STANDARD DI INTERNAL AUDIT
GRUPPO BMPS

DIREZIONE REVISIONE INTERNA

Terza edizione (febbraio 2016)

SOMMARIO

Allegati:

1. ODD 1673 "Codice Deontologico" della Funzione di Internal Audit del Gruppo BMPS
2. Organigramma e Funzionigramma Direzione Revisione Interna
3. a) Criteri di distribuzione dei rapporti di audit
   b) Autonomie di firma e visto
4. Template Rapporto Processi Centrali/Società
5. Linee guida per la compilazione del Rapporto Processi Centrali/Società
6. Check list intervento di audit
7. KPI della Funzione di IA
8. Mandatory Audit
9. Template Rapporto IA Società

1. PREMESSA

1.1 Obiettivi ed ambito di riferimento

La conformità agli *International Standards for the Professional Practice of International Auditing* dell'IIA (Institute of Internal Auditors) è essenziale per l'adempimento delle responsabilità degli auditors e dell'attività di internal auditing.

Gli Standard hanno lo scopo di:

- delineare i principi base che prescrivono come deve essere svolta l'attività di internal auditing;
- fornire un quadro di riferimento per lo sviluppo e l'effettuazione di una vasta gamma di attività di internal auditing a valore aggiunto;
- definire i parametri per la valutazione delle prestazioni dell'internal auditing;
- promuovere il miglioramento dei processi organizzativi e operativi.

Il presente documento definisce le caratteristiche che le organizzazioni e gli individui che svolgono attività di internal auditing nell'ambito del Gruppo BMPS devono obbligatoriamente possedere (*standard di connotazione*), insieme alle regole ed ai criteri da seguire nello svolgimento delle medesime attività di audit (*standard di prestazione*).

I relativi contenuti sono coerenti con gli standard professionali definiti dall'associazione di categoria (AIIA – *Associazione Italiana Internal Auditors*) che recepisce in Italia gli Standard internazionali per la professione, oltreché con le prescrizioni normative interne (direttive, policy, procedure, manuali, etc.) ed esterne in materia (BCE, Banca d'Italia, Consob, ISVAP, Regulators esteri, etc.).

Il perimetro di applicazione si estende a tutte le tipologie di attività svolte dalla Funzione di Internal Audit (di seguito Funzione di IA) ed ai singoli auditors appartenenti alla stessa.

Il Responsabile della Funzione di IA deve farsi garante della conformità agli Standard professionali quale elemento essenziale per lo svolgimento di tutte le attività di audit. Tale conformità viene, inoltre, valutata annualmente nella rendicontazione di *Corporate Quality Assurance Review* (CqAR).

1.2 Destinatari

Il presente documento è rivolto alle Funzioni di IA della Capogruppo e delle Società del Gruppo[1], che provvedono ad informare circa i relativi contenuti i rispettivi Organi Aziendali.

2. STANDARD INTERNAZIONALI E CODICE DEONTOLOGICO

Gli Standard internazionali per la professione definiscono i requisiti essenziali che devono caratterizzare la Funzione di IA ed il suo operato, ovvero indicano agli auditors il livello minimo di prestazione atteso (tale livello è quello necessario ad ottemperare alle responsabilità assegnate). Essi si distinguono in:

[1] Per ciascuna Funzione di IA operante presso le filiali estere di Banca Monte Paschi di Siena, vige l'"Internal Audit Policy and Procedure Manual".

- *Standard di Connotazione*: stabiliscono le caratteristiche che le organizzazioni e gli individui che svolgono attività di internal auditing, devono obbligatoriamente possedere (indipendenza, obiettività, competenza e diligenza professionale);

- *Standard di Prestazione*: descrivono la natura e le caratteristiche dell'attività di internal auditing (gestione attività di audit, pianificazione e svolgimento incarichi, monitoraggio, etc.) e forniscono criteri qualitativi in base ai quali valutarne l'effettuazione.

Per l'adempimento delle proprie responsabilità nello svolgimento delle attività di internal auditing, ciascun auditor si attiene ai contenuti del presente documento ed al rispetto dei principi e delle regole di condotta definite nell'ambito del "Codice Deontologico della Funzione IA[2]", riconducibili all'integrità, all'obiettività ed indipendenza, alla riservatezza, alla competenza ed alla diligenza professionale.

