MANUALE
delle
PROCEDURE di AUDIT

Edizione Maggio 2024
Revisione n. 4

Redazione (Dirigente Responsabile)	**Approvazione** (Rappresentante Legale)	**Data**
Davide Di Capua Agecontrol S.p.A. 30.05.2024 11:44:08 GMT+01:00	Lorenzo Giachini 30.05.2024 16:33:23 GMT+02:00	

Aggiornamenti del Manuale

n° revisione	Descrizione dell'aggiornamento	Responsabile	Data
1	Introduzione *par. 6.3* Adeguamento agli *International Professional Practices Framework (Gennaio 2011)* Introduzione Allegati	Dirigente della Funzione Legale Rappresentante	Maggio 2011
2	Modifica della modalità di approvazione del manuale. Modifica del riferimento al Reg. CE n.885/2006 sostituito dal Reg. CE n.907/2014, che prevede un servizio di controllo interno che esprima una valutazione distinta di audit. Estensione dei compiti della Funzione Internal Auditing per lo svolgimento delle attività rappresentate dall'Organismo di Vigilanza. Modifiche della struttura organizzativa della Funzione Internal Auditing. Definizione e formalizzazione dell'intervento di audit anche attraverso la rappresentazione grafica delle varie fasi del processo di lavoro e delle unità organizzative coinvolte, con l'indicazione delle rispettive responsabilità. Ridefinizione delle modalità di archiviazione della documentazione di audit. Modifica degli allegati al presente manuale.	Dirigente della Funzione Legale Rappresentante	Aprile 2015
3	Modifica del riferimento alla determina dell'Amministratore Unico relativa alla struttura organizzativa della Funzione Internal Auditing.	Dirigente della Funzione Legale Rappresentante	Marzo 2016
4	Adeguamento del contesto di riferimento, in merito all'audit congiunto e alla interazione con Agea, e aggiornamento della metodologia. Revisione e riordino della sequenza e delle modalità di esecuzione degli interventi di audit. Aggiornamento degli allegati.	Dirigente responsabile Legale Rappresentante	Maggio 2024

Indice

PREMESSA

Il presente documento costituisce il punto di riferimento operativo della struttura organizzativa incaricata di svolgere le attività di Internal Audit, che per brevità viene di seguito indicata come "Struttura IA".

Il manuale viene adottato con l'approvazione formale del Legale Rappresentante, su proposta del Dirigente della Struttura IA, che ne ha curato la redazione/aggiornamento con la collaborazione delle risorse assegnate alla stessa struttura. Tutto il personale assegnato alla struttura adotta i principi, le regole e la metodologia, avendo cura di adeguare i propri comportamenti alle suddette disposizioni.

Il manuale viene aggiornato in funzione delle esigenze che ne richiedono la modifica.

PARTE I

ASPETTI DI CARATTERE GENERALE

1. CONTESTO DI RIFERIMENTO

La Struttura IA si posiziona, nell'organigramma aziendale, alle dirette dipendenze del Legale Rappresentante - a cui riferisce direttamente - ed è posta in posizione di indipendenza da tutte le strutture organizzative della Società.

I suoi obiettivi, tra gli altri, sono:

- assistere il vertice e l'organizzazione aziendale nel perseguimento dei suoi obiettivi di efficacia ed efficienza mediante un'attività indipendente e obiettiva di assurance e consulenza, finalizzata alla valutazione e al miglioramento dei processi di controllo, di gestione dei rischi e di corporate governance;
- assicurare la valutazione di adeguatezza e di effettivo funzionamento del Sistema di Controllo Interno in funzione del perseguimento degli obiettivi aziendali di efficacia ed efficienza delle operazioni, conformità a leggi, regolamenti comunitari, contratti e disposizioni interne, tutela del patrimonio aziendale, correttezza dell'informazione interna e esterna, anche nell'ottica della prevenzione della responsabilità amministrativa dell'azienda (D.Lgs. 231/2001), affidata all' Organismo di Vigilanza (OdV) e in conformità agli Standard Internazionali per la Pratica Professionale;
- assicurare il supporto all'OdV e al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), per quanto necessario, nello svolgimento delle attività di competenza.

In coerenza con gli indirizzi e le politiche aziendali, nonché con le richieste ricevute dal vertice societario, la Struttura IA assicura:

- la definizione delle politiche e procedure aziendali in materia di audit e la definizione del piano di audit da sottoporre all'approvazione del vertice societario;
- la mappatura dei rischi aziendali e il supporto metodologico alle strutture nelle attività di analisi e valutazione degli stessi, anche attraverso servizi di consulenza alle strutture interessate;
- la progettazione e la realizzazione delle attività di audit pianificate e di quelle di volta in volta richieste dal vertice societario, nonché il monitoraggio dei conseguenti piani di azione;
- la formalizzazione delle relazioni periodiche da presentare al vertice aziendale;
- il supporto all'OdV, nell'esercizio dei poteri ad esso demandati, nella gestione del "Modello di organizzazione gestione e controllo ai sensi del D.Lgs. 8 giugno 2001, n. 231", laddove necessario;
- il supporto per le attività di audit rappresentate dall'OdV per le aree di competenza di quest'ultimo.

2. ASPETTI ORGANIZZATIVI

2.1 Le finalità e responsabilità

La Struttura IA espleta, su richiesta del vertice aziendale, i compiti descritti nel Cap. 1, nell'ambito degli interventi di audit, inseriti nel piano di audit annuale, di cui al Cap. 4 del presente Manuale.

2.2 I principi deontologici di riferimento per il personale assegnato

Il personale della struttura IA si attiene ai principi del **Codice Etico** dell' "Institute of Internal Auditors", il cui scopo è promuovere la cultura etica nell'esercizio della professione di "internal auditor".
La credibilità e il raggiungimento di risultati positivi dell'attività, svolta dall'Internal Auditor si basano sulla fiducia che tutti devono riporre nell'obiettività dei servizi di assurance.

Infatti l'Internal Auditing, in base ai criteri accettati a livello internazionale, è definito come segue:
"Internal Auditing è una attività indipendente e obiettiva di *assurance* e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance".

Il personale della Struttura IA nell'esercizio della propria attività, deve attenersi ai *Principi* e alle *Regole di condotta* definiti dall'Institute of Internal Auditors, che di seguito si riportano.

I ***Principi***, fondamentali per la professione e la pratica dell'Internal Auditing, sono i seguenti:

Integrità
L'integrità dell'Internal Auditor consente lo stabilirsi di un rapporto fiduciario e quindi costituisce il fondamento dell'affidabilità del suo giudizio professionale.
Obiettività

- nel raccogliere, valutare e comunicare le informazioni attinenti all'attività o al processo in esame, l'Internal Auditor deve manifestare il massimo livello di obiettività professionale.
- l'Internal Auditor deve valutare in modo equilibrato tutti i fatti rilevanti, senza venire indebitamente influenzato da altre persone o da interessi personali nella formulazione dei propri giudizi.

Riservatezza
L'Internal Auditor deve rispettare il valore e la proprietà delle informazioni che riceve ed è tenuto a non divulgarle senza autorizzazione, a meno che lo impongano motivi di ordine legale.
Competenza
Nell'esercizio dei propri servizi professionali, l'Internal Auditor utilizza il bagaglio più appropriato di conoscenze, competenze ed esperienze.

Le ***Regole di Condotta***, che descrivono le norme comportamentali che gli Internal Auditor sono tenuti a osservare, sono le seguenti:

Integrità
L'Internal Auditor:

- deve operare con onestà, diligenza e senso di responsabilità;
- deve rispettare la legge e relazionare solo in merito a quanto previsto dalle leggi e dai principi della professione;

- non deve essere consapevolmente coinvolto in nessuna attività illegale, né intraprendere azioni che possano indurre discredito per la professione o per l'organizzazione per cui opera;
- deve rispettare e favorire il conseguimento degli obiettivi dell'organizzazione per cui opera.

Obiettività

L'Internal Auditor:

- non deve partecipare ad alcuna attività o avere relazioni che pregiudichino o appaiano pregiudicare l'imparzialità della sua valutazione. In tale novero vanno incluse quelle attività o relazioni che possano essere in conflitto con gli interessi dell'organizzazione;
- non deve accettare nulla che pregiudichi o appaia pregiudicare l'imparzialità della sua valutazione;
- deve riferire tutti i fatti significativi a lui noti, la cui omissione possa dare un quadro alterato delle attività analizzate.

Riservatezza

L'Internal Auditor:

- deve esercitare la dovuta cautela nell'uso e nella protezione delle informazioni acquisite nel corso dell'incarico;
- non deve usare le informazioni ottenute per vantaggio personale o secondo modalità contrarie alla legge o che siano di nocumento ai legittimi obiettivi dell'organizzazione.

Competenza

L'Internal Auditor:

- deve intraprendere solo quelle prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza;
- deve prestare i propri servizi in pieno accordo con gli Standard per la Pratica Professionale dell'Internal Auditing;
- deve continuamente migliorare la propria preparazione professionale, nonché l'efficacia e la qualità dei propri servizi.

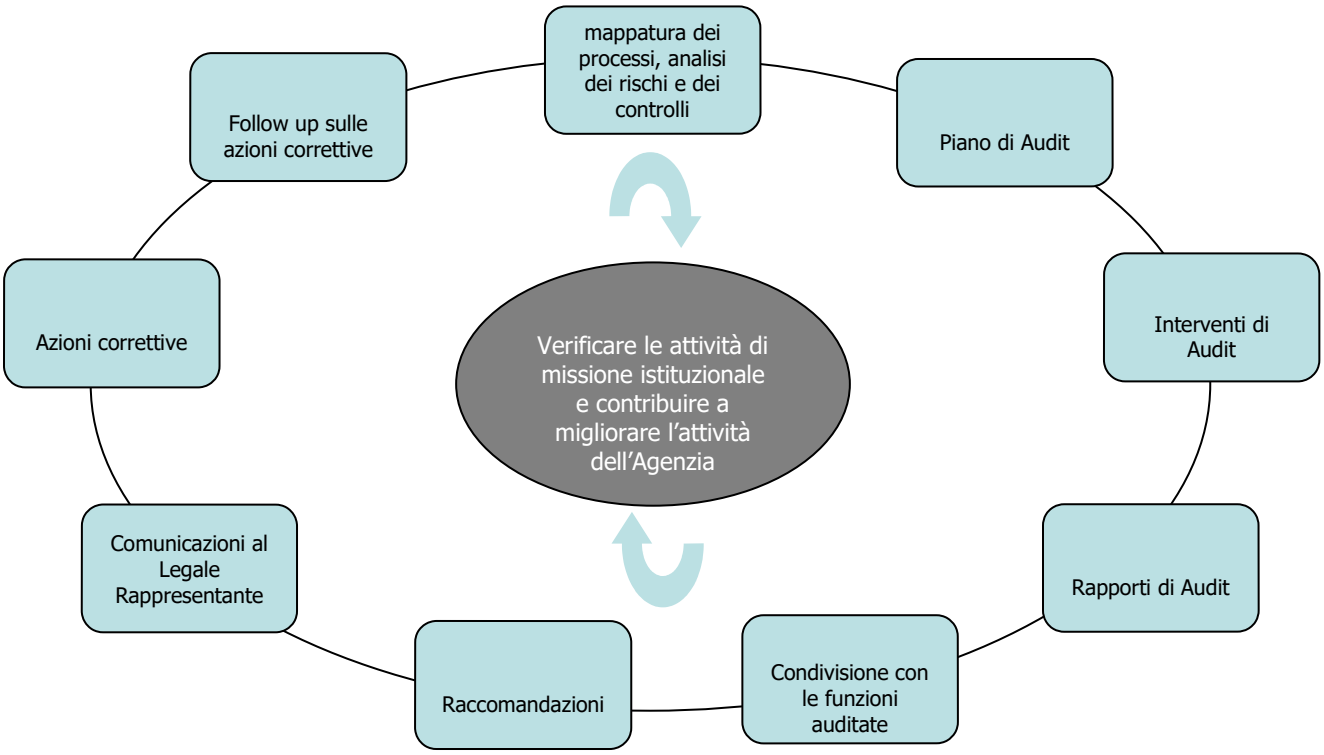
2.3 Le modalità di gestione delle informazioni della Struttura IA

Il personale assegnato ha completo accesso a tutta la documentazione e a tutte le informazioni necessarie all'esecuzione degli interventi programmati all'interno del piano di audit approvato dal Legale Rappresentante su proposta del Dirigente responsabile.
Il personale assegnato è tenuto all'assoluto riserbo relativamente alle informazioni ricevute o raccolte nel corso dell'attività e deve operare nel rispetto delle modalità di comunicazione stabilite.

2.4 Il processo di lavoro della Struttura IA

La metodologia e i criteri adottati consentono di avere un approccio dinamico, impostato al miglioramento continuo, nell'ambito del processo di audit, che prevede una interazione periodica ed un coinvolgimento attivo delle strutture della società e che può essere rappresentato come nella seguente figura.

Figura 1 – Processo di audit



Nei capitoli del presente Manuale dedicati alla descrizione degli aspetti di carattere operativo sono indicate nel dettaglio le modalità di esecuzione delle fasi tracciate nella figura soprastante.

