Agenzia provinciale per i pagamenti

Controllo interno

MANUALE DEL CONTROLLO INTERNO

Versione 5.1

VERSIONE	*N. DETERMINAZIONE DI APPROVAZIONE*	*DATA DETERMINAZIONE DI APPROVAZIONE*
1.0	***10***	***24/04/2008***
2.0	***32*** ***33***	***17/09/2008*** ***07/10/2008***
3.0	***46***	***30/09/2009***
4.0	***38***	***29/09/2011***
5.0	***12***	***14/03/2017***
5.1		

REVISIONE N.	*N. DETERMINAZIONE DI APPROVAZIONE*	*DATA DETERMINAZIONE DI APPROVAZIONE*

SOMMARIO

BASE GIURIDICA

Normativa comunitaria

Regolamento (UE) n. 1303/2013 del Parlamento Europeo e del Consiglio del 17 dicembre 2013 e ss. mm. e ii. recante disposizioni comuni sul Fondo europeo di sviluppo regionale, sul Fondo sociale europeo, sul Fondo di coesione, sul Fondo europeo agricolo per lo sviluppo rurale e sul Fondo europeo per gli affari marittimi e la pesca e disposizioni generali sul Fondo europeo di sviluppo regionale, sul Fondo sociale europeo, sul Fondo di coesione e sul Fondo europeo per gli affari marittimi e la pesca, e che abroga il regolamento (CE) n. 1083/2006 del Consiglio e successive modificazioni ed integrazioni;

Regolamento (UE) n. 1305/2013 del Parlamento europeo e del Consiglio del 17 dicembre 2013 e ss. mm. e ii. sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR) e che abroga il regolamento (CE) n. 1698/2005 del Consiglio;

Regolamento (UE) n. 1306/2013 del Parlamento Europeo e del Consiglio del 17 dicembre 2013 e ss. mm. e ii. sul finanziamento, sulla gestione e sul monitoraggio della politica agricola comune e che abroga i regolamenti del Consiglio (CEE) n. 352/78, (CE) n. 165/94, (CE) n. 2799/98, (CE) n. 814/2000, (CE) n. 1290/2005 e (CE) n. 485/2008;

Regolamento (UE) n. 1310/2013 del Parlamento europeo e del Consiglio del 17 dicembre 2013 e ss. mm. e ii., che stabilisce alcune disposizioni transitorie sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR), modifica il regolamento (UE) n. 1305/2013 del Parlamento europeo e del Consiglio per quanto concerne le risorse e la loro distribuzione in relazione all'anno 2014 e modifica il regolamento (CE) n. 73/2009 del Consiglio e i regolamenti (UE) n. 1307/2013, (UE) n. 1306/2013 e (UE) n. 1308/2013 del Parlamento europeo e del Consiglio per quanto concerne la loro applicazione nell'anno 2014;

Regolamento delegato (UE) n. 807/2014 della Commissione dell'11 marzo 2014 e ss. mm. e ii. che integra talune disposizioni del regolamento (UE) n. 1305/2013 del Parlamento europeo e del Consiglio sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR) e che introduce disposizioni transitorie;

Regolamento di esecuzione (UE) n. 808/2014 della Commissione del 17 luglio 2014 e ss. mm. e ii. recante modalità di applicazione del regolamento (UE) n. 1305/2013 del Parlamento europeo e del Consiglio sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR);

Regolamento di esecuzione (UE) n. 809/2014 della Commissione del 17 luglio 2014 e ss. mm. e ii. recante modalità di applicazione del regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda il sistema integrato di gestione e di controllo, le misure di sviluppo rurale e la condizionalità;

Regolamento delegato (UE) n. 907/2014 della Commissione dell'11 marzo 2014 e ss. mm. e ii. che integra il regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le cauzioni e l'uso dell'euro e successive modificazioni ed integrazioni;

Regolamento di esecuzione (UE) n. 908/2014 della Commissione del 6 agosto 2014 e

ss. mm. e ii. recante modalità di applicazione del regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio per quanto riguarda gli organismi pagatori e altri organismi, la gestione finanziaria, la liquidazione dei conti, le norme sui controlli, le cauzioni e la trasparenza e successive modificazioni ed integrazioni;

Regolamento (UE) n. 1407/2013 della Commissione del 18 dicembre 2013 e ss. mm. e ii. relativo all'applicazione degli articoli 107 e 108 sul funzionamento dell'Unione Europea agli aiuti "*de minimis*";

Regolamento (CE) n. 1848 della Commissione del 14 dicembre 2006 e ss.mm. e ii., relativo alle irregolarità e al recupero delle somme indebitamente pagate nell'ambito del finanziamento della politica agricola comune nonché all'instaurazione di un sistema d'informazione in questo settore e che abroga il Regolamento (CE) n. 595/1991;

Regolamento delegato (UE) 2015/1971 della Commissione di data 8 luglio 2015 e ss. mm. e ii. che integra il Regolamento (UE) n. 1306/2013 del Parlamento europeo e del Consiglio con disposizioni specifiche sulla segnalazione di irregolarità sul FEAGA e sul FEASR e che abroga il Regolamento (CE) n. 1848/2006, il quale resta tuttavia applicabile per la segnalazione di irregolarità relative ai contributi concessi a norma del Regolamento (CE) n. 1290/2005;

Regolamento di esecuzione (UE) n. 2015/1975 della Commissione di data 8 luglio 2015 e ss. mm. e ii. che stabilisce la frequenza e il formato della segnalazione di irregolarità riguardanti il FEAGA ed il FEASR, a norma del Regolamento (UE) n. 1306/2013;

Regolamento (CE/Euratom) n. 2988 del 18 dicembre 1995 "Regolamento del Consiglio relativo alla tutela degli interessi finanziari della Comunità" e ss.mm. e ii.;

Linee Direttrici della Commissione Europea – Direzione Generale dell'agricoltura e dello sviluppo rurale vigenti;

Decisione della Commissione C(2015) 5377 del 3 agosto 2015 recante approvazione del Programma di Sviluppo Rurale della Provincia Autonoma di Trento (Italia) per il periodo di programmazione 2014-2020, ai fini della concessione di un sostegno da parte del Fondo Europeo Agricolo per lo Sviluppo Rurale – CC12014ITO&RDRP011.

Normativa nazionale

Legge 24 novembre 1981, n. 689 e ss. mm. e ii. concernente "Modifiche al sistema penale";

Legge 23 dicembre 1986, n. 898 e ss. mm. e ii. concernente sanzioni amministrative e penali in materia di aiuti comunitari nel settore agricolo;

Decreto del Presidente della Repubblica 3 giugno 1998, n. 252 e ss. mm. e ii. "Regolamento recante norme per la semplificazione dei procedimenti relativi al rilascio delle comunicazioni e delle informazioni antimafia";

Decreto Legislativo 27 maggio 1999, n. 165 e ss. mm. e ii. "Soppressione dell'AIMA e istituzione dell'Agenzia per le erogazioni in agricoltura (AGEA), a norma dell'articolo 11 della Legge 15 marzo 1997, n. 59" che prevede, tra l'altro, che "le regioni istituiscono appositi servizi ed organismi per le funzioni di organismo pagatore";

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss. mm. e ii. “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”;

Decreto Legislativo 18 maggio 2001, n. 228 e ss. mm. e ii. “Orientamento e modernizzazione del settore agricolo a norma dell’art. 7 della L. 5 marzo 2001, n. 57”;

Decreto Legislativo 30 giugno 2003, n. 196 e ss. mm. e ii. - Codice in materia di protezione dei dati personali;

Decreto Legislativo 29 marzo 2004, n. 99 e ss. mm. e ii. – Disposizioni in materia di soggetti ed attività, integrità aziendale e semplificazione amministrativa in agricoltura, a norma dell’articolo 1, comma 2, lettere d), f), g) ed e) della Legge 7 marzo 2003, n. 38;

Decreto 27 marzo 2007 del Ministero delle Politiche Agricole, Alimentari e Forestali “Disposizioni attuative del Regolamento (CE) n. 885/2006 relativamente al riconoscimento degli Organismi pagatori” e ss. mm. e ii.;

Decreto 10 ottobre 2008, n. 3860, del Ministero delle Politiche Agricole, alimentari e forestali di riconoscimento dell’APPAG quale organismo pagatore per la Provincia Autonoma di Trento per la gestione delle spese del FEASR e del FEAGA;

Legge 13 agosto 2010, n. 136 e ss. mm. e ii. concernente la tracciabilità dei flussi finanziari;

Decreto Legislativo 6 settembre 2011, n. 159 “Codice delle Leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articoli 1 e 2 della Legge 13 agosto 2010, n. 136” e ss. mm. e ii.;

Deliberazione del CIPE n. 10 del 28 gennaio 2015 di definizione dei criteri di cofinanziamento pubblico nazionale dei programmi europei per il periodo di programmazione 2014-2020 e relativo monitoraggio;

Professional Practices Framework: Standard per la Pratica Professionale dell’Internal Auditing;

Linee guida del Ministero delle Politiche Agricole, Alimentari e Forestali sull’ammissibilità delle spese relative allo sviluppo rurale e a interventi analoghi, approvate dalla Conferenza permanente Stato-Regioni – Province Autonome;

Normativa provinciale

Legge provinciale 30 novembre 1992, n. 23 e ss. mm. e ii. “Principi per la democratizzazione, la semplificazione e la partecipazione all'azione amministrativa provinciale e norme in materia di procedimento amministrativo”;

Legge Provinciale 28 marzo 2003, n. 4 e ss. mm. e ii. “Sostegno dell'economia agricola, disciplina dell'agricoltura biologica e della contrassegnazione di prodotti geneticamente non modificati”;

Legge Provinciale 16 giugno 2006, n. 3 e ss. mm. e ii. “Norme in materia di governo dell’autonomia del Trentino”;

Deliberazione della Giunta provinciale n. 2960 del 23 dicembre 2010 e ss. mm. e ii. “Direttive per l’effettuazione dei controlli sulle dichiarazioni sostitutive di certificazioni e dell’atto di notorietà ed individuazione del campione minimo di pratiche da sottoporre al controllo, ai sensi dell’art. 71 del Decreto del Presidente della Repubblica n. 445 di data 28 dicembre 2000”.

Deliberazione della Giunta provinciale n. 1487 del 31 agosto 2015 “Approvazione definitiva del “Programma di Sviluppo Rurale della Provincia Autonoma di Trento 2014/2020 ai sensi del Regolamento (UE) del 17 dicembre 2013, n. 1305/2013 del Parlamento Europeo e del Consiglio sul sostegno allo sviluppo rurale da parte del Fondo europeo agricolo per lo sviluppo rurale (FEASR) - CCI 2014IT06RDRP011”;

Deliberazione della Giunta provinciale n. 2440 del 29 dicembre 2016, in particolare l’allegato D), con la quale è stato adottato il nuovo atto organizzativo dell’Agenzia Provinciale per i Pagamenti (APPAG), apportando una serie di modifiche atte ad adeguare il precedente atto organizzativo, approvato con deliberazione della Giunta provinciale n. 3193 del 30 dicembre 2010, alle normative in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio degli enti locali e dei loro organismi, previste dal Decreto Legislativo 23 giugno 2011, n. 118 e ss. mm. e ii.;

Per l’espletamento delle attività, l’Ufficio del Controllo Interno fa inoltre riferimento alla manualistica ed alle procedure adottate dal Direttore di APPAG.

1. PRINCIPI GENERALI

1.1 Funzioni e finalità

La costituzione del Controllo Interno nell'ambito dell'Organismo Pagatore (di seguito OP) è prevista dal Regolamento delegato (UE) n. 907/2014 della Commissione, Allegato I "Criteri per il Riconoscimento" punto 4, lettera B).

