati al clima e l'accuratezza dei dati relativi al clima;
- Essere in grado di accertare in che misura le comunicazioni aziendali agli stakeholder sulle iniziative per il cambiamento climatico sono supportate da dati sufficienti per evitare le accuse di *green-washing* e i relativi rischi di reputazione.

### 3.4.2 Il modello dei IV quadranti

Nella ridefinizione dell'organizzazione per contrastare i rischi emergenti, all'Internal audit è data la responsabilità dell'Assurance sul disegno e sulla funzionalità complessiva del sistema, attraverso valutazioni indipendenti, in ottemperanza ai requisiti di equilibrio e comparabilità. Inoltre, l'IA deve eseguire la sua attività in via continuativa e sistematica a livello indipendente rispetto alle attività produttive ed è considerato il facilitatore dei processi di risk assessment e dei temi di compliance, valutando anche il presidio da parte delle funzioni preposte della coerenza tra le informazioni raccolte e i reporting requirements degli standard per il reporting di sostenibilità adottati.

La società di consulenza *Ernst&Young* ha presentato nella giornata del Convegno nazionale 2022 dell'AIIA un modello che organizza in quattro quadranti le possibilità d'azione dell'internal audit in ambito ESG, che è stato, per questo motivo, chiamato *"Modello dei IV quadranti".*
Questo modello serve per tracciare nuove strategie sostenibili, e classifica il potenziale ruolo dell'internal audit secondo due principali variabili. La prima riguarda un atteggiamento proattivo rispetto ad un atteggiamento reattivo, ovvero la capacità della funzione di anticipare i problemi e supportare la visione strategica dell'organizzazione. La seconda variabile invece riguarda una visione dell'IA all'interno dell'azienda da una figura di *"Policing"* ad una di *"Partner",* che rappresenta la capacità di supportare il cambiamento qualificandosi come un valido partner per il consiglio di amministrazione andando oltre il classico ruolo di controllore. Da questo modello emergono quattro possibili categorie:

- *Anticipative Monitor:* in questo quadrante prevale la visione strategica, l'auditor è proattivo, ma mantiene la sua posizione da controllore. Ci si focalizza sulle tematiche ESG future, il responsabile IA provvede in caso di controlli, policies e procedure mancanti, provando ad anticipare quelli che saranno i cambiamenti del business model;
- *Business Counselor:* la visione preponderante è quella strategica ed innovativa, il responsabile dell'IA è proattivo e assume il ruolo di partner. Il focus è sui temi strategici, e l'auditor da supporto attivo al CdA nelle discussioni e nella promozione del problem solving. È una figura che promuove i cambiamenti e lo sviluppo delle Best Practice ed anticipa le tendenze e l'impatto che queste avranno sul business;
- *Assurance Factory:* l'internal audit è reattivo ed esercita principalmente la sua funzione come controllore, si focalizza sulle attività di ESG e di Assurance dell'attuale contesto in cui l'azienda opera.

Il vantaggio è che accresce la consapevolezza sui temi della responsabilità ambientale sociale e di governo societario attuali e storici;

- *Change Agent:* in questo quadrante c'è una visione contemporaneamente attuale e sul cambiamento, l'internal auditor è un partner che agisce in modo reattivo, il focus dell'attenzione è posato sul perché le cose falliscono in modo sistematico. C'è un approfondimento che va all'origine dei problemi e viene supportato il cambiamento in ambito ESG.

Per poter promuover un cambiamento a livello di tematiche di ESG è necessario che l'internal audit capisca il livello di maturità dell'organizzazione e su quali temi è meglio soffermarsi.

Nel caso in cui emerga che il livello di maturità dell'organizzazione sia *"Basico"* il focus dovrà essere sull'implementazione delle iniziative di volontariato e sull'incremento di relazioni pubbliche in tema di responsabilità ESG. Il reporting sarà limitato e principalmente l'obiettivo dell'approfondimento di queste tematiche sarà la riduzione dei costi, con un obiettivo temporale di breve periodo.
Quando l'organizzazione ha un livello *"Stabile"* di maturità invece, tutte le comunicazioni interne promuovono il *sustainable thinking* e vengono create una serie di relazioni con gli stakeholder proprio su temi ESG. Gli obiettivi non sono più quantitativi ma qualitativi, anche se le metriche sono su un numero di iniziative limitato.
Le tematiche ed i rischi ESG sono integrati nel processo di pianificazione strategica aziendale nel momento in cui il livello di maturità dell'organizzazione è *"Avanzato"*. In questo caso c'è un impegno costante verso i principali stakeholders, gli obiettivi sono quantitativi e sono allineati con i rischi e le opportunità aziendali, utilizzando delle metriche che sono trasversali per monitorare le prestazioni ed i progressi annuali. In questo caso anche la tecnologia supporta la gestione dei dati ESG, ed è promossa una Disclosure dei progressi e dei dati seguendo dei framework riconosciuti a livello internazionale.
Infine, in caso il livello di maturità sia *"Leading"*, la strategia ESG promuove a livello aziendale l'innovazione e le opportunità, e soprattutto si è capaci di influenzare il mercato in base alle proprie scelte in questo ambito. Gli obiettivi sono mirati alle creazioni di benefici per la società stessa ed in questo caso c'è massima trasparenza con i risultati sia in positivo che in negativo. La reportistica è integrata ed allineata allo scopo aziendale in merito alla strategia ESG ed ai risultati desiderati.

Dopo aver svolto l'analisi sul livello di maturità dell'organizzazione il responsabile IA può qualificarsi come un *partner strategico* che suggerisce approfondimenti mirati al fine di aumentare il livello di fiducia nella gestione dei rischi ESG da parte dell'azienda e di poter misurare e rendicontare i progressi degli obiettivi in questo ambito.

Gli approfondimenti dell'IA dovrebbero essere relativi a tutte le aree impattate dai rischi ESG, quindi sia nella valutazione della resilienza dell'organizzazione ai principali rischi collegati alle terzi parti; nella definizione di obiettivi e traguardi in questo ambito; nella valutazione della completezza e dell'accuratezza dell'informativa trasmessa al mercato, dell'affidabilità del calcolo delle metriche e delle asserzioni; nel definire e implementare le modalità di monitoraggio ed infine di offrire consulenza su come definire o rafforzare la governance sui temi ESG, anche attraverso degli audit mirati.

