

MANUALE OPERATIVO

UFFICIO CONTROLLO INTERNO

Agenzia Regionale Piemontese per le Erogazioni in Agricoltura
Via Bogino n. 23, 10123 Torino Tel. 011 3025100 – Fax 011 3025199

TITOLO DOCUMENTO	AREA OPERATIVA
MANUALE OPERATIVO	UFFICIO CONTROLLO INTERNO

PRIMA APPROVAZIONE	DATA DETERMINA	NUMERO DETERMINA
MANUALE OPERATIVO AREA CONTROLLO INTERNO	12/06/2008	N°121_2008
REVISIONE N.	DATA DETERMINA	NUMERO DETERMINA
<i>1</i>	<i>28/04/2015</i>	<i>78/2015</i>
<i>2</i>	<i>28/06/2021</i>	<i>173/2021</i>
<i>3</i>	<i>12/06/2024</i>	<i>173/2024</i>

SOMMARIO

1	PREMESSA	4
1.1	SCOPO E DESTINATARI DEL MANUALE	4
1.2	DEFINIZIONI E ACRONIMI	4
1.3	RIFERIMENTI NORMATIVI.....	5
1.4	GLI OBIETTIVI DELL'UFFICIO CONTROLLO INTERNO E L'AMBITO DI INTERVENTO	5
1.5	STRUTTURA ORGANIZZATIVA DEL CI	6
1.6	PROTOCOLLI DI COMUNICAZIONE.....	7
1.7	I PRINCIPI ETICI DI RIFERIMENTO PER IL PERSONALE DELL'UFFICIO CI	7
1.8	RESPONSABILITÀ DEL DIRETTORE DI ARPEA E DEI COMPONENTI DELL'UFFICIO CONTROLLO INTERNO	8
2	PIANO QUINQUENNALE E ANNUALE DI AUDIT	9
2.1	PIANO QUINQUENNALE DI AUDIT.....	10
2.2	PIANO ANNUALE DI AUDIT.....	10
2.3	ATTIVITÀ DI RISK ASSESSMENT E MODALITÀ DI VALUTAZIONE DEI RISCHI E DEI CONTROLLI	11
2.4	TIPOLOGIE DI INTERVENTO.....	15
3	L'INTERVENTO DI AUDIT	15
3.1	LA PIANIFICAZIONE DELL' INTERVENTO	15
3.1.1	<i>Acquisizione della documentazione/informazioni necessarie all'intervento di audit</i>	16
3.1.2	<i>Formalizzazione del Memorandum di Pianificazione</i>	16
3.1.3	<i>Campionamento</i>	17
3.1.3.1	Tipi di campionamento	18
3.1.3.2	La selezione sulla base del giudizio professionale	18
3.1.3.3	La scelta del metodo di campionamento.....	20
3.1.4	<i>Comunicazione d'avvio dell'attività di audit</i>	21
3.2	L'ESECUZIONE DELL'INTERVENTO DI AUDIT	21
3.2.1	<i>Svolgimento della riunione di apertura</i>	21
3.2.2	<i>Analisi del processo</i>	21
3.2.3	<i>Svolgimento dei test sui controlli</i>	22
3.2.4	<i>L'osservazione di audit</i>	24
3.2.5	<i>Predisposizione delle carte di lavoro</i>	25
3.3	RAPPORTO FINALE DI AUDIT E COMUNICAZIONE DEI RISULTATI	25
4	IL MONITORAGGIO DELLE AZIONI CORRETTIVE	27
5	L' ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI AUDIT	28
5.1	I DOCUMENTI DEL CI CHE DEBONO NECESSARIAMENTE ESSERE PROTOCOLLATI	29
6	L'AUDIT DEI SISTEMI INFORMATIVI	29
6.1	DEFINIZIONE DEGLI OBIETTIVI.....	30
6.2	ANALISI DEL "SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI"	30
7	LE ATTIVITÀ DELL'UFFICIO CONTROLLO INTERNO A SUPPORTO DELLA VALUTAZIONE ANNUALE DEL SISTEMA DI GESTIONE E CONTROLLO	31

7.1	RELAZIONE ANNUALE DELL'UFFICIO CONTROLLO INTERNO	31
7.2	ATTIVITÀ PROPEDEUTICHE ALLA CHIUSURA DEI CONTI	32
7.3	MONITORAGGIO CONTINUO DEI CRITERI DI RICONOSCIMENTO	32
7.4	ATTIVITÀ A SUPPORTO DELL'ORGANISMO DI CERTIFICAZIONE	33
8	LE ATTIVITA' DELL'UFFICIO CONTROLLO INTERNO PER LA PREVENZIONE E IL CONTRASTO DELLE FRODI	33
9	PRINCIPI DEONTOLOGICI DI RIFERIMENTO PER IL PERSONALE DEL CI.....	34

1 PREMESSA

La presente edizione del “Manuale operativo dell’Ufficio di Controllo Interno” dell’Agenzia Regionale Piemontese per le Erogazioni in Agricoltura (di seguito “ARPEA”) è redatta in conformità ai regolamenti comunitari in materia di Politica Agricola Comune (PAC) (in particolare il Regolamento UE n. 2021/2116 del Parlamento Europeo e del Consiglio, del 2 dicembre 2021, il Regolamento UE n. 2022/128 della Commissione, del 21 dicembre 2021 e il Regolamento UE n. 2022/127 della Commissione del 7 dicembre 2021).

Il Reg. (UE) n. 2021/2116 definisce le condizioni di riconoscimento e di revoca degli Organismi Pagatori e degli Organismi di Coordinamento da parte degli Stati membri (Articolo 9, comma 2: “Gli Stati membri riconoscono come organismi pagatori i servizi o gli organismi che dispongono di un'organizzazione amministrativa e di un sistema di controllo interno che offrano garanzie sufficienti in ordine alla legittimità, regolarità e corretta contabilizzazione dei pagamenti. A tal fine, gli organismi pagatori soddisfano le condizioni minime per il riconoscimento con riferimento all'ambiente interno, alle attività di controllo, all'informazione e alla comunicazione nonché al monitoraggio che la Commissione stabilisce a norma dell'articolo 11, paragrafo 1, lettera a).

I criteri per il riconoscimento ai quali gli Organismi Pagatori devono conformarsi sono riportati nell’Allegato I al Regolamento (UE) n. 2022/127.

In particolare, ai sensi dell’art.1, comma 2 del Reg. (UE) n. 2022/127, gli Organismi Pagatori devono disporre di una struttura amministrativa e di un sistema di controllo interno conformi ai criteri di cui all’allegato I dello stesso regolamento e relativi ai seguenti aspetti:

1. Ambiente interno
2. Attività di controllo
3. Informazione e comunicazione
4. Monitoraggio.

Nell’ambito del Monitoraggio opera l’Ufficio Controllo Interno che, come di seguito riportato nel presente documento, è indipendente dalle altre aree operative dell’Agenzia e riferisce direttamente al Direttore della medesima.

1.1 Scopo e destinatari del manuale

Il presente manuale descrive ruoli, responsabilità e modalità operative per lo svolgimento dell’attività di internal audit dell’Agenzia Regionale per le Erogazioni in Agricoltura della Regione Piemonte.

Oltre agli Auditor, i destinatari del manuale sono le Aree e gli Uffici di ARPEA e i soggetti che collaborano con ARPEA nella gestione delle domande di contributo per gli aiuti previsti dalla Politica Agricola Comune - fondi FEAGA e FEASR.

Il contenuto del manuale e dei suoi allegati è soggetto a periodiche valutazioni e, se del caso, revisioni in funzione a variazioni intervenute:

- nella normativa unionale, nazionale e regionale di riferimento;
- nella strategia dell’attività di auditing;

Il manuale viene aggiornato a cura dell’Ufficio Controllo Interno, viene approvato dal Direttore di ARPEA e pubblicato sul sito internet di ARPEA.

1.2 Definizioni e acronimi

ARPEA: Agenzia Regionale per le Erogazioni in Agricoltura della Regione Piemonte

Auditor (o Internal Auditor): funzionario operante presso l'Ufficio Controllo Interno e incaricato dello svolgimento degli interventi di audit

CAA: Centri di Assistenza Agricola autorizzati

CCE: Corte dei Conti Europea

CE: Commissione Europea

CI: Ufficio Controllo Interno di ARPEA - servizio di audit interno previsto dal punto 4 dell'Allegato I del Regolamento (UE) n. 2022/127

IIA: Institute of Internal Auditors

MASAF: Ministero dell'agricoltura, della sovranità alimentare e delle foreste

OD: Organismi Delegati

RA: Risk Assessment

Responsabile CI: titolare della Posizione Organizzativa del controllo interno di ARPEA

SI: Sistemi Informativi

SIAP: Sistema Informativo Agricolo Piemontese

UE: Unione Europea

1.3 Riferimenti normativi

La costituzione del CI nell'ambito dell'Organismo Pagatore è prevista dall'allegato I al Reg. (UE) n. 2022/127.

Relativamente all'Ufficio Controllo Interno, il Regolamento Unionale prevede che:

- Il servizio di controllo interno sia indipendente dagli altri servizi dell'organismo pagatore e riferisca direttamente al direttore dell'organismo (Regolamento 2022/127, Allegato I, Punto 4, b), i);
- Il servizio di controllo interno verifichi che le procedure adottate dall'organismo pagatore siano adeguate per garantire la conformità con la normativa dell'Unione e che la contabilità sia esatta, completa e tempestiva (Regolamento 2022/127, Allegato I, Punto 4, b), ii);
- Le verifiche possano essere limitate a determinate misure o a campioni di operazioni, a condizione che il programma di lavoro garantisca la copertura di tutti i settori importanti, compresi i servizi responsabili dell'autorizzazione, per un periodo non superiore a cinque anni (Regolamento 2022/127, Allegato I, Punto 4, b), ii)
- L'attività del CI sia svolta conformemente a norme riconosciute a livello internazionale, sia registrata in documenti di lavoro e i risultati di tale attività debbano figurare nelle relazioni e nelle raccomandazioni destinate alla Direzione di ARPEA.

1.4 Gli obiettivi dell'Ufficio Controllo Interno e l'ambito di intervento

Il CI si ispira agli Standard Internazionali di Internal Auditing (IIA) e adotta la metodologia di lavoro basata sull'analisi dei processi, dei rischi e dei controlli, allo scopo di ottenere i risultati di cui sopra, e al fine di migliorare e proteggere il valore dell'organizzazione, fornendo garanzie, consigli, suggerimenti e approfondimenti oggettivi, basati sul rischio e sulle performance. Fa, inoltre, riferimento allo standard ISO19011.

L'Ufficio CI di ARPEA supporta la Direzione nel garantire l'efficacia e l'efficienza del sistema di controllo interno insito nei processi, principali e di supporto, relativi all'attività di organismo pagatore di ARPEA.

Il CI assiste la Direzione nel valutare l'adeguatezza del sistema di controllo interno di ARPEA, la rispondenza ai requisiti minimi definiti dai Regolamenti dell'Unione, verifica la conformità dei comportamenti alle procedure operative definite, identifica e valuta le aree operative maggiormente esposte al rischio (attraverso l'analisi dei processi, dei relativi rischi e dei controlli predisposti per ridurre l'impatto dei rischi), proponendo e monitorando l'implementazione di misure idonee a mitigare tale rischio.

Grazie all'analisi svolta sui processi, il CI contribuisce all'individuazione delle eventuali aree ed opportunità di miglioramento nei processi stessi.

In particolare, il CI valuta e fornisce appropriati suggerimenti volti a migliorare il processo di *governance* allo scopo di:

- favorire lo sviluppo di valori e principi etici nell'organizzazione;
- garantire l'efficace gestione dell'organizzazione e l'accountability;
- comunicare informazioni sui rischi e controlli alle relative funzioni dell'organizzazione;
- coordinare le attività e il processo di scambio di informazioni su rischi e controlli tra il Direttore, l'Organismo di certificazione, gli Auditor e il management.

L'attività del CI riguarda l'intera funzione istituzionale dell'Agenzia, inclusi i processi che per effetto di delega possono essere operati da altri soggetti.