L'Allegato I del Regolamento delegato (UE) n. 907/2014 della Commissione, prevede in particolare che:

- *il Servizio di Controllo Interno deve essere indipendente dagli altri servizi dell'OP e riferire direttamente al Direttore dell'organismo;*
- *il Servizio di Controllo Interno verifica che le procedure adottate dall'OP siano adeguate per garantire la conformità con la normativa dell'Unione e che la contabilità sia esatta, completa e tempestiva. Le verifiche possono 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;*
- *l'attività del Servizio di Controllo Interno si svolge conformemente a norme riconosciute a livello internazionale, va registrata in documenti di lavoro e deve figurare nelle relazioni e nelle raccomandazioni destinate alla direzione dell'Organismo Pagatore.*

All'interno dell'Agenzia Provinciale per i Pagamenti (APPAG), il Servizio di Controllo Interno è affidato ad uno specifico Ufficio, definito appunto Ufficio Controllo Interno.

L'Ufficio Controllo Interno di APPAG coopera all'efficace funzionamento del sistema dei controlli interni adottati dall'OP attraverso una sistematica attività di internal auditing basata su una metodologia pianificata che si fonda sull'analisi dei processi, dei relativi rischi e sui controlli implementati, acquisisce gli opportuni spunti anche dal Quadro delle pratiche professionali ("*Professional Practices Framework*") e dagli Standards per la Pratica Professionale rilasciati dall'Institute of Internal Auditors ("IIA") conformemente a quanto stabilito dalle disposizioni comunitarie.

In particolare:

- verifica l'efficacia del sistema dei controlli interni adottati dall'OP;
- verifica la conformità alla normativa comunitaria, nazionale e provinciale dei sistemi suddetti;
- verifica l'accuratezza, completezza e tempestività della contabilità di APPAG;
- verifica la correttezza e la completezza delle operazioni di controllo tecnico e di autorizzazione;
-
- provvede al necessario supporto alle operazioni di controllo da parte della Commissione UE, della Corte dei Conti UE, del Ministero per le Politiche Agricole, Alimentari e Forestali e dell'Organismo di Certificazione;
- collabora con la Direzione per la definizione degli allegati alla Dichiarazione di Gestione annuale;

- coordina le attività di rendicontazione annuale (rendicontazione statistica, tabella delle X).

L'attività dell'Ufficio Controllo Interno è svolta in conformità ai criteri normativi previsti dall'Allegato I del Regolamento delegato (UE) n. 907/2014 sopra descritti.

1.2 Indipendenza della funzione

L'indipendenza della funzione è assicurata da:

a) ***Adeguata collocazione organizzativa***: Il Direttore dell'Ufficio Controllo Interno riferisce direttamente al Direttore dell'APPAG.

I rapporti diretti che assicurano un adeguato scambio di informazioni si realizzano:

1. tramite periodiche riunioni sulle materie di auditing, bilancio, organizzazione e controllo;
2. tramite l'approvazione della programmazione annuale degli audit ed eventuali modifiche alla stessa;
3. tramite la trasmissione al Direttore delle Relazioni di Controllo previste per gli audit programmati, ovvero la trasmissione diretta o "per conoscenza" dei verbali relativi all'attività di audit o di approfondimento specifico non programmata.

L'Ufficio Controllo Interno ha incondizionato accesso ai dati, alle persone, agli archivi ed ai beni dell'APPAG e degli Organismi Delegati (di seguito OD) ogni volta che ciò risulti opportuno per lo svolgimento della propria attività.

b) ***Obiettività degli addetti al controllo interno che comporta:***

1. assegnazione dei compiti in modo da evitare condizionamenti e possibili conflitti d'interesse;
2. divieto di affidare ai funzionari assegnati all'Ufficio Controllo Interno responsabilità operative connesse all'autorizzazione, all'esecuzione ed alla contabilizzazione dei pagamenti a titolo del Fondo Europeo Agricolo di Garanzia (FEAGA) e del Fondo Europeo Agricolo per lo Sviluppo Rurale (FEASR);
3. supervisione, da parte del Responsabile dell'Ufficio Controllo Interno, sull'attività svolta dai funzionari, prima dell'emissione dei rapporti di audit.

1.3 I principi deontologici di riferimento per il personale del Controllo Interno

Il personale assegnato all'Ufficio Controllo Interno svolge la propria attività seguendo i principi e le linee guida indicate dal Codice Etico dell'Institute of Internal Auditors, il cui scopo è quello di promuovere la cultura etica nell'esercizio della professione di "*internal auditor*".

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 essere 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.

Le **Regole di Condotta**, che dettano le norme comportamentali che gli internal auditors 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 dannose per i legittimi obiettivi dell'organizzazione.

♦ **Competenza**

L'*internal auditor*:

- Deve intraprendere solo quelle prestazioni per le quali abbia la necessaria conoscenza, competenza ed esperienza, prestando i propri servizi, avendo a riferimento 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.

1.4 Competenze professionali e formazione

Al personale assegnato all'Ufficio Controllo Interno sono richieste competenze adeguate nelle discipline necessarie allo svolgimento degli interventi di audit. Tali competenze specifiche non sono tuttavia richieste individualmente a ciascun auditor, ma è sufficiente che siano presenti nell'ambito del team assegnato all'Ufficio Controllo Interno.

Ad ogni singolo addetto sono richieste conoscenze di base tali da consentire all'*internal auditor* di percepire la presenza di problemi e di determinare la necessità di ulteriori approfondimenti o l'assistenza da richiedere.

Gli addetti al servizio di controllo interno devono saper gestire le relazioni interpersonali e mantenere soddisfacenti rapporti con le persone delle funzioni soggette ad audit; devono possedere una buona capacità di esposizione sia in forma scritta che orale, in modo da poter comunicare chiaramente ed efficacemente obiettivi, valutazioni, conclusioni e raccomandazioni.

Agli addetti è assicurata la possibilità di periodico aggiornamento, in modo da mantenere un adeguato livello di competenza professionale; l'aggiornamento può essere effettuato innanzitutto mediante l'organizzazione di riunioni periodiche interne, in secondo luogo mediante la partecipazione a Conferenze, Convegni, Seminari, Corsi di formazione, ecc..

1.5 Oggetto dei controlli

L'attività di controllo è rivolta essenzialmente:

- alla verifica del rispetto della separazione tra le funzioni di Autorizzazione, Esecuzione e di Contabilizzazione dei pagamenti, in particolare per quanto riguarda l'organizzazione dell'OP;
- alla verifica circa la conformità delle procedure implementate dall'OP con la normativa comunitaria, nazionale e provinciale vigente;
- alla verifica circa la corretta applicazione delle procedure adottate, da parte delle singole Unità Operative interne e da parte degli Organismi Delegati;
- all'adeguatezza (efficacia) dei controlli previsti dalle procedure stesse rispetto agli obiettivi dell'OP;
- alla compatibilità dei sistemi di contabilità adottati rispetto ai principi contabili comunitari;
- alla qualità delle registrazioni contabili ed alla produzione di informazioni finanziarie e di gestione tempestive ed affidabili;
- al rispetto delle norme sulla sicurezza informatica dei dati;
- alla prevenzione ed analisi di frodi ed errori.

2. PROGRAMMAZIONE DEGLI AUDIT

2.1 Piano quinquennale ed annuale

Considerata l'ampia gamma delle attività svolte dall'APPAG, viene predisposto dall'Ufficio Controllo Interno il **Piano quinquennale degli audit,** che definisce gli obiettivi che si intendono perseguire nell'ambito del quinquennio coperto dal piano.

Il Piano quinquennale, che è articolato in annualità, viene riesaminato ed approvato con cadenza annuale, al fine di adattarlo alle specifiche esigenze di controllo che si dovessero attualizzare nel breve periodo.

Il Piano quinquennale degli audit, che è proposto dal Responsabile dell'Ufficio Controllo Interno ed approvato dal Direttore dell'APPAG, deve:

- essere allineato alle aspettative manifestate dalla Direzione dell'OP e considerare gli esiti dell'analisi del rischio connesso ai singoli processi e singole attività;
- puntare l'attenzione sui processi aventi la maggiore rilevanza, ovvero che maggiormente concorrano al raggiungimento degli obiettivi e delle strategie dell'OP;
- considerare le esigenze poste dal legislatore comunitario ed i focus proposti dalla Commissione UE nel corso dei vari audit svolti a livello nazionale;
- considerare eventuali esigenze della Direzione dell'OP di impegnare risorse dell'Ufficio Controllo Interno per svolgere attività specifiche diverse dagli audit.

Oltre ai controlli previsti nel Piano quinquennale ed annuale, possono essere effettuati controlli/approfondimenti su iniziativa del Direttore dell'OP, del Responsabile dell'Ufficio Controllo Interno, nonché a seguito di esigenze di controllo e/o di approfondimento di tematiche specifiche.

Le possibili tipologie di intervento dell'Ufficio Controllo Interno sono le seguenti:

- ***Compliance Audit*** (Audit di conformità): si focalizza essenzialmente sulla verifica della conformità dei comportamenti alle norme, procedure e prassi interne, applicabili al contesto delle strutture operative e delle operazioni sotto esame.
- ***Operational Audit***: è il monitoraggio del rispetto degli obiettivi dell'OP, 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): sono interventi per la verifica dell'effettiva implementazione dei piani di azione correttivi concordati con i responsabili dei processi, a fronte delle osservazioni rilevate nel corso di precedenti interventi del Controllo Interno e condivise dai responsabili dei processi stessi.

2.2 Procedura di formazione del Piano di Audit quinquennale

Nella predisposizione della proposta del Piano quinquennale degli audit, il Responsabile dell'Ufficio Controllo Interno, considera inoltre i seguenti aspetti:

- rispetto della normativa comunitaria in materia di pianificazione delle attività di audit, con particolare riguardo ai servizi di controllo interno degli Organismi Pagatori (in special modo le esigenze di copertura previste dal Regolamento delegato (UE) n. 907/2014 citato in premessa);
- necessità di attribuire ai processi/settori di APPAG una priorità all'interno del Piano quinquennale sulla base dei seguenti fattori:
  - ✓ grado di rischiosità dei processi/settori;
  - ✓ grado di rilevanza dei processi/settori;
- necessità di fornire al Direttore di APPAG quante più informazioni possibili sia in termini di adeguatezza/efficacia del sistema di controllo interno di APPAG, che in termini di conformità alla normativa (comunitaria, nazionale e provinciale) delle procedure adottate da APPAG ai fini della Dichiarazione di gestione del Direttore, ai sensi dell'art. 7 del Regolamento (UE) n. 1306/2013 e dell'art. 3 del Regolamento di esecuzione (UE) n. 908/2014;
- disponibilità delle risorse (attuali e programmate) dell'Ufficio Controllo Interno di APPAG.

2.3 Raccolta delle informazioni rilevanti e valutazione dei rischi

La corretta programmazione degli audit implica la raccolta e l'analisi delle informazioni necessarie per la selezione dei processi e delle attività da sottoporre a controllo.

Va tenuto presente che l'obiettivo principale degli audit sulle attività di pagamento previste per i fondi FEAGA e FEASR, è quello di verificare l'efficacia del sistema di gestione dei controlli implementato dall'Organismo Pagatore al fine di prevenire, per quanto possibile, ovvero individuare e correggere eventuali errori e irregolarità nella realizzazione delle attività di autorizzazione, esecuzione e contabilizzazione dei pagamenti. A questo scopo gli audit vanno effettuati su determinate misure o su campioni di operazioni che permettano di trarre conclusioni, per quanto possibile in termini generali, sull'efficacia del sistema nel suo complesso.

Al fine di produrre un Piano dei Controlli che sia allineato con le esigenze di gestione del rischio proprie di APPAG, deve essere realizzata una valutazione dei rischi di ogni processo.

Detta attività è svolta dall'Ufficio Controllo Interno in collaborazione con i responsabili dei processi interessati.

L'individuazione dei rischi avviene, in prima istanza, attraverso l'analisi dei processi con il supporto del personale responsabile degli stessi. Successivamente, i rischi possono essere identificati anche sulla base dell'esperienza maturata (esiti dell'attività di audit realizzata in precedenza, di informazioni acquisite circa eventuali problematiche o criticità pregresse o in essere, ovvero con altri metodi ritenuti idonei a tal fine).