3. METODOLOGIA DI RIFERIMENTO: IL PROCESSO DI VALUTAZIONE DEL RISCHIO "RISK ASSESSMENT"

Gli standard di riferimento, ossia quelli dell'Institute of Internal Auditors, contemplano una serie di indicazioni, a supporto delle attività dell'Internal audit, indicate come best practices.
La seguente metodologia - opportunamente personalizzata e adattata in ragione del contesto in cui opera la società e del modello di governance via via prescelto - rappresenta un modello di riferimento finalizzato alla focalizzazione degli interventi di Audit che si vogliono realizzare sui processi aziendali ritenuti maggiormente critici in funzione del perseguimento degli obiettivi aziendali.

Per tali interventi, sulla base della metodologia internazionale adottata, occorre definire, in via preliminare, un modello di mappatura dei processi di lavoro, di valutazione dei relativi rischi e controlli (cd. "Risk Assessment"), avendo individuato *l'universo dei rischi.*

3.1 La mappatura dei processi, dei rischi e dei controlli

La mappatura dei processi viene realizzata in collaborazione con tutte le strutture aziendali, acquisendo e analizzando la documentazione di lavoro (normativa comunitaria e nazionale, circolari e istruzioni, manuali delle procedure, specifiche tecniche ed altri documenti di lavoro) e intervistando il management e il personale apicale responsabile.

La metodologia adottata per effettuare la mappatura dei processi prevede una distinzione tra *processi,* legati agli obiettivi istituzionali e strategici della Società, e *sottoprocessi*.
Quindi per ogni processo vengono individuati i relativi sottoprocessi e descritte le relative attività svolte dal personale coinvolto.
La rilevazione del rischio inerente e del rischio residuo di ciascuna attività svolta scaturisce da un'attenta analisi congiunta del sistema di controllo.
La mappatura dei processi e al suo interno dei rischi ha l'obiettivo di identificare i rischi che possano pregiudicare il raggiungimento degli obiettivi istituzionali e strategici della Società e di valutare l'adeguatezza dei controlli posti a presidio delle "aree di rischio".

3.2 L'individuazione e la valutazione dei rischi inerenti

L'individuazione e la valutazione dei rischi di ciascun processo viene svolta congiuntamente in collaborazione con i responsabili dei processi, sulla base della metodologia del Control Self Risk Assessment (CSRA), mediante interviste al personale responsabile dei processi analizzati.
I rischi possono altresì essere identificati anche sulla base di documentazione acquisita (ad esempio risultanze di audit precedenti) inerente ai processi analizzati e/o sulla base delle esperienze assunte da processi/unità organizzative simili o con qualunque altro metodo ritenuto idoneo a tal fine.
Nell'effettuazione della valutazione dei rischi si adotta un approccio di tipo qualitativo basato su due parametri (impatto e probabilità dell'evento).

La stima dell'***impatto*** si basa sulla valutazione degli effetti che non sono necessariamente riconducibili a valori economico/finanziari. Una possibile classificazione degli effetti si articola in:

- effetti economico/finanziari: le perdite di valore possono essere determinate da vincoli/eventi esterni o da comportamenti legati all'ambiente interno;
- effetti di tipo legale (compliance): relativi a possibili sanzioni penali, civili o amministrative;
- effetti sull'immagine: sono collegati alla capacità di gestione dei rapporti e delle comunicazioni verso l'esterno e sulla percezione della Società da parte della Commissione Europea, del Ministero che ha la competenza nel settore agroalimentare italiano e di Agea.

Figura 2 - Stima dell'impatto

Livello		Parametri per la valutazione dell'impatto		
		Economico/ Finanziario	Compliance	Immagine
4	Alto	Impatto economico su costi e ricavi superiore al 10% per l'annualità corrente	Ricorsi e/o azioni giudiziarie con elevatissima probabilità di soccombenza; sanzioni civili, amministrative o penali (a carico del personale della società) di significativa rilevanza	Manifestazione di giudizio negativo su scala europea con ripercussioni sull'onorabilità della società
3	Rilevante	Impatto economico su costi e ricavi tra il 5% e il 10% per l'annualità corrente	Ricorsi e/o azioni giudiziarie con alta probabilità di soccombenza; sanzioni civili, amministrative o penali (a carico del personale della società) rilevanti	Manifestazione di giudizio negativo da parte dell'opinione pubblica, cittadini, stampa e dei gruppi di pressione a livello nazionale
2	Medio	Impatto economico su costi e ricavi tra il 2% e il 5% per l'annualità corrente	Ricorsi e/o azioni giudiziarie con probabilità di soccombenza; sanzioni civili, amministrative o penali (a carico del personale della società)	Manifestazione di giudizio negativo da parte dell'opinione pubblica, cittadini, stampa e dei gruppi di pressione a livello regionale
1	Basso	Impatto economico su costi e ricavi non superiore al 2% per l'annualità corrente	Ricorsi e/o azioni giudiziarie attivate con scarsa probabilità di soccombenza.	Manifestazione di giudizio negativo ingiustificate e strumentale da parte dell'opinione pubblica, cittadini, stampa e dei gruppi di pressione a livello locale

Per quanto riguarda la stima della ***probabilità***, sono previsti quattro livelli di probabilità di accadimento di un evento.

Per facilitare la stima della probabilità da parte del *Risk Owner*, sono identificate, per ciascuno dei livelli previsti, classi rappresentative dell'arco temporale nel quale si presume accada l'evento.

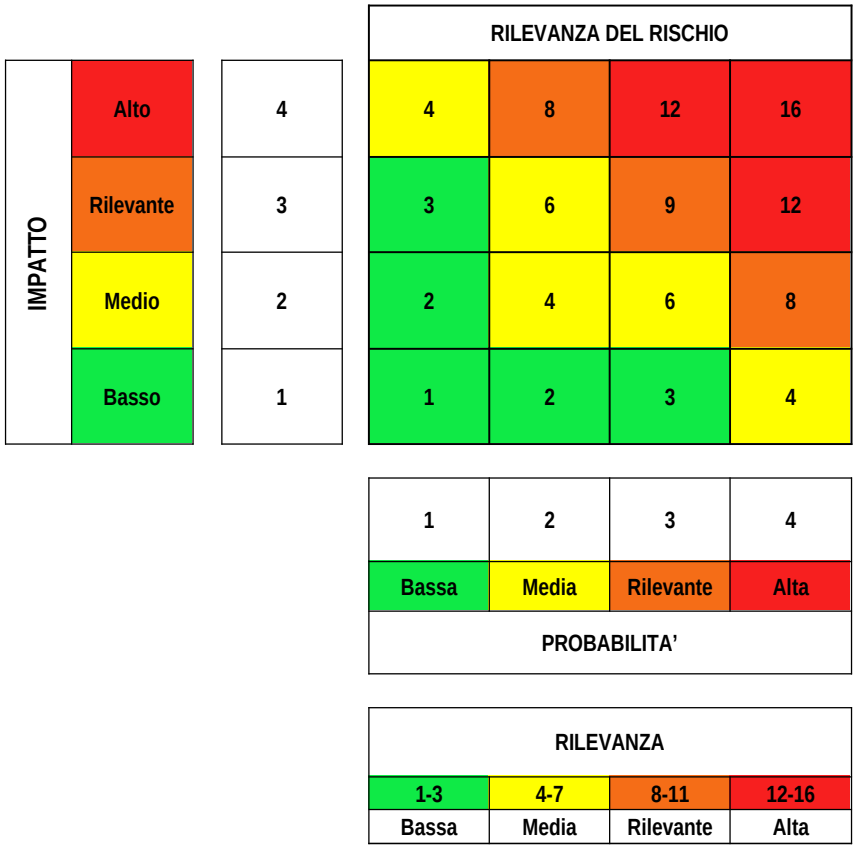
Figura 3 - Stima della probabilità

PROBABILITA'	BASSA	MEDIA	RILEVANTE	ALTA
	1	2	3	4
Frequenza attesa	una volta in più di 3 anni	Una o più volte in 3 anni	Una volta all'anno	Più volte all'anno

Sulla base della probabilità e dell'impatto definiti, è quindi possibile procedere con la valutazione del rischio inerente attraverso l'utilizzo dell'apposita matrice di raccordo.

La ***rilevanza di un rischio inerente*** (Alta, Rilevante, Media e Bassa) ***è determinata dal mix di probabilità e impatto*** secondo le possibili combinazioni (da 1 a 16) rappresentate nella seguente tabella.

Figura 4 - Matrice di raccordo "probabilità – impatto" per la valutazione dei rischi inerenti



3.3 La valutazione del sistema di controllo interno

A fronte dei rischi inerenti identificati, devono essere individuati quei controlli che consentono la loro mitigazione entro livelli accettabili.

Per la valutazione del sistema di controllo interno viene attribuito un rating o punteggio a ogni controllo (Adeguato = 0,2; Migliorabile = 0,6; Inadeguato = 1) sulla base di alcuni parametri di riferimento per la valutazione del controllo medesimo:

Figura 5 –Parametri di valutazione del sistema di controllo interno

Rating		Alcuni parametri di riferimento
0,2	ADEGUATO	▪ Esiste una adeguata struttura organizzativa formalizzata ▪ Il processo è disciplinato da procedure e politiche aziendali ▪ Sono presenti attività di controllo documentate ▪ Risulta un adeguato livello di segregazione delle mansioni ▪ Adeguata formalizzazione di deleghe e procure ▪ Il personale dispone delle necessarie competenze e know-how ed è svolta adeguata attività di formazione specifica ▪ Esistono adeguati sistemi informativi di supporto ▪ Esiste un'adeguata attività di monitoraggio del processo/attività
0,6	MIGLIORABILE	▪ La struttura organizzativa è definita e formalizzata ma le responsabilità non sono adeguatamente attribuite al personale ▪ Il processo è regolato da procedure applicabili, ancorché non aggiornate o carenti in alcuni aspetti ▪ Parziale segregazione delle mansioni ▪ Sono presenti attività di controllo ma non sono adeguatamente formalizzate ▪ I poteri/procure per operare non sono adeguatamente aggiornati ▪ Il personale sta consolidando il know-how ma necessita di aggiornamento o di formazione specifica ▪ Carenza dei sistemi informativi aziendali (completezza/accuratezza delle informazioni) ▪ Carente attività di monitoraggio del processo/attività
1	INADEGUATO	▪ La struttura organizzativa non è formalmente definita e formalizzata e le responsabilità non sono formalmente definite e attribuite al personale ▪ Assenza di procedure ▪ Assenza di segregazione delle mansioni ▪ Assenza di attività di controllo e relativa formalizzazione ▪ Assenza di poteri/procure formalmente conferiti ▪ Il personale non dispone di adeguate competenze e know-how e scarsa formazione del personale per lo svolgimento del processo/attività ▪ Assenza di sistemi informativi di supporto ▪ Assenza di sistemi di monitoraggio del processo/attività

3.4 La valutazione del rischio residuo

La valutazione del rischio residuo, ossia del livello di rischio conseguente alla riduzione del rischio inerente in misura corrispondente all'effetto del sistema di controllo interno, viene effettuata considerando il valore di rilevanza del rischio inerente (vedi paragrafo 3.2) e il livello del parametro associato al sistema di controllo interno rilevato (vedi paragrafo 3.3).

Figura 6 –Livelli di rischio residuo

			RISCHIO RESIDUO		
RILEVANZA	Alto	16	3,2	9,6	16
	Alto	12	2,4	7,2	12
	Rilevante	9	1,8	5,4	9
	Rilevante	8	1,6	4,8	8
	Medio	6	1,2	3,6	6
	Medio	4	0,8	2,4	4
	Basso	3	0,6	1,8	3
	Basso	2	0,4	1,2	2
	Basso	1	0,2	0,6	1
			0,2	0,6	1
			Adeguato	Migliorabile	Inadeguato

Il valore ottenuto ricadrà all'interno di uno dei quattro intervalli esplicativi del livello di rischio residuo, come evidenziato nella Tabella seguente, consentendo di determinare il rischio residuo (Alto, Rilevante, Medio, Basso).

RISCHIO RESIDUO			
0-3	3,1-7	7,1-11	11,1-16
Basso	Medio	Rilevante	Alto

I rischi inerenti con rilevanza alta e un sistema di controllo interno inadeguato determinano un rischio residuo alto, che dovrà essere oggetto di specifica attenzione e iniziative immediate da parte del vertice della società. Rischi inerenti con rilevanza alta e un sistema di controllo interno migliorabile o anche rilevanti e un sistema di controllo interno inadeguato dovranno essere adeguatamente presidiati con iniziative dei responsabili di processo da assoggettare ad approvazione da parte del vertice aziendale.

3.5 Il processo di aggiornamento del Risk Assessment

Il modello di Risk Assessment è aggiornato periodicamente, al fine di disporre di una situazione costantemente allineata della rischiosità dei processi, utile alla predisposizione del piano di audit.

L'aggiornamento del Risk Assessment comporta lo svolgimento delle seguenti attività nel corso di tutti gli audit programmati:

a) confermare e/o modificare la mappatura dei processi in oggetto di ciascun singolo intervento;
b) confermare e/o modificare la completezza dei rischi associati ai processi analizzati e i relativi controlli;
c) confermare e/o modificare la valutazione dei rischi già rilevati ed effettuare la valutazione dei nuovi rischi, in collaborazione con il responsabile del processo in oggetto;
d) esprimere un giudizio in merito ai controlli in essere, sulla base delle risultanze dell'intervento di audit svolto sul processo.

Il process owner aggiorna il modello dei processi gestito nell'ambito della propria struttura organizzativa sulla base:

- dei risultati delle attività di audit svolte;
- delle modifiche della normativa comunitaria e nazionale (es. introduzione di nuovi aiuti).