In sintesi, pertanto, i principali obiettivi dell'Ufficio CI sono i seguenti:

- assicurare il rispetto della normativa nazionale e unionale;
- verificare la legalità e la regolarità delle operazioni e delle transazioni;
- garantire la conformità dei comportamenti alle procedure operative stabilite;
- monitorare l'efficacia e l'efficienza dei controlli insiti nelle procedure operative stesse;
- identificare, prevenire e gestire i potenziali rischi operativi cui l'Agenzia è soggetta (compresi i rischi di frode);
- verificare che i controlli previsti siano effettivamente eseguiti, segnalando gli eventuali disallineamenti e le possibili azioni correttive;
- consentire l'individuazione di opportunità di miglioramento dell'efficacia e dell'efficienza del sistema dei controlli dell'Agenzia.

Le principali responsabilità, in termini di controllo, afferiscono ai seguenti ambiti:

- le procedure adottate, il sistema di controllo e di monitoraggio di ARPEA;
- i beneficiari.
- le attività eventualmente delegate ai soggetti convenzionati con ARPEA;
- i Sistemi informativi;
- la contabilizzazione e le rendicontazioni / comunicazioni trasmesse all'ente di Coordinamento a livello di Stato membro (AGEA Coordinamento) e agli enti di controllo unionali (es. Commissione Europea, Corte dei Conti Europea).

I risultati dell'attività svolta dal CI supportano, infine, la "Dichiarazione di gestione" del Direttore di ARPEA (di cui all'articolo 90, primo comma, lettera c), punto iii), del regolamento (UE) n. 2021/2116).

1.5 Struttura organizzativa del CI

Il CI dipende direttamente dal Direttore di ARPEA, pertanto è indipendente da altre Aree e Uffici dell'Agenzia stessa.

Il CI, in caso di condizionamenti nell'indipendenza organizzativa o nell'obiettività individuale, deve tempestivamente comunicare al Direttore le circostanze di tali avvenimenti.

Tra i fattori che possono condizionare l'indipendenza o l'obiettività si possono annoverare conflitti di interesse individuali, limitazione del campo di azione, restrizioni dell'accesso a dati e persone e vincoli di risorse, tra cui quelle finanziarie.

Il CI per poter svolgere correttamente le proprie funzioni deve poter avere accesso:

- alla documentazione relativa alle singole pratiche presenti presso le Strutture di ARPEA, degli OD, dei CAA, dei beneficiari;
- a tutti i dati contenuti nelle banche dati utilizzate da ARPEA (es. SIGOP, SIAP, DoQui, BDN, ecc.);
- alle registrazioni contabili (cartacee e informatiche) gestite da ARPEA e dal suo Tesoriere;
- a ogni altra informazione che ritenga utile.

Il CI per poter mantenere l'indipendenza e l'oggettività di giudizio:

- non deve avere responsabilità diretta nei processi oggetto del controllo;
- non deve occuparsi direttamente del disegno, dell'installazione e dell'esecuzione dei processi operativi, né della definizione delle procedure.

Tuttavia, ai funzionari del CI è richiesto di avviare e mantenere un approccio di positiva collaborazione con le unità oggetto di audit, pur tenendo in adeguata considerazione i propri compiti di controllo.

1.6 Protocolli di comunicazione

I membri del CI sono tenuti al massimo riserbo relativamente alle informazioni ricevute o raccolte nel corso del loro ufficio e debbono operare all'interno di chiari protocolli di comunicazione.

Le comunicazioni dell'Ufficio Controllo Interno sono essenzialmente rivolte verso le seguenti tre classi di soggetti:

a. i soggetti auditati

Sono i primi destinatari dei rapporti di audit. Le modalità di comunicazione con tali soggetti, esplicitate nel successivo capitolo 3, sono regolate dal presente manuale per quanto concerne sia la fase preliminare ed esecutiva dell'intervento di audit, sia la fase di rendicontazione dei risultati dell'intervento stesso.

b. il Direttore di ARPEA

È il primo destinatario dei rapporti di audit elaborati dal CI.

Il Direttore è inoltre responsabile dell'approvazione del piano di audit annuale e delle sue eventuali variazioni nel corso dell'anno.

Infine, il Direttore dell'Agenzia è il destinatario della relazione finale di sintesi sull'attività svolta (per maggiori dettagli si rimanda al paragrafo "Relazione annuale dell'Ufficio Controllo Interno").

c. la Commissione Europea, la Corte dei Conti Europea, l'Organismo di certificazione ed il MASAF

Gli Organi comunitari, l'Organismo di certificazione e il MASAF hanno libero accesso, su loro richiesta, ai rapporti degli interventi ed ai piani di audit. Nei confronti di tali soggetti, il CI deve adottare un approccio collaborativo e, laddove opportuno, di supporto.

1.7 I principi etici di riferimento per il personale dell'Ufficio CI

Il CI si ispira al Codice Etico dell'AIIA, Associazione Italiana Internal Auditors, il cui scopo è quello di promuovere una cultura etica nell'esercizio della professione di Internal Auditor.

Al paragrafo 9 sono riportati i principi deontologici di riferimento degli Auditors.

1.8 Responsabilità del Direttore di ARPEA e dei componenti dell'Ufficio Controllo Interno

All'interno dell'Ufficio Controllo Interno sono distinguibili tre livelli di responsabilità gerarchica, oltre agli Auditor impegnati nelle attività di natura più strettamente operativa. Ruoli, compiti e responsabilità sono descritti di seguito.

Il **Direttore di ARPEA**, con riferimento all'attività di CI:

- nell'ambito dei protocolli di comunicazione previsti, supervisiona l'attività del CI, in conformità a quanto previsto dal Regolamento 2022/127, secondo cui il Controllo Interno "riferisce direttamente al direttore dell'organismo";
- approva il piano annuale di audit e il piano quinquennale, il manuale di controllo interno e le relative proposte di variazione;
- approva il Piano Antifrode triennale e le relative proposte di variazione;
- approva i rapporti di audit, in presenza di osservazioni tali da rendere necessario il recupero, totale o parziale, degli aiuti erogati e/o il ridimensionamento della spesa ammissibile a contributo;
- attiva le collaborazioni con soggetti esterni ad ARPEA, per l'affidamento di incarichi mirati di auditing;
- gestisce le risorse umane, strumentali e finanziarie assegnate al CI, assicurando un'idonea formazione del personale.

Il **Coordinatore del CI** si occupa delle seguenti attività:

- coordina e supervisiona la pianificazione delle attività del CI;
- individua le aree di controllo da verificare nel piano quinquennale e annuale di audit, sentito il Responsabile dell'ufficio CI;
- supporta, in collaborazione con il Responsabile del CI, il Direttore in occasione delle verifiche da parte delle autorità di certificazione, delle autorità di controllo comunitarie, nazionali e regionali e della Corte dei Conti;
- coordina la strategia antifrode, individuando misure idonee a prevenire e segnalare frodi o sospette frodi nel processo dei pagamenti comunitari.

Il **Responsabile del CI** ha il compito di:

- assistere il Direttore di ARPEA nel valutare il funzionamento del sistema dei controlli e delle procedure operative e supportare il Direttore nella predisposizione della Dichiarazione di Gestione;
- coordinare e supervisionare la pianificazione annuale delle attività dell'Ufficio Controllo Interno;
- predisporre il piano annuale e quinquennale di audit e curare la redazione della relazione annuale dell'Ufficio Controllo Interno;
- predisporre il Piano Antifrode triennale, curarne eventuali aggiornamenti/modifiche in armonizzazione con il Piano Triennale della Prevenzione della Corruzione e predisporre le misure di competenza del Controllo Interno idonee a prevenire e segnalare frodi o sospette frodi nel processo dei pagamenti comunitari;
- assicurare il regolare svolgimento delle attività programmate all'interno del piano di audit annuale approvato dal Direttore di ARPEA, garantendone l'esecuzione anche attraverso l'affiancamento degli Auditor per le verifiche più complesse;
- approvare il memorandum di pianificazione e i rapporti finali di audit;
- proporre e coordinare le collaborazioni con soggetti esterni per l'affidamento di attività di Internal audit;
- garantire il supporto alle operazioni di controllo da parte dell'organismo di certificazione, della CE, della CCE e del MASAF, ove richiesto dal Direttore di ARPEA;

- assistere il Direttore di ARPEA, con la collaborazione degli uffici interessati, nello svolgimento delle attività inerenti il riconoscimento di ARPEA;
- assistere i Responsabili degli uffici e dei processi nell'identificazione e nella valutazione delle aree maggiormente esposte ai rischi, curando la salvaguardia degli obiettivi e delle finalità di ARPEA;
- curare il periodico aggiornamento del manuale rispetto agli standard dell'attività di auditing;
- garantire la raccolta, l'ordinamento e l'archiviazione di tutta la documentazione e le evidenze necessarie a supportare le conclusioni tratte nel corso degli interventi di audit;
- coordinare e garantire il tempestivo reperimento dei commenti degli uffici oggetto di audit, da includere nel rapporto finale di ciascun intervento;
- programmare gli interventi di riscontro (follow-up) relativi alla correzione delle anomalie di controllo, alla mitigazione dei rischi e al recepimento delle raccomandazioni, anche curando il periodico aggiornamento del Master Plan;
- assicurare e curare direttamente il presidio di internal audit con riferimento al GDPR, anche mediante programmazione separata;
- gestire le risorse umane, strumentali e finanziarie assegnate al CI, assicurando un'adeguata formazione del personale;
- supportare l'organismo certificatore nelle verifiche ed analisi finalizzate alla certificazione dei conti e alla redazione dei relativi atti;
- coordinare le attività inerenti alla presentazione dei conti alla Commissione Europea e la redazione della Dichiarazione di Gestione unitamente ai relativi allegati.

Gli **Auditor** hanno il compito di:

- predisporre e/o aggiornare le mappature dei processi oggetto di audit ed effettuare il relativo Risk Assessment, anche con riferimento ai rischi di frode, considerando anche le analisi dei processi e dei risultati degli interventi di audit;
- svolgere tutte le attività necessarie a pianificare e svolgere i singoli interventi di audit;
- raccogliere, ordinare ed archiviare tutta la documentazione e le evidenze necessarie a supportare le conclusioni tratte nel corso degli interventi di audit;
- redigere le bozze dei Memorandum di Pianificazione dell'Intervento e dei rapporti di audit;
- al termine di ciascun intervento, sottoporre agli interessati le proprie conclusioni e le proprie eventuali osservazioni, raccogliendone i commenti;
- effettuare gli interventi di riscontro (follow up) relativi alla correzione delle anomalie di controllo, alla mitigazione dei rischi e al recepimento delle raccomandazioni;
- aggiornare le tavole di "follow-up" al termine di ciascun singolo intervento di audit;
- partecipare agli specifici percorsi di formazione;
- monitorare periodicamente il rispetto e il mantenimento dei criteri di riconoscimento, come previsto dal Reg. (UE) 2022/127, attraverso la predisposizione di specifici report;
- supportare l'organismo certificatore nel corso delle sue attività;
- supportare il Responsabile del CI nella redazione degli atti inerenti la Dichiarazione di Gestione.

2 PIANO QUINQUENNALE E ANNUALE DI AUDIT

L'attività dell'Ufficio Controllo Interno di ARPEA è pianificata mediante il piano quinquennale e il piano annuale di audit.

Nei successivi paragrafi vengono, pertanto, illustrate le linee guida per la definizione del piano quinquennale e del piano annuale di audit.

2.1 Piano quinquennale di Audit

Il piano quinquennale di audit, come anche il piano annuale (si veda paragrafo seguente), ha lo scopo di individuare gli obiettivi dell'Organismo Pagatore, come richiesto dall'allegato I del Regolamento n. 2022/127, al punto 1, lettera c); l'individuazione di tali obiettivi è propedeutica alla valutazione dei rischi, incluse potenziali irregolarità o frodi legati a tali obiettivi (a tale proposito si veda quanto specificato in seguito a proposito della valutazione dei rischi).