Al fine di limitare il più possibile la discrezionalità nella valutazione dei rischi, viene presa come riferimento la "Matrice per la valutazione del rischio" (vedi Figura 1).

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

2.4 Criteri utilizzati per la valutazione del rischio dei processi

Ai fini della pianificazione pluriennale degli audit, la "valutazione del rischio", avviene valutando i processi nel loro complesso, prendendo in considerazione l'impatto generato dal rischio delle attività così come descritte nei manuali APPAG, nonché dei controlli ad oggi messi in atto per eliminare o minimizzare i rischi, che risultano anch'essi documentati nei manuali APPAG.

La valutazione così realizzata definisce il livello di rischio del processo nel suo complesso e la rilevanza ad esso attribuita dall'Ufficio Controllo Interno, in accordo con la Direzione di APPAG.

Per detta attività è stata utilizzata, quale riferimento, la metodologia di "valutazione del rischio" che tiene conto degli elementi che seguono:

Rischio	Evento la cui manifestazione ha un impatto sul raggiungimento degli obiettivi dell'Ente o del processo	
Impatto del rischio	Livello in cui il manifestarsi del rischio influenzerebbe il raggiungimento delle strategie e degli obiettivi	Può essere: Grave, Moderato, Basso
Probabilità del rischio	Probabilità che l'accadimento dell'evento si verifichi	Può essere: Grave, Moderata, Bassa
Rilevanza del rischio	Stato del rischio, definito dai Funzionari dell'Ufficio Controllo Interno e concordato con i Responsabili dei processi e con la Direzione di APPAG	Può essere: Grave, Moderata, Bassa

Figura 1

Matrice per la valutazione del rischio (RACM)

VALUTAZIONE DELLA FREQUENZA DEL RISCHIO

La miglior valutazione della frequenza dovrebbe essere basata sull'esperienza e capacità di giudizio, utilizzando i riferimenti della seguente Tabella:

PROBABILITA'		DESCRIZIONE
ALTA	⇨	La probabilità di accadimento dell'evento è che si ripeta continuamente o quasi.
MODERATA	⇨	La probabilità di accadimento dell'evento è che si verifichi frequentemente ma non continuamente, in particolare in maniera occasionale.
BASSA	⇨	La probabilità di accadimento dell'evento è che si verifichi raramente, in particolare appare improbabile che il rischio si verifichi.

VALUTAZIONE DELL'IMPATTO DEL RISCHIO

L'impatto del rischio è il livello in cui il manifestarsi del rischio influenzerebbe il raggiungimento delle strategie e degli obiettivi dell'OP, ad esempio:
- perdita dei requisiti per il riconoscimento ad Organismo Pagatore;
- rettifiche finanziarie della CE;
- inadeguatezza delle procedure applicate;
- eccessivo carico amministrativo in capo all'utenza;
- perdita di fondi.

IMPATTO		DESCRIZIONE
GRAVE	⇨	Impatto significativo sul raggiungimento degli obiettivi strategici dell'OP, ad esempio: • perdita di requisiti per il riconoscimento ad OP; • inefficacia dei sistemi informatici; insoddisfazione dei beneficiari a causa della inaccessibilità delle informazioni e/o delle difficoltà amministrative delle domande; • perdita di fondi per correzioni finanziarie, etc..

MODERATO	⇨	Inefficienza delle normali operazioni con un effetto limitato sul raggiungimento degli obiettivi strategici dell'OP, ad esempio: ● interruzioni o significative inefficienze nel processo delle domande; ● problemi temporanei di qualità/servizio; ● inefficienze nei flussi e nelle operazioni, etc..
BASSO	⇨	Nessun impatto concreto sulla strategia dell'OP (si tratta di situazioni diverse dalla norma che richiedono comunque azioni correttive).

2.5 Descrizione sintetica dei processi realizzati da APPAG

Processi principali:

Direzione

Processo finalizzato a definire, governare e controllare gli obiettivi ed i contenuti di tutti i processi dell'APPAG per assicurare, nel rispetto della normativa di riferimento, un efficiente servizio di pagamento ai beneficiari degli aiuti/premi.

Autorizzazione Premi ed Autorizzazione Investimenti

Processi finalizzati all'effettuazione dell'istruttoria delle domande di pagamento ed alla verifica delle attività delegate ai fini dell'autorizzazione del pagamento degli aiuti/premi relativamente alle Misure del Programma di Sviluppo Rurale a premio e ad investimento, nonché alla Domanda Unica di Pagamento.

Esecuzione Pagamenti

Processo finalizzato al pagamento degli aiuti/premi ai beneficiari nel rispetto della normativa di riferimento, previa effettuazione dei controlli amministrativi e finanziari previsti dalle procedure di pagamento adottate dall'APPAG. Gestione del Registro delle Garanzie.

Contabilizzazione Pagamenti

Processo finalizzato sia alla completa, corretta e tempestiva contabilizzazione delle entrate e dei pagamenti nel sistema di contabilità dell'APPAG, che alla predisposizione e trasmissione alla Commissione Europea (per il tramite di AGEA Organismo di Coordinamento) dei dati e delle rendicontazioni periodiche e finali con riguardo ai fondi FEAGA e FEASR.

Gestione dei recuperi

Processo finalizzato alla ricezione degli atti di contestazione dagli organi di controllo, all'istruttoria ed eventuale sospensione dei pagamenti, al tempestivo aggiornamento del Registro dei Debitori ed attivazione della procedura di recupero, al fine di garantire un'efficace azione di recupero delle somme indebitamente percepite dai beneficiari.

Processi di Supporto:

Tecnico

Processo finalizzato:

1) allo studio ed analisi della normativa di riferimento ai fini della predisposizione delle procedure e modalità operative per l'esecuzione delle attività di autorizzazione e di controllo;
2) al coordinamento, assistenza e supporto all'attività realizzata sia dagli Organismi Delegati, per un efficace ed efficiente svolgimento delle attività ad essi affidate/delegate, che all'Autorità di Gestione (Provincia Autonoma di Trento) del Programma di Sviluppo Rurale, al fine di ottenere la produzione di bandi in linea con la normativa vigente e con le esigenze di APPAG;
3) alla realizzazione delle attività di estrazione dei campioni di competenza di APPAG, sia per quanto riguarda i controlli in loco che per quanto riguarda i controlli di II livello sugli OD;
4) alla realizzazione dei controlli in loco ed ex post previsti dalla normativa comunitaria e che non sono delegati ad altre entità esterne.

Sistemi Informativi

Processo finalizzato a pianificare ed organizzare l'ambiente dei sistemi di informazione (SI) e la relativa infrastruttura, definendo gli standard tecnici e di servizio necessari all'erogazione dei servizi IT garantendo, inoltre, l'applicazione degli standard relativi alla sicurezza delle informazioni. Gestione dei contratti relativi all'acquisto, sviluppo e manutenzione dei sistemi, nonché degli altri servizi connessi ai SI. Gestione dei sistemi al fine di mantenere la disponibilità, la riservatezza e l'integrità delle informazioni. Supporto agli utenti dei sistemi informativi.

Controllo Interno

Processo finalizzato ad assicurare la verifica indipendente dell'efficacia del sistema dei controlli interni adottati da APPAG, alla verifica circa la conformità dell'attività realizzata da APPAG e dagli Organismi Delegati alla normativa comunitaria, nazionale, e provinciale.

Supportare la Direzione di APPAG nella raccolta ed elaborazione delle informazioni necessarie per le rendicontazioni statistiche previste dalla normativa comunitaria e per la predisposizione della Dichiarazione di gestione, ai sensi dell'art. 7 del Regolamento (UE) n. 1306/2013 e dell'art. 3 del Regolamento di esecuzione (UE) n. 908/2014.

2.6 Selezione dei processi/attività da sottoporre a controllo sulla base della valutazione dei rischi e individuazione del campione di beneficiari/operazioni/documenti ecc. da sottoporre a controllo.

Sulla base dei fattori predetti viene assegnato un grado di rischio complessivo ad ogni processo, così da pervenire ad una scala di priorità e frequenza degli argomenti da sottoporre ad audit nell'arco del quinquennio considerato.

Va sottolineato in ogni caso, che gli audit sono necessariamente realizzati a campione.

L'obiettivo dell'Ufficio Controllo Interno, nella definizione dell'estensione del campione di beneficiari/operazioni/documenti ecc. da sottoporre a verifica nell'ambito di ciascun audit (detta decisione è necessariamente condizionata da diversi fattori, quali il tempo a disposizione per realizzare l'attività, la disponibilità di risorse, ecc.), è quello di acquisire un grado di certezza **ritenuto sufficiente**, circa la conformità ed efficacia del processo/attività verificati.

2.7 Modalità di estrazione del campione di beneficiari/operazioni/documenti ecc. da sottoporre a controllo.

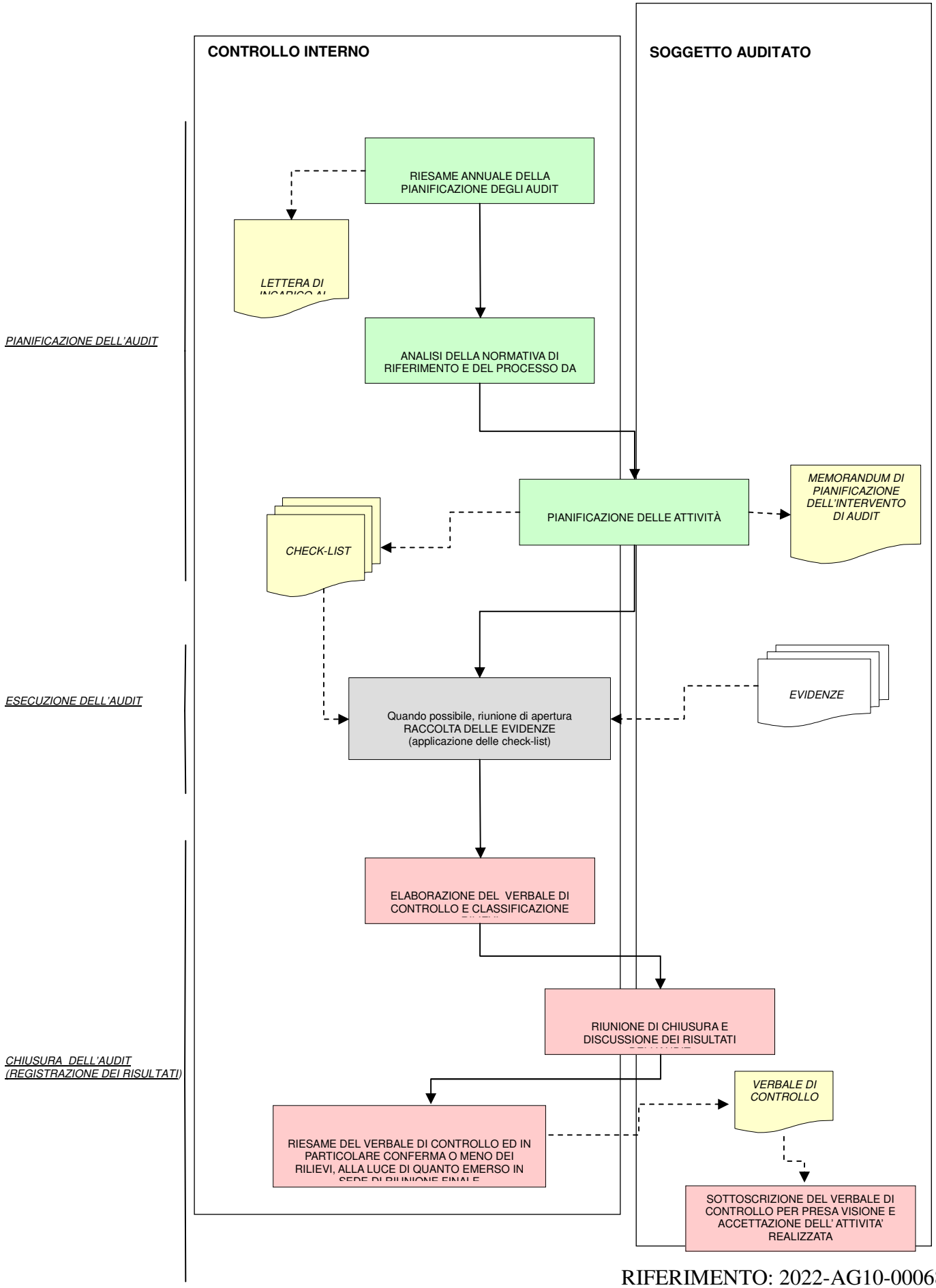
Fatti salvi i casi in cui, a causa dei particolari fattori di rischio, che devono essere evidenziati prima della selezione del campione, i controlli riguardano uno specifico gruppo di beneficiari /operazioni/documenti ecc., di regola il campione viene individuato mediante estrazione casuale (random).