3. STANDARD DI CONNOTAZIONE

Gli standard di connotazione fanno riferimento a:

› *Finalità, Poteri e Responsabilità*.
L'attività di internal auditing deve essere definita in un formale Mandato scritto[3] - coerente con la definizione di internal auditing, il Codice Etico e gli Standard - approvato dagli Organi competenti, che ne precisi finalità, autorità e responsabilità. Il Responsabile della Funzione di IA deve periodicamente verificare tale Mandato e sottoporlo agli Organi competenti per l'approvazione.

Nel Mandato di internal audit deve, inoltre, essere definita la natura dei servizi di assurance e consulenza forniti all'organizzazione.

L'attività di consulenza fornita dalla Funzione di IA è sostanzialmente riconducibile ad un'attività di supporto ed assistenza, per lo più espletata attraverso suggerimenti e raccomandazioni forniti ad altre Funzioni che hanno l'obiettivo di apportare valore aggiunto all'organizzazione, migliorando i processi di governance, gestione dei rischi e controllo.

L'attività di consulenza svolta è finalizzata all'individuazione di soluzioni idonee a garantire il superamento dei punti di debolezza del sistema dei controlli interni (SCI). Tale contributo si manifesta sia nel momento in cui emergono disallineamenti tra lo SCI e il modello di business e di governo adottato dall'azienda, sia nella fase di impianto/revisione dei principali processi aziendali, con l'obiettivo di garantire coerenza e linearità all'intero impianto dei controlli e al presidio dei rischi.

› *Indipendenza e Obiettività*.
L'indipendenza della Funzione di IA è assicurata da un adeguato posizionamento gerarchico (riporto diretto al CdA) che consenta al Responsabile il pieno adempimento delle proprie responsabilità; l'obiettività è l'approccio imparziale che consente agli internal auditors di svolgere le proprie mansioni in assenza di compromessi e sottomissione a giudizi altrui, evitando possibili conflitti di interesse.

Se indipendenza ed obiettività sono compromesse o appaiono tali, le circostanze dei condizionamenti devono essere riferite ad un livello appropriato. La natura dell'informativa dipende dal tipo di condizionamento.

[2] Cfr. allegato n.1.
[3] Per la Capogruppo le responsabilità del Mandato sono normate nel Regolamento n.1 (D0751) – Organizzazione della Banca MPS.

In linea di principio, al fine di non mettere in discussione il giudizio indipendente ed obiettivo esprimibile dalla Funzione di IA, i nuovi auditors, provenienti da altre strutture della Banca, devono attenersi alle seguenti indicazioni per l'avvio dell'attività come internal auditor:

- primi 6 mesi: esclusa partecipazione agli interventi di audit e alla stesura dei rapporti;
- da 6 mesi a 1 anno: preferibile l'esclusione di cui sopra; ove ciò non sia possibile per motivi organizzativi della Funzione, la responsabilità delle eventuali evidenze rappresentate nel rapporto è esclusivamente in capo al Responsabile dell'audit team.

› *Competenza e Diligenza Professionale*.
Gli internal auditors devono possedere le conoscenze, la capacità e le competenze necessarie all'adempimento delle proprie responsabilità individuali; per svolgere l'attività di audit con diligenza professionale gli internal auditors devono tenere in considerazione i seguenti fattori:

- ampiezza del lavoro necessaria per raggiungere gli obiettivi dell'incarico;
- complessità e significatività dell'attività oggetto di assurance;
- adeguatezza ed efficacia dei processi di risk management, governance e controllo;
- probabilità della presenza di significativi errori, frodi o non conformità;
- costi/benefici dell'assurance.

Gli internal auditors devono migliorare le proprie conoscenze, capacità e competenze attraverso un aggiornamento professionale continuo.

Gli internal auditor del Gruppo BMPS sono incoraggiati a dimostrare la propria competenza conseguendo le opportune certificazioni e qualifiche professionali come quella di "*Certified Internal Auditor*" (cd. CIA) ed altre certificazioni rilasciate dal "*The Institute of Internal Auditors*" nonché da altri organismi professionali riconosciuti.