Il piano quinquennale di audit definisce le linee programmatiche di medio termine delle attività svolte dall'Ufficio Controllo Interno e viene redatto in modo da garantire che "il programma di lavoro garantisca la copertura di tutti i settori importanti, compresi i servizi responsabili dell'autorizzazione, per un periodo non superiore a cinque anni", ai sensi di quanto previsto dall'Allegato I, par. 4, lett. B punto ii) del Reg. (UE) 2022/127.

Nell'ambito della redazione del piano, dapprima, sono individuati tutti i processi strategici di ARPEA. Nell'ambito di tali processi rientrano quelli relativi alle specifiche misure/linee di finanziamento, i processi trasversali (autorizzazione, esecuzione e contabilizzazione dei pagamenti), i processi secondari /di supporto (gestione del registro debitori, delle garanzie e dei capitoli di bilancio), la corretta operatività degli uffici interni e degli Organismi Delegati, la sorveglianza dei processi per i quali sono state in precedenza riscontrate significative criticità, la gestione della sicurezza delle informazioni (Sistemi Informativi), la conformità a quanto previsto dal GDPR (Regolamento 2016/679) in tema di privacy.

Inoltre, il CI tiene in considerazione i seguenti aspetti rilevanti:

- aspettative e indicazioni del Direttore, con riferimento alla mitigazione di rischi segnalati e/o al coinvolgimento in progetti speciali;
- disposizioni del legislatore nazionale / unionale;
- rilevanza e rischiosità dei processi/linee di finanziamento;
- risultanze delle indagini da parte degli Organismi e Servizi di controllo (Commissione Europea, Corte dei Conti, MASAF, ecc.)

Sulla base delle conseguenti valutazioni, vengono distribuiti gli interventi di auditing nel quinquennio di riferimento.

Il piano quinquennale viene rivisto annualmente parallelamente alla redazione del piano annuale, al fine di prendere in considerazione eventuali ampliamenti dell'attività di ARPEA, modifiche normative, cambiamenti organizzativi, eventuali segnalazioni di Organi di Controllo, segnalazioni da parte della Commissione Europea o della Autorità Competente.

Il piano quinquennale di audit è approvato dal Direttore di ARPEA su proposta del Coordinatore del CI e del Responsabile del CI.

2.2 Piano annuale di Audit

Il piano quinquennale di audit viene attuato attraverso il **piano annuale** che definisce in dettaglio i programmi e gli obiettivi del CI per l'anno in corso.

L'attività prevista nel piano annuale deve:

- essere coerente rispetto alle linee guida definite nel piano quinquennale di audit;
- dare risposte adeguate alle aspettative del management e del Direttore, in termini di mitigazione dei rischi segnalati;
- supportare il Direttore di ARPEA nella predisposizione della "Dichiarazione di Gestione" (di cui all'articolo 90, primo comma, lettera c), punto iii), del regolamento (UE) n. 2021/2116);
- allocare le risorse sugli interventi aventi la maggiore rilevanza, ovvero che maggiormente concorrano al raggiungimento degli obiettivi di ARPEA;

- tenere in considerazione eventuali altre esigenze del management per l'effettuazione di attività particolari (es. progetti speciali);
- verificare le aree non coperte dai precedenti piani.

Il piano annuale di audit, pertanto, individua all'interno dei macro-ambiti previsti dal Piano quinquennale le attività che verranno svolte dall'Ufficio Controllo Interno sui processi di ARPEA nell'anno corrente.

Il Piano annuale deve riportare per ciascun intervento di audit in programma le seguenti informazioni:

- *Tipologia*: descrive la tipologia di intervento effettuata, distinta tra Follow-up, Compliance, Operational o Altro
- *Descrizione*: codice e nome attribuito all'intervento
- *Processi Principali soggetti ad audit*: nome dei processi principali che sono soggetti ad audit nel corso dello svolgimento dell'intervento
- *Unità auditate / processi secondari auditati*: unità organizzative e nome dei processi secondari che sono auditati nel corso dello svolgimento dell'audit
- *Obiettivo*: descrive gli obiettivi che si intendono perseguire con l'esecuzione dell'intervento di audit. Inoltre descrive, quando applicabile, le strategie di audit che sono adottate e, sempre quando applicabile, le modalità di svolgimento dell'audit
- *Periodo previsto*: riporta il periodo nel quale è indicativamente prevista l'esecuzione dell'intervento.

Il piano annuale di audit viene presentato al Direttore di ARPEA per l'approvazione in tempo utile per lo svolgimento delle attività di audit pianificate entro il termine della chiusura dell'esercizio finanziario o al più tardi per la presentazione alla Commissione della Dichiarazione di gestione annuale dei conti. Il piano annuale di audit può essere opportunamente modificato, nel corso dell'anno, in funzione di eventuali cause di forza maggiore o di particolari e straordinarie esigenze tecniche di programmazione operativa. Tali modifiche sono soggette all'approvazione del Direttore.

2.3 Attività di Risk Assessment e modalità di valutazione dei rischi e dei controlli

In considerazione delle novità introdotte dai regolamenti che disciplinano la nuova PAC a partire dall'anno 2023, particolare importanza riveste il tema della valutazione dei rischi, dal momento che è stato inserito tra i criteri che ogni Organismo Pagatore deve rispettare al fine di mantenere il riconoscimento di cui all'articolo 9, paragrafo 2 del Regolamento n. 2021/2116. L'allegato I, punto 1, lettera c) al Regolamento n. 2022/127 richiede infatti che l'Organismo Pagatore garantisca l'individuazione dei rischi, incluse potenziali irregolarità o frodi, per il conseguimento dei propri obiettivi e l'analisi di tali rischi come base per determinare le modalità di gestione del rischio.

Al fine di supportare l'esecuzione delle attività di audit garantendo la copertura dei rischi, il CI si dota dunque di mappe dei processi dell'Agenzia, dei rischi inerenti e dei relativi controlli; tali mappature sono funzionali alla valutazione dei rischi (anche con riferimento ai rischi di frode) .

La valutazione dei rischi viene fatta sulla base dei parametri di probabilità e di impatto e la graduazione di tali parametri consente di costruire la griglia, usata per classificare i rischi individuati in ciascun processo e ai quali è stato attribuito un livello di probabilità e uno d'impatto.

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

Il CI valuta ciascun controllo in termini di efficacia nel mitigare il rischio e di avvenuta implementazione del controllo stesso. A tal fine le mappature intercettano anche i *Key and Ancillary Controls* (KAC) definiti dalla

Commissione Europea e pertinenti a ciascun processo, il cui confronto con i controlli mappati supporta gli Auditor nella valutazione complessiva dell'adeguatezza dei controlli a presidio dei rischi.

La definizione del livello di rischio di un processo è la sintesi della valutazione di tutti i rischi e dei relativi controlli.

Le mappature vengono predisposte/aggiornate dagli Auditor nel corso degli interventi di audit; nel corso degli anni vengono dunque mappati e tenuti sotto controllo tutti i processi. Il risk assesment è dunque un'attività di esame periodico che nell'arco di cinque anni copre tutti i settori dell'organismo pagatore; alcuni processi ad alto rischio vengono mappati ogni anno, altri, considerati meno rischiosi in base anche alle risultanze degli audit svolti in annate precedenti, mantengono differente cadenza periodica.

La predisposizione/aggiornamento del Risk Assessment richiede al CI di svolgere le seguenti attività nel corso di tutti gli audit programmati:

- a. confermare la propria comprensione dei processi in oggetto per ciascun singolo intervento;
- b. confermare la completezza del portafoglio dei rischi associati ai processi analizzati e i relativi controlli;
- c. confermare o modificare la valutazione dei rischi già rilevati e/o 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 condotto sul processo.

L'individuazione e la valutazione dei rischi di ciascun processo viene svolta dal CI in collaborazione con i responsabili dei processi stessi.

L'individuazione dei rischi avviene, in prima istanza, attraverso l'intervista al personale responsabile dei processi analizzati. In alternativa, i rischi possono essere identificati direttamente dal personale del CI sulla base delle esperienze maturate presso processi simili o con qualunque altro metodo ritenuto idoneo a tal fine. Ad ogni modo, il personale del CI è sempre tenuto a condividere le valutazioni effettuate con il personale responsabile dei processi analizzati.

Al fine di limitare il più possibile la discrezionalità nell'effettuazione della valutazione dei rischi, il CI si avvale della "Matrice per la valutazione dei rischi".

Attraverso l'applicazione ragionata dei contenuti della matrice vengono definiti Probabilità e Impatto di ciascun rischio oggetto di valutazione.

Nell'ambito della definizione della **probabilità** del rischio occorre effettuare la valutazione della frequenza di accadimento di tale rischio. In particolare, la probabilità che un rischio si verifichi può essere:

1. **Bassa:** la probabilità di accadimento del rischio è molto contenuta e appare improbabile che il rischio si verifichi durante l'attuazione di una misura/operazione;
2. **Moderata:** la probabilità di accadimento del rischio è frequente, ma non continua, e il rischio potrebbe verificarsi in maniera occasionale durante l'attuazione di una misura/operazione;
3. **Alta:** la probabilità di accadimento del rischio è elevata ed è probabile che il rischio si verifichi continuamente, e comunque più di una volta, durante l'attuazione di una misura/operazione.

La valutazione dell'**impatto** del rischio consente di definire il livello in cui il manifestarsi del rischio influenzerebbe il raggiungimento delle strategie e degli obiettivi dell'Agenzia. In particolare, l'impatto può essere classificato come:

1. **Grave:** si verifica un impatto significativo sul raggiungimento degli obiettivi strategici dell'Organismo Pagatore (es.: frodi o malversazioni; perdita di requisiti per il riconoscimento dell'Organismo Pagatore; perdita o significativa riduzione della credibilità/immagine nei confronti

- dei beneficiari, degli OD o di altri portatori di interesse; sanzioni penali a carico dei funzionari; perdita di fondi per correzioni finanziarie);
2. Moderato: si verifica quando si registra un'inefficienza delle normali operazioni con un effetto limitato sul raggiungimento degli obiettivi strategici dell'Organismo Pagatore (es.: interruzione o significative inefficienze nel processo delle domande; problemi temporanei di qualità/servizio; inefficienze nei flussi e nelle operazioni);
 3. Insignificante: non si registra alcun impatto concreto sulla strategia dell'Organismo Pagatore. Si tratta di situazioni diverse dalla norma che richiedono comunque azioni correttive.

Sulla base della Probabilità e dell'Impatto definiti, è quindi possibile concludere la valutazione del rischio attraverso l'utilizzo dell'apposita matrice di raccordo (vedi Figura 1).

Figura 1 - Matrice di raccordo probabilità - impatto per la valutazione dei rischi

IDENTIFICAZIONE E VALUTAZIONE DEL RISCHIO ATTRAVERSO LA
"RISK ASSESSMENT CRITERIA MATRIX"

I M P A T T O	3 grave	M	A	A
	2 moderata	B	M	A
	1 insignificante	B	B	M
		1 bassa	2 moderata	3 alta

Definizioni :

A = Alto

M = Medio

B = Basso

PROBABILITÀ

A fronte dei rischi identificati, sono poi individuati quei controlli che consentono la loro mitigazione entro livelli accettabili.

Il CI deve valutare ciascun controllo in funzione di due aspetti:

- efficacia del controllo nel mitigare il rischio sottostante
- effettività nello svolgimento del controllo

La valutazione dell'efficacia dei controlli nel mitigare i rischi sottostanti viene effettuata valutando il raggiungimento degli obiettivi del controllo ad essi applicabili, di seguito riepilogati nella tabella 1.