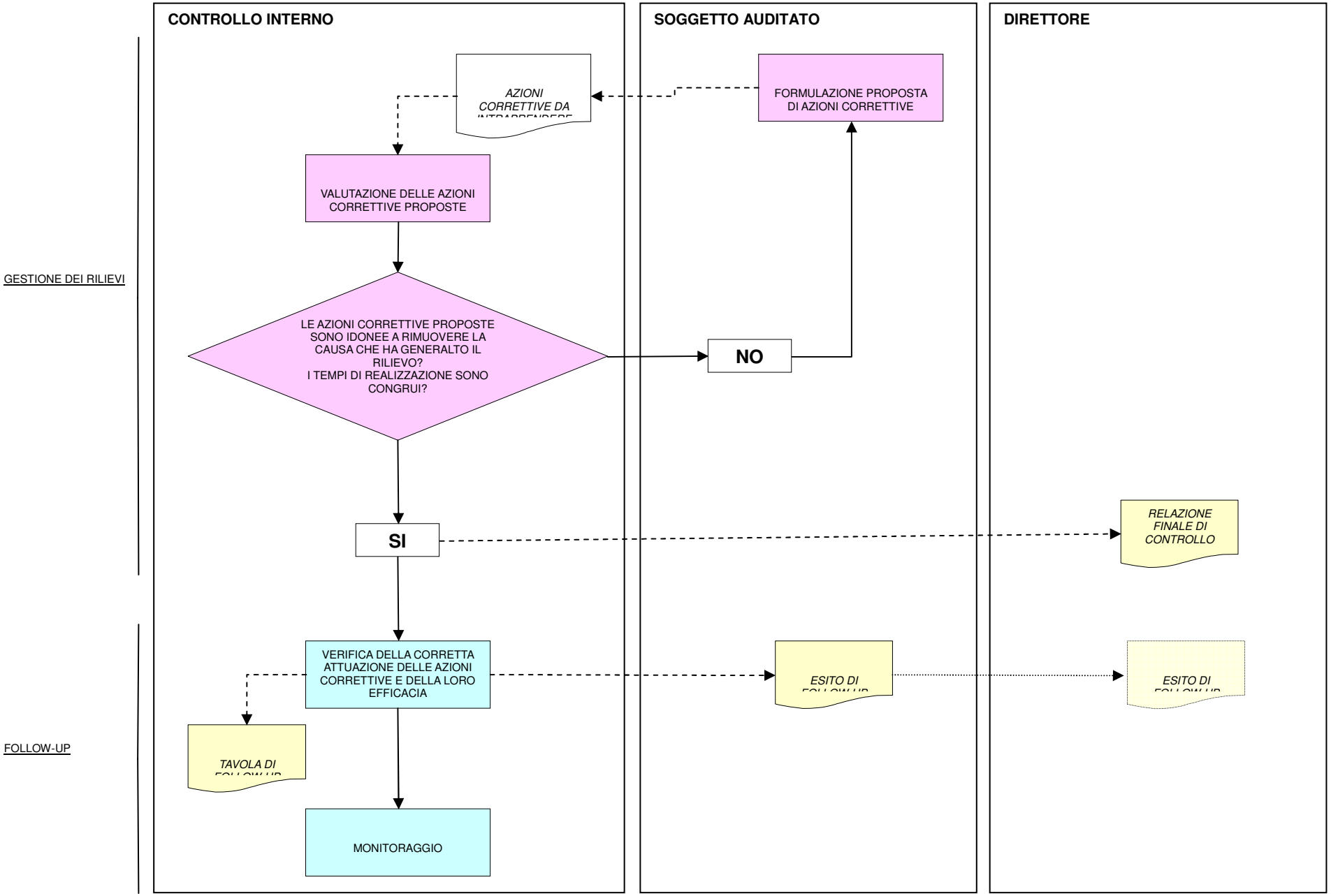
Per l'estrazione del campione casuale si procede avvalendosi delle funzioni a ciò dedicate dei programmi informatici disponibili, garantendo in ogni caso la tracciabilità della procedura seguita.

Laddove sia prevista, per l'estrazione del campione casuale, una (o più) fase discrezionale è sempre richiesta la pluralità dei dipendenti per lo svolgimento dell'operazione. In tali casi, al momento dell'estrazione del campione casuale devono essere presenti almeno due dipendenti dell'Ufficio Controllo Interno, che attestano lo svolgimento di questa operazione non appena conclusa mediante la redazione di un apposito verbale, che viene sottoscritto da entrambi.

3. PROCESSO DI GESTIONE DEGLI AUDIT

3.1 Diagramma di flusso




CONTROLLO INTERNO
SOGGETTO AUDITATO
DIRETTORE
GESTIONE DEI RILIEVI
FOLLOW-UP
AZIONI CORRETTIVE DA
FORMULAZIONE PROPOSTA DI AZIONI CORRETTIVE
VALUTAZIONE DELLE AZIONI CORRETTIVE PROPOSTE
LE AZIONI CORRETTIVE PROPOSTE SONO IDONEE A RIMUOVERE LA CAUSA CHE HA GENERALTO IL RILIEVO?
I TEMPI DI REALIZZAZIONE SONO CONGRUI?
NO
SI
RELAZIONE FINALE DI CONTROLLO
VERIFICA DELLA CORRETTA ATTUAZIONE DELLE AZIONI CORRETTIVE E DELLA LORO EFFICACIA
ESITO DI
ESITO DI
TAVOLA DI
MONITORAGGIO

3.2 Programmazione dei tempi, del calendario e del personale responsabile del controllo

In questo stadio vanno definiti il periodo in cui sarà svolto l'audit e la durata prevista.

Vanno inoltre individuate le risorse umane necessarie allo svolgimento dell'audit, in particolare:

- il numero dei componenti e la competenza del gruppo dei controllori devono essere definiti sulla base di una valutazione della natura e della complessità del lavoro, dei vincoli di tempo e delle risorse disponibili;
- ai fini della selezione dei funzionari a cui affidare l'incarico, debbono essere prese in considerazione le conoscenze, capacità e competenze complessive del personale della funzione dell'Ufficio Controllo Interno;
- nei casi ove siano necessarie conoscenze, capacità e competenze aggiuntive a quelle presenti nell'Ufficio Controllo Interno, deve essere considerata l'opportunità di utilizzare risorse esterne.

Il funzionario individuato per l'esecuzione dell'audit è incaricato formalmente da parte del Responsabile dell'Ufficio Controllo Interno con specifica lettera.

Ricevuto formalmente l'incarico, l'auditor provvede ad aprire il fascicolo di controllo relativo alla verifica da realizzare, nel quale sarà archiviata tutta la documentazione prodotta nel corso dell'audit. Tali fascicoli devono essere numerati ed accuratamente conservati.

Sul frontespizio del fascicolo vanno indicate le generalità dell'auditor e del soggetto controllato, l'oggetto del controllo, le date di avvio e conclusione del controllo, nonché l'indicazione se si tratti di audit programmato o non programmato.

Ad ogni intervento di audit programmato è attribuito un codice identificativo, che è quello definito all'interno del Piano quinquennale/annuale degli audit.

3.3 Analisi del processo da verificare

Una corretta preparazione è decisiva ai fini della buona esecuzione dell'audit.

A tale scopo, l'auditor deve procedere secondo le seguenti tappe e registrarne i risultati nella relazione di audit:

-
- condurre un'appropriata "ricognizione" preliminare della normativa di riferimento, della manualistica APPAG dove è descritto il processo/attività ed i punti di controllo ad oggi definiti, che consenta di prenderne sufficiente familiarità, così da identificare i punti critici e le aree di approfondimento dell'audit e sollecitare suggerimenti e commenti da parte del soggetto controllato.

La "ricognizione" costituisce un processo di raccolta delle informazioni sulle attività

da esaminare, senza sottoporle a verifiche dettagliate. I suoi scopi sono:

- comprendere natura e caratteristiche dell'attività sottoposta ad esame;
- identificare i punti critici, che richiedono speciali approfondimenti;
- ottenere informazioni da utilizzare nello svolgimento dell'audit;
- determinare se siano necessarie ulteriori risorse per raggiungere l'obiettivo di audit prefissato.

La ricognizione permette un approccio più consapevole alla pianificazione ed allo svolgimento dell'audit e costituisce un efficace strumento per individuare le aree in cui le risorse dell'Ufficio Controllo Interno possono essere applicate più efficacemente.

Per effettuare una ricognizione ci si può servire di:

- discussioni con il soggetto controllato;
- interviste, non solo con persone coinvolte nell'attività, ma anche con coloro che ne utilizzano i risultati;
- osservazioni sul posto;
- acquisizione di rapporti e di studi sugli argomenti oggetto d'esame;
- acquisizione di esiti di attività di audit pregressa;
- predisposizione di schemi di flusso delle operazioni;
- documentazione dei controlli fondamentali svolti.

La ricognizione dovrebbe permettere di aver acquisito informazioni sufficienti su:

- obiettivo dell'audit e risultati attesi (in termini di evidenze da acquisire);
- punti critici, temi da approfondire e ragioni per farlo;
- informazioni rilevanti da sviluppare ulteriormente;
- possibili ulteriori obiettivi di audit da conseguire, procedure e approcci particolari da applicare;
-
- stime preliminari di tempo e risorse da impiegare;
-
- eventuali motivi per non dar corso all'audit.

Prima dell'avvio delle attività di verifica, l'auditor incaricato condivide con il Responsabile dell'Ufficio Controllo Interno la pianificazione delle attività, in particolare:

-
- gli obiettivi dell'audit;
- l'ampiezza e la profondità delle verifiche necessarie per raggiungere gli obiettivi stabiliti per ogni fase dell'audit;
- le modalità e gli strumenti di lavoro che intende adottare per la raccolta delle evidenze (es. check list, ecc);
- aspetti tecnici, i rischi, i processi e l'estensione del campione di beneficiari/operazioni/documenti/ecc. da esaminare;

•

Il Responsabile dell'Ufficio Controllo Interno redige quindi un Memorandum di pianificazione dell'intervento di audit (vedi ALLEGATO 1) che trasmette al responsabile soggetto da auditare e per conoscenza al Direttore dell'OP.

Una sintesi delle attività realizzate nella fase di pianificazione delle attività è in ogni caso riportata nel Verbale di controllo relativo a ciascun audit.

Fra gli strumenti di lavoro da predisporre in questa fase, sicuramente il principale è rappresentato dalla check list.

La check list rappresenta un elenco organico di punti che l'auditor deve verificare per mettere in evidenza il grado di corrispondenza fra il "com'è" (la realtà) e il "come dovrebbe essere" in base a quanto previsto dalle regole applicabili. Essa rappresenta lo strumento che è opportuno utilizzare come guida, al fine di rendere efficace ed organica l'attività di verifica e la raccolta delle evidenze di audit.