Il Responsabile della Funzione di IA deve dotarsi di opportuna assistenza e consulenza se gli internal auditors non possiedono le conoscenze, le capacità e altre competenze necessarie all'esercizio delle proprie responsabilità. In tali casi la Funzione di IA può ricorrere a soggetti terzi (consulenti esterni) per un supporto finalizzato allo svolgimento di taluni incarichi o per l'acquisizione di servizi/supporti per lo svolgimento delle attività.

› *Programma di Assicurazione e Miglioramento della Qualità*.
La Funzione di IA deve sviluppare e sostenere un programma di assurance e miglioramento della qualità che copra tutti gli aspetti dell'attività di audit. Tale programma permette una valutazione di conformità agli Standard, consente di verificare il rispetto del Codice Deontologico da parte degli auditors e si deve avvalere di valutazioni sia interne che esterne.

3.1 Valutazioni delle prestazioni della Funzione di IA

Il programma di assurance e miglioramento della qualità deve includere valutazioni sia interne che esterne.

La valutazione interna della Funzione di IA prevede:

- valutazioni conclusive sulla qualità delle prestazioni in atto e sulle azioni di follow up intraprese, per assicurare che vengano attuati gli opportuni miglioramenti. Il monitoraggio continuo della prestazione dell'attività di internal auditing ne costituisce parte integrante ed è incorporato nelle procedure utilizzate per gestire l'attività stessa;

- una autovalutazione, annuale, che viene effettuata avviando un programma interno di assicurazione e miglioramento della qualità, cosiddetto "CqAR" - *Corporate Quality Assurance Review*[4], al fine di supportare:

    - la valutazione dell'efficienza ed efficacia delle attività che istituzionalmente sono attribuite ad ogni Funzione di IA del Gruppo;
    - la valutazione della conformità dell'attività di audit agli Standard Internazionali;
    - il percorso di adeguamento all'utilizzo delle metodologie e strumenti esistenti a livello di Gruppo.

In sintesi, la Funzione di IA è chiamata ad esprimersi su specifiche variabili connesse alla complessiva attività di audit svolta, avendo riguardo sia ad "aspetti generali" (organizzazione e struttura della Funzione ed impostazione metodologica), che alla gestione dell'attività medesima (pianificazione, esecuzione, reporting, monitoraggio).

La Funzione di IA della Capogruppo si avvale di un set articolato di indicatori di performance (KPI) per valutare il livello di efficacia ed efficienza delle attività svolte in coerenza con il proprio mandato e con le aspettative degli Organi Aziendali (Cfr. Allegato n.7).

Le valutazioni esterne - cosiddette *External Quality Assessment* - la cui periodicità dovrebbe essere almeno quinquennale[5], possono essere effettuate secondo due approcci:

- completa valutazione effettuata da un soggetto esterno qualificato ed indipendente o da un team di valutatori con gli stessi requisiti;
- un programma di autovalutazione interna, cui fa seguito l'intervento di un valutatore esterno qualificato ed indipendente o di un gruppo di valutatori con gli stessi requisiti che effettuino una convalida dell'autovalutazione e del report predisposto dall'internal audit (cd. Autovalutazione con Convalida Indipendente).

Ai fini della validità dell'approccio scelto risulta necessaria la completa ottemperanza alle dettagliate e specifiche prescrizioni degli Standard.

Le valutazioni esterne coprono tutte le attività di audit e di consulenza e non devono limitarsi alla valutazione del programma di assurance e miglioramento della qualità. L'ambito di intervento dovrebbe includere il benchmarking, ossia l'identificazione e l'esposizione delle best pratices che possono aiutare l'internal audit a divenire maggiormente efficace ed efficiente.

Si sottolinea, infine, che qualora la Funzione di IA ottenga esito positivo dal Programma di assurance e miglioramento della qualità, è previsto che possa indicare all'interno della documentazione/reportistica prodotta che le attività sono svolte in conformità degli "Standard Internazionali per la Pratica Professionale dell'Internal Auditing"[6].

[4] Il CqAR è alimentato anche dai "Prospetti di autovalutazione della Funzione di IA" allegati alla Relazione annuale delle Funzioni di IA locali del Gruppo, ove presenti.