PARTE II

ASPETTI DI CARATTERE OPERATIVO

4. IL PIANO DI AUDIT

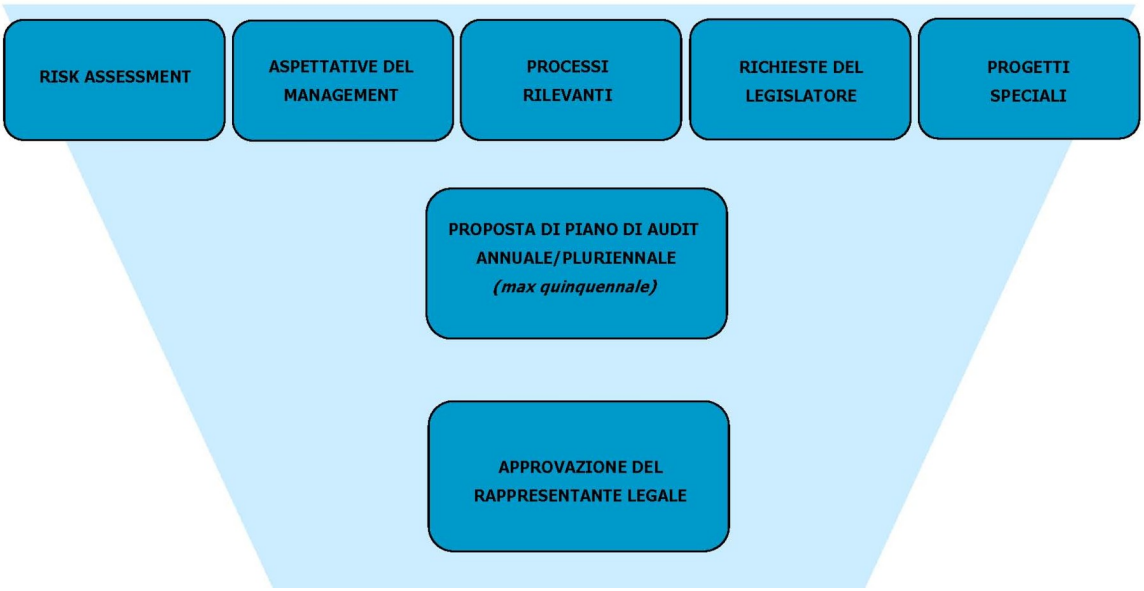
4.1 L'approccio metodologico alla formazione del piano di audit

L'attività annuale della Struttura IA è pianificata mediante il piano di audit proposto dal Dirigente responsabile (si veda allegato n.1) che recepisce le indicazioni del Vertice aziendale.

Il piano di audit deve:

- essere allineato alle esigenze di copertura del rischio determinate nel corso della periodica rilevazione delle aspettative dell'alta direzione e dell'attività di Risk Assessment;
- allocare le risorse sui processi aventi la maggiore rilevanza, ovvero che maggiormente concorrano al raggiungimento degli obiettivi istituzionali e degli obiettivi strategici della Società;
- tenere in considerazione eventuali altre esigenze manifestate dal vertice aziendale - nell'effettuazione di incarichi di consulenza e supporto finalizzati al miglioramento del sistema di controllo interno;
- tenere in considerazione l'esito degli interventi relativi ai Piani di audit degli anni precedenti.

Figura 6 - Processo di formazione del piano di Audit



4.2 Lo sviluppo congiunto delle aspettative per l'individuazione degli interventi sui processi critici aziendali

Per la definizione delle proposte di intervento da includere nel Piano di Audit è previsto lo sviluppo congiunto delle aspettative, basato su approfondimenti interni alla Struttura IA e tra il Dirigente Responsabile e il vertice aziendale.

Sono previste, in particolare, le seguenti attività:

- verifica delle esigenze del vertice aziendale nella copertura dei rischi;
- aggiornamento della "Matrice per la valutazione dei rischi", utilizzata nella valutazione di probabilità e impatto dei rischi dei processi, in caso di attuazione della metodologia di riferimento;
- verifica della disponibilità di risorse sulle quali la Struttura IA potrà contare nell'esercizio successivo, in considerazione delle eventuali richieste del vertice aziendale di svolgere progetti speciali;
- aggiornamento degli obiettivi cui deve tendere la Struttura IA.

Sulla base delle informazioni emerse in fase di sviluppo congiunto delle aspettative, si procede alla definizione della rilevanza dei processi da assoggettare all'attività di audit.

4.3 Le varie tipologie di intervento

Le tipologie di intervento della Struttura IA sono le seguenti:

- **Compliance Audit (Audit di conformità):** si focalizza sulla verifica della conformità alla normativa delle procedure adottate dalla Società e alla verifica di conformità dei comportamenti alle norme e procedure interne, applicabili al contesto delle strutture operative e delle operazioni sotto esame;
- **Operational Audit:** verifica/valuta l'adeguatezza, regolarità, affidabilità e funzionalità dei sistemi e processi/procedure, dei metodi (codificazione) e delle risorse in rapporto agli obiettivi, delle strutture organizzative;
- **Financial audit**: sono interventi finalizzati alla verifica dell'adeguatezza dei controlli contabili, amministrativi e finanziari esistenti. Il loro obiettivo è la verifica che vi sia una corretta e tempestiva rilevazione nella contabilità dell'ente e che i rendiconti economico-finanziari presentino in modo "veritiero e corretto" i risultati dell'esercizio e la situazione finanziaria e patrimoniale al termine dell'esercizio stesso. Sinteticamente le finalità di un audit finanziario possono riguardare l'affidabilità dei conti, la legittimità e regolarità delle operazioni e la verifica della sana gestione finanziaria;
- **Follow-up (Monitoraggio delle azioni correttive):** sono interventi per la verifica dell'effettiva implementazione dei piani di azione correttivi concordati con i responsabili dei processi, a fronte delle osservazioni rilevate nel corso di precedenti interventi di audit o di mappatura dei processi, della Funzione e condivise dai responsabili dei processi stessi.

4.4 La definizione del calendario secondo le priorità e l'individuazione del personale responsabile del controllo

Nella preparazione del Piano di Audit annuale, la Struttura IA verifica con il vertice aziendale il numero di persone necessarie per svolgere gli interventi pianificati e la necessità di effettuare inserimenti di risorse per il periodo di riferimento.

Tali valutazioni sono considerate nella predisposizione del Piano di audit.

4.5 La formalizzazione del Piano di audit e le sue eventuali variazioni

Le attività sui processi critici aziendali sono formalmente approvate, su proposta del Dirigente responsabile della Struttura IA formulata a seguito delle esigenze manifestate dal vertice aziendale, entro la fine dell'anno precedente quello cui il piano si riferisce.

Nel caso fosse ritenuto necessario apportare delle *modifiche al Piano di Audit*, queste devono essere comunicate al Rappresentante Legale e da questi formalmente approvate.

Per quanto concerne eventuali variazioni apportate alla pianificazione temporale degli interventi e delle risorse, queste debbono essere portate a conoscenza del vertice aziendale solo laddove significative.

4.6 Il contenuto del Piano di Audit

Il Piano annuale delle attività di audit riporta almeno le seguenti informazioni (si veda allegato n.1):

- **Processo:** processo aziendale posto sotto osservazione;
- **Struttura di riferimento:** la Funzione aziendale che svolge il ruolo principale nel processo auditato;
- **Tipologia di audit**: (audit di conformità, audit operativo, follow-up, risk assessment, altro);
- **Oggetto dell'intervento:** oggetto dell'audit e obiettivi che si intendono perseguire con l'esecuzione dell'intervento.

4.7 La pianificazione degli interventi

La pianificazione degli interventi inseriti nel Piano non va considerata immodificabile. Infatti, eventuali esigenze espresse dai responsabili dei processi e/o unità auditate potranno dar luogo, sulla base di elementi oggettivi, a una nuova pianificazione delle attività previste nel Piano di Audit.

5. L'INTERVENTO DI AUDIT

L'allegato n.2 *"Intervento di audit"* illustra il flusso completo delle attività di audit, che coinvolgono la Struttura IA, il vertice aziendale e l'unità organizzativa presso cui si svolge l'intervento di audit (struttura auditata).

Per ogni fase del flusso è riportato (in alto a sinistra) il numero del paragrafo in cui sono descritte in modo più dettagliato le attività che vengono svolte.

5.1 Definizione dell'oggetto di audit e riunione di apertura

Dopo aver svolto un'analisi sui tempi e le modalità da seguire per l'intervento in questione, viene preparata una comunicazione di "avvio" audit, da inviare alla struttura auditata e, per conoscenza, al vertice aziendale. Nella comunicazione, oltre a convocare la riunione di apertura, sono evidenziati:

- l'oggetto e le finalità dell'audit;
- i tempi e le modalità di svolgimento;
- la documentazione da predisporre.

Durante la *riunione di apertura,* di cui verrà dato apposito resoconto, devono essere presentati e discussi i seguenti argomenti:

- lo scopo e gli obiettivi dell'intervento, già definiti nella comunicazione di cui sopra;
- le modalità operative di esecuzione dell'intervento (ad esempio: interviste con il personale, analisi delle operazioni rilevanti, walk-through test[1], test sulle attività, rilevazione dei rischi, ecc.) e l'arco temporale ritenuto necessario, in via di massima;
- la documentazione che verrà prodotta (Relazione finale) e i relativi contenuti;
- le date dei successivi incontri da svolgere durante e al termine dell'intervento, sia con i responsabili della Funzione, sia con il personale operativo;
- varie ed eventuali.

Si sottolinea, infine, che nella riunione è importante evidenziare la finalità propositiva e migliorativa dell'intervento, allo scopo di ottenere la massima disponibilità e la positiva collaborazione del personale auditato.

5.2 Verbale di riunione e memorandum di pianificazione

Conclusa la riunione di apertura, ne verrà dato riscontro in un apposito verbale predisposto dall'internal auditor, a cui sarà allegato il "*Memorandum di Pianificazione dell'Intervento"* (si veda allegato n.3), contenente il dettaglio del Piano di attività dell'intervento di audit.
Il memorandum contiene la descrizione sintetica dell'intervento di audit e l'arco temporale previsto per l'esecuzione. Contiene inoltre l'elenco della documentazione da richiedere all'unità auditata.

Il "Memorandum di Pianificazione dell'Intervento" è composto dai seguenti paragrafi:

- **informazioni generali**
  brevi informazioni circa l'intervento pianificato;
- **aree/processi auditati**
  processi oggetto di audit e motivi per i quali sono stati selezionati;

[1] Il ***Walk-through test*** è un test attraverso cui l'internal auditor, acquisendo copia di tutti i documenti del flusso procedurale o delle porzioni del processo che intende esaminare, verifica la corretta rilevazione del processo o della procedura in esame.

- **obiettivi dell'audit**
  obiettivi generali dell'intervento;
- **dettagli di pianificazione - lista dei documenti necessari**
  modalità di esecuzione dell'audit e lista dei documenti (normativa, procedure, ecc.) che dovranno essere resi disponibili presso gli uffici dell'unità auditata.

In definitiva, il "Memorandum di Pianificazione dell'Intervento" rappresenta il disegno di massima dei tempi e delle attività necessarie allo svolgimento dell'intervento e consente, quindi, di stimare il livello di supporto atteso da parte dei responsabili dei processi auditati.

5.3 Acquisizione e analisi della documentazione necessaria all'intervento

Sulla base di quanto stabilito nel "Memorandum di Pianificazione dell'Intervento", dovrà essere assicurata la disponibilità delle seguenti informazioni/documentazioni e approfonditi gli aspetti di seguito indicati:

- individuazione dei responsabili dei processi interessati, che dovranno essere contattati per concordare lo svolgimento dell'intervento;
- informazioni/dati sui quali operare il campionamento delle operazioni che saranno analizzate nel corso dell'intervento;
- disposizioni normative comunitarie e nazionali, procedure e piani operativi del regime di aiuto dei quali deve essere verificata l'applicazione (solo per interventi di audit in ambito ispettivo);
- interviste formalizzate e condivise con i soggetti coinvolti nelle attività;
- risultati e rapporti di interventi precedenti sulle unità/processi auditati;
- carte di lavoro e check-list prodotte per lo svolgimento di precedenti interventi su processi/unità auditate o interventi simili in termini di strategie/obiettivi/processi/unità auditate;
- risultati e rapporti emanati da organismi di controllo comunitario o da altri organismi di controllo esterni (es. Corte dei Conti, Ministero che ha la competenza nel settore agroalimentare italiano, Commissione UE, Agea);
- manuali di procedure;
- mappa dei processi;
- contratti/convenzioni/protocolli/specifiche tecniche;
- eventuale altra documentazione ritenuta utile allo svolgimento dell'intervento.

I responsabili dei processi interessati inviano quanto richiesto nei termini stabiliti e formalizzati nella riunione di apertura, nonché nel formato cartaceo e/o elettronico specificato.
L'inosservanza dei tempi concordati formerà oggetto di specifica osservazione nella Relazione conclusiva.
Qualora le attività programmate subiscano, per motivi esterni e indipendenti dall'operatività degli auditor, dei ritardi tali da poter pregiudicare il completamento del Piano annuale di Audit, il Dirigente della Struttura IA ne porta formalmente a conoscenza il vertice aziendale.