Per concludere, a parte la valutazione di temi trasversali, si richiede principalmente all'internal audit di focalizzarsi sui temi ESG nel monitoraggio dei controlli, nel rafforzamento della trasparenza ed affidabilità dei processi mirati ad aumentare la performance ESG e le relative disclosure, e di supportare la connessione tra temi ESG ed Entreprise Risk Management, cioè di gestione del rischio d'impresa.

## Conclusioni

In un contesto esposto ad un innumerevole quantità di rischi come quello attuale è condizione necessaria dell'internal audit dover aggiornare, ed a volte dover ripensare completamente, le proprie competenze. Più in generale per le aziende, la strada del cambiamento organizzativo deve essere verso un ambiente flessibile capace di adattarsi alle esigenze del contesto in cui è immerso.

In linea con l'obiettivo posto all'inizio di questa tesi, è emerso chiaramente come il ruolo dell'internal audit non è esente da queste necessità, addirittura come risulta dai commenti del Risk in Focus 2023, l'IA deve essere il promotore del cambiamento e di conseguenza deve evolvere le proprie competenze per far si che lo stesso avvenga.

I risultati ottenuti dalle analisi e dagli approfondimenti svolti da AIIA nel corso del 2022 e dei primi mesi del 2023, a seguito della pubblicazione da parte dell'IIA del nuovo Competency Framework della professione, evidenziano l'importanza di consolidare alcune hard skills soprattutto nei confronti dei nuovi rischi emergenti, ma soprattutto la necessità di lavorare sull'ottenimento e l'implementazione delle cosiddette soft skills. È ricercata la capacità relazionale, di gestire un team di persone con competenze diverse, la gestione dei conflitti, la propensione a diventare un role model per le figure con meno esperienza, la capacità di comunicazione e di problem solving, ed in generale la capacità di essere perspicace e proattivo.

Il lavoro attualmente svolto dall'IIA in merito all'aggiornamento dell'IPPF che verranno pubblicati entro la fine del 2023, sarà una nuova guida per gli auditor, in quanto i precedenti "Implementation standard", che erano semplicemente raccomandati e che trattano proprio l'applicazione concreta degli standard, diventeranno obbligatori, rendendo la guida dell'associazione ancora più precisa e capace di coprire tutta l'area di azione degli internal auditor. In particolare, i nuovi IPPF, oltre a ribadire i principi chiave della professione, in particolare indipendenza, integrità e obiettività, incentivano la promozione del ruolo strategico della Funzione nei confronti del board e del top management. Tale ruolo può essere ricoperto solo se la Funzione dimostra di possedere le competenze hard e soft necessarie ad affrontare la valutazione dei rischi attuali e del conseguente sistema di controllo da implementare.

A tal fine, nell'immediato futuro sarà sicuramente necessario formare al meglio le risorse già presenti in azienda, ma soprattutto essere in grado di far conciliare le competenze dei singoli individui con le necessità dell'organizzazione. Questo processo vale sia per la formazione del team di audit, ma è anche un processo che va svolto all'interno di tutte le funzioni aziendali ed al quale l'auditor deve fornire continuo supporto.

Una prospettiva futura, ormai diventata certezza, è il cambiamento dell'attività di audit nel suo complesso, in quanto attualmente si presta ad essere identificata come un'attività flessibile, riorganizzabile in base agli avvenimenti e soprattutto con una gestione dei rischi integrata a tutti i livelli aziendali. Proprio per questo le competenze che un internal audit deve possedere per riuscire ad allineare gli obiettivi a livello di aziendale, sono principalmente quella di una corretta e continua comunicazione ed informazione, ed in generale coltivare relazioni fruttifere con tutti gli stakeholders.

I risultati evidenziati dai gruppi di lavoro di AIIA, anche grazie allo sviluppo di un tool a supporto della valutazione delle competenze disponibili nella funzione di internal audit, evidenziano in sintesi come:

- I chief audit executive possano garantire la disponibilità delle risorse competenti non solo tramite percorsi di formazione degli internal auditor, ma anche tramite il ricorso all'outsourcing per le competenze altamente specialistiche necessarie per interventi ad hoc. L'affiancamento degli internal auditor a specialisti esterni rappresenta un'ottima opportunità di training on the job;
- Gli internal auditor possano migliorare le proprie conoscenze anche grazie allo svolgimento di attività congiunte con le funzioni competenti interne all'azienda che, per prime, sono tenute ad essere tempestivamente aggiornate sull'evoluzione tecnologica, normativa e di mercato secondo il proprio ambito di attività. L'affiancamento degli auditor alle funzioni interne in sede di analisi e studio dei processi aziendali non deve essere visto come una minaccia all'indipendenza della funzione (che in ogni caso deve essere garantita in fase di testing e in fase di valutazione finale dell'adeguatezza del sistema di controllo) ma come un'opportunità di knowledge sharing.

Gli esiti del Risk in Focus 2023 hanno fatto emergere in particolare, 3 rischi che le funzioni di audit devono essere in grado affrontare sia con le adeguate competenze che con gli strumenti più opportuni in relazione alla natura e alla tipologia di dati disponibili:

- *Cybersecurity*: una competenza che ormai risulta fondamentale ottenere per lo svolgimento della professione è quella legata al mondo informatico, con una duplice prospettiva. L'internal audit deve avere a disposizione le competenze idonee a valutare se il sistema di controllo interno applicato ai processi di Information & Communication Technology sia idoneo ed efficace a tutelare l'integrità delle informazioni aziendali. Parallelamente, l'Internal Audit dovrebbe sfruttare la tecnologia in modo efficace in tutti gli ambiti di operatività, con l'utilizzo di strumenti orientati a migliorare la comprensione e la valutazione dei rischi e ad aiutare ad individuare eventuali anomalie.
- *Human capital, diversity and talent management*: il mercato del lavoro ha subito un'evoluzione repentina negli ultimi 3 anni tale da far diventare "la necessità di garantire la presenza delle adeguate competenze in azienda" un rischio condiviso da tutte le funzioni e a tutti i livelli dell'organizzazione.

L’internal audit deve quindi modificare il proprio punto di vista passando da un’analisi sul disegno dell’organizzazione e sull’idoneo dimensionamento degli organici, alla necessità di verificare che esista una mappatura delle competenze necessarie per ciascuna funzione, incluso l’audit stesso, e che esistano strumenti adeguati a supportare l’integrazione delle competenze eventualmente mancanti.