[5] Standard AIIA n.1312: "Il responsabile internal auditing deve discutere con il board:
- la necessità di valutazioni esterne più frequenti;
- le qualifiche e l'indipendenza del valutatore o del team di valutatori esterni, inclusa l'esistenza di qualsiasi possibile situazione di conflitto di interessi.

[6] Cfr Standard AIIA n.1321.

3.2 Il Modello di Internal Audit del Gruppo.

Il Gruppo BMPS ha optato per un modello di internal audit "decentrato", in cui le entità del Gruppo più complesse sono dotate di una Funzione di IA indipendente e svincolata da rapporti gerarchici con i responsabili delle strutture operative.

Nella Capogruppo le responsabilità in materia di internal auditing sono assegnate alla Direzione Revisione Interna, che risulta articolata in strutture di primo e secondo livello (Area, Servizi, Staff di Direzione), in funzione delle specializzazioni richieste dalle singole attività.

Le strutture di IA delle Società del Gruppo rispondono funzionalmente alla Funzione di IA della Capogruppo. Esse sono responsabili, per le società di appartenenza, dello svolgimento dell'attività di internal auditing nel rispetto delle linee guida definite dalla Capogruppo. In particolare, le medesime Funzioni di Audit:

- assumono, per gli aspetti ad esse applicabili nell'ambito delle proprie realtà aziendali, le medesime responsabilità della Funzione di IA della Capogruppo, svolgendo le conseguenti attività;
- si coordinano con le strutture di revisione interna della Capogruppo da cui ricevono gli opportuni indirizzi riguardo alle procedure di controllo interno ed agli obiettivi dell'attività di revisione, per la pianificazione e la definizione degli interventi e per l'inoltro di flussi informativi sull'attività effettuata;
- trasmettono alle strutture di revisione interna della Capogruppo i rapporti di audit caratterizzati da particolari elementi di attenzione/criticità, anche per quanto attiene alle materie di conformità;
- monitorano nel continuo la risoluzione delle criticità rilevate nel corso dell'attività di audit;
- richiedono, per il tramite degli organi di riporto, l'intervento della Funzione di IA della Capogruppo ove ravvisino criticità su aspetti particolarmente complessi che richiedano conoscenze specialistiche non disponibili internamente o la necessità di interventi strutturati su questioni attinenti la funzionalità di aree, segmenti operativi, processi o progetti aziendali;
- supportano gli auditors della Capogruppo in eventuali attività in *joint*.

Le suddette responsabilità sono riconducibili anche alle Funzioni di IA delle Filiali Estere.

Nel caso in cui le dimensioni e la rischiosità dell'azienda non giustifichino l'utilizzo a tempo pieno di risorse dedicate ai controlli mediante la costituzione di un'apposita struttura, deve essere comunque garantita un'adeguata attività di verifica da parte dei vertici dell'esecutivo, in modo da assicurare un sufficiente monitoraggio dell'operatività. Per le aziende prive di proprie strutture operative, partecipate da altre Società del Gruppo, l'attività di verifica sarà assicurata da queste ultime, previa specifica delibera del CdA dell'azienda interessata.

Nell'ambito delle strategie di Gruppo, l'attività può essere accentrata - in tutto o in parte - presso una delle Società del Gruppo stesso, sentito il parere della Funzione di IA di Capogruppo. Tale impostazione deve essere preventivamente comunicata alle competenti Autorità di Vigilanza (per le banche – ad oggi - alla Banca d'Italia).

L'accentramento va realizzato nel rispetto delle leggi e delle norme regolamentari vigenti, provvedendo alla redazione di specifici accordi (*Service Level Agreement*), i cui contenuti sono di regola recepiti nella normativa interna di ciascuna entità. Vengono in proposito definiti:

- gli obiettivi, la metodologia e la frequenza dei servizi forniti;
- le modalità e la frequenza dei rapporti agli Organi di riporto sulle verifiche effettuate;
- i collegamenti con i compiti svolti dal Collegio Sindacale e dai revisori contabili;
- la possibilità di rivedere le condizioni del servizio al verificarsi di modifiche di un certo rilievo nell'operatività e nell'organizzazione delle società interessate;

- la possibilità di effettuare controlli al verificarsi di esigenze improvvise;
- gli obblighi di riservatezza e la proprietà esclusiva dei fornitori di servizi sui risultati conseguiti;
- l'accesso completo e immediato delle Autorità di Vigilanza alla documentazione prodotta dai soggetti terzi;
- le modalità di gestione e risoluzione delle eventuali controversie.