In seguito all'analisi del materiale esistente e in funzione degli obiettivi dell'intervento dovranno essere definite le priorità in termini di verifiche, nonché le procedure di controllo da seguire.
Dovranno essere individuati, pertanto, gli aspetti significativi da porre sotto osservazione (ad esempio il rispetto delle procedure autorizzative, della normativa di riferimento, ecc.) al fine di verificare che i processi della struttura auditata siano in linea con gli obiettivi definiti, le deleghe sottoscritte, le procedure di riferimento, la legislazione vigente e quant'altro pertinente.

L'analisi della documentazione si conclude con la predisposizione di una o più check-list sulla base delle quali eseguire i controlli.
Il formato della check-list (si veda allegato n.4) prevede, per ogni item:

- l'esito del controllo (non applicabile, positivo, negativo);
- l'evidenza del controllo (non applicabile, documentale, elettronica, intervista, osservazione);
- eventuali commenti;
- eventuali riferimenti al documento di definizione dell'oggetto, di cui al punto 5.2.

Le evidenze riscontrate e registrate nelle check-list, anche se emerse dall'analisi di un sottoinsieme di casi esistenti (attraverso il campionamento), costituiscono gli elementi oggettivi (le "osservazioni") di sostegno alla dimostrazione di eventuali "criticità", e sono inoltre funzionali all'indicazione del percorso da seguire con le azioni correttive/migliorative da intraprendere.

5.4 L'esecuzione dell'intervento di audit

Nel corso dell'esecuzione dell'intervento di audit, gli auditor devono raccogliere tutti gli elementi necessari a supportare, con adeguate prove documentali, le criticità riscontrate. Tutte queste evidenze (documentazione, analisi svolte, carte di lavoro, ecc.) devono essere adeguatamente archiviate per dimostrare l'inequivocabilità e l'oggettività di quanto rilevato.

Per individuare un sottoinsieme di casi significativi da porre sotto osservazione, laddove sia improponibile l'esame dell'intero universo, si dovrà seguire la metodologia del "campionamento" descritta nel paragrafo 5.10.

Al termine dell'intervento, l'auditor garantisce che tutta la documentazione, di supporto al rapporto dell'intervento, sia stata raccolta e archiviata presso la Struttura IA.

Inoltre, l'auditor rileva le esigenze di aggiornamento del Risk Assessment confermando i rischi esposti, riportando quelli individuati nel corso dell'intervento ed esponendo la valutazione dei controlli rilevati.

5.4.1 Lo svolgimento dei test sui controlli dei processi

Nell'ipotesi di porre sotto osservazione il sistema di controllo dei processi, limitatamente ad alcuni specifici aspetti, l'obiettivo dell'intervento di audit sarà valutare l'adeguatezza dei controlli posti in essere per mitigare i rischi collegati al processo.

L'attività di audit ha un primo scopo nella verifica e valutazione dell'efficacia del controllo posto in essere per ridurre il rischio. Scopo ulteriore consiste nel verificare l'efficienza del controllo e, quindi, rilevare casi di rischi eccessivamente controllati, che richiedono una razionalizzazione dei presidi in essere.

In particolare, in fase di identificazione e valutazione dei controlli associati ai rischi è necessario:

- identificare i controlli associati ai rischi significativi;
- valutare l'efficacia del controllo nel prevenire il rischio;
- identificare aree di miglioramento nei processi e nei relativi controlli;
- identificare le criticità e condividerle con il management.

L'attività di identificazione dei controlli dei processi è effettuata nella fase di rilevazione e analisi dei processi. Sulla base di quanto emerso in questa attività, viene predisposto un programma di test

sui controlli. In particolare l'auditor deve eseguire i test descritti in tale programma, avendo valutato se il disegno dei controlli è adeguato ovvero se è possibile individuare aree di miglioramento.

Nell'eseguire il test su un controllo di processo, si effettua una valutazione al fine di determinare se:

- opera come dovrebbe;
- è applicato per tutto il periodo di tempo previsto per la copertura efficace del rischio associato;
- è eseguito tempestivamente tutte le volte che si rende necessario;
- copre tutte le operazioni a cui è applicabile;
- si fonda su informazioni affidabili (ad esempio l'utilità di un controllo su un report dipende dall'affidabilità dai dati contenuti);
- corregge tempestivamente gli errori che identifica.

Se a presidio di un'unica fase del processo esaminato sono previsti più controlli, non è necessario testarli tutti, ma solo quelli che si ritengono più affidabili/efficaci nella mitigazione del rischio. La scelta dipende dalla valutazione se:

- è probabile che il controllo riesca a raggiungere gli obiettivi per cui è stato istituito;
- il controllo può essere testato in modo più efficace ed efficiente di altri controlli;
- si ritiene che un controllo copra più rischi, lo stesso test di quel controllo può supportare tutti gli obiettivi di controllo dei rischi.

In tal caso, occorrerà rilevare la situazione sopra descritta facendola emergere tra gli aspetti di miglioramento.

Durante l'esecuzione del test, l'auditor deve esaminare, osservare e verificare l'evidenza fisica dei risultati della procedura di controllo, inclusi quelli di routine. La modalità con cui viene rilevata l'evidenza è indicata nella check-list (si veda allegato n. 4).

Ad esempio, nel testare una riconciliazione di routine si può:

- **Esaminare (colonna "Intervista" della check.list)**. Si può chiedere al personale che prepara la riconciliazione, quali sono le voci normalmente da riconciliare, il perché sono tali, e la procedura in essere che assicura che eventuali anomalie nelle registrazioni contabili sono costantemente individuate e tempestivamente corrette. Si può inoltre domandare come il Management si assicura che le riconciliazioni siano corrette, predisposte tempestivamente e costantemente riviste e approvate da personale terzo rispetto a chi ha eseguito le riconciliazioni stesse.

- **Osservare (colonna "Osservazione"" della check.list)**. Si può osservare la predisposizione di una riconciliazione, pur sapendo che il personale, quando è osservato, conduce l'attività più diligentemente.

- **Verificare l'evidenza fisica (colonna "Documentale" della check.list)**. Si devono esaminare i documenti di supporto alle voci in riconciliazione aventi maggiore significatività, al fine di ottenere l'evidenza che le procedure sono state eseguite correttamente. Inoltre, è auspicabile ottenere evidenze di come eventuali eccezioni o elementi inusuali sono stati trattati, in modo da verificare se questi sono stati gestiti in maniera adeguata. In quest'ambito viene verificata la tracciabilità dei controlli effettuati dal soggetto auditato.

- **Acquisire le evidenze (colonna "Elettronica" della check.list).** Si può ottenere l'evidenza del controllo effettuato attraverso applicazioni informatiche, al fine di ottenere l'evidenza che le procedure sono state eseguite correttamente.

Nell'esecuzione del test, l'auditor deve acquisire l'evidenza fisica/documentale dei controlli effettuati e, in caso di assenza di evidenze fisiche dell'efficacia del controllo ovvero di registrazione del medesimo, dovrà maturare il proprio giudizio professionale sulla efficacia dei controlli, utilizzando più di una tra le diverse modalità di verifica soprariportate, alternandole e integrandole secondo la più efficace combinazione possibile.

È necessario utilizzare il proprio giudizio professionale nel determinare l'estensione dei test sui controlli dei processi. Ciò avviene mediante il metodo del campionamento, di cui al punto 5.9.

I fattori da considerare sono:

L'affidabilità del controllo. I livelli di affidabilità/confidenza (o certezza) mutano in relazione agli strumenti utilizzati: controlli manuali ovvero automatizzati, di cui al punto 6.3. Laddove i processi, le operazioni da verificare e i controlli poggiano su specifiche applicazioni e tecnologie informatiche, occorre effettuare un preliminare audit di sistema, per verificare l'esistenza di importanti punti di debolezza e in tal caso affermare che il rischio di errori rilevanti è elevato (con un livello di affidabilità fornito dal sistema basso e il livello di confidenza alto) e maggiori saranno le dimensioni del campione. Se il sistema non presenta importanti punti di debolezza, il rischio di errori rilevanti è basso e il livello di affidabilità fornito dal sistema è alto, il che significa che il livello di confidenza che deve essere applicato per il campionamento delle operazioni sarà basso e minori saranno le dimensioni del campione. Allo stesso modo il test sui controlli manuali, per loro natura di minore affidabilità, deve essere esteso.

La persuasività dell'evidenza prodotta dal controllo. Se i risultati del controllo forniscono evidenze scarse o indirette che il controllo opera efficacemente, il test fornisce la garanzia necessaria. D'altra parte, se l'evidenza è persuasiva, si può decidere di esaminare solo un ammontare limitato di evidenze.

Necessità di assicurare che il controllo operi come previsto per tutto il periodo preso in considerazione. Nel pianificare le procedure di verifica, si deve valutare l'arco temporale da considerare e le evidenze da produrre in tempi diversi all'interno del periodo di riferimento. Più è lungo l'arco temporale, più è necessario aumentare il livello di controllo.

Altri fattori relativi alla probabilità che il controllo operi come previsto. Nel determinare l'estensione dei test sui controlli, si devono considerare i fattori che riguardano la percezione della probabilità che il controllo operi come previsto durante tutto il periodo di riferimento. Questi includono:

- il livello di turn over del personale;
- supervisione del lavoro svolto;
- formazione e competenza del personale;
- la probabilità che il controllo sia omesso durante periodi di lavoro intenso (picchi di lavoro);
- la possibilità di omettere il controllo da parte del responsabile;
- la presenza di fattori di rischi di frode che sono stati identificati e non sufficientemente mitigati da altri controlli.

Nel valutare i controlli si deve esprimere un giudizio sulla loro efficacia. Nel caso in cui dal test emerga che il controllo in essere garantisce, in riferimento alle procedure di controllo eseguite, la copertura del rischio, il controllo si deve ritenere efficace. Viceversa se dal test emerge l'inefficacia del controllo, l'auditor deve assicurarsi di avere tutte le *prove documentali* necessarie per dimostrare in modo oggettivo che il controllo analizzato non garantisce la copertura del rischio associato. Questo aspetto è fondamentale per sostenere le proprie argomentazioni in fase di condivisione delle criticità con il responsabile del processo auditato.

L'attività svolta deve essere sintetizzata nella check-list di cui al paragrafo 5.3, secondo le modalità ivi descritte.

5.4.2 La documentazione da produrre nel corso di un intervento di audit

Tutta la documentazione ricevuta e prodotta durante l'attività, se ritenuta significativa, deve essere referenziata e allegata alle carte di lavoro relative al test svolto.

L'attività di documentazione ha la funzione di:

- fornire traccia del lavoro eseguito anche per i successivi interventi;
- mantenere le evidenze delle criticità riscontrate;
- fornire una base per la revisione dell'attività di audit.

Elementi essenziali da prodursi e allegarsi al fascicolo dell'intervento sono i seguenti:

- corrispondenza e comunicazioni intercorse con i soggetti auditati e con il "committente";
- verbali di riunione;
- memorandum di pianificazione;
- moduli di rilevazione delle evidenze (check-list) ;
- documentazione di supporto alle osservazioni incluse nella Relazione finale;
- Relazione finale.

5.5 La Relazione finale di audit

La Relazione finale di un intervento di audit (si veda allegato n.5) rappresenta il punto conclusivo dell'attività svolta, nonché il momento di assunzione della responsabilità in ordine all'interpretazione dei fatti osservati e alla formulazione delle valutazioni e dei suggerimenti.

Tale Relazione deve rappresentare il resoconto obiettivo, essenziale e completo di quanto fatto in sede di accertamento e, allo stesso tempo, l'esposizione veritiera, motivata e documentata delle evidenze significative analizzate.

Se durante l'intervento venissero rilevate anomalie gravi, queste dovranno essere immediatamente comunicate alla struttura auditata e al vertice aziendale, affinché siano apportati gli opportuni interventi correttivi.

Una bozza della Relazione finale dovrà essere inviata in via preliminare alla struttura auditata affinché, in sede di riunione di chiusura, gli argomenti trattati, le criticità riscontrate e gli interventi correttivi o migliorativi proposti possano essere valutati e – possibilmente – già condivisi.

Nella Relazione finale dovranno essere elencate le attività e i processi esaminati e cioè gli elementi che vengono definiti come *l'oggetto e l'ampiezza dell'Audit*. Questi due elementi sono

fondamentali: chiunque riceva una Relazione di audit deve conoscere, infatti, chiaramente i limiti che hanno caratterizzato la portata dell'operazione di accertamento, anche al fine di valutarne e interpretarne correttamente i risultati.

Se nel corso della verifica l'auditor ha fatto ricorso a test di accertamento e convalida, occorrerà che ne siano precisati i limiti e che siano illustrati i criteri di scelta dei campioni utilizzati, nel caso in cui ciò incida sulla significatività dei risultati.

Particolare importanza riveste la *segnalazione dell'epoca* in cui l'audit è stato effettuato: i fenomeni rilevati ed espressi in termini quantitativi e qualitativi risultano validi e significativi nel momento dell'accertamento e pertanto, in tempi successivi, devono essere considerati alla luce della situazione ambientale del momento di osservazione e delle successive evoluzioni della normativa e della realtà aziendale.