Tabella 1– Obiettivi di controllo

Obiettivo	Esempio
Legittimità e regolarità dell'attività	Il controllo in essere garantisce che l'attività sia svolta conformemente ad adeguati percorsi autorizzativi ed alle procedure ed ai dettami giuridici esistenti
Efficacia dell'attività	Il controllo in essere garantisce che l'attività sia svolta in modo da assicurare il raggiungimento degli obiettivi del processo
Efficienza dell'attività	Il controllo in essere garantisce che l'attività sia svolta in modo da raggiungere gli obiettivi del processo, nei tempi e con le risorse desiderate
Correttezza delle operazioni	Il controllo in essere garantisce che le operazioni siano svolte correttamente
Completezza ed accuratezza delle operazioni	Il controllo in essere garantisce che le operazioni siano svolte completamente e accuratamente
Tracciabilità delle operazioni	Il controllo in essere garantisce la completezza e la rintracciabilità della documentazione relativa alle transazioni
Realtà delle operazioni	Il controllo in essere garantisce che le transazioni sono effettivamente realizzate
Valutazione delle transazioni	Il controllo in essere garantisce che le transazioni sono correttamente valutate
Imparzialità delle valutazioni	Il controllo in essere garantisce che le valutazioni siano effettuate con imparzialità (indipendenza)
Evidenza del controllo	Il controllo svolto è adeguatamente documentato

La valutazione dell'effettività di un controllo è eseguita solo per i controlli giudicati efficaci nella mitigazione dei rischi sottostanti.

Valutare l'effettività del controllo significa riscontrarne la costante effettuazione in conformità con quanto previsto nella sua definizione.

La valutazione del controllo avviene attraverso l'esecuzione di specifici test sui controlli.

La valutazione dei controlli fa riferimento al rischio sottostante ed è quindi espressa come nella seguente tabella 2.

Tabella 2– Valutazione del controllo

Valutazione del controllo	Descrizione della Valutazione
Non adeguatamente controllato	I controlli previsti non consentono un'efficace riduzione del rischio oppure i controlli previsti non sono effettivamente eseguiti.
Adeguatamente controllato	I controlli previsti consentono un'efficace riduzione del rischio e sono effettivamente eseguiti.
Sovra controllato	I controlli previsti sono eseguiti e consentono una riduzione del rischio oltre il livello accettabile.
Non valutato	L'attività svolta dall'Ufficio di Controllo Interno non consente di valutare l'efficacia e l'effettività dei controlli.

Nel caso il controllo non possa essere valutato attraverso l'esecuzione di adeguati test sui controlli, il CI si limita a rilevare l'esistenza dei controlli o a raccomandarne l'implementazione, rilevando lo stato del controllo come esposto nella seguente tabella 3.

Tabella 3 – Stato del controllo

Stato del controllo	Descrizione dello Stato
Rilevato	I controlli che dovrebbero consentire un'efficace riduzione del rischio sono stati rilevati nel corso dell'intervista con il responsabile del processo.
Raccomandato	I controlli che dovrebbero consentire una riduzione del rischio non sono stati rilevati

2.4 Tipologie di intervento

Le tipologie di intervento del CI sono le seguenti:

- **Compliance Audit (Audit di conformità):** si focalizza essenzialmente sulla verifica della conformità dei comportamenti a norme, procedure e prassi interne, rispetto a quanto richiesto dal legislatore. Rientra in questa tipologia di intervento anche l'analisi della completezza e conformità delle procedure definite da ARPEA rispetto ai Regolamenti unionali, alle circolari di Agea Coordinamento e del MASAF.
- **Operational Audit:** riguarda il monitoraggio del rispetto degli obiettivi di ARPEA, per ogni livello di processo. Si tratta quindi di interventi volti a valutare l'efficacia e l'efficienza dei processi e dei controlli in essi previsti.
- **Follow-up (Monitoraggio delle azioni correttive):** interventi per la verifica dell'effettiva implementazione dei piani di azione concordati con i responsabili di processo, a fronte delle osservazioni rilevate nel corso di precedenti interventi dell'Ufficio Controllo Interno e condivise dai responsabili dei processi stessi.

3 L'INTERVENTO DI AUDIT

3.1 La pianificazione dell' intervento

Gli interventi previsti dal piano di audit annuale sono pianificati in termini di obiettivi, modalità operative e tempi nel "Memorandum di pianificazione", preparato dagli Auditor responsabili dell'esecuzione dell'intervento, approvato dal Responsabile CI e inviato ai Responsabili dei processi oggetto di audit, ai soggetti coinvolti, al Coordinatore del CI e al Direttore di ARPEA.

Durante la fase di pianificazione operativa, sono eseguite le seguenti attività:

- Ricerca/richiesta di informazioni sulle attività oggetto di analisi, volta alla predisposizione del programma di lavoro; tale attività viene svolta tramite ricerca da parte degli auditor o tramite interviste con i responsabili o i referenti dei processi interessati.
- Esame e valutazione delle informazioni ottenute/raccolte e predisposizione del programma di lavoro delle attività che saranno svolte sul campo, tramite la redazione del Memorandum di pianificazione;
- Comunicazione d'avvio dell'attività di audit a tutti i soggetti coinvolti nel processo oggetto di verifica, tramite invio del sopra citato Memorandum di pianificazione.

3.1.1 Acquisizione della documentazione/informazioni necessarie all'intervento di audit

In base alle attività da realizzare, gli Auditor assegnati al progetto predispongono, ove necessario, una lista della documentazione da ottenere dal responsabile del processo, prima della realizzazione del lavoro sul campo.

Tale documentazione è funzionale allo sviluppo di una conoscenza preliminare del processo oggetto di audit, così da poter effettuare un'adeguata pianificazione dell'intervento. Tra la documentazione esaminata in questa fase rientrano:

- carte di lavoro relative a precedenti audit sulla medesima area oggetto di verifica;
- eventuale tabella di follow up;
- manualistica interna;
- normativa di riferimento;
- bandi per la presentazione delle domande di aiuto;
- esiti delle verifiche eseguite sullo stesso processo da parte di altri organismi di controllo (es. organismo di certificazione, Corte dei Conti);
- dati quantitativi relativi alle domande finanziate, presenti nei sistemi informativi.

3.1.2 Formalizzazione del Memorandum di Pianificazione (Allegato 2)

Quanto stabilito nel piano annuale di audit, in termini di strategie / obiettivi dell'intervento, dovrà essere maggiormente dettagliato nel Memorandum di Pianificazione attraverso le seguenti fasi preliminari:

- analisi della mappatura del processo o dei processi (esame dei processi secondari, dei relativi rischi e controlli);
- analisi di leggi, regolamenti e disposizioni operative di riferimento di cui andrà verificata la corretta applicazione;
- analisi dei rapporti e delle carte di lavoro prodotte nel corso di precedenti interventi sui processi/unità auditate o di interventi simili in termini di strategie/obiettivi /processi/unità auditate;
- contatto informale con i responsabili dei processi auditati che può avvenire tramite colloquio telefonico, videochiamata, oppure riunione informale in presenza.

Il Memorandum di pianificazione, che rappresenta il risultato della preparazione iniziale dell'audit, contiene un approfondimento sulle motivazioni alla base dell'esecuzione dell'intervento di audit, la sua estensione, gli obiettivi e le risorse ad esso dedicate. È prevista, inoltre, una sintesi della documentazione da richiedere al responsabile del processo oggetto di audit / soggetti coinvolti, la cui preparazione deve essere effettuata prima dell'inizio dell'intervento di audit.

In generale, il "Memorandum di Pianificazione dell'Intervento" deve contenere i seguenti elementi essenziali:

- Informazioni generali
- Aree/processi selezionati
- Obiettivi e modalità di svolgimento dell'audit
- Criteri di campionamento / numerosità indicativa del campione
- Lista dei documenti richiesti
- Calendario della pianificazione e risorse coinvolte

Nel dettaglio, Il "Memorandum di Pianificazione dell'Intervento" è suddiviso tra i seguenti paragrafi, secondo lo schema dell'Allegato 2 al presente Manuale:

- **Informazioni generali**

Contiene brevi informazioni circa l'intervento di audit pianificato.

- **Aree/processi selezionati**

Indica le aree, le funzioni, i processi, le misure che devono essere sottoposte ad audit e le ragioni per cui sono stati selezionati. Se necessario, specifica le attività principali dei processi da sottoporre ad audit.

- **Obiettivi dell'audit**

Indica gli obiettivi generali dell'intervento di audit.

- **Modalità di svolgimento dell'audit**

Descrive le fasi e le attività in cui si articola l'intervento di audit.

- **Criteri di selezione dei soggetti da auditare (OD e CAA), criteri di campionamento e numerosità del campione di transazioni da verificare, ove applicabili;**

Contiene la sintesi dei criteri di campionamento (es. casuale, rischio, misto) che si prevede di adottare per la selezione degli item oggetto di audit.

- **Documenti richiesti**

Lista delle pratiche e dei documenti che dovranno essere resi disponibili quando si giungerà presso gli uffici del soggetto auditato.

- **Calendario dei lavori e risorse coinvolte**

Pianificazione preliminare dell'intervento con evidenza dei soggetti coinvolti durante l'esecuzione dell'intervento in oggetto, in particolare viene indicato:

- il responsabile dell'intervento di audit all'interno dell'Ufficio Controllo Interno;
- il personale operativo dell'Ufficio Controllo Interno che parteciperà all'intervento ed i rispettivi ruoli;
- il personale del processo / area / funzione auditato la cui partecipazione all'incontro è ritenuta indispensabile; in particolare dovrà essere richiesta la partecipazione dei responsabili del processo / area / funzione auditate ed i suoi collaboratori che supporteranno direttamente l'intervento.

Se possibile, all'interno del "Memorandum di Pianificazione dell'Intervento", dovrebbe essere già anticipato il periodo di discussione del rapporto finale dell'intervento e la scadenza per la ricezione di feedback da parte degli uffici interessati in merito ad eventuali osservazioni sorte nel corso dell'intervento.

3.1.3 Campionamento

Nella fase preliminare dell'audit vengono definiti:

- i soggetti da auditare, con particolare riferimento agli OD e ai CAA, sulla base di parametri quantitativi (es: numero e importo delle domande gestite) e qualitativi (es: esiti di precedenti controlli, tempo trascorso dall'ultimo controllo effettuato)
- l'universo delle transazioni all'interno del quale effettuare il campionamento.

Il numero delle transazioni da selezionare è deciso dagli Auditor incaricati dell'intervento, in accordo con il Responsabile CI, sulla base del giudizio professionale.

È comunque facoltà dell'Auditor controllare un ulteriore campione di transazioni, nel caso in cui vengano riscontrati errori sostanziali nel campione oggetto di verifica.

La modalità di scelta delle transazioni da controllare deve garantire che il campione sia il più possibile rappresentativo all'interno della popolazione di riferimento.

3.1.3.1 Tipi di campionamento

La selezione del campione può essere effettuata sulla base di due distinti metodi o dalla combinazione dei due: il metodo statistico ed 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 rispetto al metodo non statistico in cui l'ampiezza del campione è decisa dal personale dell'Ufficio Controllo Interno sulla base della propria valutazione professionale.

La decisione se utilizzare un metodo statistico o meno per la selezione di un campione di transazioni è lasciato al giudizio professionale del Responsabile del CI, in relazione alla modalità ritenuta maggiormente efficiente per ottenere evidenze di revisione nelle specifiche circostanze. Ad esempio nella selezione dei test dei controlli nella fase esecutiva, l'analisi dell'auditor 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 dalle circostanze. Indipendentemente dalla scelta fatta, il Responsabile del CI deve operare per fare sì che il metodo utilizzato dia sufficiente evidenza per raggiungere gli obiettivi prefissati nel test. Egli deve, inoltre, approvare la scelta della metodologia di campionamento utilizzata.

In generale, per fornire un indirizzo operativo, la selezione basata sul giudizio professionale è generalmente ritenuta più efficiente nel contesto delle attività tipiche dell'Ufficio Controllo Interno, non essendo primario obiettivo dell'ufficio la determinazione di conclusioni aventi rigore statistico e probabilistico, quanto piuttosto l'evidenziazione alla Direzione di eventuali rischiosità non adeguatamente governate/presidiate.

Tuttavia in specifiche circostanze potrebbe essere necessario dover effettuare approfondimenti che richiedono rigore statistico, anche - ad esempio- a seguito di richieste da parte della Direzione,.

3.1.3.2 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 item;
- la selezione a campione non statistico.