E' altresì perseguibile all'interno del Gruppo il riferimento di tutta o parte dell'attività di internal auditing a soggetti prestatori esterni[7] dotati di requisiti idonei in termini di professionalità e indipendenza (esternalizzazione). In proposito occorre rispettare le regole vigenti e le norme definite in materia dalle Autorità di Vigilanza[8].

Le Banche del Gruppo che intendono esternalizzare, in tutto o in parte, la Funzione di IA nominano uno specifico referente che coordina le diverse attività, condividendo, tra l'altro, informazioni ed eventualmente metodologie e strumenti, al fine di assicurare un'adeguata copertura e minimizzare le possibili duplicazioni, in coerenza anche con il principio secondo cui l'affidamento di servizi di internal auditing a soggetti esterni non esime l'organizzazione dalla responsabilità dell'efficacia dell'attività svolta.

Ove si ricorra a soggetti prestatori esterni è, altresì, necessario verificare nel continuo che gli stessi eseguano le attività affidate nel rispetto dei principi sanciti dagli Standard internazionali della professione di internal audit e, in particolare, secondo i principi di obiettività ed indipendenza.

E', inoltre, necessario definire un apposito accordo di esternalizzazione che chiarisca:

- obiettivi, metodologia e frequenza dei controlli;
- modalità e frequenza della reportistica dovuta al referente per l'attività esternalizzata e agli Organi aziendali sulle verifiche effettuate;
- obblighi di riservatezza delle informazioni acquisite nell'esercizio della funzione;
- collegamenti con le attività svolte dall'Organo con funzione di controllo (Collegio Sindacale);
- possibilità di richiedere specifiche attività di controllo al verificarsi di esigenze improvvise;
- proprietà esclusiva della Banca dei risultati dei controlli.

4. STANDARD DI PRESTAZIONE

"L'Internal Auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione; essa 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".[9]

Il responsabile della Funzione di IA deve gestire in modo efficace l'attività al fine di assicurare che essa porti valore aggiunto all'organizzazione; l'attività di audit è gestita efficacemente quando:

- i risultati ottenuti permettono di raggiungere le finalità indicate nel Mandato di internal audit;
- l'attività svolta è conforme alla definizione di Internal Auditing e agli Standard;
- coloro che svolgono le attività di audit dimostrano di conoscere e applicare il Codice Deontologico della Funzione di IA ed i relativi Standard di Audit.

[7] Il ricorso a soggetti prestatori esterni è generalmente previsto qualora gli internal auditor non possiedano le conoscenze, le capacità o altre competenze necessarie per lo svolgimento di tutto o di parte di un incarico (Cfr. Standard AIIA n. 1210).
[8] Cfr. 285 del 17 dicembre 2013 di Banca d'Italia e successivi aggiornamenti.
[9] Cfr: Standard AIIA – Definizione di Internal Auditing

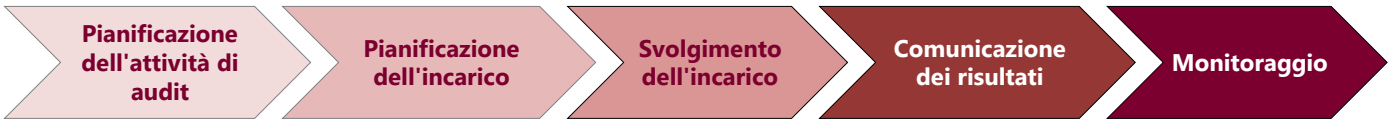
L'attività di internal audit deve valutare e fornire appropriati suggerimenti volti a migliorare il processo di governance nel raggiungimento dei seguenti obiettivi:

- favorire lo sviluppo di appropriati valori e principi etici;
- garantire l'efficace gestione dell'organizzazione e la responsabilità incondizionata;
- comunicare informazioni su rischi e sistemi di controllo alle relative funzioni aziendali
- coordinare le attività e il processo di scambio di informazioni tra gli internal auditor, gli Organi aziendali, i revisori esterni e le altre funzioni aziendali di controllo.