Il contenuto della Relazione finale si articola idealmente in tre parti:

- la prima parte è introduttiva e ha lo scopo di descrivere l'intervento di audit (durata, luogo, lettera d'incarico, ecc.), il processo analizzato con i sub processi in esame (facendo anche riferimento alle strutture organizzative interne interessate dall'intervento) e infine la documentazione di riferimento (descrivendo sinteticamente la normativa esterna e interna, cioè le circolari e/o procedure operative esistenti);

- la seconda parte descrive le modalità di svolgimento del lavoro (interviste effettuate, selezione del campione da sottoporre a test, esecuzione dei test);

- nella parte conclusiva, infine, vengono esposte le criticità emerse e le relative raccomandazioni e spunti di miglioramento.

Le criticità possono scaturire:
- da una *non-conformità* fra procedura di riferimento e comportamento organizzativo rilevato;
- dall'inefficacia del controllo a limitare il rischio esistente;
- da un'eccessiva presenza di controlli per uno stesso rischio che, in una valutazione di costi-benefici, rappresenta una diminuzione di efficienza.

La presenza o meno della criticità richiede all'auditor di esprimere un parere professionale per la rimozione della stessa. Questo parere costituisce una "raccomandazione"[2].
In presenza di osservazioni che non costituiscono criticità, ma temi di attenzione del sistema di controllo interno, l'auditor li formalizza come *azioni migliorative*.

5.6 La riunione di chiusura

Come detto nel precedente paragrafo, la Relazione finale viene inviata in bozza ai responsabili dei processi interessati dall'intervento, che hanno gli strumenti per porre in essere le azioni correttive e/o migliorative proposte, per essere poi oggetto di discussione nell'ambito di una specifica riunione.

Lo scopo della riunione è condividere i risultati dell'attività di audit per assicurarsi che non ci siano stati fraintendimenti o interpretazioni errate dei fatti evidenziati, e fornire ai responsabili delle

[2] Lo standard professionale dell'Associazione Italiana Internal Auditors (AIIA) di riferimento è quello del **2024**.

Funzioni auditate l'opportunità di chiarire specifici argomenti o di esprimere i propri punti di vista circa i rilievi, le conclusioni e le raccomandazioni esposte nella Relazione.

Nel corso della riunione di chiusura si dovranno discutere e condividere le raccomandazioni e gli spunti di miglioramento con gli adeguati livelli di responsabilità, al fine di elaborare azioni idonee a rimuovere le criticità emerse. Sebbene l'auditor abbia già indicato tra le raccomandazioni e gli spunti di miglioramento le azioni idonee alla rimozione della criticità, ciò non toglie che il Responsabile della struttura auditata possa proporre azioni ritenute maggiormente appropriate.

In particolare nel corso della riunione devono essere necessariamente concordate:

- le azioni ritenute idonee a rimuovere le criticità riscontrate (qualora vi sia dissenso tra raccomandazioni proposte e azioni definite dalla struttura auditata, tale dissenso deve essere esplicitato);
- la data entro la quale il Responsabile della struttura auditata si impegna a inviare alla Struttura IA il *Piano di azione.* L'invio del Piano di azione deve essere necessariamente previsto entro un congruo periodo di tempo (in linea di massima un mese), a partire dalla data in cui si è svolta la riunione di audit.

L'esito della riunione di chiusura deve essere formalizzato con un *verbale di riunione,* redatto a cura di uno degli auditor, e composto dalle seguenti sezioni:

- luogo e data della riunione;
- nome e ruolo dei partecipanti alla riunione;
- descrizione degli argomenti oggetto di discussione;
- osservazioni emerse in sede di riunione, quali soprattutto:
    - modifiche – condivise - da apportare alla Relazione finale di audit;
    - data prevista per la comunicazione del Piano di azione da parte della struttura auditata.

Il verbale di riunione deve essere condiviso con il Dirigente della struttura auditata.

La piena condivisione delle criticità, delle raccomandazioni e degli spunti di miglioramento risulta estremamente importante per consentire di formalizzare entro tempi brevi la Relazione finale di audit, per l'invio al vertice aziendale.

5.7 La chiusura dell'audit – invio Relazione finale

La Relazione di audit, già eventualmente integrata con le ulteriori osservazioni emerse nel corso della riunione di chiusura, viene inviata al vertice aziendale e alla struttura auditata.

Nella comunicazione a cui è allegata la Relazione finale è necessario esplicitare che si è concordata la realizzazione del Piano di azione, da parte della struttura auditata, entro un termine definito e che l'effettiva attuazione delle azioni correttive/migliorative descritte nel Piano sarà oggetto di verifica, da parte dell'Internal Auditing, mediante l'intervento di *follow-up*.

5.8 L'intervento di follow-up (Monitoraggio delle azioni correttive/migliorative)

5.8.1 La pianificazione dell'intervento – la tavola di follow-up

La riunione di chiusura di audit sancisce, di fatto, l'avvio dell'attività di follow-up, attraverso la quale si dovrà accertare se quanto raccomandato, discusso e condiviso nella riunione, e successivamente confermato nel Piano di azione, è poi stato effettivamente attuato.

Il follow-up è l'intervento per la verifica dell'effettiva implementazione dei piani di azione concordati con i responsabili dei processi, a fronte delle osservazioni rilevate nel corso di precedenti interventi della Struttura IA e condivise dai responsabili dei processi stessi.

In altre parole, si effettua un monitoraggio sulla realizzazione delle azioni correttive inserite dalla struttura auditata nel Piano di azione al fine di valutare l'efficacia, nonché la tempestività dello stesso, nel rimuovere le anomalie riscontrate.

La Tavola di follow-up (si veda allegato n.6) è lo strumento utilizzato per raccogliere, monitorare e analizzare lo stato di realizzazione dei piani d'azione predisposti dalla struttura auditata.

La tavola, oltre a riportare - nell'intestazione - l'indicazione del processo e dell'eventuale sub-processo, dell'unità auditata, della data di trasmissione della relazione finale e della data di rilevazione delle azioni da implementare, è costituita dalle seguenti sezioni:

- **Tipo**: riporta la tipologia dell'osservazione rilevata. A tal fine sono state stabilite le seguenti codifiche:
  - CI= la raccomandazione è volta a migliorare l'efficacia del sistema di controllo interno;
  - EF= la raccomandazione è volta a rendere maggiormente efficiente il processo analizzato.
- **Osservazione**: descrive sinteticamente l'osservazione, il rischio e la raccomandazione riportata nella Relazione finale di audit.
- **Azione da implementare**: riporta la specifica azione che la struttura auditata si era impegnata a implementare, con il Piano di azione, per rimuovere la criticità riscontrata durante l'intervento di audit. Nel corso delle verifiche di follow-up, le azioni possono subire variazioni, non solo perché il responsabile può aver modificato la propria idea originaria, ma anche per impossibilità oggettive che si sono manifestate nel frattempo. In tal caso l'auditor ne darà evidenza nella Relazione finale.
- **Data prevista:** riporta la data (dal Piano di azione) entro la quale la struttura auditata si è impegnata a implementare l'azione di riferimento, sia con un proprio intervento che attraverso il coinvolgimento di altre unità organizzative aziendali. Anche in questo secondo caso la responsabilità dell'effettiva implementazione dell'azione ricade sulla struttura auditata.
- **Data completamento**: riporta la data nella quale è stata completata l'azione e quindi la decadenza dell'osservazione. Ovviamente tale data è riportata solamente se nel corso dell'intervento di follow-up viene riscontrata l'effettiva implementazione di adeguate azioni correttive alla criticità riscontrata originariamente.
- **Status**: riporta lo stato di avanzamento della raccomandazione inserita nel Piano di azione. A tal fine sono state stabilite le seguenti codifiche:
  - **I**= l'azione è stata implementata e quindi l'osservazione ha perso la sua ragione d'essere;
  - **N**= l'azione non è stata implementata e quindi l'osservazione è ancora in essere.
    In questo caso è necessario esplicitare le motivazioni che non hanno permesso l'implementazione dell'azione (es.: ritardi non dipendenti dalla volontà della struttura

auditata, cambiamento normativo/organizzativo interno che non richiede più alcuna azione, ecc.).

- **Note**: eventuali indicazioni esplicative.

5.8.2 La Relazione finale di follow-up

Al termine di ciascun intervento dovranno essere comunicati i risultati raggiunti al vertice aziendale e alla struttura auditata. Tale comunicazione avviene mediante la Relazione predisposta dal Dirigente della Struttura IA.

Nella Relazione deve essere evidenziato se i risultati attesi sono stati raggiunti o se persistono carenze nel sistema di controllo interno relative a rischi che, anche se ritenuti "alti" o "rilevanti", sono accettati nella esclusiva responsabilità della struttura auditata (si veda il paragrafo 5.8.3).

In dettaglio, la Relazione di follow-up (si veda allegato n.7) si articola idealmente in tre parti:

- la prima parte è introduttiva e ha lo scopo di richiamare l'intervento di audit da cui sono emerse le criticità rilevate nel sistema di controllo interno;
- la seconda parte descrive le modalità di svolgimento del lavoro;
- la terza parte riepiloga gli esiti delle attività di follow up, con evidenza delle azioni correttive intraprese, distinte fra implementate e non implementate (come indicato nel paragrafo precedente). In tale parte viene anche espresso un giudizio in relazione alla capacità delle azioni intraprese di mitigare i rischi e/o alla sussistenza di carenze nel sistema di controllo interno che, come precedentemente detto, sono accettati nella esclusiva responsabilità della struttura auditata.

5.8.3 L'accettazione del rischio

Il responsabile della struttura auditata, qualora ritenga che non si renda più necessario o risulti troppo complessa o onerosa l'attuazione degli interventi proposti nel Piano di azione (si veda il paragrafo 3.2), può assumersi la responsabilità della mancata implementazione accettandone il rischio conseguente, anche se ritenuto "alto" o "rilevante".

L'accettazione del rischio deve sempre risultare dalla Relazione di follow-up.

5.9 Il Campionamento

L'attività di verifica nell'intervento di audit non consente di norma, né ha come obiettivo, di esaminare il 100% di un determinato "fenomeno" oggetto di analisi.

Il personale della Struttura IA, dovendo tuttavia formulare un giudizio professionale sul "fenomeno" stesso, potrà ricorrere alla selezione e analisi di alcuni "item" che fanno parte del fenomeno, per cercare di comprenderlo nel suo complesso. Tale attività di selezione costituisce il "campionamento".

5.9.1 I metodi di campionamento

La selezione del campione di oggetti può essere effettuata sulla base di due distinti metodi o dalla combinazione dei due: il **metodo statistico** e il metodo basato sul **giudizio professionale** (*metodo non statistico*).

La selezione effettuata sulla base del metodo statistico determina l'ampiezza del campione sulla base del calcolo delle probabilità.
Nel metodo non statistico l'ampiezza del campione viene decisa dal personale della Struttura IA, che ne informa il Dirigente, sulla base della propria valutazione professionale.

La decisione se utilizzare un metodo statistico o meno per la selezione di un campione di operazioni attiene al giudizio professionale dell'auditor riguardo alla modalità ritenuta maggiormente efficace per ottenere evidenze di revisione nelle specifiche circostanze. Ad esempio, nella selezione dei test dei controlli, l'analisi del revisore sulla natura e sulla causa degli errori è certamente più importante che non l'analisi statistica della mera presenza o assenza degli errori. In questa situazione un approccio di selezione non statistico potrebbe essere più appropriato.

La scelta di quale approccio seguire dipende quindi dalla situazione esaminata; tuttavia il metodo utilizzato deve garantire prove evidenti per raggiungere gli obiettivi prefissati nel test.

5.9.2 La scelta del metodo di campionamento

Come già evidenziato, il metodo di campionamento da preferire è la selezione non statistica, in particolare nel caso in cui l'universo da esaminare è composto da un limitato numero di oggetti.

L'utilizzo eventuale di tecniche statistiche può essere necessario in caso di specifiche esigenze di approfondimento di eventuali temi o anomalie riscontrate, oppure nel caso di popolazioni numerose.

La metodologia da adottare è individuata, comunque, dopo aver valutato i dati qualitativi e quantitativi più significativi, quali, a titolo di esempio:

- analisi dei requisiti dei controlli richiesti;
- analisi dei soggetti controllati (struttura, dimensioni, ubicazione);
- numero di controlli con esito negativo;
- numero di sanzioni erogate a beneficiari;
- risultanze di precedenti audit e follow-up.

5.9.3 La selezione sulla base del giudizio professionale

Rientrano sotto questa categoria le seguenti tipologie di selezione:

- la selezione del 100% della popolazione;
- la selezione di specifici items;
- la selezione a campione non statistico.

Selezione di tutti gli items: il personale della Struttura IA può decidere di esaminare l'intera popolazione di items che compongono l'universo oggetto di test.
L'esame del 100% delle operazioni può essere applicato alle procedure di verifica di sostanza e potrebbe essere appropriato nel caso di popolazioni costituite da un limitato numero di items di grande valore finanziario, o quando i controlli non diano sufficienti garanzie.