Per alcune tipologie di audit (ad es. aventi ad oggetto la verifica di conformità: alla Convenzione/Accordi stipulata/i con APPAG, alla normativa applicabile, a manuali e procedure APPAG, da realizzarsi presso gli OD, ecc.) il modello di check list da utilizzare è quello standard approvato dal Responsabile dell'Ufficio Controllo Interno e disponibile in apposita cartella all'interno dell'archivio informatico dell'Ufficio. Al modello, se del caso, possono essere apportate le integrazioni ritenute opportune per il caso specifico, che sono in ogni caso approvate dal Responsabile dell'Ufficio Controllo Interno.

Per altre tipologie di audit (ad es. su processi, attività, ecc.) la check list da utilizzare viene preparata "ad hoc". L'Auditor, dopo aver acquisito ed analizzato i documenti prescrittivi applicabili (es. bandi, manuali, ecc.), dopo aver raccolto ed analizzato le opportune informazioni sul processo, attività, ecc. da verificare, ed aver pianificato e condiviso con il Responsabile dell'Ufficio Controllo Interno l'estensione e la metodologia del controllo da realizzare, provvede ad elaborare la check list che, prima di essere utilizzata, è approvata dal Responsabile dell'Ufficio Controllo Interno.

4. ESECUZIONE DEGLI AUDIT

Qualora possibile, all'inizio della fase di esecuzione dell'audit - prima di dare inizio alla raccolta delle evidenze - l'auditor tiene una riunione di apertura con i responsabili del soggetto sottoposto ad audit e/o, se appropriato, con i Responsabili delle attività/processi oggetto dell'audit, al fine di:

- confermare la pianificazione prevista per le attività di audit;
- sintetizzare le modalità che saranno adottate per realizzare le attività di audit;
- confermare i canali di comunicazione precedentemente stabiliti;
- offrire al soggetto sottoposto ad audit la possibilità di fare delle domande.

Nel corso dell'audit vengono acquisiti i dati e le informazioni ed effettuate le necessarie verifiche utilizzando, per quanto possibile, le check list precedentemente predisposte ed approvate dal Responsabile dell'Ufficio Controllo Interno. L'acquisizione dei dati e delle informazioni che costituiscono evidenze dell'audit, avviene di norma mediante riesame di documenti, consultazione di banche dati, accertamenti tecnici, interviste, osservazione di attività, ovvero mediante altre forme idonee.

La verifica della conformità alla normativa vigente e la corretta attuazione delle procedure formalizzate di autorizzazione, esecuzione e contabilizzazione dei pagamenti a carico del FEAGA e del FEASR può essere realizzata tramite controlli presso le strutture interne all'APPAG, presso gli OD, nonché tramite eventuali controlli presso i beneficiari degli aiuti/premi.

Qualora dai controlli realizzati emergano evidenze di rilievi che potrebbero avere rilevanza dal punto di vista penale o amministrativo, ovvero che potrebbero implicare l'avvio di provvedimenti finalizzati al recupero di somme erogate, l'auditor dovrà con sollecitudine informare il Responsabile dell'Ufficio Controllo Interno ed il Direttore dell'APPAG per l'avvio degli atti conseguenti.

4.1 Classificazione dei rilievi

L'Ufficio Controllo Interno, nella propria attività di audit, classifica i rilievi in base alla loro gravità, definendoli come di seguito:

Non Conformità (NC) quando riscontri:

a. la totale assenza di documentazione e/o la sistematica inadeguatezza nell'applicazione di una o più regole applicabili;
b. il non soddisfacimento di una regola che determina significativa incertezza circa la capacità dell'attività realizzata di fornire un risultato conforme a quanto atteso;
c. un insieme di Raccomandazioni (RACC), riconducibili ad un singolo elemento di una regola applicabile che implichi una inadeguatezza significativa dell'attività relativamente a tale elemento;
d. il persistere nel tempo del mancato soddisfacimento di una regola applicabile.

Quando, nel corso di un audit, sono rilevate NC, l'auditor incaricato ne informa immediatamente il Responsabile dell'Ufficio Controllo Interno, al fine di permettere l'assunzione dei provvedimenti ritenuti necessari.

Raccomandazione (RACC) quando riscontri il mancato soddisfacimento di una regola applicabile che, pur non essendo tale da compromettere l'efficacia dell'attività realizzata, necessita di un'Azione Correttiva (AC) da attuarsi nei tempi e nei modi concordati con APPAG.

Commento (COMM) quando riscontri una difformità/irregolarità puntuale, non sistematica e di lieve entità, che non rappresenta una situazione oggettiva di mancato soddisfacimento di una regola applicabile ma che, a giudizio dell'auditor, merita chiarimenti, ulteriori approfondimenti o migliorie. Qualora non venga adeguatamente gestita, la stessa potrebbe degenerare nel mancato soddisfacimento di una regola applicabile.

Il Commento in ogni caso non pregiudica il giudizio di conformità sull'attività realizzata.

I rilievi formalizzati dall'auditor costituiscono la base di riferimento per i futuri controlli (follow-up).

5. CHIUSURA DEGLI AUDIT (REGISTRAZIONE DEI RISULTATI)

Al termine della fase di raccolta delle evidenze (in occasione della riunione finale dell'audit) gli errori e le principali carenze del sistema devono essere discussi con i responsabili del soggetto controllato: è in tal modo possibile accertare la comprensione della natura di tali errori e punti deboli da parte del soggetto controllato, nonché discutere e concordare eventuali interventi necessari per correggere gli errori stessi e migliorare i sistemi. In occasione della riunione finale, è concesso ai responsabili dell'organismo controllato di formulare eventuali osservazioni e/o riserve, di cui l'auditor terrà conto nella redazione del Verbale di controllo.

L'attività di controllo si conclude con la redazione e la sottoscrizione da parte dell'auditor di apposito Verbale di controllo (vedi ALLEGATO 2), che è trasmesso al soggetto controllato. Tale Verbale contiene il resoconto delle singole attività di controllo svolte e riporta in forma chiara i rilievi riscontrati. Il Verbale dovrà essere sottoscritto dal soggetto controllato per presa visione ed accettazione dei suoi contenuti.

Nel caso in cui il controllato si rifiuti di sottoscrivere il Verbale, dovrà darne motivazione scritta. Qualora, pur firmando il Verbale, ritenga di formulare proprie osservazioni o riserve in merito ai rilievi elevati, ciò dovrà avvenire in modo formale, attraverso nota scritta.

Il Verbale di controllo rappresenta lo strumento principale per la comunicazione dei risultati dell'audit: deve quindi essere chiaro e conciso, deve contenere un riassunto dei principali risultati acquisiti nel corso della verifica, nonché descrivere i rilievi (errori e carenze) riscontrati, in modo tale da permettere ai soggetti controllati di rettificare detti errori e carenze in tempi opportuni.

Il Verbale di controllo deve presentare i risultati e le conclusioni dell'audit in modo tale da dimostrare all'organismo controllato i punti deboli del sistema.

Esso deve inoltre specificare come l'auditor intenda dare seguito al controllo per verificare se siano stati adottati gli adeguati correttivi, per esempio chiedendo all'organismo controllato di presentare una relazione scritta sugli interventi che intende attuare in risposta ai rilievi riscontrati.

6. AZIONI SUCCESSIVE ALL'AUDIT

6.1 Gestione dei rilievi

L'auditor incaricato deve dar seguito all'audit per assicurarsi che adeguate azioni correttive siano state intraprese a fronte dei rilievi riscontrati nel corso delle verifiche, che queste siano state tempestive, efficaci e stiano ottenendo i risultati desiderati.

L'organismo controllato è responsabile di proporre all'Ufficio Controllo Interno, in modo formale, le azioni appropriate da intraprendere ed i relativi tempi di attuazione. Il Responsabile dell'Ufficio Controllo Interno ha la responsabilità di valutarne l'adeguatezza, al fine di dare una efficace e tempestiva soluzione ai rilievi evidenziati.

Oggetto, tempi e portata delle verifiche successive sono pertanto definiti dal Responsabile dell'Ufficio Controllo Interno in base alla gravità del rilievo.

Fattori che devono essere considerati nel definire appropriate procedure di controllo successivo sono:

- la significatività dei rilievi riportati (Non Conformità, Raccomandazione, Commento);
- l'impegno ed i costi necessari per correggere le condizioni riportate;
- le conseguenze di un fallimento dell'azione correttiva;
- la complessità dell'azione correttiva;
- il periodo di tempo richiesto.

In termini generali, la procedura definita per i controlli successivi considera quanto segue:

I rilievi classificati come **Non Conformità** richiedono azioni immediate da parte di chi ne ha la responsabilità. Dato l'effetto che potrebbero avere sull'organizzazione, tali condizioni devono essere tenute sotto continua osservazione fino alla loro completa sistemazione e la verifica circa la corretta attuazione ed efficacia avviene anche in tempi ristretti.

Per i rilievi classificati come **Raccomandazioni**, può essere giudicata sufficiente l'approvazione, da parte del Responsabile dell'Ufficio Controllo Interno, delle azioni correttive e dei relativi tempi di attuazione proposti formalmente dall'organismo controllato, rimandando la verifica circa la corretta attuazione ed efficacia ad una verifica di follow-up programmata a distanza di tempo.

I rilievi classificati come **Commenti** non richiedono obbligatoriamente una proposta di azioni correttive da parte del soggetto controllato; l'Ufficio Controllo Interno, tuttavia, raccomanda anche in questi casi di definire ed intraprendere misure per superare le criticità segnalate.

L'Ufficio Controllo Interno deve in ogni caso assicurare che le azioni intraprese pongano davvero rimedio ai rilievi riscontrati; pertanto il responsabile provvede a programmare le attività di controllo successivo come parte del programma di audit.

Il Responsabile dell'Ufficio Controllo Interno deve stabilire opportune regole

relativamente:

- ai limiti temporali entro i quali la risposta ai rilievi dell'audit deve pervenire da parte del soggetto controllato in modo formale;
- alle modalità con cui avviene la valutazione delle risposte ottenute (se sono idonee a risolvere il problema);
- alle modalità con cui avviene la verifica dell'azione correttiva attuata (se necessaria);
- al sistema per sottoporre al Direttore dell'OP le risposte e le azioni ritenute insoddisfacenti.

6.2 Verifiche di follow-up

L'auditor che è incaricato di eseguire un "*follow-up*" raccoglie le osservazioni rilevate e riportate nel Verbale di audit e aggiorna con le stesse la "Tavola di follow-up" (vedi ALLEGATO 4).

La "Tavola di follow-up" è lo strumento utilizzato al fine di raccogliere, monitorare e analizzare lo stato dei piani di miglioramento (o piani d'azione), preventivamente concordati con i Responsabili dei processi.

La Tavola è costituita indicativamente dalle seguenti sezioni:

- **Processo**: riporta il nome del processo al quale è riferito il rilievo.
- **Data Audit**: riporta la data dell'audit.
- **Rilievo riscontrato**: riporta la descrizione sintetica del rilievo riscontrato.
- **Classificazione Rilievo**: riporta la tipologia del rilievo riscontrato (NC, RACC, COMM).
- **Azione da implementare**: riporta l'azione correttiva che il soggetto auditato è impegnato ad attuare per risolvere il rilievo.
- **Data attuazione Azione Correttiva**: riporta la data un cui deve essere completata da parte del soggetto auditato l'implementazione dell'azione correttiva.
- **Data Verifica Chiusura Rilievo**: riporta la data nella quale è stata verificata da parte dell'auditor l'effettiva e completa implementazione dell'azione correttiva ed è stato accertato che l'azione intrapresa risulta effettivamente efficace a rimuovere la causa che ha generato il rilievo riscontrato originariamente.
- **Audit Status**: riporta lo stato della raccomandazione. A tal fine sono state stabilite le seguenti codifiche:
  - I = l'azione è stata implementata/il rilievo ha perso la sua ragione d'essere;
  - N= l'azione non è stata implementata/il rilievo è ancora in essere;
  - R= si è verificato un ritardo nell'implementazione dell'azione, dovuto a motivazioni non dipendenti dalla volontà del soggetto auditato;
  - Z= si è verificata un'impossibilità ad implementare l'azione, dovuta a motivazioni non dipendenti dalla volontà del soggetto auditato;

- S= si è verificato un cambiamento normativo/organizzativo interno che non richiede più alcuna azione;
- C= da completare.