- *Tematiche ESG*: non si tratta di un unico rischio, ma di una molteplicità di fattori, ambiti di intervento e normative di riferimento per i quali, anche secondo numerosi studi recenti, le aziende devono avviare veri e propri progetti interni di analisi dei processi interessati e di riallineamento delle strategie e delle scelte operative in conformità ai requisiti normativi. L’internal audit, secondo i medesimi studi, deve avere un ruolo all’interno del progetto stesso, che si tratti di interlocutore diretto a supporto del disegno del nuovo sistema di controllo o, al limite, in affiancamento come supporto, al fine di identificare le competenze chiave e attivarsi al suo interno per garantirne la disponibilità.

Rischi come l’Human, la cybersecurity e tutte le tematiche ESG, sono solo tre della più vasta gamma che le aziende si trovano a dover fronteggiare, ma sono serviti come esempio per comprendere che è necessario ridisegnare i processi organizzativi per mitigare gli effetti di questi eventi all’interno dell’azienda. I diversi assessment presentati nei vari paragrafi non sono tecnicamente diversi dalle solite operazioni che l’auditor è solito compiere per normali mappature del rischio, la principale differenza che richiedono questi processi è sulle competenze, che devono essere quella di saper comunicare con i vertici aziendali, di possedere una continuità operativa, *il Continuous audit* come strumento di predittività, e soprattutto si richiede all’internal auditor di essere un interlocutore strategico per tutto il sistema di controllo aziendale.

**Bibliografia & Sitografia**


AIIA, "*Internal audit Competency mapping: mappatura delle competenze presenti e occorrenti all'interno dei Team di Internal Audit"*, Febbraio 2023

AIIA, "*Internal audit Competency framework: attuale livello di maturità delle competenze della Funzione IA vs aspettative future",* Febbraio 2022

AIIA, "Internal audit appetite for human capital & talent management", Settembre 2022

AIIA, *"NEXT GENERATION: innovazione e trasformazione digitale stanno guidando il futuro dell'internal audit?",* Maggio 2022

AIIA Academy, "ESG & Processi Gestionali", 22 febbraio 2023

Alberto Oliva, Patrizia Riva, *"La* figura professionale dell'*Internal Auditor* (IA) e le fasi della sua attività"

Associazione Italiana Internal Audit, https://www.aiiaweb.it

CIA, Study book Unit one, Gleim Publication, 2019

CIA, Study book Unit two, Gleim Publication, 2019

Codice di Corporate governance, Gennaio 2020

Competency Mapping Tool

Deloitte, "*Cybersecurity and the role of internal audit; An urgent call to action*"

D'Onza G., "*L'internal auditing"*, Torino, G. Giappichelli Editore, 2013

*Ethics and Sustainability in Accounting and Finance,* Springer, Singapore, 2021.

ECIIA, Risk in focus 2023

EY, *"Internal Audit e rischi ESG*", Evento nazionale AIIA, 15 novembre 2022

Ferrari, Massimo, "*Revisione Interna, Compliance e Gestione dei Rischi aziendali"*, Luiss Guido Carli, 2022- 2023.

Flemming, Ruud T., "*Recent developments and trends in internal auditing"*, University of St. Gallen, Marzo 2012.

Franco Potani, "*La Revisione Contabile nel Mondo Occidentale Dal Medioevo all'Età Contemporanea*", Pavia, Febbraio 2015

Grabmann, Elisabeth; Hofer, Daniel, *"Impact factors on the development of Internal Auditing in the 21st century*", ACRN Journal of Finance and Risk Perspectives, Novembre 2014.

Gallagher, Russell, "*Risk Management: "A new phase of Cost Control*", Harvard Business Review, 1956

Hazar, H.B., et al *"New Paradigm in Auditing: Continuous Auditing"*

Internal Audit Competency framework

Provitti, "*The Future of Work Is Here and Opportunities Are Around Every Corner*", Internal Auditing Around the World, Volume XVIII

PWC, "*Internal Auditing nelle società quotate"*, 2° Edizione

Roberto Rosato, "*The IIA Standards: The IPPF Framework"*, 2015

Robert R. Moeller, "*Brink's Modern Internal Auditing*", Eight Edition, John Wiley & Sons, Inc. 2016

Ricci, Sante, "*Revisione Interna, Compliance e Gestione dei Rischi aziendali"*, Luiss Guido Carli, 2022-2023.

T. A. Lee, "*The Historical Development of Internal Control from the Earliest Times to the End of the Seventeenth Century* ", Wiley

The IIA, "*Global Perspective & Insights, Updating Standards for a Changing World",* Febbraio 2023

The Institute of Internal Auditors, *Standard internazionali per la pratica professionale dell'internal auditing (Standard)*, 2017.

The IIA, "*The iia's global internal audit competency framework"*, 2014

The IIA, "*Global perspectives & insights, Cybersecurity in 2022*"

The IAA, All in a day's work a look at the varied responsibilities of internal auditors

WEF, *"Future of Jobs Report"*, 2023

https://www.ypulse.com/article/2021/11/02/why-the-great-resignation-is-happening-in-western-europe-too/

https://www.sec.gov/news/speech/spch113005mag.htm

https://www.dirittobancario.it/art/internal-auditing-evoluzione-della-professione-tra-obblighi-disclosure/

https://www.aiiaweb.it/knowledge-center/international-professional-practices-framework

https://www.portalecompliance.it/internal-auditing.html

https://www.riskcompliance.it/news/un-nuovo-ruolo-per-l-internal-audit/

**Riassunto**

Le aziende si trovano nel momento attuale a dover esercitare la propria attività in un contesto che è stato definito come la "*Tempesta perfetta*". L'evento meteorologico è usato come metafora per rappresentare in termini economici tutta una serie di circostanze straordinarie che si verificano e minano l'andamento dei processi aziendali. Attualmente la situazione è aggravata da diversi fattori: la pandemia da COVID-19, la guerra in Ucraina con i conseguenti effetti inflattivi su tutti i mercati e l'emergere di ulteriori nuovi rischi che si stanno progressivamente consolidando e hanno portato i governi ad accelerare lo sviluppo e l'adozione di nuove normative obbligatorie. In aggiunta a questi elementi, se si guardano con attenzione i mutamenti intervenuti contestualmente nel contesto sociale, occorre considerare la necessità di rivedere le modalità di ingresso nel mondo del lavoro della Generazione Z, che sta dimostrando di avere esigenze, competenze e obiettivi diversi dalle precedenti.