Selezione di specifici items: il Personale della Struttura IA può decidere di selezionare specifici items di una popolazione di dati, basandosi su fattori quali la conoscenza del settore, la propria preliminare valutazione del rischio, nonché sulla base delle caratteristiche della popolazione da esaminare.
La selezione basata sul giudizio professionale di specifici item è soggetta al rischio di non campionamento, ovvero al rischio che sia stata scelta una tecnica di selezione non appropriata alle circostanze. La selezione degli specifici items può includere:

- *items di valore significativo o key items;* può essere deciso di selezionare specifici items in una popolazione, quali ad esempio quelli di importo significativo o con caratteristiche di anormalità, in quanto operazioni inusuali, particolarmente rischiose o caratterizzate da errori nel passato;
- *tutti gli items superiori a un determinato ammontare*; può essere deciso di esaminare gli items il cui valore eccede un determinato ammontare, in modo da sottoporre ai test una percentuale significativa della spesa o delle specifiche operazioni;
- *items selezionati al fine di ottenere informazioni*; può essere deciso di esaminare taluni specifici items al fine di ottenere informazioni su particolari problematiche, sulla natura delle operazioni, sulla contabilità e sulle procedure;
- *items per testare una procedura*; il personale può far ricorso al proprio giudizio professionale per selezionare ed esaminare specifici items al fine di verificare se la procedura esaminata sia stata applicata o meno.

La selezione e l'esame di specifici items può costituire un metodo efficiente, ma non rappresenta un campionamento. I risultati delle procedure di audit effettuate sugli specifici items selezionati non possono essere estesi all'intera popolazione. Occorre valutare l'eventuale necessità di ottenere appropriate evidenze relativamente alla restante parte della popolazione.

Selezione a campione: l'auditor deve considerare gli obiettivi del test da svolgere e gli attributi della popolazione da cui il campione deve essere estratto. In riferimento agli obiettivi, occorre considerare la natura del test da svolgere e l'evidenza di audit necessaria nel definire ciò che costituisce un errore, e la sua rilevanza ai fini di una eventuale proiezione sull'universo. In riferimento alla popolazione l'auditor deve accertarsi che la stessa sia appropriata agli obiettivi della procedura di audit, nonché risulti completa.

La dimensione del campione è funzione del rischio e del giudizio professionale dell'auditor nel correlare il grado di rischio individuato all'estensione del campione, ponderando i seguenti fattori:

- *la valutazione del rischio inerente e del rischio residuo:* un incremento di rischiosità nella valutazione del rischio comporta un aumento del campione;
- *la valutazione del rischio sui controlli:* un incremento di rischiosità nella valutazione del rischio sui controlli comporta un incremento nella dimensione del campione;
- *l'utilizzo di eventuali altre procedure di revisione:* l'utilizzo di eventuali ulteriori procedure di revisione finalizzate allo stesso obiettivo, in aggiunta a quelle per le quali si sta effettuando il campionamento comporta un decremento nel campione;
- *il livello di significatività eventualmente richiesto*: maggiore è il livello di significatività pianificato ovvero l'ampiezza della presenza di errori che si è disposti ad accettare nell'ambito dell'universo oggetto di esame, minore sarà la dimensione del campione;
- *l'ammontare degli errori che l'auditor si aspetta di riscontrare nella popolazione*: maggiori sono gli errori che l'auditor si aspetta di riscontrare nella popolazione, maggiore sarà la dimensione del campione;
- *la stratificazione della popolazione:* quando esiste una grande variabilità di ammontare nella popolazione, può essere indicato effettuare dei sub campionamenti per classi di valore (strati) caratterizzati da minore variabilità, al fine di ridurre la dimensione del campione;

- *la numerosità della popolazione*; tanto maggiore è la dimensione della popolazione tanto minore è l'effetto sulla dimensione del campione.

I principali metodi di selezione del campione basata su un approccio non statistico sono:

- l'utilizzo di *numeri casuali* generati dal computer o dalle tavole numeriche;
- la *selezione sistematica*, in cui il numero di items dell'universo è diviso per il numero di items del campione, al fine di individuare l'intervallo di campionamento, per esempio 50, e avendo scelto un punto di partenza dentro i primi 50 items, si procederà selezionando di lì in avanti un items ogni 50 (cosiddetto "passo campionario");
- *selezione casuale*, in cui il revisore effettua una selezione senza seguire una tecnica strutturata;
- *la selezione stratificata*, in cui in si applica la selezione casuale o con l'utilizzo di numeri casuali nell'ambito di determinati strati di popolazioni aggregati da fattori comuni (ad esempio zona geografica, classi di importo, tipologie di beneficiari etc). Tale metodo si applica quando i fattori sopra indicati risultano significativamente diversi l'uno con l'altro.

Ulteriori metodi possono essere individuati anche attraverso la combinazione delle tecniche sopra illustrate, tenuto conto delle finalità e degli obiettivi dell'intervento di audit.

5.9.4 Esempio di selezione con metodo non statistico

Qualora l'oggetto di un intervento di audit sia l'effettuazione di verifiche sull'attività ispettiva, nella fase di pianificazione del singolo intervento, occorre prevedere l'acquisizione della lista delle verifiche effettuate, sulla quale effettuare il campionamento.

L'universo all'interno del quale effettuare la selezione può essere individuato con riferimento all'anno solare.

Il numero dei controlli da selezionare è deciso tenendo in considerazione i seguenti aspetti:

- obiettivi dell'intervento;
- tempi e risorse pianificate per l'intervento;
- esperienza dell'auditor nell'effettuare interventi aventi questa tipologia;
- complessità delle attività di controllo da espletare;
- complessità e localizzazione dell'unità auditata.

Una volta stabilito il numero dei controlli da selezionare, la loro ripartizione è effettuata in funzione degli importi finanziati.

Sarà compito dell'auditor individuare di volta in volta la tecnica di selezione che preserva la casualità, rapportata alla facilità di applicazione del metodo di selezione, alla popolazione oggetto di esame. Tale attività deve essere sempre comunque documentata nelle carte di lavoro.

5.9.5 Il Campionamento statistico

Il **campionamento per variabili** è la metodologia che più di ogni altra risulta statisticamente corretta per determinare campioni di valori monetari che siano rappresentativi dell'universo. In

particolare è possibile determinare entro i limiti di precisione[3] e di livello di confidenza[4] determinati, il valore aggregato di una determinata popolazione, attraverso la determinazione del valore medio di un campione rappresentativo della stessa. La numerosità del campione, affinché la sua media aritmetica sia rappresentativa della popolazione intera, (a parità di livelli di precisione e di confidenza) è funzione della variabilità dell'universo. Quanto maggiore risulta la variabilità dell'universo, tanto maggiore dovrà essere l'ampiezza del campione affinché esso sia rappresentativo dell'universo stesso (a parità di livelli di precisione e di confidenza). La variabilità di una popolazione viene misurata statisticamente attraverso gli scostamenti dal valore medio della stessa (scarto quadratico medio). Tale metodologia risulta essere molto complessa, nella sua applicazione pratica, conduce alla determinazione di campioni di operazioni numerosi e per tale motivo è raramente usata.

Altra metodologia di campionamento è il campionamento per attributi. Tale metodologia non risulta immediatamente applicabile per verificare un numero di operazioni monetarie e quindi, sulla base dei risultati raggiunti, per estendere le conclusioni all'intera popolazione. Il campionamento per attributi infatti serve a determinare le caratteristiche totali di un universo attraverso l'esame delle caratteristiche di un campione di operazioni. Se ad esempio avessimo un contenitore con un numero predeterminato di palline, la cui caratteristica, quella di essere bianche o nere è a noi ignota, potremmo conoscere, con approssimazione statistica (livello di confidenza e probabilità di errore) la frequenza della caratteristica pallina bianca e della caratteristica pallina nera, su tutto l'universo, attraverso l'esame di un campione rappresentativo di palline, selezionato in maniera casuale (specifiche tavole statistiche possono essere velocemente utilizzate conoscendo i parametri di livello di confidenza, errore atteso, e numerosità dell'universo, per stabilire l'ammontare di un campione rappresentativo della popolazione). Se noi applicassimo questo metodo a un universo di operazioni (pagamenti), potremmo certamente determinare l'attributo, pagamento corretto, o pagamento errato, ma non avrebbe senso sapere che su 2,5 milioni di pagamenti un certo numero degli stessi, per probabilità statistica, risulta errato poiché non sarebbe possibile conoscerne l'ammontare, ovvero il peso in termini di valore monetario dell'errore. Tale tipologia di campionamento potrebbe al contrario essere applicata per analizzare uno specifico attributo non monetario nell'ambito di una popolazione, ad esempio Controllo senza errore/Controllo con errore oppure check-list compilata/check-list non compilata, qualora si decidesse di voler effettuare una analisi su specifici attributi piuttosto che un intero flusso di operazioni legate alla domanda.

6. LA REVISIONE INTERNA DEI SISTEMI IT

6.1 La definizione degli obiettivi

L'utilizzazione dei sistemi informatici a supporto dello svolgimento delle attività operative (utilizzazione delle check list su pc, trattamento dei dati ispettivi sui sistemi centrali, etc.) e di quelle gestionali e di supporto (gestione del personale, gestione amministrativa, etc.) richiede normalmente che si ponga attenzione ai sistemi IT, al fine di garantire l'attendibilità delle informazioni e la gestione di eventuali rischi legati ai sistemi IT stessi.

[3] Il livello di precisione rappresenta l'errore che l'auditor è disposto ad accettare nell'ambito di una popolazione oggetto di esame. Tale livello, detto anche livello di "significatività" o "materialità" può essere espresso in valore assoluto, ovvero come un ammontare monetario, oppure un numero di errori formali ritenuti accettabili, oppure in valore percentuale.

[4] Il livello di confidenza è il grado di certezza con cui l'auditor può estendere all'universo della popolazione le conclusioni raggiunte, attraverso le verifiche svolte sul campione selezionato statisticamente. Tanto più è alto il livello di confidenza che l'auditor vuole ottenere, tanto più ampio sarà il campione statistico necessario per poter garantire tale livello.

I sistemi IT devono quindi essere sottoposti ad audit e gli obiettivi fondamentali in materia di IT auditing sono i seguenti:

- individuare le aree di maggiore esposizione ai rischi nelle attività di gestione dell'infrastruttura informatica e a supporto dell'attività operativa, misurarne il grado di controllo esistente, rilevando le potenziali criticità e proponendo, se necessario, le misure per il ripristino del livello di controllo desiderato;
- supportare l'audit operativo:
  - nel fornire il conforto atteso circa l'efficacia dei controlli, laddove fortemente automatizzati;
  - nell'elaborazione e analisi dei dati con strumenti informatici.

6.2 L'analisi del processo "Gestione delle informazioni e della relativa tecnologia"

Al fine di cogliere il primo degli obiettivi riportati nel precedente paragrafo, la metodologia adottata dalla Struttura IA propone un'analisi del processo principale "Gestione delle informazioni e della relativa tecnologia", in cui sono sintetizzate tutte le attività di gestione degli aspetti informatici dell'Agecontrol.

Tale analisi, coerentemente con l'analisi dei processi, può essere scomposta nelle tre fasi principali:

- IT Risk Assessment
- il Piano di audit IT;
- l'esecuzione di test sull'ambiente IT.

6.2.1 L'IT Risk Assessment

Le attività preliminari a tale fase sono la mappatura dell'architettura e delle infrastrutture tecnologiche esistenti, la rilevazione del parco hardware della Società e della struttura organizzativa preposta alla gestione dell'IT in azienda. Tali informazioni dovranno essere sempre tenute in considerazione durante tutta l'attività di IT auditing.

Segue l'attività vera e propria di IT Risk Assessment, durante la quale il processo principale viene suddiviso nei seguenti processi secondari:

- pianificare e organizzare l'ambiente IT;
- acquisire e implementare le risorse IT;
- erogare il servizio IT;
- monitorare l'ambiente IT (quest'ultimo può essere inserito all'interno di pianificare e organizzare l'ambiente IT).

Tramite interviste con il personale IT, per ciascun processo secondario, coerentemente con la metodologia generale di Risk Assessment usata nei processi operativi, vengono individuati gli scopi, gli obiettivi, gli owner e le descrizioni delle attività principali, i confini, gli input/output e gli indicatori di performance.

Successivamente, congiuntamente con il management, vengono identificati i rischi principali insiti nelle attività descritte e si procede alla loro valutazione come descritto nel capitolo 3.
Poi ne vengono mappate le attività di controllo a cui, sempre congiuntamente con il responsabile, viene dato un giudizio preliminare in merito alla loro capacità di mitigare il rischio in oggetto. Contestualmente è possibile eseguire delle attività di confronto di quanto rilevato con le migliori

pratiche in merito alle attività di controllo e, quindi, identificare le aree di miglioramento già in fase di intervista.

6.2.2 I Piani di audit IT

La fase di piano di audit IT rientra nella fase più generale di pianificazione in cui vengono analizzate le aree di rischio a livello societario al fine di scegliere gli interventi di audit da eseguire.

Qualora si decida di includere, in fase di Piano di audit IT, l'esecuzione di interventi di audit conseguenti a rischi valutati alti nei processi di information technology è bene considerare i seguenti aspetti per poter dare delle indicazioni precise sul perimetro dell'intervento:

- rischio principale a cui l'intervento fa riferimento;
- elenco delle attività di controllo poste in essere per mitigare il rischio;
- aree dell'infrastruttura tecnologica e/o applicativi impattati da tali rischio;
- aree di business servite dalle aree di infrastruttura tecnologica e/o applicativi citati al punto precedente e danno presunto in caso di manifestazione del rischio.

In tal modo si hanno le informazioni necessarie sia per limitare eventualmente l'ambito dell'intervento a favore di una maggiore efficienza, sia per stimare correttamente le risorse in termine di tempo e di competenze.

6.2.3 L'esecuzione di test sull'ambiente IT

La fase di esecuzione di test sull'ambiente IT ha come input tutti gli elementi indicati nel Piano di audit IT: il rischio rilevato, le attività di controllo da testare, le aree di infrastruttura e/o gli applicativi di riferimento, ecc. e il budget in termini di tempo per risorsa.