Al termine dell'intervento di follow-up, il Responsabile dell'Ufficio Controllo Interno verifica il corretto aggiornamento della Tavola di follow-up.

La Tavola, gestita su formato elettronico, è mantenuta ed archiviata presso l'Ufficio Controllo Interno ed utilizzata nella pianificazione dei futuri interventi di follow-up, oltre che alla produzione di eventuali statistiche sulle percentuali di implementazione delle azioni correttive conseguenti a rilievi formalizzati dall'Ufficio Controllo Interno.

L'esito dell'attività di follow-up è comunicato in modo formale da parte del Responsabile dell'Ufficio Controllo Interno all'organismo controllato ed alla Direzione dell'OP.

7. LA RELAZIONE FINALE DI CONTROLLO

Al termine dell'attività di audit, dopo aver valutato positivamente la proposta di azioni correttive inoltrata dal soggetto controllato, viene predisposta la Relazione finale di controllo (vedi ALLEGATO 3), che è firmata dall'auditor e dal Responsabile dell'Ufficio Controllo Interno e da questi trasmessa al Direttore dell'APPAG.

La Relazione finale di controllo deve contenere almeno le seguenti informazioni:

- oggetto dell'audit;
- soggetto auditato;
- obiettivi dell'intervento di audit;
- risultati e conclusioni;
- descrizione dei rilievi riscontrati;
- azioni correttive concordate con il soggetto auditato.

8. L'ARCHIVIAZIONE DELLA DOCUMENTAZIONE DEL CONTROLLO INTERNO

L'ufficio Controllo Interno è dotato di un archivio cartaceo e di un archivio informatico.

Negli archivi dell'Ufficio sono conservate la documentazione e le comunicazioni, "da" e "verso" l'esterno relativamente agli interventi di audit svolti, la documentazione di pianificazione e gestione delle proprie attività, copia del presente manuale e copia di altri documenti di interesse dell'Ufficio, al fine di permetterne una facile ed immediata consultazione al personale.

Gli spazi fisici in cui risiede l'archivio cartaceo sono organizzati all'interno di appositi armadi, accessibili al solo personale dell'Ufficio Controllo Interno.

L'archivio informatico risiede in specifica cartella di rete denominata "X002 Controllo Interno", all'interno dell'area riservata ad APPAG "Unità di Rete U - USERS151".

Come previsto dal "Manuale di Gestione del Protocollo Informatico dei documenti e dell'Archivio", il tempo di conservazione dei documenti prodotti da APPAG è di almeno 10 anni.

Archivio cartaceo:

Nell'archivio cartaceo sono conservati a cura del personale dell'Ufficio Controllo Interno:

- ✓ La documentazione relativa all'attività di audit svolta, che è conservata in fascicoli cartacei denominati "fascicoli di controllo". Detti fascicoli sono generalmente organizzati in sezioni, come di seguito:
  - **Pianificazione:** all'interno di tale sezione vengono archiviati la lettera di incarico all'auditor, il Memorandum di Pianificazione dell'intervento e l'eventuale Verbale di estrazione del campione;
  - **Check list, Verbale di controllo ed evidenze:** raccoglie le check list utilizzate ed il Verbale di controllo redatto nel corso dell'intervento di audit, nonché eventuali evidenze documentali raccolte nel corso dello svolgimento dell'audit;
  - **Relazione finale:** all'interno di tale sezione viene archiviata la Relazione finale di controllo;
  - **Corrispondenza:** raccoglie e documenta tutte le comunicazioni intervenute tra l'Ufficio Controllo Interno e i soggetti controllati in tutte le fasi dell'intervento di audit;
  - **Documenti prescrittivi:** contiene tutti i documenti (bandi, manuali, circolari, linee guida, normativa ecc.) sulla base dei quali si è svolto l'audit;
  - **Altra documentazione:** raccoglie l'eventuale altra documentazione che il team di lavoro incaricato dell'intervento di audit ritiene rilevante e da mantenersi archiviata;
  - **Follow-up:** raccoglie copia cartacea delle Tavole di follow-up relative all'intervento di audit, nonché tutta la documentazione prodotta nel corso di questa fase.

- ✓ Altra documentazione (corrispondenza, documentazione relativa ad attività interna, ecc.) è conservata in apposti contenitori o cartelle sui quali sono riportati tutti i riferimenti al proprio contenuto.

E' possibile l'archiviazione informatica di documenti relativi ad un fascicolo di controllo. In questo caso, all'interno del fascicolo di controllo cartaceo, è inserito specifico riferimento, idoneo a permettere l'immediata rintracciabilità del documento all'interno dell'archivio informatico.

Archivio informatico:

Sono archiviati in apposite cartelle e sub-cartelle residenti all'interno dell'archivio informatico dell'Ufficio Controllo Interno:

- ✓ una copia del presente Manuale e dell'altra documentazione operativa necessaria a supportare lo svolgimento delle attività dell'Ufficio;
- ✓ una copia del Piano quinquennale ed annuale degli audit;
- ✓ documenti prodotti nel corso dell'audit e facenti parte del "fascicolo di controllo", di cui è conservata la copia informatica;
- ✓ altra documentazione (corrispondenza, documentazione relativa ad attività interna, ecc).

Ciascuna cartella e sub-cartella di archiviazione è denominata in modo tale da permettere una immediata rintracciabilità dei suoi contenuti.

La struttura dell'archivio informatico è descritta nel documento "Struttura archivio informatico", approvato dal Responsabile dell'Ufficio Controllo Interno e conservato nella cartella **X002 - Controllo Interno/Archivio da ottobre 2011/ VARIE / STRUTTURA ARCHIVIO INFORMATICO.**

9. L'AUDIT DEI SISTEMI IT

9.1 Definizione degli obiettivi

La sempre maggiore dipendenza dei processi dell'Organismo Pagatore dall'informatica determina l'applicazione, da parte dell'Ufficio Controllo Interno, di tecniche di audit anche in materia di Information Technology (IT).

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;
- supportare l'audit operativo nel fornire il conforto atteso circa l'efficacia dei controlli, che sono fortemente automatizzati;
- supportare l'audit operativo nell'elaborazione ed analisi dei dati attraverso strumenti informatici;
- verificare se gli Standard di Sicurezza dei Sistemi Informativi (Sistemi di Informazione) adottati dall'Organismo Pagatore sono conformi alla normativa di riferimento.

9.2 Analisi del "Sistema di Gestione della Sicurezza delle informazioni"

Al fine di cogliere il primo degli obiettivi riportati nel precedente paragrafo, la metodologia adottata dall'Ufficio Controllo Interno propone un'analisi del processo in cui sono sintetizzate tutte le attività di gestione degli aspetti informatici dell'OP.

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

- IT Risk Assessment
- Piano di audit IT
- Esecuzione di test sull'ambiente IT

9.2.1 IT Risk Assessment

Le attività preliminari a tale fase sono la mappatura delle infrastrutture tecnologiche esistenti, la rilevazione del parco applicativo dell'OP e della struttura organizzativa dei Sistemi Informativi. Tali informazioni dovranno essere sempre tenute in considerazione durante tutta l'attività di IT auditing.

Segue l'attività vera e propria di IT Risk Assessment, durante la quale il processo di supporto è suddiviso nei seguenti processi secondari (sub-processi):

- Pianificare ed organizzare l'ambiente dei Sistemi Informativi (SI);
- Sviluppare ed acquisire le soluzioni dei SI;
- Gestire l'operatività dei SI;
- Monitorare l'ambiente dei SI (quest'ultimo può essere inserito all'interno di Pianificare ed organizzare l'ambiente dei SI).

Tramite interviste con il personale IT dell'OP, per ciascun processo secondario, coerentemente con la metodologia generale di Risk Assessment (usata nei processi principali), sono individuati gli scopi, gli obiettivi, i Responsabili del processo e le descrizioni delle attività principali, i confini, gli input/output e gli indicatori di performance.

Successivamente, congiuntamente con il Responsabile del processo, sono identificati i rischi principali insiti nelle attività descritte e si procede alla loro valutazione in termini di impatto e probabilità. Poi ne vengono mappate le attività di controllo a cui, sempre congiuntamente con il Responsabile del processo, viene dato un giudizio preliminare in merito alla loro capacità di mitigare il rischio in oggetto.

Contestualmente è possibile eseguire delle attività di confronto di quanto rilevato con i controlli previsti dallo standard di riferimento in merito alle attività di controllo e quindi identificare delle aree di miglioramento già in fase di intervista.

9.2.2 Piani di audit IT

La fase di piano di audit IT, che formalmente è incluso nel Piano di Audit, rientra nella fase più generale di pianificazione in cui sono analizzate le aree di rischio a livello di OP, al fine di scegliere gli interventi di audit da eseguire.

Qualora si decida di includere l'esecuzione di interventi di audit conseguenti a rischi valutati alti nei processi di Information Technology, è bene considerare i seguenti aspetti, per poter dare delle indicazioni precise sui confini dell'intervento già in fase di piano di audit IT:

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

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

9.2.3 Esecuzione di test sull'ambiente IT

La fase di esecuzione di test sull'ambiente IT ha come input tutti gli elementi indicati nel Piano di Audit IT, il rischio in considerazione, le attività di controllo da testare, le aree di infrastruttura e/o gli applicativi di riferimento, i controlli definiti dallo standard di riferimento, ecc., ed il budget in termini di tempo per risorsa.

Durante questa fase le risorse devono analizzare i dati in loro possesso e definire un programma di lavoro indicando:

- gli obiettivi generali che si intendono perseguire;
- le informazioni e la documentazione necessaria come input all'esecuzione dell'intervento e che può essere analizzata prima della partenza dello stesso;
- un'agenda delle interviste necessarie con gli obiettivi delle interviste;

- un'agenda dei test sull'elaboratore con gli obiettivi di tali test;
- una check-list dei punti di controllo salienti che non devono essere tralasciati dall'insieme di interviste e test.

Il sistema di reporting delle evidenze riscontrate è sostanzialmente identico a quello indicato per i processi principali.

9.3 Utilizzo di standard di riferimento

Proprio per poter rispondere in maniera efficiente alla complessità di tali impegni, l'auditor dei Sistemi Informativi si affida, ormai da tempo, a standard collaudati che permettono all'auditor di seguire linee guida, sempre in evoluzione, nello svolgimento dell'attività.

In particolare è possibile creare una buona integrazione tra la metodologia adottata dal Controllo Interno e lo Standard ISO 27001 – ISO 27002.

Dal momento che l'informazione è un bene a valore aggiunto, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. L'obiettivo dello Standard ISO 27001, e conseguentemente dello Standard IS0 27002, il quale contiene le linee guida per l'implementazione dei controlli, è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato Sistema di Gestione della Sicurezza delle Informazioni finalizzato ad una corretta gestione delle informazioni rilevanti per l'organizzazione.

Lo Standard ISO 27001 è stato introdotto nel 2005 in sostituzione delle varie versioni locali della norma inglese BS 7799 parte 2 e si basa sul modello di Deming (o PDCA - Plan, Do, Check, Act) come mezzo per l'introduzione e l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI).

Il Sistema di Gestione per la Sicurezza delle Informazioni (Information Security Management System, ISMS) ha come obiettivo principale l'implementazione di adeguati controlli, sotto forma di strutture organizzative, policy operative, istruzioni, procedure e funzioni software atti ad assicurare il soddisfacimento di specifici obiettivi di sicurezza definiti dall'organizzazione.