Per le organizzazioni risulta di fondamentale importanza doversi adattare al nuovo contesto e la figura dell'Internal Audit svolge un ruolo cruciale in questo processo.

Prima di parlare dell'attuale attività svolta dall'auditor è necessario fare un excursus sulla professione dell'IA ed in generale sulla regolamentazione della figura.

La definizione del ruolo è fornita da "*The Institute of internal auditors" (The IIA)* e permette di delineare alcune caratteristiche richieste nello svolgimento di tale funzione.

*"L'internal audit è un'attività di garanzia e consulenza indipendente e obiettiva, finalizzata ad aggiungere valore e a migliorare le operazioni di un'organizzazione. Aiuta un'organizzazione a raggiungere i propri obiettivi attraverso un approccio sistematico e disciplinato per valutare e migliorare l'efficacia dei processi di gestione del rischio, di controllo e di governance."*

Emerge come l''Internal Audit aiuti le organizzazioni a raggiungere i propri obiettivi identificando aree di miglioramento e fornendo consulenza per mitigare i rischi e migliorare le prestazioni. L'indipendenza è una caratteristica chiave che consente un'esecuzione oggettiva e libera da interferenze esterne. Inoltre, viene richiesto alla funzione di generare valore aggiunto attraverso le sue attività e le sue metodologie analitiche, tramite mirati suggerimenti e raccomandazioni.

Ripercorrendo negli ultimi decenni l'evoluzione delle normative applicabile e del conseguente significato di controllo interno all'azienda, si nota come fin dalle origini, il focus sia stato fortemente dedicato al controllo contabile e al processo di formazione del bilancio. Ad oggi, la stessa funzione di internal audit ha subito importanti ampliamenti del proprio ambito di attività. Vale la pena quindi, in tal senso, specificare la differenza tra revisione contabile ed internal audit, in quanto quest'ultimo, concentra l'attenzione sul controllo interno, sulla valutazione di tutti i processi aziendali e sulle conseguenti raccomandazioni per il miglioramento, mentre il revisore contabile è una figura esterna all'organizzazione che esprime una valutazione sulla rappresentazione veritiera e corretta della situazione patrimoniale e finanziaria della società. Gli internal audit svolgono quindi

diverse attività, come l'audit operativo per valutare l'efficacia ed efficienza dei processi; l'audit finanziario per verificare i controlli interni nell'ambito contabile; l'audit di conformità per garantire l'osservanza delle norme interne ed esterne, e l'audit antifrode per identificare e prevenire frodi e irregolarità finanziarie.

Nel 1942 è stata fondata l'IIA (The Institute of Internal Auditors) da revisori interni che desideravano condividere le proprie esperienze e conoscenze in questo campo professionale emergente. In Italia, è stata creata l'Associazione Italiana Internal Auditors (AIIA) come affiliata dell'IIA, diventando un punto di riferimento per il controllo interno, la corporate governance, la conformità e la gestione del rischio.
L'IIA ha svolto un ruolo fondamentale nell'evoluzione del governo societario verso gli standard internazionali e ha contribuito all'affermazione dell'internal auditor come figura professionale. Inoltre, anche a livello italiano l'associazione si impegna anche nella promozione della professione, collaborando con organizzazioni del settore, istituzioni accademiche e organi di governo per aumentare la consapevolezza della funzione di audit interno e dell'importanza della gestione dei rischi nelle organizzazioni.
Il primo riconoscimento nella storia alla figura dell'IA è dovuto all'istituzione della Securities and Exchange Commission (SEC), nel 1934, propose come azione legislativa correttiva per sanare la grave crisi economica che il mondo stava attraversando, che tutte le imprese registrate presso di essa dovessero fornire bilanci certificati da revisori indipendenti. Questo requisito ha spinto le aziende a creare dipartimenti di revisione interna, ma con l'obiettivo principale di assistere i revisori indipendenti.

In Italia l'internal audit ha subito un'evoluzione significativa, dal punto di vista normativo, a partire dagli anni '90, quando il governo italiano ha iniziato ad adottare regolamentazioni più stringenti per migliorare la trasparenza e l'efficacia delle attività di audit interno all'interno delle organizzazioni. La vera svolta però per il sistema di controllo interno e, implicitamente, per l'introduzione dell'internal audit si ha nell'1998 con l'entrata in vigore del "Testo Unico della Finanza - TUF" (D.lgs. n. 58 del 24 febbraio 1998, noto anche come "legge Draghi") che formalizza l'importanza del Sistema di Controllo Interno, introducendo per la prima volta nella legislazione italiana tale espressione. Attualmente uno standard setter per la definizione del ruolo e dell'attività dell'IA è il *Codice di Corporate Governance* delle società quotate, il quale è, inoltre, il principale punto di riferimento nazionale in tema di corporate governance e si rivolge a tutte le società con azioni quotate sul mercato. Ciascun articolo del Codice è suddiviso in principi che definiscono gli obiettivi di una buona governance, e in raccomandazioni, che indicano i comportamenti che il Codice reputa adeguati a realizzare gli obiettivi indicati nei principi. È importante sottolineare che il codice si basa sul principio di *"Comply or Explain",* ciò vuol dire che le società non sono obbligate ad implementare il modello, ma se dovessero differire dallo stesso dovrebbero motivare la loro scelta nella relazione annuale sul governo societario. Ogni società

che aderisce al Codice fornisce nella relazione sul governo societario informazioni accurate, di agevole comprensione ed esaustive, se pur concise, sulle modalità di applicazione del Codice.

Inoltre, la regolamentazione dell'internal audit è stata influenzata anche dalle normative internazionali, in particolare dagli standard internazionali per la pratica dell'internal audit definiti dall'IIA. Gli standard IIA sono stati adottati anche in Italia, e costituiscono un punto di riferimento per gli internal auditor italiani.