Durante questa fase si deve definire un programma di lavoro, indicando:

- gli obiettivi generali che si intendono perseguire;
- le informazioni e la documentazione necessaria come input all'esecuzione dell'intervento e che può essere analizzata prima dell'inizio dello stesso;
- un'agenda delle interviste necessarie con gli obiettivi delle interviste;
- un'agenda dei test sull'elaboratore con gli obiettivi di tali test;
- una check-list dei punti di controllo salienti che non devono essere tralasciati dall'insieme di interviste e test.

La Relazione in cui sono descritte le evidenze riscontrate è sostanzialmente identica a quella prescritta per i processi operativi.

6.2.4 L'utilizzo di standard di IT auditing

Proprio per poter rispondere in maniera efficiente alla complessità di tali impegni, l'auditor dei sistemi IT si affida, per prassi consolidata, a standard collaudati che permettono di seguire linee guida, sempre in evoluzione, nello svolgimento dell'attività.

In particolare è possibile creare una buona simbiosi tra la metodologia adottata dalla Struttura IA e lo standard COBIT (Control Objectives for Information and Related Technology) di proprietà di Information Systems Audit and Control Foundation (ISACF).

COBIT illustra le buone norme per la gestione dei processi IT incontrando le necessità di molteplici tipologie di aziende e fornendo i collegamenti tra rischi di business, elementi di tecnologia, necessità di controllo e indicatori di performance.

6.3 Il supporto all'audit

Il secondo obiettivo indicato per le attività di IT auditing è di supportare l'audit operativo nel fornire un certo grado di conforto sull'efficacia dei controlli, laddove fortemente automatizzati, e di supportare l'audit operativo nell'elaborare analisi di quantitativi ingenti di dati attraverso strumenti informatici.

6.3.1 I controlli automatizzati

Per questo fine è opportuno impostare progetti di audit cui partecipano risorse con competenze multidisciplinari in ambito IT e conoscitive dell'area operativa di riferimento.

Congiuntamente il team di audit dovrà comprendere il funzionamento teorico del controllo automatizzato, raccogliendo tutte le casistiche che possono innescare percorsi diversi all'interno dello stesso.

La verifica del suo effettivo funzionamento può avvenire nei seguenti modi:

- verificando la correttezza semantica del codice sorgente dei programmi che compongono il controllo;
- istituendo un ambiente informatico di test, identico a quello di produzione, su cui fare verifiche e prove;
- utilizzando tecniche miste di verifica codice sorgente/test applicativi e, al limite, suddividendo il controllo in più fasi, che possano essere analizzate anche con tecniche differenti.

6.3.2 L'analisi dei dati

Nel caso di elaborazione massiva di dati con strumenti informatici è indispensabile istituire team multidisciplinari con competenze nelle aree operative interessate e con competenze di strumenti informatici di gestione dei dati. Gli obiettivi delle elaborazioni devono essere indicati dall'auditor operativo, mentre è scopo dell'auditor IT di sviluppare le tecniche di analisi dei dati, di individuare lo strumento informatico che meglio consente l'esecuzione di tali tecniche analitiche e di implementare le stesse attraverso lo strumento informatico prescelto.

7. IL RAPPORTO ANNUALE SULL'ATTIVITÀ DELLA FUNZIONE INTERNAL AUDITING

7.1 Il Rapporto annuale sulle attività svolte in relazione ai processi critici aziendali

Entro la fine del mese di gennaio dell'anno successivo a quello di svolgimento del Piano dell'audit, il Responsabile della Struttura IA redige un Rapporto sull'attività svolta sui processi critici aziendali destinato al vertice aziendale. L'attività di rendicontazione sulle attività svolte verrà utilizzata anche come base per la successiva pianificazione pluriennale e annuale delle attività di Internal Audit.

Il Rapporto annuale comprende i contenuti descritti di seguito.

- **Attività di consulenza e/o supporto al vertice aziendale.**
- **Copertura del piano di audit**: all'interno del quale è riepilogato quanto effettivamente svolto nel corso del periodo, in comparazione con quanto era stato previsto; vengono giustificate tutte le variazioni intervenute rispetto alla programmazione iniziale, all'interno di questo capitolo viene inoltre dato un resoconto delle altre attività svolte dal personale della Struttura IA e non indirizzate alla realizzazione di interventi di audit (ad esempio attività di formazione, progetti speciali, etc..).
- **Sintesi delle principali osservazioni**: all'interno della quale viene data una sintesi delle principali osservazioni rilevate nel corso degli interventi svolti.
- **Esito delle attività di follow-up**: all'interno del quale viene data una sintesi del grado di implementazione dei piani di azione concordati nel corso dei periodi/annualità antecedenti e oggetto di specifici interventi di follow-up nel corso del periodo/annualità appena conclusa.
- **Aggiornamento Risk assessment.**
- **Formazione,** secondo il Piano di formazione annuale approvato.
- **Varie.**

8. L' ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI AUDIT

La Struttura IA si impegna a promuovere la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità della documentazione di audit in modalità digitale, per un miglioramento dell'efficienza e dell'efficacia dei processi aziendali e nella prospettiva di una digitalizzazione completa del trattamento dei documenti; si organizza ed agisce a tale fine utilizzando, con le modalità più appropriate, le tecnologie dell'informazione e della comunicazione.

8.1 Il protocollo

8.1.1 L'approccio della Struttura IA

Con riferimento alle attività della Struttura IA sono state individuate alcune comunicazioni in entrata o in uscita (ad esempio rapporti ufficiali, lettere di pianificazione, etc.), che debbono essere necessariamente protocollate, mentre altre comunicazioni in entrata o in uscita (ad esempio bozze di rapporti, richieste di documentazione, documenti vari, etc.) che vengono protocollate solamente se debbono assumere una valenza ufficiale.

8.1.2 I documenti della Struttura IA

La documentazione in *uscita* è la seguente:

- Piano di audit annuale proposto dal Dirigente del responsabile della struttura IA e approvato dal Rappresentante Legale;
- lettere di pianificazione definitive e relativi allegati;
- relazioni degli interventi di audit e di follow-up;
- Rapporto annuale sull'attività propria della Struttura IA.

La documentazione in *entrata* è la seguente:

- comunicazioni dei "committenti" di richiesta di specifici interventi di audit;

- commenti dei Responsabili alle osservazioni emerse nel corso degli interventi di audit e di follow-up, quando sono considerati definitivi e saranno inclusi nelle Relazioni finali;
- documenti che comportano integrazioni o variazioni a documenti già protocollati;
- altro.

8.2 L'archivio cartaceo

8.2.1 L'organizzazione dell'archivio cartaceo della Struttura IA

La Struttura IA ha presso i propri uffici spazi adeguati a raccogliere e archiviare la documentazione e le comunicazioni, da e verso l'esterno, sia relativamente agli interventi svolti, sia relativamente alla pianificazione e gestione delle attività.

Gli spazi fisici sono organizzati all'interno di appositi armadi accessibili al solo personale della Struttura IA.

La documentazione è mantenuta presso gli uffici della Struttura IA durante l'anno di riferimento e, ove necessario mediante archiviazione remota, per i successivi 10 anni dalla chiusura del fascicolo. Al termine di tale periodo la documentazione, se divenuta superflua dal punto di vista giuridico, amministrativo e storico, viene scartata.

8.2.2 Il fascicolo dell'intervento, la sua organizzazione e la sua archiviazione

Per ciascun intervento di audit, la Struttura IA mantiene adeguata documentazione, al fine di:

- documentare le attività di pianificazione svolte e le relative comunicazioni con i soggetti auditati;
- mantenere memoria del lavoro eseguito (programmi delle verifiche svolti, modalità di esecuzione dei test, ecc.);
- mantenere memoria delle informazioni ottenute nel corso dell'intervento (descrizione dei processi/attività, osservazioni, conclusioni, raccomandazioni);
- supportare, con adeguate evidenze, le conclusioni tratte nella Relazione finale dell'intervento.

Il fascicolo dell'intervento è aperto, dall'auditor responsabile dell'intervento, all'atto di procedere alla pianificazione dell'intervento stesso.

L'organizzazione del fascicolo dell'intervento di audit avviene secondo lo schema di seguito indicato:

PARTE A: contiene le **disposizioni normative comunitarie, nazionali e aziendali.**
Le *disposizioni comunitarie* dovranno essere ordinate, cronologicamente e gerarchicamente per regolamenti del Consiglio, regolamenti della Commissione, direttive, decisioni, pareri, documenti di lavoro dispositivi.
Le *disposizioni nazionali* dovranno essere ordinate cronologicamente secondo la gerarchia delle fonti (leggi, decreti legislativi, D.P.R., decreti interministeriali, decreti ministeriali).
In questa sezione andranno anche inserite le disposizioni emanate da Agea e da Agecontrol, comprendenti in ordine cronologico: delibere, circolari, manuali procedurali, disposizioni di specifiche tecniche, contratti e convenzioni, note interpretative e/o dispositive.

PARTE B: contiene le **comunicazioni formali.** In questa sezione dovranno essere archiviate cronologicamente le comunicazioni formali inerenti all'esecuzione dell'intervento quali, ad

esempio: corrispondenza esterna, ordini di servizio, comunicazioni, ricezione documenti e/o osservazioni.

PARTE C: contiene le **evidenze documentali.** In questa sezione dovrà essere ordinata la documentazione che supporta oggettivamente, in relazione a ogni voce e punto per punto, l'intervento di audit, le osservazioni e i temi di attenzione evidenziati.

PARTE D: contiene i **documenti di lavoro**, classificati in documenti acquisiti e documenti prodotti dalla Funzione di Internal Auditing. Riguardo a questi ultimi si fa riferimento, in particolare, al programma di audit, alla pianificazione del lavoro, alla check-list, al memo di campionamento, alla/e bozza/e di relazione, alla Relazione finale di audit.

PARTE E: contiene la documentazione inerente all'**IT audit**. In questa sezione verranno classificati e archiviati i documenti acquisiti a supporto dell'attività di IT auditing; nel caso la documentazione pervenuta rappresenti una notevole mole di dati è necessario predisporre un apposito supporto informatico, opportunamente etichettato e datato.

PARTE F: contiene la documentazione del **follow-up**. In questa sezione verranno classificati e archiviati i documenti inerenti all'incarico di esecuzione del monitoraggio delle azioni correttive, i documenti di lavoro prodotti o acquisiti dalla Struttura IA e la Relazione finale di follow-up.

La documentazione, prodotta o acquisita, ordinata come sopra descritto, dovrà contenere nel primo faldone, se più di uno, l'indice generale, i successivi faldoni dovranno contenere l'indice della parte di competenza. Ciascun faldone deve essere numerato secondo la sequenza 1/n° totale di faldoni. La documentazione ricevuta per posta elettronica dovrà essere prodotta in formato cartaceo oppure su un supporto informatico opportunamente etichettato e datato.

Al termine di ciascun intervento, l'auditor rivede la documentazione prodotta e si assicura che il fascicolo sia completo e che i relativi contenuti siano ordinati e corretti. In quest'ultimo caso il fascicolo può essere archiviato.

In particolare, la classificazione e l'archiviazione dei documenti dell'attività di follow-up derivante dal Control Risk Self Assessment, avviene secondo il seguente schema:

1. la tavola di follow-up;
2. le evidenze documentali;
3. le comunicazioni formali;
4. i documenti di lavoro;
5. i documenti a supporto dell'IT audit.

Il faldone dovrà riportare la lettera F e essere seguita dal numero identificativo del rischio.

8.2.3 L'archiviazione cartacea dei documenti prodotti nello svolgimento delle attività interne

La documentazione relativa alle attività interne svolte dalla Struttura IA sulla base delle indicazioni del Dirigente responsabile della stessa struttura sono, nella maggior parte dei casi, archiviate informaticamente.

Gli unici documenti relativi all'attività interna e archiviati in formato cartaceo, oltre a essere archiviati elettronicamente, sono i seguenti:

- Piano annuale di audit;
- Rapporto annuale sull'attività della Struttura IA;
- corrispondenza con soggetti esterni, non relativa a singoli interventi di audit, e avente particolare rilevanza.

Tali documenti sono archiviati all'interno di specifici fascicoli, contrassegnati sul dorso dall'indicazione del contenuto e dell'anno di riferimento, e riportanti in testa i contenuti dei fascicoli stessi.

8.3 L'archivio informatico

8.3.1 La struttura dell'archivio informatico

L'archivio informatico della Struttura IA è organizzato secondo una struttura a cartelle descritta di seguito.

- **Procedure e Manuali:** contiene tutta la documentazione operativa necessaria a supportare lo svolgimento delle attività della Struttura IA. Tale cartella è a sua volta suddivisa nelle seguenti sezioni:
  - **Check-list comuni:** contiene tutte le check-list e i programmi di lavoro adattabili a regolare lo svolgimento di interventi simili;
  - **Manuale:** contiene il presente Manuale Operativo e le sue eventuali successive elaborazioni; contiene inoltre altri manuali operativi utilizzati nell'attività della Funzione;
  - **Procedure Interne:** contiene le procedure interne della Struttura IA;
  - **Documentazione varia:** contiene documentazione operativa necessaria a supportare lo svolgimento delle attività della Struttura IA, ad esempio le procedure, diagrammi di flusso, etc.