Selezione del 100% della popolazione: il Responsabile del CI, anche su proposta del Coordinatore del CI, può decidere che potrebbe essere maggiormente appropriato esaminare l'intera popolazione di item che compongono un capitolo di bilancio, o di un elenco di pagamenti, di domande di aiuto etc. L'esame del 100% degli item, sebbene sia non frequente nel caso dei test sui controlli, può essere applicato alle procedure di verifica di sostanza. Ad esempio l'esame del 100% delle transazioni potrebbe essere appropriata nel caso di popolazioni costituite da un limitato numero di item di grande valore, e quando i rischi non diano sufficienti garanzie.

Selezione di specifici item: il Responsabile del CI, anche su proposta del Coordinatore del CI, può decidere di selezionare specifici item di una popolazione di dati basandosi su fattori quali la conoscenza del settore, la propria preliminare valutazione del rischio, l'evidenza di situazioni particolari emerse a seguito di precedenti interventi di audit, da indagini di organi esterni, da segnalazioni provenienti da altri uffici, 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 nelle circostanze. La selezione degli specifici item può includere:

- *items di valore significativo*: il Responsabile del CI può decidere di selezionare specifici item in una popolazione perché sono di importo significativo;
- *items che si trovano in particolari situazioni*: il responsabile del CI può decidere di selezionare specifici items perché ad esempio si tratta di transazioni inusuali, particolarmente rischiose o che siano state caratterizzate da errori nel passato;
- *tutti gli item superiori ad un determinato ammontare*: il Responsabile del CI può decidere di esaminare gli item il cui valore eccede un predeterminato ammontare in modo da verificare una percentuale significativa della spesa, o delle specifiche transazioni;
- *item selezionati al fine di ottenere informazioni*: il Responsabile del CI può scegliere di esaminare taluni specifici item al fine di ottenere informazioni su particolari problematiche, sulla natura delle transazioni, sulla contabilità e sul controllo interno nonché al fine di approfondire le conoscenze del settore;
- *item per testare una procedura*: il Responsabile del CI può usare il proprio giudizio per selezionare ed esaminare specifici item l'esame dei quali può risultare utile al fine di determinare se una determinata procedura sia stata correttamente applicata.

È importante evidenziare che, mentre da un lato la selezione e l'esame di specifici item è spesso un metodo efficiente, dall'altro non costituisce un campionamento. I risultati delle procedure di audit effettuate su specifici item selezionati non possono essere estesi all'intera popolazione. Tale modalità deve dunque essere utilizzata con particolare moderazione e adeguatamente motivata.

Il Responsabile del CI deve considerare la necessità di ottenere una appropriata evidenza relativamente alla restante parte della popolazione quando la restante parte è materiale.

La selezione a campione non statistico: per procedere alla selezione a campione il Responsabile del CI, anche su proposta del Coordinatore del CI, deve considerare gli obiettivi del test da svolgere e gli attributi della popolazione da cui il campione deve essere estratto. Più in particolare, con riferimento agli obiettivi, occorre considerare la natura del test da svolgere e dell'evidenza di audit necessaria anche al fine di definire ciò che costituisce un errore, e la loro rilevanza ai fini di una eventuale proiezione. Con riferimento alla popolazione l'auditor deve accertare che la popolazione sia appropriata rispetto agli obiettivi dell'intervento di audit, nonché completa.

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

- *la valutazione del rischio inerente*: un incremento di rischiosità nella valutazione del rischio inerente 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 audit*: l'utilizzo 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 pianificato*: 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*: prima di procedere all'estrazione, si suddivide la popolazione in due o più gruppi secondo una o più caratteristiche conosciute sulle unità statistiche. Si procede quindi all'estrazione delle unità indipendentemente per ogni gruppo (strato). Questa modalità di pianificazione del campione consente di ottenere stime più precise, a parità di dimensione del campione, rispetto al campione casuale semplice purché all'interno degli strati le unità statistiche siano fra loro omogenee riguardo alle variabili oggetto di studio;
- *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 basato su un approccio non statistico sono:

- l'utilizzo di numeri casuali generati dal computer, dalle tavole numeriche o da specifici programmi/tool/app dedicati;
- la selezione sistematica, in cui il numero di item dell'universo è diviso per il numero di item del campione, al fine di individuare l'intervallo di campionamento, per esempio 100, ed avendo scelto un punto di partenza dentro i primi 100 item, si procederà selezionando di lì in avanti un item ogni 100;
- la selezione casuale, in cui l'auditor effettua una selezione senza seguire una tecnica strutturata;
- la selezione stratificata, in cui 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, ecc.).

Ulteriori metodi possono di volta in volta essere individuati dal Responsabile del CI, anche attraverso la combinazione delle tecniche sopra illustrate, sulla base della propria esperienza, tenuto conto delle finalità e degli obiettivi dell'intervento di audit.

3.1.3.3 La scelta del metodo di campionamento

Come precedentemente accennato non è sempre necessario effettuare una selezione di un campione rappresentativo statisticamente. In genere il metodo di campionamento da preferire nelle attività di verifica da parte dell'Area Controllo Interno è la selezione non statistica, specie se ci si trova di fronte ad un universo composto da un limitato numero di richiedenti il contributo/aiuto. Pur tuttavia, l'utilizzo di tecniche statistiche può essere necessario per specifiche esigenze di approfondimento di eventuali temi o anomalie riscontrate, oppure nel caso di popolazioni numerose.

L'individuazione della metodologia di campionamento deve essere comunque effettuata dopo aver valutato i seguenti dati qualitativi e quantitativi:

- esborso finanziario nell'ultima campagna pagata;
- numero di domande presentate;
- numero di domande liquidate;
- risultanze di precedenti audit e follow up;
- disomogeneità della tipologia di aiuti all'interno del processo;
- distribuzione territoriale (concentrazione) degli aiuti;

- numerosità e caratteristiche degli OD coinvolti nel processo (es. dotazione di addetti di ciascun OD per l'effettuazione delle attività di istruttoria, in rapporto al numero di domande istruite ed agli importi erogati; numero di sanzioni erogate nel periodo precedente, assumendo come indicatore di efficienza dei controlli un maggior indice di sanzioni erogate in relazione alle domande istruite; ecc.).

Le operazioni di campionamento vengono tracciate dagli Auditor redigendo un **memorandum di estrazione**, di cui si riporta lo schema di riferimento nell'Allegato 3.

3.1.4 Comunicazione d'avvio dell'attività di audit

L'avvio di un'attività di audit deve essere sempre comunicato in forma scritta da parte del Responsabile CI alle Aree/ Uffici / soggetti che saranno coinvolti nell'audit.

Alla comunicazione d'avvio delle attività di audit viene allegato il Memorandum di Pianificazione.

La comunicazione è inviata per conoscenza anche al Direttore di ARPEA.

3.2 L'esecuzione dell'intervento di audit

3.2.1 Svolgimento della riunione di apertura

All'interno del Memorandum di Pianificazione, il Responsabile del CI indica il periodo nel quale verranno avviate e presumibilmente terminate le attività di audit; L'attività viene svolta tramite uno o più incontri con i responsabili o referenti dell'area/ufficio responsabile del processo oggetto di audit.

Durante il primo incontro, di norma, sono presentati e discussi i seguenti argomenti:

- scopo e obiettivi dell'intervento di audit, già definiti nel Memorandum di Pianificazione;
- modalità operative di esecuzione dell'intervento (ad esempio interviste con il personale, analisi delle transazioni rilevanti, "walk-through test", test sulle attività, rilevazione dei rischi, ecc.) e il tempo stimato necessario;
- la documentazione che verrà prodotta (es.: check-list, ecc) ed i relativi contenuti;
- le date indicative dei successivi incontri da svolgere durante ed 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 di audit, rispetto al processo in esame, allo scopo di ottenere la massima disponibilità e la positiva collaborazione dell'ufficio o area sottoposto ad audit.

3.2.2 Analisi del processo

L'attività di analisi dei processi si svolge mediante interviste con i responsabili delle attività e il personale operativo e con l'analisi dei documenti esistenti, quali procedure e manuali, flow chart, modulistica operativa, ecc.

Nella fase di analisi del processo, gli Auditor analizzano l'efficacia dei controlli dal punto di vista strutturale ("design effectiveness"): valutano, cioè, se ciascun controllo sia strutturato in modo adeguato a coprire un'area di rischio all'interno del processo.

Seguendo il piano delle interviste concordato inizialmente, l'Auditor contatta il responsabile o il personale operativo per effettuare l'incontro.

In particolare, attraverso il colloquio con il personale del processo auditato, devono essere individuati gli elementi essenziali dei processi e/o delle attività:

- inizio e fine del processo/attività;
- le risorse coinvolte;
- il risultato del processo/attività;
- le modalità operative;
- le responsabilità;
- le informazioni gestite;
- le normative di riferimento applicabili.

Pertanto, attraverso l'intervista vengono acquisiti elementi che permettono la predisposizione o l'aggiornamento della mappatura del processo (Risk Assessment) da parte dell'Auditor che ha effettuato l'intervista, sotto la supervisione del Responsabile del CI.

Gli aspetti ritenuti critici devono essere approfonditi ulteriormente con il responsabile del processo/attività, richiedendo ulteriore documentazione specifica o effettuando specifici test allo scopo di individuare le possibili cause, o concordando ulteriori incontri.

Dall'effettuazione dei test sul processo, l'Auditor deve essere in grado di valutare se il processo presenta dei rischi, se i controlli in essere sono (in via preliminare) efficaci/efficienti e se esistono opportunità di miglioramento delle attività.

3.2.3 Svolgimento dei test sui controlli

Sulla base di quanto previsto nel Memorandum di Pianificazione, l'Auditor esegue i test sui controlli rilevati in fase di mappatura del processo, al fine di raccogliere evidenze, verificare e valutare l'efficacia dei controlli posti in essere da parte del responsabile del processo oggetto di audit. Tale attività viene condotta su un campione di controllo adeguatamente identificato.

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

- valutare l'efficacia del controllo nel prevenire il rischio ed eventuali rischi di frode individuati (fraud list), anche alla luce di eventuali KAC applicabili;
- identificare aree di miglioramento nei processi e nei relativi controlli;
- identificare le criticità e condividerle con i responsabili dei processi.

L'attività di identificazione è stata effettuata preliminarmente nelle fasi di:

- Risk Assessment;
- predisposizione del Memorandum di pianificazione;
- analisi dei processi.

Per l'esecuzione dei test deve essere predisposta apposita check-list, integrata, ove applicabile, con una sezione dedicata ai controlli a presidio dei rischi di frode (in base alla "fraud list" individuata nell'ambito della mappatura del processo), in base alla quale l'Auditor esegue le procedure di controllo descritte e valuta l'efficacia e l'effettività dei controlli, individuando eventuali aree di miglioramento.

Il test deve verificare che il controllo:

- operi come dovrebbe;
- sia applicato per tutto il periodo di tempo previsto per la copertura efficace del rischio associato;
- sia eseguito tempestivamente tutte le volte che si rende necessario;
- copra tutte le transazioni a cui è applicabile;
- si fondi su informazioni affidabili;

- corregga tempestivamente gli errori che identifica;
- sia in linea con gli eventuali KAC applicabili al processo oggetto di audit.

Durante l'esecuzione della procedura di controllo, l'Auditor deve indagare, osservare e verificare l'evidenza fisica dei risultati del controllo, inclusi quelli di routine.

L'indagine e l'osservazione possono non fornire sufficiente evidenza che un controllo opera per tutto il periodo preso in considerazione. In tal caso la verifica dell'evidenza fisica/documentale può dare l'evidenza dell'efficace operazione di controllo. Inoltre, se la funzione auditata non genera evidenze fisiche dell'efficacia del controllo e non mantiene la registrazione di tale operazione, non è possibile valutare se il controllo funziona come previsto.