L'IIA ha definito la missione dell'internal audit come quella di arricchire e proteggere il valore dell'organizzazione attraverso attività di Assurance, consulenza e strategiche basate su una preventiva analisi del rischio. Per raggiungere questo obiettivo, è stato creato l'International Professional Practices Framework (IPPF), che contiene le linee guida dell'IIA e rappresenta i global standard setter per la professione dell'internal audit. Il framework include regole obbligatorie e raccomandazioni che gli internal auditor devono seguire, come i principi fondamentali, il codice etico e gli standard veri e propri.
I principi fondamentali rappresentano la base dell'efficacia dell'audit interno e includono l'integrità, la competenza e la dovuta attenzione professionale, l'obiettività, l'allineamento con gli obiettivi e i rischi dell'organizzazione, il posizionamento adeguato e le risorse adeguate, la qualità e il miglioramento continuo, la comunicazione efficace, le garanzie basate sul rischio, l'orientamento al futuro e la promozione del miglioramento organizzativo.
Il codice etico definisce le regole comportamentali per i professionisti dell'internal audit e promuove una cultura etica nella professione. Esso include i principi di integrità, obiettività, riservatezza e competenza.
Gli standard sono parte integrante del Framework e sono fondamentali per praticare l'internal audit. Essi guidano l'adesione agli elementi obbligatori dell'IPPF, forniscono un quadro di riferimento per l'esecuzione dei servizi di internal audit, stabiliscono le basi per valutare le prestazioni dell'audit interno e promuovono il miglioramento dei processi organizzativi e delle operazioni. Gli standard sono articolati in standard di attributo, standard di performance, interpretazioni e standard di implementazione, e trattano vari aspetti dell'attività di internal audit. Risulta di fondamentale importanza il fatto che l'IIA stia attualmente rivedendo gli standard per rispondere alle esigenze del futuro e fornire servizi di internal audit tempestivi, pertinenti e d'impatto. Gli standard saranno organizzati in cinque domini che affrontano diversi aspetti della professione: lo scopo dell'internal auditing, l'etica e la professionalità, il governo della funzione di revisione interna, la gestione della funzione di revisione interna e l'esecuzione dei servizi di revisione interna. La ridefinizione degli standard mira a promuovere il ruolo strategico dell'internal audit e a garantire la qualità delle prestazioni.
Gli standard e le interpretazioni dell'IIA sottolineano l'importanza delle competenze nell'esercizio della professione di internal auditor. Lo standard 1210, nello specifico, afferma che gli internal auditor devono possedere le conoscenze, le capacità e altre competenze necessarie per adempiere alle proprie responsabilità.

Le competenze necessarie per svolgere la professione di internal auditor non si limitano alle conoscenze teoriche, ma richiedono anche la capacità di applicare le conoscenze in modo concreto.
Il "Global Internal Audit Competency Framework" dell'IIA fornisce una guida per la formazione, lo sviluppo e la valutazione delle competenze degli internal auditor. Il framework è flessibile e può essere adattato alle esigenze specifiche e alle diverse fasi di carriera degli internal auditor. Le competenze sono suddivise in competenze professionali e competenze personali. Le competenze professionali riguardano le conoscenze tecniche e le abilità specifiche dell'internal audit, mentre le competenze personali riguardano le caratteristiche personali e le abilità trasversali necessarie per avere successo nella professione.

Il framework identifica dieci competenze principali: etica professionale, gestione dell'internal audit, applicazione dell'IPPF, governance, rischio e controllo, conoscenza del business, comunicazione, persuasione e collaborazione, pensiero critico, consegna dell'internal audit, miglioramento e innovazione. Per raggiungere la padronanza delle competenze, l'etica professionale e la gestione dell'internal audit sono considerate fondamentali. Nello specifico il framework valuta le competenze in quattro ambiti: *Professionalism, Performance, Environment e Leadership&Communications*. Ogni area ha diverse aree di conoscenza e viene valutata a livelli di competenza che vanno da una conoscenza generale a un'applicazione avanzata e all'expertise. Nell'ambito *del Professionalism*, si vanno a definire i connotati dell'Auditor, partendo dai principi etici alla base del suo operato arrivando alle competenze professionali necessarie a svolgere al meglio la funzione essendo autorevoli ed ispirando fiducia degli altri membri dell'organizzazione. All'IA, è richiesta l'indipendenza organizzativa, l'obiettività individuale, il comportamento etico, la dovuta cura professionale e lo sviluppo professionale stesso. La parte del Framework inerente alla Performance descrive le modalità operative per eseguire il mandato di IA, per pianificare tutta l'attività in conformità con quanto dettato dagli Standard. Il Framework poi valuta anche l'Environment, cioè dove viene creato il valore. Questo ambito ricopre sia aspetti professionali che tecnici per identificare, monitorare, affrontare ed in alcuni casi prevenire, i rischi specifici dell'ambiente in cui opera un'organizzazione. Ultimo ambito analizzato è quello della Leadership & Communications. In questo caso si va ad analizzare a chi va offerto il servizio, serve per dare una guida e per rafforzare le relazioni sia con il team che con gli Stakeholder. Le aree in cui viene valutato questo aspetto sono tutti quelli di pianificazione, quindi quella strategica e di gestione dell'internal audit, quella di coordinamento degli sforzi dell'audit.

Inoltre, il framework non è utilizzato solo dagli internal audit, ma può essere d'aiuto ad altre figure interne o esterne all'azienda, come ad esempio gli sviluppatori di corsi e gruppi di certificazione, oppure dalla comunità accademica per essere in grado di fornire un elenco di competenze critiche da considerare nello sviluppo dei corsi per preparare gli studenti all'ingresso nella professione di revisore interno. All'interno del contesto

aziendale è utilizzato dai datori di lavoro o altri professionisti come riferimento o benchmark rispetto ai quadri di competenza.