- **Planning:** contiene, suddivisa per anno, la documentazione e le informazioni indicative della programmazione delle attività della Struttura IA, oltre a informazioni e strumenti necessari allo svolgimento delle ulteriori attività di programmazione. Contiene, inoltre, il foglio excel utilizzato per mantenere costantemente aggiornata la pianificazione temporale degli interventi definiti nel Piano di audit e delle relative risorse associate.

- **Documentazione esterna:** contiene la corrispondenza e i data base degli indirizzi utili per la Funzione. Tale cartella è a sua volta suddivisa nelle seguenti sezioni:
  - **Corrispondenza IN-OUT:** contiene tutta la corrispondenza ricevuta o inviata dalla Struttura IA e indirizzata a soggetti esterni all'Agecontrol.
  - **Comunicazioni IN-OUT:** contiene tutte le comunicazioni ricevute o inviate dalla Struttura IA indirizzate al Legale Rappresentante, alla Direzione Generale e alle altre strutture aziendali.
  - **DB Indirizzi:** contiene il data base degli indirizzi utili allo svolgimento delle attività della Funzione.
  - **Agea:** contiene altra documentazione inviata dall'Agea.

- **Interventi:** contiene la documentazione degli interventi di audit eseguiti nel corso degli anni. La cartella contiene, a sua volta, le seguenti altre:

  - **Interventi per anno di attività:** contenente la documentazione degli interventi svolti nel corso dell'anno, suddivisi per:
    - **Processo auditato:** per ciascun processo è creata una cartella che contiene il materiale relativo all'intervento. Per ogni intervento effettuato la documentazione è archiviata analogamente a quanto viene fatto per la documentazione cartacea.

- **Follow-up:** è suddivisa per anno di attività e contiene la tavola di follow-up relativa alle osservazioni effettuate.
- **Rapporti annuali:** contiene i Rapporti annuali sull'attività svolta inviati al vertice aziendale. Tale cartella è a sua volta suddivisa nelle seguenti sezioni:
  - **Rapporti dell'anno** (per ciascun anno di attività)**:** contiene i Rapporti per ogni anno di attività.

L'archivio informatico è organizzato secondo una struttura che potrà, in base alle sopravvenute necessità, essere modificata con l'introduzione di altre cartelle e sottocartelle.

La gestione e l'aggiornamento della struttura dell'archivio informatico e dei suoi contenuti è effettuata dal personale della Struttura IA .

L'accesso in lettura ad altri soggetti, non appartenenti alla Struttura IA, deve essere esplicitamente autorizzata per iscritto dal Dirigente responsabile.

9. ALLEGATI

- 1 - Piano di Audit
- 2 - Intervento di audit
- 3 - Memorandum di pianificazione
- 4 - Check-list
- 5 - Relazione finale di Audit
- 6 - Tavola di follow-up
- 7 - Relazione di follow-up

Allegati

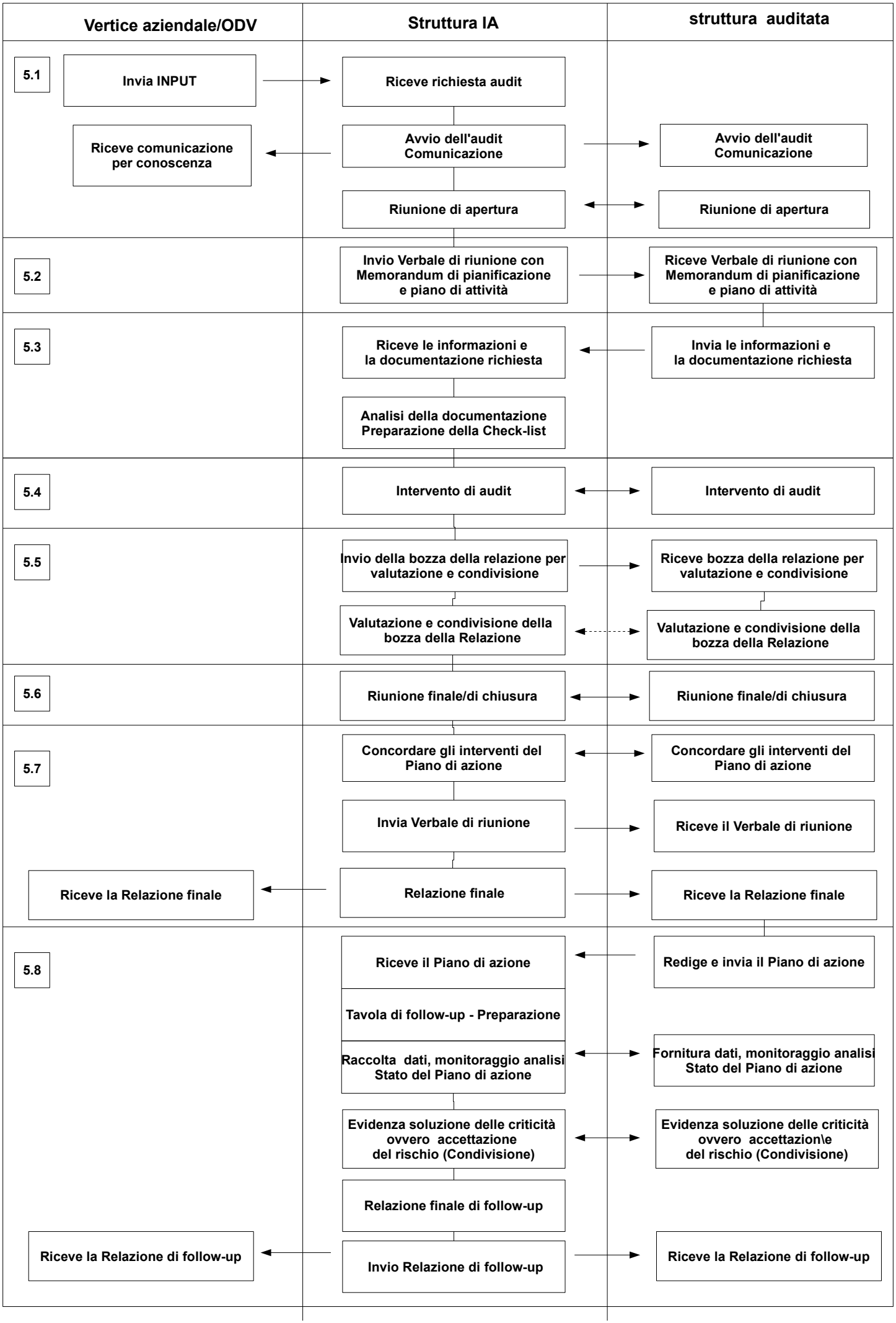
Attività di audit: Piano aaaa

Area Controllo Interno e Supporto

Documento per l'Amministratore Unico

Roma, gg/mm/aaaa

Processo/Attività	*Struttura di riferimento*	*Tipologia di audit/attività*	*Origine*	*Oggetto dell'intervento di audit e/o delle attività svolte*	*Output/Note*	*Tempi di lavoro*	*Tempi di completamento delle attività*									
						(gg/uomo)	*feb*	*mar*	*apr*	*mag*	*giu*	*lug*	*set*	*ott*	*nov*	*dic*
						0										


Vertice aziendale/ODV
Struttura IA
struttura auditata
5.1
Invia INPUT
Riceve richiesta audit
Riceve comunicazione per conoscenza
Avvio dell'audit Comunicazione
Avvio dell'audit Comunicazione
Riunione di apertura
Riunione di apertura
5.2
Invio Verbale di riunione con Memorandum di pianificazione e piano di attività
Riceve Verbale di riunione con Memorandum di pianificazione e piano di attività
5.3
Riceve le informazioni e la documentazione richiesta
Invia le informazioni e la documentazione richiesta
Analisi della documentazione Preparazione della Check-list
5.4
Intervento di audit
Intervento di audit
5.5
Invio della bozza della relazione per valutazione e condivisione
Riceve bozza della relazione per valutazione e condivisione
Valutazione e condivisione della bozza della Relazione
Valutazione e condivisione della bozza della Relazione
5.6
Riunione finale/di chiusura
Riunione finale/di chiusura
5.7
Concordare gli interventi del Piano di azione
Concordare gli interventi del Piano di azione
Invia Verbale di riunione
Riceve il Verbale di riunione
Riceve la Relazione finale
Relazione finale
Riceve la Relazione finale
5.8
Riceve il Piano di azione
Redige e invia il Piano di azione
Tavola di follow-up - Preparazione
Raccolta dati, monitoraggio analisi Stato del Piano di azione
Fornitura dati, monitoraggio analisi Stato del Piano di azione
Evidenza soluzione delle criticità ovvero accettazione del rischio (Condivisione)
Evidenza soluzione delle criticità ovvero accettazion\e del rischio (Condivisione)
Relazione finale di follow-up
Riceve la Relazione di follow-up
Invio Relazione di follow-up
Riceve la Relazione di follow-up

Allegato 3 – Memorandum di pianificazione

AGECONTROL s.p.a. agenzia pubblica per i controlli in agricoltura	**MEMORANDUM DI PIANIFICAZIONE**	Area Controllo Interno e Supporto Data: __/__/____

A:

e, p.c.:

OGGETTO: AUDIT …….

1. Informazioni generali

   l'audit "……", da eseguire su incarico del (Legale Rappresentante, OdV) è inserito nel Piano di audit Agecontrol approvato per l'annualità .....

2. Strutture/Processi auditati

   nell'ambito del settore "....", le attività di audit saranno concentrate sulle fasi del processo di .....

3. Obiettivi dell'audit

   vengono indicate le attività ritenute meritevoli di controllo e sulle quali verrà incentrata l'analisi dell'auditor al fine verificare il corretto raggiungimento di un obiettivo stabilito o per evidenziare i problemi che ne hanno impedito il raggiungimento.

4. Dettagli di pianificazione - lista dei documenti necessari

   descrive i tempi di realizzazione dell'intervento di audit, gli strumenti impiegati (normativa, check list, campione, etc.), le richieste inoltrate alla struttura auditata.

   Richiama l'attenzione sul rispetto dei tempi da parte della struttura auditata per la predisposizione del materiale richiesto, che impattano sui tempi complessivi di esecuzione delle attività di audit.

Allegato 4 – Check list

Check-list
Audit: ……

Data: __/__/____

Struttura auditata:

		Esito				Evidenze del controllo						
N.	**Item**	**non applicabile**	**positivo**	**negativo**		**non applicabile**	**documentale**	**elettronica**	**intervista**	**osservazione**	**Commenti**	**eventuali riferimenti al documento di definizione dell'oggetto di audit**
1												
2												
3												
4												
5												
6												
7												

Allegato 5 – Relazione finale di Audit

AGECONTROL s.p.a. agenzia pubblica per i controlli in agricoltura	**Relazione di audit**	Area Controllo Interno e Supporto Data: __/__/____

AUDIT ……..

SUBPROCESSO ……..

PIANO DI AUDIT 2024

Indice

1 Descrizione e finalità dell'incarico di Audit

…….

…….

……..

Il Dirigente

Agecontrol s.p.a.

Tavola di follow up

Audit …….
Subprocesso ……

Struttura auditata:

Data Relazione finale di audit: __/__/____
Data rilevazione delle azioni da implementare: __/__/____

TIPO	OSSERVAZIONE (/Rischio/Raccomandazione descritto nella Relazione finale di audit)	AZIONE DA IMPLEMENTARE (Piano di azione del --/--/----)	DATA PREVISTA	DATA COMPLETAMENTO	STATUS	NOTE
EF			__/__/____	__/__/____	**I**	
CI			__/__/____	__/__/____	**N**	

TIPO
- **CI** raccomandazione volta a migliorare l'efficacia del sistema di controllo interno
- **EF** raccomandazione volta a migliorare l'efficienza del processo analizzato

STATUS
- **I** azione implementata
- **N** azione non implementata

Il Responsabile Audit ……

Allegato 7 – Relazione di follow-up

AGECONTROL s.p.a. agenzia pubblica per i controlli in agricoltura	**Relazione di Follow up**	Area Controllo Interno e Supporto Data: __/__/____

AUDIT …….

SUBPROCESSO ……

RELAZIONE DI FOLLOW UP

Allegato 7 – Relazione di follow-up

AGECONTROL s.p.a. agenzia pubblica per i controlli in agricoltura	**Relazione di Follow up**	Area Controllo Interno e Supporto Data: __/__/____

Introduzione

…….

Modalità di svolgimento del follow-up

….....

Esiti del follow-up

La tavola di follow-up, allegata alla presente relazione, riporta e classifica le evidenze riscontrate in questa fase dell'attività.

La sintesi dei risultati della rilevazione sullo stato di implementazione delle azioni correttive è riportata nella tabella che segue.

Azione	n.	Tipologia del problema			Riferimenti alla tavola di follow-up
		controllo interno (CI)	efficienza (EF)	controllo interno / efficienza (CI/EF)	
I - Implementata					
N - Non implementata					
Totale					

Le azioni sono classificate sulla base dello stato di implementazione e la tipologia di problema e di azione intrapresa è classificata anche distinguendo tra azioni volte a migliorare l'efficacia del sistema di controllo interno (CI), azioni volte a rendere maggiormente efficiente il processo analizzato (EF) e quelle che sono caratterizzate da entrambi gli aspetti (CI/EF).

In dettaglio, le azioni implementate riguardano i punti elencati di seguito e già riportati nella tavola di follow-up allegata.

Allegati

A – Tavola di follow-up

Il Dirigente