È necessario utilizzare il proprio giudizio professionale nel determinare l'estensione dei test. I fattori da considerare sono:

- frequenza del controllo: tanto meno frequentemente è svolto un controllo manuale tanto maggiore deve essere l'estensione dei test;
- affidabilità del controllo: più elevato è il livello di affidabilità che si pone sul controllo, tanto meno esteso deve essere il test;
- evidenza prodotta dal controllo: se i risultati del controllo forniscono evidenze scarse o indirette che il controllo operi efficacemente, il test non fornisce la garanzia necessaria. D'altra parte, se l'evidenza è persuasiva, si può decidere di contenere l'ampiezza del test.
- periodo di riferimento del controllo nel tempo: in considerazione della necessità di assicurare che il controllo sia operante per tutto il periodo verificato, nella pianificazione dei test, si deve tenere conto dell'arco temporale sottoposto a verifica e delle evidenze da produrre in tempi diversi all'interno del periodo. Più il periodo di riferimento è lungo, più è necessario aumentare l'ampiezza dei test e la loro articolazione nel tempo;
- Esistenza di una combinazione di controlli che può ridurre il livello di garanzia necessario per ogni singolo controllo: quando i controlli relativi a un determinato obiettivo di controllo sono esistenti e testati, il livello di garanzia che si rende necessario per ciascun controllo può essere meno elevato rispetto all'esistenza di un unico controllo.
- Altri elementi relativi alla probabilità che il controllo operi come previsto: relativamente alla probabilità che il controllo operi come previsto nell'arco di tempo considerato, nella determinazione dell'ampiezza dei test vanno considerati i seguenti elementi:
 - la competenza del personale che esegue il controllo, il livello con cui il dipendente è controllato dai superiori e il turn over del personale;
 - la probabilità che il controllo sia omissso durante periodi di lavoro intenso (picchi di lavoro);
 - la possibilità di omettere il controllo da parte del responsabile del processo o da parte del personale preposto;
 - la presenza di fattori di rischi di frode che sono stati identificati e non sufficientemente mitigati da altri controlli.

Conclusi i test, si deve esprimere un giudizio sull'efficacia dei controlli. Nel caso in cui dal test emerga che il controllo in essere garantisce 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 evidenze 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.

La check list di controllo, che traccia le evidenze dei test effettuati, deve garantire un'adeguata pista di controllo e deve essere sottoscritta dall'auditor incaricato ad effettuare le verifiche.

L'attività svolta dall'Auditor deve essere sintetizzata in un *rapporto provvisorio di audit*, che documenta la natura, l'estensione ed i risultati del test.

In particolare devono essere indicati:

- gli elementi identificativi dell'attività (codice intervento, processo, responsabile del processo, riferimento al Memorandum di pianificazione, data, Auditor);
- l'obiettivo del test;
- l'attività svolta (selezione del campione, informazioni analizzate, tipo di verifica e modalità, ecc.);
- le risultanze del test (sintesi dei dati analizzati);
- le considerazioni emerse (presenza o meno di anomalie e osservazioni, i rischi possibili ed eventualmente i suggerimenti che si possono dare per mitigare o coprire il rischio).

Il Responsabile del CI, infine, rivede il rapporto provvisorio di audit per garantire la sostenibilità delle conclusioni e delle eventuali osservazioni proposte e procedere così alla stesura del rapporto finale di audit.

3.2.4 L'osservazione di audit

Le osservazioni emerse nel corso dello svolgimento delle attività di audit devono essere riportate, da parte dell'Auditor che le riscontra, all'interno di un apposita tabella di sintesi riportata nel report provvisorio audit. Le osservazioni possono essere graduate in osservazioni di primaria importanza, se riferite alla sfera dei controlli identificati come *chiave* dalla Commissione europea, o di secondaria importanza, se riferite alla sfera dei controlli identificati come *ausiliari*; infine, i rilievi possono essere graduati in temi di attenzione, se rilevano un margine di miglioramento in capo ad un controllo comunque funzionante.

Nella suddetta tabella sono indicate le seguenti informazioni:

- gli elementi identificativi dell'osservazione (processo principale, codice osservazione, argomento, area/ufficio responsabile del processo auditato);
- la descrizione dell'osservazione;
- il rischio potenziale (includere la probabilità e l'impatto valutate possibilmente in collaborazione con il responsabile del processo in oggetto);
- il suggerimento formulato dall'Auditor per la soluzione della criticità, possibilmente già valutato col responsabile del processo in oggetto;
- i commenti del responsabile del processo col quale si è effettuata la prima condivisione della criticità;
- data prevista per l'implementazione del piano d'azione concordato.

La fase successiva prevede la condivisione delle osservazioni con il responsabile del processo / unità / funzione auditata.

A tal fine devono essere organizzati incontri con i responsabili delle aree/uffici in cui è stata rilevata l'osservazione per esporre i risultati emersi, le considerazioni sollevate, ricevere ulteriori commenti e informazioni sull'attività in esame e per ottenere una conferma dell'oggettività dell'osservazione riscontrata.

3.2.5 Predisposizione delle carte di lavoro

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

Tale attività ha la funzione di:

- fornire traccia del lavoro eseguito anche per i successivi interventi;
- mantenere le evidenze delle osservazioni 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;
- Memorandum di Pianificazione dell'intervento, firmato e referenziato dagli Auditor ed eventualmente dal coordinatore/responsabile;
- Memorandum di estrazione;
- Check list compilate;
- documentazione di supporto alle osservazioni incluse nel report;
- Rapporto finale di audit.

Per gli audit svolti presso OD o CAA o comprendenti sopralluoghi presso le aziende dei beneficiari, è previsto un verbale contenente gli elementi essenziali dell'audit, che deve essere datato e sottoscritto da tutti i partecipanti (tra cui i funzionari incaricati dell'audit e il responsabile del processo oggetto di audit) e rilasciato in copia al beneficiario (si veda Allegato 5 - Verbale controllo in situ).

A conclusione dell'intervento, tutte le carte di lavoro devono essere adeguatamente archiviate a cura dell'Auditor incaricato in formato elettronico e/o cartaceo in una cartella denominata con il codice dell'intervento.

3.3 Rapporto finale di audit e comunicazione dei risultati (Allegato 4)

Alla conclusione di ogni intervento viene predisposto il rapporto provvisorio di audit che deve contenere le eventuali osservazioni emerse nel corso della verifica.

Il rapporto provvisorio di audit contiene le seguenti informazioni:

- elementi essenziali dell'audit;
- valutazione conclusiva, ove pertinente, sull'adeguatezza del sistema di controllo alla mitigazione dei rischi;
- descrizione delle eventuali osservazioni emerse nel corso dell'audit con le relative raccomandazioni formulate dal CI.

Il rapporto può prevedere inoltre una sezione relativa alle aree di miglioramento/temi di attenzione che può essere compilata dal CI al fine di portare all'attenzione del responsabile del processo e delle Aree/Uffici coinvolti tematiche di rilievo emerse nel corso della verifica, anche se non direttamente legate all'inefficacia del sistema di controllo interno.

La valutazione conclusiva deve considerare gli obiettivi dell'audit e deve essere sempre sostenuta da informazioni sufficienti, affidabili, pertinenti e utili.

Qualora il Responsabile CI ritenga che il responsabile del processo abbia approvato un livello di rischio residuo inaccettabile per l'organizzazione, deve inviare una specifica segnalazione al Direttore.

Il rapporto provvisorio di audit viene condiviso dal Responsabile CI con i soggetti auditati; nel caso in cui nel corso delle verifiche siano emerse osservazioni tali da rendere necessario il recupero, totale o parziale, degli aiuti erogati e/o il ridimensionamento della spesa ammissibile a contributo, il rapporto provvisorio di audit viene trasmesso con nota del Direttore di ARPEA.

Invece, nel caso in cui nel corso delle verifiche non siano emerse osservazioni e non siano state formulate raccomandazioni, non sono necessarie considerazioni da parte del soggetto auditato e il rapporto, inviato dal Responsabile CI, è considerato finale e condiviso.

Eventuali considerazioni sulle raccomandazioni formulate devono pervenire al CI entro trenta giorni dal ricevimento del rapporto provvisorio di audit.

Se il responsabile del processo oggetto di audit è interno all'Agenzia, la condivisione del rapporto provvisorio di audit avviene attraverso l'organizzazione da parte degli Auditor incaricati di un incontro finale a cui vengono invitati:

- il Responsabile del CI
- i referenti e il responsabile del processo oggetto di audit.

In seguito a tale incontro di condivisione viene comunque inviato da parte del Responsabile del CI il rapporto finale di audit, contenente le valutazioni e le raccomandazioni in capo alle aree/uffici auditati.

Il Rapporto finale di audit può contenere le seguenti sezioni, così come indicato nell'Allegato 4 al presente Manuale:

- Sommario per la Direzione;
 - *Obiettivi dell'Intervento di audit*: riassume lo scopo e l'obiettivo dell'intervento di audit nel suo complesso;
 - *Test*: descrive le modalità di svolgimento dell'intervento, evidenziando eventuali scostamenti avvenuti nel corso della verifica rispetto a quanto definito in via preliminare nel Memorandum di pianificazione, esplicitandone le ragioni;
- Risultanze: sintesi delle principali irregolarità emerse nel corso della verifica nel caso in cui siano state riscontrate, oppure attestazione che il processo è correttamente gestito;
- Conclusioni:
 - Osservazioni: Vengono riportate sotto forma di tabella le osservazioni e le criticità aventi la maggiore rilevanza. Più in dettaglio, ciascun campo della tabella delle osservazioni è organizzato come segue:
 - Osservazione: riporta la criticità riscontrata. Se necessario, deve essere integrato, nella parte iniziale del campo, con le informazioni di contesto che permettono un'agevole comprensione dell'osservazione.
 - Rischio: riporta il rischio che, a causa dell'osservazione rilevata, risulta non essere adeguatamente controllato.
 - Raccomandazione: riporta le azioni necessarie alla soluzione della criticità riscontrata, in altre parole quelle azioni che presumibilmente comporterebbero la decadenza dell'osservazione.
 - Piano d'azione del Responsabile del processo: all'inizio riporta il commento generale del responsabile del processo, ovvero se questi è d'accordo o meno con l'osservazione e quindi se intende agire a riguardo oppure ritiene opportuno assumersi il rischio di non procedere ad alcuna implementazione di ulteriori controlli e/o migliorie nei processi. A seguito, all'interno dello stesso riquadro, nel caso il responsabile del processo esprima accordo con l'osservazione e convenga nell'opportunità a procedere all'implementazione di ulteriori controlli e/o migliorie nei processi, è riportato il piano d'azione per la loro realizzazione.
 - Data e Responsabile: questo campo è riempito solo nel caso in cui responsabile del processo abbia convenuto nell'implementazione di ulteriori controlli e/o migliorie nei processi. In questo caso è riportata la data in cui si prevede tali implementazioni saranno completate e la persona / funzione / area responsabile di tali azioni. Il

coordinatore deve verificare che la persona / funzione / area responsabilizzata dell'implementazione delle azioni concordate, sia al corrente della responsabilità attribuitagli e concordi con essa

- Temi di attenzione: analogamente a quanto riportato per le osservazioni, in questa sezione sono poi riportati eventuali temi di attenzione riscontrati relativamente ai controlli interni e all'efficienza dei processi.
- Follow up delle osservazioni degli audit precedenti: In questa sezione è riportata la situazione aggiornata delle azioni previste dal precedente intervento di audit, se esistente, prima in una tabella sintetica e successivamente indicando nel dettaglio le azioni non ancora implementate.
- Appendici / allegati (qualora necessari): in questa sezione è possibile allegare una o più check list per riportare i dati più rappresentativi dei test effettuati, nonché la documentazione a supporto delle evidenze emerse

Analizzate eventuali considerazioni pervenute, il Responsabile CI trasmette ai soggetti auditati e al Direttore di Arpea il rapporto finale di audit contenente il piano di azione condiviso.

In caso di presenza di osservazioni di primaria importanza tali da rendere necessario il recupero totale o parziale, degli aiuti erogati e/o il ridimensionamento della spesa ammissibile a contributo, il rapporto finale viene sottoscritto ed inviato dal Direttore di Arpea; in tale caso il Direttore di ARPEA invia inoltre al beneficiario e per conoscenza all'Organismo Delegato anche un verbale contenente l'esito del sopralluogo e del controllo svolto.