Nel 2022, in un webinar dell'AIIA, è stato discusso il livello di maturità raggiunta delle competenze della funzione di IA rispetto a quelle stabilite dal Competency framework. Analizzando i risultati di una survey sottoposta ad un panel di 50 società, sono stati utilizzati i modelli AS-IS e TO-BE sono utilizzati per descrivere lo stato attuale di un sistema o di un'organizzazione (AS-IS) e lo stato futuro desiderato (TO-BE). Quest'analisi è stata svolta su tutte le aree del framework e le principali differenze tra i i modelli AS-IS e TO-BE sono emerse sul tema del comportamento etico, per il quale la maggior parte del sampling ha dimostrato una generale conformità al codice etico, ma una minore proattività nella promozione degli standard etici stessi; il tema delle frodi che ha portato a diversi spunto di riflessione per raggiungere un livello di competenza più elevato, come definire degli indicatori di frode, definiti "red flag", e di conseguenza creare una Fraud Library, cioè degli schemi di frode e soprattutto risulta necessario segnalare repentinamente al CdA e adottare un approccio di continuous auditing; sulle modalità del risk assessment in fase di pianificazione, in cui la principale differenza tra i diversi livelli di competenza in questo ambito è relativa alla capacità di riuscire a valutare il rischio durante il periodo dell'incarico dell'audit e non successivamente nel caso in cui il rischio, che doveva essere prevenuto, si è effettivamente verificato; infine è emerso sul tema delle soft skill ed innovation come queste siano meritevoli di molta formazione, valutando il tutoring o mentoring o coaching delle risorse senior.

Sempre grazie al supporto del Competency Framework, nello stesso anno, uno studio condotto da dei professionisti di AIIA ha portato alla creazione di un Competency Assessment Tool, volto ad identificare le competenze chiave che è auspicabile siano presenti, seppur con un diverso livello di granularità e maturità, all'interno dei Team di Internal Audit. Sono state identificate circa settanta competenze chiave ed è stato creato un tool mappato sulle quattro aree in cui il Competency framework raggruppa le competenze che un IA deve possedere, e per ognuna delle competenze esaminate, è stata effettuata una valutazione in merito alla sua rilevanza e al livello di maturità attesa in base alla seniority dei membri del Team. Il livello di seniority è articolato su quattro figure: Junior Auditor, Senior Auditor, Audit Manager e Chief Audit Executive. Nonostante ogni team non sia doverosamente composto da tutte queste figure, avrà al suo interno un buon mix degli stessi. Le competenze poi sono classificate in base al fatto di essere *Mandatoria, Raccomandate oppure Nice to Have e Outsorced*.

Quest'analisi è svolta con la consapevolezza che "No One Size Fits It All", cioè che il tool potrà essere una base di partenza per tutte le aziende, ma non è possibile creare uno strumento che corrisponda alle necessità di ognuna essendo ogni impresa una realtà a sé stante.

*Il competency assesstment tool* può rappresentare un utile riferimento per comprendere quali competenze sviluppare e mantenere all'interno del proprio audit team investendo prima sulle aree ritenute maggiormente critiche e successivamente su quelle meno rilevanti. Dallo svolgimento di ulteriori analisi svolte sempre da professionisti associati all'AIIA, è emerso che nelle prime fasi le principali skill da imparare sono di tipo Hard, come la conoscenza degli standard e dei generali metodi di controllo, mentre con l'aumento della maturity aumenta anche la richiesta di soft skills come la capacità di gestire i conflitti ed essere un modello di comportamento. In generale poi emerge un concetto importantissimo alla base di ogni competenza, ovvero quello prima di tutto di dover imparare, sviluppare e consolidare le stesse, ma poi successivamente di diffonderle a tutte le persone di grado inferiore ed anche superiore. Sviluppare una condivisione non solo della conoscenza ma anche della competenza.

Inoltre, il tool si sofferma anche sulla necessità di dover andare a fronteggiare i cambiamenti del mutevole contesto, definito *"new normal"*, in cui al giorno d'oggi l'internal auditor si trova a dover lavorare, e quindi soprattutto le competenze emergenti da tale contesto. Acquisisce sempre maggior rilevanza la capacità di adattamento ai cambiamenti, di resilienza e di gestione delle situazioni nuove e conflittuali e *distruptive*, da qui la necessità di dover pianificare in modo agile gli audit, e rivalutare periodicamente le priorità. In questo contesto così mutevole, risulta un valore aggiunto possedere all'interno dei team di audit competenze specifiche non solo sui modelli del frame work di controllo tradizionale, ma anche su quelli emergenti, in ambito ESG Reporting, Cyber Security, Tax Control Framework, Health, Safety & Environment

Nella tesi è presentato anche un caso di applicazione concreta del nuovo tool. Sempre grazie alle attività svolte dall'AIIA, in una grande società italiana quotata, appratente al settore industriale dotata di una funzione di audit di oltre 150 persone, è stato avviato un processo di formazione collegato alla mappatura delle skill e delle competenze all'interno del gruppo di audit. Prima di tutto è stato costruito un database, chiamato corporate skills library, con le competenze minime attese per ciascun livello di audit, dopodiché database è stato richiesto a ciascun auditor di dare il proprio self-assessment, in base alle proprie capacità attuali e quelle derivanti da esperienze precedenti e soprattutto focalizzandosi sulle nuove skills richieste come quella di lavorare da remoto, di analisi dei dati e di condivisione dei risultati e degli action plan. Il risultato di questo self-assessment ha evidenziato alcuni punti di miglioramento su alcune competenze minime che ciascun auditor dovrebbe avere, sui quali sono poi statti programmati dei percorsi di formazione, e rende presente quali sono le

competenze di ciascun auditor in base agli obiettivi di crescita del gruppo e stimolare la crescita di ciascun auditor nel breve periodo, creando così un bacino per i nuovi manager del futuro.

Come anticipato precedentemente, al giorno d'oggi le imprese si trovano a dover operare in un contesto mutevole, che richiede alle stesse continui cambiamenti organizzativi per permettere una continuità dell'attività aziendale e questo influenza inevitabilmente il ruolo dell'interno all'audit.
Per questo motivo l'AIIA ogni anno prende parte alla redazione di un report, insieme alle altre associazioni di internal audit a livello europeo, chiamato "Risk in focus" che presenta i principali rischi di mercato su quali è necessario orientare la professione dell'IA.
L'affiorare di nuovi rischi sul mercato comporta per l'IA la necessità di aggiornare le proprie competenze per affrontare rapidamente le nuove necessità delle aziende e dare supporto alle stesse in situazioni rischiose, incerte e volatili. L'internal audit per fronteggiare l'attuale contesto mutevole, sono deve soffermarsi sulle soft skills, cioè non competenze tecniche, generalmente definite Hard skills. Le soft skill che attualmente risultano imprescindibili nel praticare la professione dell'IA sono, come affermato anche dal Competency assessment Tool, la capacità di valorizzare promuovere le diversità, di avere interazioni frequenti con il top management, di ascolto attivo ed empatico e di gestione di situazioni e dinamiche conflittuali. Le competenze tecniche restano di fondamentale importanza, infatti per fronteggiare e valutare ciascun rischio è richiesta almeno una conoscenza di base delle normative che ogni anno vengono aggiornate.
I chief audit executive che hanno partecipato al Risk in Focus 2023 hanno evidenziato cinque rischi come prioritari: incertezza geopolitica, cambiamento climatico, cultura organizzativa, rischio informatico e dei dati, digitalizzazione e intelligenza artificiale.