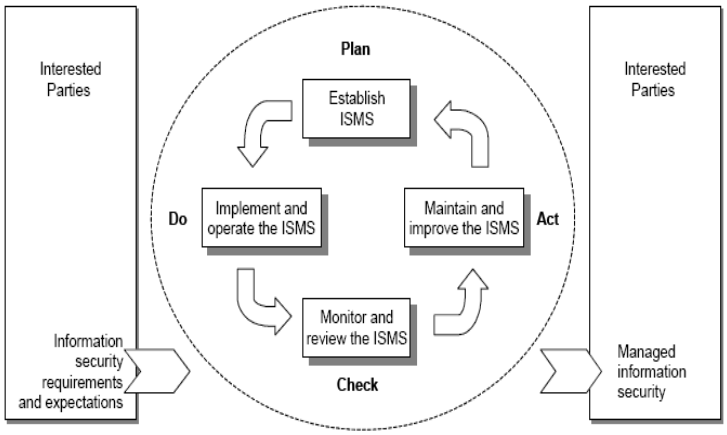


Figura 1: Modello PDCA applicato al processo SGSI

Nello Standard ISO 27001 le fasi del ciclo PDCA sono indirizzate a:

- **Pianificare (Plan):**
  - definire il campo di applicazione del SGSI;
  - definire la politica per la sicurezza delle informazioni;
  - definire e condurre una valutazione sistematica del rischio, al livello del singolo dato dell'informazione;
  - individuare e valutare alternative per il trattamento di questi rischi;
  - selezionare gli obiettivi di controllo ed i controlli per ogni decisione di trattamento del rischio;
  - redigere lo Statement of Applicability (SoA).
- **Attuare (Do):**
  - redigere il piano di trattamento del rischio, inclusi i processi pianificati e le procedure;
  - implementare il piano di trattamento del rischio e relativi controlli;
  - fornire formazione e trasmettere consapevolezza al personale;
  - gestire le attività e le risorse in linea con il SGSI;
  - implementare procedure e contromisure per l'enunciazione e la risposta agli incidenti di sicurezza.
- **Controllare (Check):**
  - questa è la fase del monitoraggio, controllo, audit e riesame.
- **Agire (Act):**
  - quanto emerso dalla fase "Check" deve essere analizzato e costituire la base su cui avviare azioni, incluse quelle necessarie per affrontare delle variazioni in uno qualsiasi degli elementi che influenzano il rischio.

È di fondamentale importanza l'appendice A dell'ISO 27001, che contiene i 133 "controlli" a cui l'organizzazione che intende applicare la norma deve attenersi. Essi sono raggruppati in 11 macrocategorie di controllo principali e sono rivolti a tutte le aree potenziali di rischio: essi vanno dalla politica e l'organizzazione per la sicurezza alla gestione dei beni e alla sicurezza delle risorse umane, dalla sicurezza fisica e ambientale alla gestione delle comunicazioni e dell'operativo, dal controllo degli accessi fisici e logici

alla gestione di un monitoraggio e trattamento degli incidenti (relativi alla sicurezza delle informazioni).

La gestione della Business Continuity e il rispetto normativo, completano l'elenco degli obiettivi di controllo.

Di seguito si elencano le 11 macrocategorie di controlli estratte dall'appendice A dell'ISO 27001:

- A. 5 Security policy
- A. 6 Organizzazione della sicurezza delle informazioni
- A. 7 Gestione delle risorse
- A. 8 Sicurezza delle risorse umane
- A. 9 Sicurezza fisica e ambientale
- A.10 Gestione delle comunicazioni e della operatività
- A.11 Controllo accessi
- A.12 Acquisizione, sviluppo e manutenzione dei sistemi informativi
- A.13 Gestione degli incidenti di sicurezza delle informazioni
- A.14 Gestione della continuità aziendale (Business Continuity)
- A.15 Rispetto della normativa

Secondo lo Standard ISO 27001, l'organizzazione deve motivare quali di questi controlli non sono applicabili all'interno del suo SGSI.

I suddetti controlli sono poi approfonditi all'interno dello Standard ISO 27002:2005 (che ha sostituito nel luglio 2007 il precedente ISO 17799:2005); tale ulteriore documento definisce le linee guida per la definizione delle contromisure, ovvero iniziative, per la gestione e la mitigazione di specifici rischi.

In particolare, mentre l'ISO 27001 è il documento normativo al quale un'organizzazione che intenda certificarsi deve far riferimento, l'ISO 27002 fornisce delle indicazioni non prescrittive per proteggere il patrimonio informativo di un'azienda conformemente a quanto definito a livello normativo. In altre parole è una raccolta di linee guida sulla predisposizione di un SGSI: infatti, le clausole dello Standard ISO 27002 coincidono con le 11 macrocategorie elencate nell'allegato A dell'ISO 27001.

9.3.1 Applicazione dei contenuti dello Standard ISO 27001 – 27002 alla metodologia del Controllo Interno

È possibile implementare la metodologia del Controllo Interno per i processi IT sfruttando i contenuti dello Standard ISO 27001 - 27002 e descrivendo i propri processi secondari e sotto processi in rapporto ai controlli definiti nelle aree di controllo ISO 27001 - 27002 ritenute come applicabili.

Di seguito saranno illustrate le tre fasi fondamentali della metodologia del Controllo Interno per mettere in evidenza la possibilità di sfruttare i contenuti dello Standard ISO27001 – 27002 nelle stesse fasi.

9.3.2 Risk Assessment con ISO 27001-27002

La fase di IT Risk Assessment basata sullo Standard ISO 27001 - 27002 non modifica lo scopo e gli obiettivi indicati nel precedente paragrafo "IT Risk Assessment", ma sfrutta semplicemente la struttura ISO 27001 - 27002, per la mappatura preventiva dei processi, dei rischi e dei controlli inseriti nell'ambito del Sistema di Gestione della Sicurezza delle Informazioni, con specifico riferimento ai processi informatici. Tali mappature preliminari saranno poi personalizzate tramite le interviste ai Responsabili dei processi IT. Infatti, la descrizione dei processi è tale da consentire, per ciascun processo secondario, la definizione dello scopo, degli obiettivi, degli owner e delle descrizioni, dei confini e degli input/output.

Secondo lo Standard ISO 27001 – 27002, il Risk Assessment è un processo iterativo; in generale, l'analisi dei rischi deve essere sviluppata considerando:

- le attuali condizioni del sistema;
- la situazione a seguito dell'adozione delle contromisure ipotizzate.

Il risultato della differenza è il "rischio residuo", che la Direzione deve valutare ed accettare, per implementare il SGSI.

- Nello specifico, la metodologia di implementazione di un sistema di un SGSI conforme allo Standard ISO 27001 – 27002, integrata con quella del Controllo Interno, si può configurare nelle seguenti quattro fasi, di cui il Risk Assessment rappresenta la terza:
  1 Identificazione degli asset: realizzare il censimento dei beni (asset), intendendo con "bene" qualcosa a cui un'organizzazione assegna direttamente un valore e che, di conseguenza, richiede un'opportuna protezione.
  2 Classificazione degli asset: definire la sensibilità degli asset rispetto ai parametri di sicurezza indicati dalle diverse normative vigenti: Riservatezza, Integrità e Disponibilità.
  3 Valutazione del Rischio: definizione del livello di rischio a cui l'APPAG è esposta, in considerazione al contesto in cui operano i propri processi ed alle minacce esistenti, tramite una valutazione delle possibili vulnerabilità del sistema dei controlli, implementato rispetto a quanto previsto dallo Standard ISO 27001 – 27002.
  4 Gestione del Rischio: fornire dei criteri per la scelta, da parte di APPAG, delle modalità di gestione ottimale dei rischi individuati con possibili impatti sugli asset, e valutati nelle fasi precedenti.
- In tale ambito, le 11 macrocategorie saranno preventivamente mappate sui processi informatici, in modo tale da poter associare i controlli previsti dallo Standard con i 4 processi secondari di gestione dell'ambiente IT, e di conseguenza procedere alla valutazione dei controlli esistenti.

9.3.3 Piano di audit IT con ISO 27001-27002

Come descritto nel paragrafo "Piano di audit IT", la valutazione dei rischi guida la scelta delle aree su cui eseguire la fase operativa di test. Nell'applicazione della metodologia integrata con lo Standard ISO 27001 – 27002, ogni rischio è fortemente legato agli asset individuati come rilevanti e ai controlli selezionati come applicabili.

9.3.4 Esecuzione di test sull'ambiente IT con ISO 27001-27002

Tale fase avviene coerentemente con quanto descritto nel paragrafo "Esecuzione di test sull'ambiente IT".

Nell'applicazione della metodologia con i contenuti ISO 27001 - 27002, è necessario tenere in opportuna considerazione la mappatura eseguita delle 11 macrocategorie di controllo definite dallo Standard sui 4 processi secondari definiti dalla metodologia stessa, al fine di poter procedere alla rilevazione degli eventuali gap tra quanto definito dallo Standard e quanto effettivamente implementato.

9.4 Supporto all'audit

9.4.1 Controlli automatizzati

Il secondo obiettivo indicato per le attività di IT auditing è di supportare l'audit operativo nel fornire un certo grado di conforto sull'efficiacia dei controlli che sono fortemente automatizzati.

A tal fine è opportuno impostare progetti di audit multidisciplinari con competenze IT e competenze nell'area operativa di riferimento.

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

La verifica del controllo applicativo può poi avvenire nei seguenti modi:

- istituendo un ambiente informatico di test, identico a quello di produzione, su cui eseguire piani di test volti a validare il funzionamento del controllo rispetto al comportamento previsto;
- verificando, ad esempio tramite affiancamento all'utente durante la normale attività lavorativa, il funzionamento del controllo direttamente in ambiente di produzione e su casi di lavoro reali;
- definendo un set significativo di dati di input, e verificando che l'output di sistema coincida con quanto atteso secondo i requisiti dei processi dell'APPAG.

I controlli in oggetto sono comunque effettuati in accordo con quanto previsto dal Piano di Audit pluriennale.

9.4.2 Analisi dati

L'ultimo obiettivo indicato per le attività di IT auditing è di supportare l'audit nell'elaborare analisi di dati attraverso strumenti informatici.

Anche a tal fine è indispensabile istituire team multidisciplinari con competenze nelle aree operative interessate e con competenze di strumenti informatici di gestione dei dati. Gli obiettivi delle elaborazioni devono essere indicati dall'auditor operativo, mentre è scopo dell'auditor IT di sviluppare le tecniche analitiche di analisi dei dati, di individuare lo strumento informatico (es. ACL, Ms Access, Monarch, ecc.) che meglio consente

l’esecuzione di tali tecniche analitiche e di implementare le stesse attraverso lo strumento informatico prescelto.

ALLEGATO 1 – Format Memorandum di pianificazione dell'intervento di audit

APPAG - Agenzia provinciale per i pagamenti
Via G. B. Trener, 3 – 38121 Trento - tel. 0461 495877
fax 0461 495810 - e-mail: appag@provincia.tn.it
Ufficio Controllo interno

Spettabile
(Soggetto auditato)

e, p.c. Egregio Signore
(nominativo Direttore APPAG)
Direttore Agenzia Provinciale per i Pagamenti

S E D E

Trento,

Prot. n. PAT/S151/201…./ /8.3 o 8.4

Oggetto: Codice intervento di audit – Memorandum di pianificazione dell'intervento di audit.

Con la presente siamo a comunicare l'intervento di audit che è stato pianificato dall'Ufficio Controllo Interno di APPAG presso la/il Vostra/o Unità/Organismo Delegato, così come previsto dal Piano quinquennale degli audit, approvato con determinazione del Direttore di APPAG n. …….. di data ……..…..

L'audit si realizzerà nelle seguenti fasi:

i. …….
ii. ..……..
iii. …….

Gli obiettivi dell'audit possono essere così riassunti:

1) ……
2) ……
3) ……

(Qualora applicabile):

Le pratiche estratte a campione da sottoporre ad audit sono di seguito riportate:

1) …….