Al termine dell'intervento gli Auditor garantiscono che tutta la documentazione sia raccolta e archiviata presso l'Ufficio Controllo Interno o nello share di rete condiviso.

Gli organismi di controllo (es: Commissione Europea, organismo di certificazione) hanno libero accesso, su richiesta, ai rapporti di audit, oltre che al piano annuale di audit e ai relativi allegati.

4 IL MONITORAGGIO DELLE AZIONI CORRETTIVE

I criteri e le metodologie di svolgimento dell'attività di audit accettate a livello internazionale, cui rimanda l'allegato I al regolamento (UE) n. 2022/127 (punto 4 lett. B) par. iii), prevedono un'azione determinata alla verifica nel tempo delle ottemperanze alle osservazioni formulate durante le attività di audit. Tale operazione viene definita come "follow-up".

Le azioni correttive rilevate presso le attività interne ad ARPEA sono monitorate attraverso l'aggiornamento periodico del Masterplan, un documento che raccoglie gli esiti delle azioni di *follow up* eseguite dal CI.

Periodicamente, nel corso dell'esercizio finanziario, il personale del CI provvede a richiedere ai Responsabili di ciascun processo per cui sussistono piani di azione ancora non completati o parzialmente completati, evidenza delle azioni correttive messe in atto per valutare l'implementazione o meno dei suggerimenti e delle osservazioni in essere. Tale verifica viene effettuata tramite l'invio di mail o tramite colloqui (telefonici o di persona) con i responsabili/referenti dei processi interessati.

Il Masterplan rappresenta, pertanto, il principale strumento di monitoraggio sul seguito dato alle risultanze segnalate. Periodicamente, anche operando per trimestri o quadrimestri, si richiede all'auditato se la raccomandazione è stata effettuata, per monitorare il progresso della messa in atto delle raccomandazioni.

Il Masterplan è costituito indicativamente dalle seguenti sezioni:

- **Data audit:** riporta la data dell'audit (corrispondente alla data di ultimazione dell'intervento stesso).
- **N. osservazione:** codice univoco riferito alla osservazione o al tema di attenzione, come riportato nel report finale dell'intervento di audit.

- **Processo principale:** riporta il nome del processo al quale è riferita l'osservazione.
- **Argomento osservazione:** descrive sinteticamente l'osservazione.
- **Livello di criticità:** indica se si tratta di osservazioni di primaria o secondaria importanza, e se tali da rendere necessario il recupero, totale o parziale.
- **Piano d'azione:** riporta il piano d'azione correttivo concordato con il process owner e il suggerimento riportato nel Rapporto dell'Intervento.
- **Responsabilità:** riporta il nome dell'unità organizzativa/funzione/area/Ufficio/ente alla quale è riferita l'osservazione e che è responsabile dell'azione correttiva.
- **Data scadenza:** riporta la data di scadenza dell'azione di riferimento.
- **Data completamento:** riporta la data nella quale è stata completata l'azione e quindi la decadenza dell'osservazione. Tale campo è valorizzato solamente se nel corso dell'intervento di *follow up* è stata riscontrata l'effettiva implementazione di adeguate azioni correttive alla criticità riscontrata originalmente.
- **Audit Status:** riporta lo *status* della raccomandazione e del relativo Piano d'azione / raccomandazione. A tal fine sono state stabilite le seguenti codifiche:
 - I = l'azione è stata attuata / l'osservazione ha perso la sua ragione d'essere;
 - PI = l'azione è stata parzialmente attuata ma non ancora al punto da risolvere l'
 - N= l'azione non è stata implementata / l'osservazione è ancora in essere;
 - R= si è verificato un ritardo nell'implementazione dell'azione, dovuto a motivazione non dipendenti dalla volontà del responsabile;
 - Z= si è verificata un'impossibilità ad implementare l'azione, dovuta a motivazione non dipendenti dalla volontà del responsabile;
 - S= si è verificato un cambiamento normativo/organizzativo interno che non richiede più alcuna azione.

Al termine dell'intervento di *follow up*, il coordinatore coordina e verifica il corretto aggiornamento della tavola.

Il Masterplan, gestito in formato elettronico, è mantenuto e archiviato presso l'Ufficio Controllo Interno ed utilizzato nella pianificazione dei futuri interventi di *follow up*, oltre che alla produzione di eventuali statistiche sulle percentuali di implementazione delle osservazioni prodotte dall'Ufficio Controllo Interno. In fase di pianificazione dell'audit, il Responsabile dell'Ufficio Controllo Interno o il Coordinatore possono decidere che l'aggiornamento del Masterplan con riferimento ad un determinato *follow up* sia parte dell'audit riguardante il relativo processo o un processo strettamente correlato al tema dell'osservazione. In questo all'interno del Rapporto Finale di audit verrà inserita una tabella aggiornata in merito all'esito del *follow up* svolto.

5 L' ARCHIVIAZIONE DELLA DOCUMENTAZIONE DI AUDIT

Il CI raccoglie e conserva, in formato cartaceo e/o elettronico, tutta la documentazione utilizzata e prodotta nel corso della propria attività (es. documentazione relativa agli interventi di audit e consulenza, normativa e manualistica di riferimento, piano annuale e quinquennale di audit, ecc.).

La documentazione protocollata viene anche conservata sul sistema di Archiviazione ufficiale dell'Ente, Doqui Acta, in appositi fascicoli annuali.

I riferimenti dei documenti che compongono l'audit e le risultanze vengono tracciate all'interno dell'applicativo del SIAP- CONAGRI, nella sezione Controlli di Livello Superiore.

La gestione e l'aggiornamento dei fascicoli cartacei e delle cartelle elettroniche sono effettuati dagli Auditor per gli interventi in cui sono coinvolti e dal Responsabile CI per la documentazione di carattere generale (es. piano annuale e quinquennale di audit, manuale, relazione annuale del controllo interno, ecc.).

Il materiale cartaceo viene custodito all'interno di appositi armadi, accessibili al solo personale del CI. La documentazione è mantenuta presso gli uffici del CI per i 10 anni successivi all'anno di riferimento e viene poi conservata presso l'archivio storico di ARPEA.

5.1 I documenti del CI che debbono necessariamente essere protocollati

La documentazione in uscita / interna che deve essere necessariamente protocollata è la seguente:

- Memorandum di pianificazione, quando inviato ai relativi destinatari;
- Rapporti degli interventi di audit, quando considerati definitivi e non successivamente modificabili;
- Rapporti prodotti nell'ambito dell'attività di monitoraggio continuo dei criteri di riconoscimento dell'Organismo Pagatore;
- Scheda MASAF;
- Tabella dei criteri di riconoscimento;
- Relazione annuale sull'attività del Controllo Interno, dopo essere stata presentata al Direttore dell'Agenzia.

La documentazione in entrata che deve essere necessariamente protocollata è la seguente:

- Controdeduzioni dei responsabili di processo alle osservazioni emerse nel corso degli interventi, quando sono considerati definitivi e saranno inclusi nel rapporto di audit;
- Documenti che comportano integrazioni o variazioni a documenti già protocollati.

In conformità con quanto previsto dal Regolamento (UE) 2016/679, e da ogni altra legge applicabile in materia di protezione dei dati personali, il CI inoltre provvede a specificare all'interno della documentazione redatta (es. Rapporto finale di audit) di trattare i dati personali ivi contenuti strettamente necessari alla finalità del trattamento.

Tenuto conto dello stato dell'arte, costi di implementazione, natura, scopo, contesto e finalità di trattamento, nonché la probabilità e gravità di violazioni ai diritti e alle libertà degli interessati, il CI si impegna a implementare le misure tecniche ed organizzative adeguate, atte a garantire un livello adeguato di sicurezza contro tali evenienze.

A titolo esemplificativo e non esaustivo, qualora atti e documenti in formato cartaceo contengano dati personali, anche particolari e/o giudiziari, gli stessi devono essere custoditi sotto chiave dagli incaricati del CI, negli appositi armadi, in maniera che ad essi non accedano persone prive di autorizzazione, in conformità con le istruzioni approvate con Determinazione di Arpea n. 189 del 13/07/2021, ed inviate tramite mail a tutti i dipendenti.

Nel caso di conservazione nell'archivio informatico di dati personali, in particolare se particolari e/o giudiziari, gli stessi devono essere trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità. In ogni caso, i dati particolari idonei a rivelare lo stato di salute e/o la vita sessuale dei rispettivi soggetti interessati sono conservati separatamente da altri dati personali.

6 L'AUDIT DEI SISTEMI INFORMATIVI

Analogamente ai processi di gestione delle diverse linee di finanziamento, ai processi operativi delle funzioni di autorizzazione, esecuzione e contabilizzazione, al sistema complessivo dei controlli interni, sono oggetto di audit anche i Sistemi Informativi di ARPEA. Si tratta di una delle aree più importanti e significative per l'audit, essendo i sistemi informativi essenziali per lo svolgimento delle attività di ARPEA e tali da garantire livelli di affidabilità e di sicurezza elevati.

6.1 Definizione degli obiettivi

La sempre maggiore dipendenza dei processi di ARPEA dall'informatica determina, pertanto, l'applicazione, da parte dell'Ufficio Controllo Interno, di tecniche di audit anche relativamente alla gestione della sicurezza delle informazioni.

In particolare gli obiettivi fondamentali in materia di **IT auditing** sono i seguenti:

- individuare le aree di maggior esposizione ai rischi nelle attività di gestione dell'infrastruttura informatica e 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 (risk assesment sui controlli automatici di processo);
- eseguire i test dei controlli automatici individuati per verificarne l'efficacia;
- supportare eventualmente l'audit operativo nel fornire il conforto atteso circa l'efficacia dei controlli, che sono fortemente automatizzati;
- supportare eventualmente l'audit operativo nell'elaborazione ed analisi dei dati attraverso strumenti informatici.

6.2 Analisi del "Sistema di Gestione della Sicurezza delle Informazioni"

Di primaria importanza sono gli aspetti connessi alla sicurezza dei SI e delle informazioni; come esplicitamente richiesto dal Reg. (UE) 2022/127 (Allegato I, punto 3, lettera B), ARPEA ha adottato, in coerenza alle disposizioni del Sistema Informativo Regionale, lo standard internazionale per la sicurezza UNI ISO 27001. Tale standard impone l'adozione e il rispetto di regole organizzative e operative, declinate in policy e in disposizioni di dettaglio. Al fine di mantenere in riconoscimento viene garantito da parte dell'Ufficio Controllo Interno un presidio continuativo di verifica sugli obiettivi di controllo stabiliti dallo standard e i requisiti di norma.

È previsto il coinvolgimento di tutte le strutture interne ed esterne che gestiscono i dati necessari allo svolgimento dei compiti dell'Agenzia.

Le attività di controllo fanno riferimento ai macro-ambiti sotto riportati e garantiscono, nell'ambito della pianificazione quinquennale, il presidio dei requisiti prioritari:

1. **Manage Access** (gestione degli accessi): controllo sulle modalità di accesso ai Sistemi Informativi e sulla compliance dei relativi processi IT (attività di creazione/modifica utenze, terminazione utenze, rivalidazione utenze, password e parametrizzazioni di sicurezza, gestione e controllo delle utenze privilegiate);
2. **Manage Change** (gestione dei cambiamenti): controllo sulle modalità di gestione e modifica dei Sistemi Informativi e compliance dei relativi processi IT (flusso autorizzativo e test per le attività di modifica/implementazione del codice applicativo, segregazione logica degli ambienti applicativi, segregazione organizzativa, accesso ai dati in produzione e relativo monitoraggio);
3. **Manage IT Operations** (gestione dei processi IT): controllo sulle modalità di gestione di accessi fisici, automatismi e incidenti dei Sistemi Informativi (backup, attività schedate, gestione incidenti e problemi infrastrutturali).

La metodologia adottata dall'Ufficio Controllo Interno propone un'analisi del processo interessato dagli obiettivi di controllo ricadenti nella verifica in cui sono sintetizzate tutte le attività di gestione degli asset informativi e delle relative risorse informatiche utilizzate per il loro trattamento da parte di ARPEA.