In generale come risultato di questa edizione del Risk in Focus emerge come, in primis, i board debbano concentrarsi sui rischi sistemici che creano vulnerabilità in molte parti dell'organizzazione contemporaneamente e garantire che le attività di valutazione e gestione del rischio forniscano al consiglio di amministrazione una chiara supervisione di tali rischi. Inoltre, bisogna verificare che il CdA abbia aggiornato la propria propensione al rischio, al fine di fornire chiarezza nel rapido processo decisionale strategico. Nello svolgere questa tipologia di valutazione dei rischi è necessario garantire che le attività di governance, gestione e controllo del rischio siano collegate e coerenti rispetto ai rischi strategici. Per questo motivo al CdA è anche chiesto di collaborare con il chief audit executive per garantire che la funzione dedichi tutto il tempo necessario alle aree di rischio strategico e sistemico emergenti e soprattutto fornire all'intera funzione di audit il profilo, l'autorità e le risorse necessarie per supportare adeguatamente l'organizzazione nel raggiungimento dei suoi obiettivi strategici.

Nello specifico la tesi si è focalizzata sull'analisi di tre rischi: *Cybersecurity, Human capital, diversity and talent management, Tematiche ESG.*

L'impatto dirompente della tecnologia e la velocità del relativo progresso, oltre che fonte indiscutibile di opportunità, espone contemporaneamente le organizzazioni a nuovi e significativi rischi, che devono essere ben compresi e gestiti con strumenti efficaci. Negli ultimi anni le minacce informatiche hanno assunto un ruolo di primo piano dovuto, oltre che al progresso tecnologico, ad un mix di eventi che comprendono la crisi ucraina, le persistenti minacce COVID-19 e le crescenti tensioni tra Stati Uniti e Cina. Ad oggi, per queste variabili e altre ancora, la cybersecurity ha posto significativo tra i rischi della professione. L'importanza di questo rischio è legata al fatto che l'internal audit ha un ruolo fondamentale nell'aiutare le organizzazioni a gestire le minacce informatiche, sia fornendo una valutazione indipendente dei controlli esistenti e necessari, sia aiutando il comitato controllo interno e il consiglio di amministrazione a comprendere e affrontare i diversi rischi del mondo digitale.
Per aiutare a garantire la supervisione del programma di cybersecurity da parte delle strutture di governance, a livello statunitense la SEC ha emanato due proposte che, se integraste nei normali processi di assessment, potrebbero portare ad avere una copertura maggiore del rischio.

La prima proposta si concentra sui consulenti d'investimento registrati, sulle società d'investimento registrate e sulle società o fondi di sviluppo aziendale. In base alle norme proposte, i consulenti e i fondi sarebbero tenuti ad adottare ed implementare politiche e procedure scritte di cybersecurity, successivamente segnalare alla SEC, tramite un modulo riservato, gli incidenti significativi di cybersecurity che interessano il consulente o i suoi clienti di fondi o fondi privati stessi. Inoltre, la proposta prevede di divulgare pubblicamente i rischi di cybersecurity e gli incidenti significativi di cybersecurity verificatisi negli ultimi due anni fiscali nelle brochure e nelle dichiarazioni di registrazione. La seconda proposta, invece, consiste nel segnalare gli incidenti di cybersecurity, ed è diretta a tutte le società quotate in borsa con l'obiettivo di ottenere un'informativa sul rischio di cybersecurity migliore e puntare verso una standardizzazione della stessa.

Uno studio di Deloitte, *"Cybersecurity and the role of internal audit An urgent call to action"*, afferma che la minaccia di attacchi cyber è significativa e in continua evoluzione. È stato progettato un processo di risk assessment che il responsabile internal audit dovrebbe seguire per fornire all'azienda indicazioni su un nuovo livello di protezione dai rischi di cybersecurity. Questo processo viene avviato per cercare di adeguare il proprio sistema di controlli su uno dei tre livelli proposti dalla società di consulenza. I livelli sono: "Secure" in cui la maggior parte delle organizzazioni stabilisce controlli come difese piramidali, protezione dei dati per proteggersi dalle minacce note; "Vigilant" le informazioni sulle minacce, e il monitoraggio della sicurezza

vengono utilizzate per rilevare attività dannose, utilizzate per aiutare l'organizzazione rispondere al panorama mutevole delle minacce; "Resilient " in cui i protocolli di risposta agli incidenti, le analisi forensi ed i piani di continuità operativa vengono messi in atto per recuperare il più rapidamente possibile e l'impatto degli stessi.

Dalla proposta di questo assessment si può dedurre che una competenza che ormai risulta fondamentale ottenere per lo svolgimento della professione è quella legata al mondo informatico, con una duplice prospettiva. L'internal audit deve avere a disposizione le competenze idonee a valutare se il sistema di controllo interno applicato ai processi di Information & Communication Technology sia idoneo ed efficace a tutelare l'integrità delle informazioni aziendali. Parallelamente, l'Internal Audit dovrebbe sfruttare la tecnologia in modo efficace in tutti gli ambiti di operatività, con l'utilizzo di strumenti orientati a migliorare la comprensione e la valutazione dei rischi e ad aiutare ad individuare eventuali anomalie.