2) …….

3) …….

Siamo pertanto a richiedere di volerci mettere a disposizione la documentazione necessaria per l'effettuazione della verifica.
(qualora ritenuto opportuno, inserire l'elenco della documentazione richiesta)

L'intervento di audit avrà inizio in data ……. e si concluderà entro il mese di ……..…….

Il Team di audit incaricato è composto da (nome e cognome dei componenti del team incaricato).

Informiamo che, in conformità a quanto definito dal Manuale operativo APPAG applicabile, l'Ufficio Controllo Interno, nella propria attività di audit, classifica i rilievi in base alla loro gravità, definendoli come di seguito:

Non Conformità (NC) quando riscontri:

a. la totale assenza di documentazione e/o la sistematica inadeguatezza nell'applicazione di una o più regole applicabili;
b. il non soddisfacimento di una regola che determina significativa incertezza circa la capacità dell'attività realizzata di fornire un risultato conforme a quanto atteso;
c. un insieme di Raccomandazioni (RACC), riconducibili ad un singolo elemento di una regola applicabile che implichi una inadeguatezza significativa dell'attività relativamente a tale elemento;
d. il persistere nel tempo del mancato soddisfacimento di una regola applicabile.

Quando, nel corso di un audit, siano rilevate Non Conformità, l'auditor incaricato ne informa immediatamente il Responsabile dell'Ufficio Controllo Interno, al fine di permettere l'assunzione dei provvedimenti ritenuti necessari.
I rilievi classificati come Non Conformità richiedono azioni immediate da parte di chi ne ha la responsabilità. Dato l'effetto che potrebbero avere sull'organizzazione, tali condizioni devono essere tenute sotto continua osservazione fino alla loro completa sistemazione e la verifica circa la corretta attuazione ed efficacia avviene anche in tempi ristretti.

Raccomandazione (RACC) quando riscontri il mancato soddisfacimento di una regola applicabile che, pur non essendo tale da compromettere l'efficacia dell'attività realizzata, necessita di un'Azione Correttiva (AC) da attuarsi nei tempi e nei modi concordati con APPAG.
Per i rilievi classificati come Raccomandazioni, può essere giudicata sufficiente l'approvazione, da parte del Responsabile dell'Ufficio Controllo Interno, delle azioni correttive e dei relativi tempi di attuazione proposti formalmente dall'organismo controllato, rimandando la verifica circa la corretta attuazione ed efficacia ad una verifica di follow-up programmata a distanza di tempo

Commento (COMM) quando riscontri una difformità/irregolarità puntuale, non sistematica e di lieve entità, che non rappresenta una situazione oggettiva di mancato soddisfacimento di una regola applicabile ma che, a giudizio dell'auditor, merita chiarimenti, ulteriori approfondimenti o migliorie. Qualora non venga adeguatamente gestita, la stessa potrebbe degenerare nel mancato soddisfacimento di una regola applicabile. Il Commento in ogni caso non pregiudica il giudizio di conformità sull'attività realizzata.
I rilievi classificati come Commenti, non richiedono obbligatoriamente una proposta di azioni correttive da parte del soggetto controllato; l'Ufficio Controllo Interno, tuttavia, anche in questi casi raccomanda di definire ed intraprendere misure per superare le criticità segnalate.

Distinti saluti.

Il Responsabile dell'Ufficio Controllo Interno

_____

ALLEGATO 2 - Format Verbale di controllo

APPAG - Agenzia provinciale per i pagamenti
Via G. B. Trener, 3 – 38121 Trento - tel. 0461 495877
fax 0461 495810 - e-mail: appag@provincia.tn.it

Ufficio Controllo interno

VERBALE DI CONTROLLO

Codice intervento di audit:	
Data:	Soggetto auditato:
Referente soggetto auditato:	Auditor incaricati:

L'audit ……..., avente ad oggetto ……, è previsto dal Piano quinquennale degli audit, approvato con determinazione del Direttore di APPAG n. …… di data ……...

Obiettivi dell'audit:

(elencare gli obiettivi come da Memorandum di controllo)

Modalità di svolgimento dell'audit:

(descrivere sinteticamente le modalità adottate per l'effettuazione dell'audit)

Disposizioni normative applicabili:

(riportare i riferimenti normativi sulla base dei quali è stato svolto l'audit)

Modalità adottate per la classificazione dei rilievi:

Non Conformità (NC) quando siano stati riscontrati:

a. la totale assenza di documentazione e/o la sistematica inadeguatezza nell'applicazione di una o più prescrizioni applicabili;
b. il non soddisfacimento di una prescrizione che determina significativa incertezza circa la capacità dell'attività realizzata di fornire un risultato conforme a quanto atteso;
c. un insieme di Raccomandazioni (RACC), riconducibili ad un singolo elemento di una prescrizione applicabile che implichi una inadeguatezza significativa dell'attività relativamente a tale elemento;
d. il persistere nel tempo del mancato soddisfacimento di una prescrizione applicabile.

Quando, nel corso di un audit, siano rilevate Non Conformità, l'auditor incaricato ne informa immediatamente il Responsabile dell'Ufficio Controllo Interno, al fine di permettere l'assunzione dei provvedimenti ritenuti necessari.

I rilievi classificati come Non Conformità richiedono azioni immediate da parte di chi ne ha la responsabilità. Dato l'effetto che potrebbero avere sull'organizzazione, tali condizioni devono essere tenute sotto continua osservazione fino alla loro completa sistemazione e la verifica circa la corretta attuazione ed efficacia avviene anche in tempi ristretti.

Raccomandazione (RACC) quando sia stato riscontrato il mancato soddisfacimento di una prescrizione applicabile che, pur non essendo tale da compromettere l'efficacia dell'attività realizzata, necessita di un'Azione Correttiva (AC) da attuarsi nei tempi e nei modi concordati con APPAG.

Per i rilievi classificati come Raccomandazioni, può essere giudicata sufficiente l'approvazione, da parte del Responsabile dell'Ufficio Controllo Interno, delle azioni correttive e dei relativi tempi di attuazione proposti formalmente dall'organismo controllato, rimandando la verifica circa la corretta attuazione ed efficacia ad una verifica di follow-up programmata a distanza di tempo.

Commento (COMM) quando sia stata riscontrata una difformità/irregolarità puntuale, non sistematica e di lieve entità, che non rappresenta una situazione oggettiva di mancato soddisfacimento di una prescrizione applicabile ma che, a giudizio dell'auditor, merita chiarimenti, ulteriori approfondimenti o migliorie. Qualora non venga adeguatamente gestita, la stessa potrebbe degenerare nel mancato soddisfacimento di una prescrizione applicabile. Il Commento in ogni caso non pregiudica il giudizio di conformità sull'attività realizzata.

I rilievi classificati come Commenti, non richiedono obbligatoriamente una proposta di azioni correttive da parte del soggetto controllato; l'Ufficio Controllo Interno, tuttavia, anche in questi casi raccomanda di definire ed intraprendere misure per superare le criticità segnalate.

Fasi della verifica:

(descrivere ciascuna attività di verifica realizzata dall'auditor, es. estrazione del campione, acquisizione documentazione, ecc.)

Risultanze dell'audit:

(descrivere i rilievi riscontrati nel corso dell'audit)

Gestione dei rilievi segnalati:

(utilizzare solo i riferimenti alla tipologia di rilievo effettivamente riscontrato, ovvero qualora ritenuto opportuno utilizzare indicazioni diverse definite per il caso specifico)

Per ciascuna **Non Conformità** descritta nel presente Verbale, all'organismo controllato è richiesto di formalizzare una risposta, da inoltrare all'Ufficio Controllo Interno di APPAG entro …… (*es. 7 gg. lavorativi, ecc.*) dalla data di ricezione del presente Verbale. Detta risposta deve fare riferimento alle Azioni Correttive che si intende intraprendere per risolvere il rilievo, i tempi di attuazione previsti ed il responsabile incaricato dell'attuazione. L'Ufficio Controllo Interno comunicherà successivamente i tempi e le modalità con cui sarà verificata l'avvenuta corretta attuazione dell'Azione Correttiva concordata.

Per ciascuna **Raccomandazione** descritta nel presente Verbale, all'organismo controllato è richiesto di formalizzare una risposta, da inoltrare all'Ufficio Controllo Interno di APPAG entro …… *(es. 15 giorni lavorativi, ecc.)* dalla data di ricezione del presente Verbale. Detta risposta deve fare riferimento alle Azioni Correttive che si intende intraprendere per risolvere il rilievo, i tempi di attuazione previsti ed il responsabile incaricato dell'attuazione.

Anche se per i **Commenti** non sono richieste obbligatoriamente delle Azioni Correttive, l'Ufficio Controllo Interno invita l'organismo controllato a definire ed intraprendere misure per superare le criticità segnalate.

Dichiarazioni rilasciate dal soggetto auditato in sede di riunione finale:

(Riportare eventuali dichiarazioni rilasciate dal soggetto auditato)

Firma auditor: _____ Data: _____

Firma soggetto auditato: _____ Data: _____

Visto:
Il Responsabile dell'Ufficio Controllo Interno

_____

Nota:

Come previsto dal Manuale del Controllo Interno dell'APPAG, nel caso in cui il controllato si rifiuti di sottoscrivere il Verbale, dovrà darne motivazione scritta. Qualora, pur firmando il Verbale, ritenga di formulare proprie osservazioni o riserve in merito ai rilievi elevati, ciò dovrà avvenire attraverso nota scritta.

ALLEGATO 3 - Format Relazione finale di controllo

APPAG - Agenzia provinciale per i pagamenti
Via G. B. Trener, 3 – 38121 Trento - tel. 0461 495877
fax 0461 495810 - e-mail: appag@provincia.tn.it
Ufficio Controllo interno

Egregio Signore
(nominativo del Direttore APPG)
Direttore Agenzia Provinciale per i Pagamenti

S E D E

Trento,

Prot. n. PAT/S151/201…./ /8.3 o 8.4

Oggetto: Codice intervento di audit – Relazione finale di controllo.

OGGETTO DELL'AUDIT:

SOGGETTO AUDITATO:

OBIETTIVI DELL'INTERVENTO DI AUDIT:

RISULTATI, CONCLUSIONI E RILIEVI:

Riportare di seguito un sintetico giudizio circa l'esito finale della verifica (positivo/negativo), facendo riferimento ai seguenti aspetti:

- ✓ *alla situazione in cui si è svolta (ambiente collaborativo/non collaborativo), e ad eventuali difficoltà e criticità riscontrate nello svolgimento dell'attività;*
- ✓ *allo stato di conformità generale del processo/attività valutato.*

L'audit ha avuto i risultati descritti nella tabella che segue:

RILIEVI E AZIONI CORRETTIVE CONCORDATE CON IL SOGGETTO CONTROLLATO			
DESCRIZIONE RILIEVO	**CLASSIFICAZIONE**	**AZIONE CORRETTIVA CONCORDATA**	**DATA ATTUAZIONE Azione Correttiva**
	(es. NC, RACC, COMM)		**Data prevista:**

Trento, li _____

Firma auditor: _____

Firma Responsabile dell'Ufficio Controllo Interno: _____

ALLEGATO 4 - Format Tavola di follow-up

APPAG - Agenzia provinciale per i pagamenti
Via G. B. Trener, 3 – 38121 Trento - tel. 0461 495877
fax 0461 495810 - e-mail: appag@provincia.tn.it

Ufficio Controllo interno

N.	Processo	Data Audit	Rilievo riscontrato (Descrizione del Rilievo)	Classificazione Rilievo (N.C. - RACC. - COMM.)	Azione da implementare	Data attuazione Azione Correttiva	Data Verifica Chiusura Rilievo	Audit Status	NOTE

Legenda Audit Status:

I azione implementata
N azione non implementata
R ritardo sull'azione
Z impossibilità ad implementare l'azione
S cambiamento organizzativo interno e/o normativo
C da completare

Auditor incaricato _____