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

- Risk Assessment ISO27001

- Analisi dei requisiti di norma
- Esecuzione di test sull'ambiente IT in relazione agli obiettivi di controllo ISO27001

Gli interventi di audit vengono pianificati e realizzati secondo la metodologia descritta nei capitoli precedenti; essi si attuano attraverso:

- valutazione della conformità alle normative di riferimento e agli standard adottati
- riconoscimento e valutazione dei flussi,
- accertamento dell'allineamento ai requisiti di norma mediante analisi documentale delle policy,
- accertamento dei controlli a sistema e della loro affidabilità in relazione agli obiettivi di controllo.

I risultati delle verifiche di audit permettono di accertare eventuali aree di criticità e di concordare interventi correttivi per il riallineamento delle policy e delle prassi operative allo standard e alle normative adottate.

7 LE ATTIVITÀ DELL'UFFICIO CONTROLLO INTERNO A SUPPORTO DELLA VALUTAZIONE ANNUALE DEL SISTEMA DI GESTIONE E CONTROLLO

7.1 Relazione annuale dell'Ufficio Controllo Interno

Al termine di ogni annualità, in conformità a quanto previsto dal Regolamento (UE) 2022/127, articolo 2, commi 2 e 3, il Responsabile CI redige una relazione sull'attività svolta, destinata al Direttore di ARPEA. Questa rendicontazione a consuntivo è tra l'altro propedeutica alla definizione del piano di audit dell'annualità successiva.

La relazione annuale viene presentata dal Responsabile CI al Direttore di ARPEA unitamente alla firma della Dichiarazione di gestione con riguardo all'anno finanziario appena concluso e fa riferimento all'anno solare. All'interno della relazione sono inclusi i seguenti capitoli:

- **Obiettivi del documento**
- **Quadro normativo di riferimento:** sintesi dei principali riferimento normativi comunitari, nazionali e regionali di riferimento per l'operato del CI;
- **Descrizione dell'attività:** sintesi delle principali attività svolte nel corso dell'annualità da parte dell'Ufficio Controllo Interno;
 - Aggiornamento del risk assessment di processo
 - Attività di audit
 - Master Plan
 - Criteri di riconoscimento
 - Monitoraggio missioni e indagini comunitarie e scheda monitoraggio MASAF
 - Supporto all'attività di chiusura dei conti
 - Attività Antifrod
- **Valutazione dei risultati:** consiste in una disamina dell'operato e delle eventuali difficoltà emerse, delle possibilità di intervento per incrementare qualità ed efficacia dell'azione di audit, sia a livello di organizzazione interna dell'ufficio che di sviluppo delle professionalità e delle competenze degli Auditor, nonché una sintesi del grado di implementazione delle attività definite nel Piano di audit annuale e la valutazione finale che i controlli effettuati non abbiano evidenziato situazioni di criticità tali da sollevare una riserva in Dichiarazione di Gestione per l'affidabilità del sistema di controllo interno di ARPEA.

Nel paragrafo relativo alle attività di audit svolte nel corso dell'anno vengono riportati i risultati di ciascun intervento realizzato, con le informazioni relative ad osservazioni e piani di azione emersi nel corso delle attività di audit.

L'obiettivo principale di tale attività consiste nel fornire alla Direzione una valutazione del sistema di controllo interno attraverso la predisposizione di tutta la documentazione utile all'esame e valutazione da parte del Direttore di ARPEA delle risultanze (Dichiarazione di Gestione):

- degli interventi di audit condotti dall'Ufficio Controllo Interno;
- dell'attività di verifica sull'efficacia dei controlli chiave mappati nelle mappature dei processi;
- dell'aggiornamento della mappatura dei criteri di riconoscimento per l'esercizio finanziario in chiusura.

7.2 Attività propedeutiche alla chiusura dei conti

Preliminarmente alla fase di rendicontazione, l'attività dell'Ufficio Controllo Interno si concentra sulla predisposizione dei seguenti prospetti di sintesi, allegati alla Dichiarazione di Gestione secondo quanto stabilito dalla Linea Diretrice n° 4 della Commissione Europea:

- (1) Allegato I "Sintesi annuale delle relazioni finali di audit e dei controlli effettuati";
- (2) Allegato II "Documenti e attività che sono alla base della Dichiarazione di gestione";
- (3) Allegato III "Riserve e verifica dei progressi compiuti nell'attuazione dei piani d'azione";
- (4) Allegato IV "Qualità ed affidabilità del sistema di comunicazione e dei dati sugli indicatori";
- (5) Allegato V "Analisi delle statistiche di controllo per regime-misure";
- (6) Allegato VI "Analisi dei tassi di errore per popolazione".

7.3 Monitoraggio continuo dei criteri di riconoscimento

L'attività di "Analisi dei criteri di riconoscimento" prevede la raccolta di documentazione e l'elaborazione di un documento riassuntivo che viene redatto nel corso dell'anno di riferimento e terminato entro la data utile per la redazione dei conti annuali, in conformità a quanto prescritto dal Regolamento n. 2022/127. A tal fine, durante l'arco dell'anno, viene svolta un'attività di "Monitoraggio continuo dei criteri di riconoscimento" che prevede una verifica delle attività degli Uffici dell'Organismo Pagatore che si sviluppa attraverso l'analisi di documentazione e la focalizzazione su specifici aspetti. In caso di eventuali criticità vengono individuati GAP, gestiti con piani di azione, che vengono segnalati agli uffici interessati per mezzo di apposita reportistica (si veda Allegato 6 - Monitoraggio continuo - apertura GAP). Si prevede inoltre attività di follow-up dei piani di azione, per cui si svolgono verifiche successive per valutare l'adeguatezza delle azioni correttive intraprese nei confronti dei rilievi.

Scheda MASAF (Allegato 7)

L'Ufficio Controllo Interno, nell'ambito del monitoraggio continuo dei criteri di riconoscimento, si occupa con cadenza trimestrale della redazione della scheda di monitoraggio tramite la quale il MASAF, in qualità di Autorità competente, esercita la costante supervisione sugli organismi pagatori nell'ambito del sistema istituito dal Ministero con il DM 27 marzo 2007.

Tale scheda, predisposta dal MASAF, fornisce informazioni sui seguenti aspetti:

1. Dotazione organica ripartita per servizio, in base al pertinente provvedimento piu' recente e dotazione organica prevista/teorica;
2. Dotazione effettiva per servizio, relativa al trimestre in oggetto;
3. Politica sulla rotazione del personale;

4. Movimentazione del personale, relativo al passaggio di unità lavorative da una categoria all'altra o all'assunzione di nuovo personale;
5. Modifiche relative all'organigramma grafico intervenute nel trimestre in oggetto;
6. Altri provvedimenti presi nel trimestre di riferimento;
7. Valutazione del rischio;
8. Disposizioni emanate nel trimestre di riferimento a seguito di circolari di Agea coordinamento;
9. Modifiche della manualistica;
10. Attività di formazione svolta nel trimestre in oggetto;
11. Requisiti ISO;
12. Modifiche che hanno interessato i sistemi informativi;
13. Indagini - criticità rilevate dalla commissione europea;
14. Criticità rilevate dall'organismo di certificazione;
15. Compiti affidati a soggetti terzi;
16. Movimentazione registro debitori;
17. Importi complessivi pagati nel trimestre di riferimento;
18. Interventi di audit eseguiti dal servizio di controllo interno;

7.4 Attività a supporto dell'Organismo di Certificazione

Secondo quanto previsto dalla normativa unionale vigente, in particolare l'articolo 12 del Regolamento 2021/2116, ciascuno Stato Membro nomina un Organismo di Certificazione il quale esprime un parere, elaborato in base ai principi di audit riconosciuti a livello internazionale, che stabilisce se:

- a) I conti dell'Organismo Pagatore forniscono un quadro fedele e veritiero;
- b) I sistemi di governance istituiti dagli Stati membri funzionano in modo adeguato;
- c) la comunicazione dell'efficacia dell'attuazione in merito agli indicatori di output, e la comunicazione dell'efficacia dell'attuazione in merito agli indicatori di risultato sono corrette;
- d) Le spese per cui è stato chiesto il rimborso alla Commissione sono legittime e regolari.

Il CI supporta lo svolgimento delle attività dell'Organismo di Certificazione, per il quale rappresenta il referente interno ad ARPEA, in un'ottica sinergica di massima collaborazione.

Tale supporto, che si concreta nella produzione di tutta la documentazione richiesta anche in collaborazione con gli uffici interessati, è rivolto ad agevolare le attività di verifica dell'Organismo di certificazione e la redazione degli atti finali che sono espressione del parere di audit sulla certificazione dei conti dell'Organismo Pagatore.

8 LE ATTIVITA' DELL'UFFICIO CONTROLLO INTERNO PER LA PREVENZIONE E IL CONTRASTO DELLE FRODI

Lo sviluppo di una cultura di opposizione alla frode è essenziale sia in quanto elemento dissuasivo per i potenziali soggetti fraudolenti sia per rafforzare l'impegno del personale nella lotta contro la frode in seno ad ARPEA.

In tale ottica l'Ufficio Controllo Interno promuove e monitora l'attuazione della politica antifrode di ARPEA e svolge attività di controllo trasversale su tutti i processi dell'Organismo Pagatore, tra cui la verifica dei controlli previsti per mitigare i rischi di frode e, laddove opportuno, conduce specifici interventi di *Fraud auditing*, nell'ambito degli interventi previsti all'interno del piano annuale di audit.

Al fine di definire la strategia dell’Agenzia nelle attività di prevenzione ed individuazione di frodi e irregolarità nell’ambito dell’erogazione di contributi e finanziamenti al mondo agricolo a valere sul FEAGA e sul FEASR, l’Ufficio Controllo Interno è responsabile della predisposizione del Piano Antifrode.

In un contesto in continua evoluzione caratterizzato da nuovi meccanismi di finanziamento, sviluppo di strumenti informatici e, più in generale, abitudine e professionalità negli atteggiamenti inclini alla frode, si sottolinea, pertanto, l’importanza di adottare una strategia regolarmente aggiornata, pertinente ed efficace.

L’Agenzia si dota, pertanto, di un Piano triennale Antifrode per l’esecuzione di attività e l’adozione di strumenti volti a intercettare eventuali schemi di frode, ovvero le fattispecie operative secondo le quali sono commesse e si manifestano le frodi e ne garantisce l’aggiornamento annuale: nel documento sono individuate le attività su cui concentrarsi nel corso del triennio di riferimento.

Il Piano, oltre agli strumenti di natura più strettamente operativa, definisce anche le attività di formazione intraprese dall’Agenzia per sensibilizzare, informare e allineare il personale dell’Organismo Pagatore e degli Organismi Delegati coinvolti nelle attività amministrative e di controllo sulle norme rilevanti in materia di frode e su come gestire documenti e strumenti interni.

In caso di eventuali variazioni di contesto significative o qualora si riscontrasse la presenza di circostanze particolari, il Piano Antifrode può essere rivisto e modificato nel corso dell’anno.

L’aggiornamento del Piano, oltre alle sue eventuali successive modifiche, è approvato dal Direttore di ARPEA su proposta del Responsabile dell’Ufficio Controllo Interno e del Coordinatore del CI.

9 PRINCIPI DEONTOLOGICI DI RIFERIMENTO PER IL PERSONALE DEL CI

“L’internal auditing è un’attività indipendente ed 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 del CI, nell’esercizio della propria attività deve attenersi ai principi e alle regole di condotta definite dall’Institute of Internal Auditors e al *codice di comportamento* adottato da Arpea.

1. 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 l’attività o il 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 o etico.
 - *Competenza*: nell’esercizio dei propri servizi professionali, l’Internal Auditor utilizza il bagaglio più appropriato di conoscenze, competenze ed esperienze.
2. Le **Regole di Condotta**, che descrivono le norme comportamentali che gli Internal Auditor sono tenuti ad 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, quando etici e conformi alla legge.
- *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 nocimento 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.