Il mercato del lavoro ha subito un'evoluzione repentina negli ultimi tre anni tale da far diventare "la necessità di garantire la presenza delle adeguate competenze in azienda" un rischio condiviso da tutte le funzioni e a tutti i livelli dell'organizzazione. Questa evoluzione comporta che il tema dell'Human capital, diversity e talent management si trovi al secondo posto dei rischi che attualmente un'internal auditor si trova a dover fronteggiare, con una crescita esponenziale ogni anno che passa. L'internal audit deve quindi modificare il proprio punto di vista passando da un'analisi sul disegno dell'organizzazione e sull'idoneo dimensionamento degli organici, alla necessità di verificare che esista una mappatura delle competenze necessarie per ciascuna funzione, incluso l'audit stesso, e che esistano strumenti adeguati a supportare l'integrazione delle competenze eventualmente mancanti.
Unica certezza di questo cambiamento è che le persone saranno sempre di più attori protagonisti del proprio sviluppo e della propria crescita. Quindi risulta necessario fornire alle persone le risorse per poter gestire il loro sviluppo all'interno di un'organizzazione, con strumenti adatti a garantire alle persone di poter dichiarare le proprie ambizioni e portele sviluppare e dall'altro canto permettere all'organizzazione di intercettare questi talenti e combaciarli con le proprie necessità.

Per poter aiutare le persone a riconoscere il proprio potenziale, una società multinazionale nel settore farmaceutico ("La multinazionale") ha creato un meccanismo per il quale viene chiesto alle persone, secondo un processo di people development, di pensare alle proprie abilità e competenze e poi successivamente di poterne discutere con il proprio manager, in un processo di performance management, per poter impostare un possibile iter di formazione che viene poi seguito da un leadership team con la creazione di veri e propri percorsi di carriera. La multinazionale ha creato un piano che è articolato in tre passaggi principali: *La fissazione dei "Goal"; L'ottenimento delle risorse; La misurazione dei risultati.* Nella fase iniziale bisogna

coinvolgere i singoli per definire gli obiettivi di crescita, combinando talento e potenziale, dopo averli individuati è necessario valutare anche l'impatto degli stessi sul business, sulla performance e sulla carriera, e definire i KPI (Key Performance Indicator) per misurare l'apprendimento. La seconda fase definisce il piano di sviluppo, ricercando le risorse adatte per promuoverlo eseguendo un approccio 70-20-10 per creare un piano individuale di apprendimento. Tale approccio si basa su una formazione basata al 10% sul "Formal Learning", quindi e-learning, self study e classi di training o seminari, sul 70% sul "*Learning by doing*", quindi basato sull'esperienza pratica ed infine il 20% riservato ad attività di tipo relazionale, *"Learning from others",* cioè un apprendimento correlato a dei "role models" dai quali apprendere, seguendoli ed accompagnandoli nell'esercizio di determinate attività. L'ultima fase, che in realtà è svolta in maniera continuativa durante tutto il percorso di apprendimento, è la fase di misurazione. Attraverso i KPI, definiti all'inizio del percorso, si misura l'avanzamento del piano e si apportano delle modifiche nel caso in cui sia necessario. Nel caso in cui gli obiettivi personali cambino, oppure debbano essere implementati, queta fase comprendere la possibilità di sostituire i KPI e consolidare nuove skills.

Infine, quando si affrontano le tematiche ESG, cioè la responsabilità che un azienda deve avere in ambito Ambientale, sociale e di governo societario, non si tratta di un unico rischio, ma di una molteplicità di fattori, ambiti di intervento e normative di riferimento per i quali, anche secondo numerosi studi recenti, le aziende devono avviare veri e propri progetti interni di analisi dei processi interessati e di riallineamento delle strategie e delle scelte operative in conformità ai requisiti normativi. I programmi e le iniziative ESG messi in atto dalle organizzazioni sono partiti da semplici attività filantropiche e di volontariato dei dipendenti, fino ad oggi ad arrivare ad un'integrazione a tutti i livelli aziendali. Questo cambiamento è dovuto ad un maggiore riconoscimento dei rischi collegati alla responsabilità ESG insieme ad un forte incentivo normativo di leggi e regolamenti tra cui *"Legge europea sul clima"* emanata nel 2021 e una nuova direttiva 2022/2464 UE sulla rendicontazione societaria di sostenibilità, la *CSRD*, *Corporate Sustainability Reporting Directive* emanata nel 2022.Attualmente questa è una sfida che coinvolge anche la funzione internal audit, che oltre aiutare il management a definire strategie e obiettivi, deve contribuire alla sensibilizzazione e al sostegno significativo delle iniziative ambientali. Bisogna coinvolgere tutte le persone presenti in azienda e fissare obiettivi, sia dal basso che dall'alto dell'azienda, per creare un processo completo che sia guidato da persone che vogliono che il cambiamento avvenga. L'internal audit, quindi deve avere un ruolo all'interno del progetto stesso, che si tratti di interlocutore diretto a supporto del disegno del nuovo sistema di controllo o, al limite, in affiancamento come supporto, al fine di identificare le competenze chiave e attivarsi al suo interno per garantirne la disponibilità.

La società di consulenza *Ernst&Young* ha presentato nella giornata del Convegno nazionale 2022 dell'AIIA un modello che organizza in quattro quadranti le possibilità d'azione dell'internal audit in ambito ESG, che è stato, per questo motivo, chiamato *"Modello dei IV quadranti"*. Questo modello serve per tracciare nuove strategie sostenibili, e classifica il potenziale ruolo dell'internal audit secondo due principali variabili. La prima riguarda un atteggiamento proattivo rispetto ad un atteggiamento reattivo, ovvero la capacità della funzione di anticipare i problemi e supportare la visione strategica dell'organizzazione. La seconda variabile invece riguarda una visione dell'IA all'interno dell'azienda da una figura di *"Policing"* ad una di *"Partner",* che rappresenta la capacità di supportare il cambiamento qualificandosi come un valido partner per il consiglio di amministrazione andando oltre il classico ruolo di controllore.

Rischi come l'Human, la cybersecurity e tutte le tematiche ESG, sono solo tre della più vasta gamma che le aziende si trovano a dover fronteggiare, ma sono serviti come esempio per comprendere che è necessario ridisegnare i processi organizzativi per mitigare gli effetti di questi eventi all'interno dell'azienda. I diversi assessment presentati nei vari paragrafi non sono tecnicamente diversi dalle solite operazioni che l'auditor è solito compiere per normali mappature del rischio, la principale differenza che richiedono questi processi è sulle competenze, che devono essere quella di saper comunicare con i vertici aziendali, di possedere una continuità operativa, *il Continuous audit* come strumento di predittività, e soprattutto si richiede all'internal auditor di essere un interlocutore strategico per tutto il sistema di controllo aziendale.