L'attività di internal audit deve inoltre valutare l'adeguatezza e l'efficacia sia del processo di valutazione dell'esposizione al rischio che dei controlli introdotti relativamente a:

- affidabilità e integrità delle informazioni contabili, finanziarie e operative;
- efficacia ed efficienza delle operazioni e delle procedure;
- salvaguardia del patrimonio aziendale;
- conformità a leggi/regolamenti interni ed esterni;
- raggiungimento degli obiettivi strategici aziendali.

Ciascuna attività di audit ripercorre, in sintesi, le seguenti fasi (cd. *Processo di Audit*):



In linea generale dette fasi si presentano per tutte le attività di audit, seppure con caratteristiche e differenziazioni formali a seconda delle diverse fattispecie. Nel presente documento si ripercorre ciascuna fase in relazione principalmente alla tipologia di attività riconducibile agli interventi di revisione, poiché, data la maggiore articolazione, consentono di evidenziare in modo più completo le peculiarità di ciascuna fase.

4.1 Pianificazione delle attività di Audit

La pianificazione delle attività costituisce il momento in cui il Responsabile della Funzione di IA, sulla base della valutazione dei rischi e al fine di determinarne la priorità in linea con gli obiettivi aziendali, individua almeno una volta all'anno:

- gli obiettivi da raggiungere;
- le modalità di realizzazione;
- la relativa tempistica e frequenza;
- le conseguenti risorse da impiegare.

La base della pianificazione è costituita da un'accurata attività *di risk control assessment*, che tiene conto dei processi aziendali di gestione del rischio e dei limiti di accettabilità dello stesso stabiliti dagli Organi Aziendali per le diverse attività, rappresentate coerentemente con la struttura del Modello dei Processi di Gruppo.

I principali fattori che incidono nella definizione della pianificazione fanno riferimento ai risultati forniti dagli strumenti di monitoraggio dei rischi tipici dell'attività finanziaria, agli esiti delle precedenti visite, alle rilevazioni scaturite dalle attività di *self-assessment*, nonché alle risultanze del monitoraggio a distanza. Tali fattori consentono di orientare le attività di controllo verso i processi aziendali a maggiore grado di rischiosità residua (al netto dell'effetto del sistema dei controlli).

La pianificazione, deve essere fondata - ove possibile – anche su indicatori di rischio quantitativi e deve essere coerente con il Risk Appetite Framework (RAF) del Gruppo ed integrarsi con i piani delle altre Funzioni Aziendali di Controllo[10], al fine di evitare sovrapposizioni e di sfruttare possibili sinergie nella copertura delle aree ritenute esposte a rischio.

La pianificazione deve, inoltre, tenere conto delle specifiche disposizioni ed istanze delle Autorità di Vigilanza, nonché delle richieste presentate dagli Organi aziendali[11].

Il piano delle attività di internal audit deve essere sottoposto al CdA per il relativo esame ed approvazione.

La Funzione di IA predispone una pianificazione di audit pluriennale ed annuale.

4.1.1 Pianificazione pluriennale

La pianificazione pluriennale è definita in relazione al perseguimento dei seguenti obiettivi:

- miglioramento dell'efficacia e dell'efficienza delle azioni di controllo e, in ottica generale, del sistema dei controlli interni;
- razionalizzazione delle attività di controllo in funzione dell'entità/significatività dei rischi da presidiare, anche in relazione al raggiungimento degli obiettivi strategici individuati;
- individuazione di punti di debolezza nei processi aziendali;
- riduzione degli impatti economici derivanti dal manifestarsi dei rischi (perdite operative, sanzioni da parte degli Organi di Vigilanza, inefficienze, etc.);
- presidio sui progetti strategici e sulle nuove iniziative di business;
- validazione di modelli interni finalizzati anche all'ottimizzazione degli assorbimenti patrimoniali.

Gli obiettivi di audit vengono pianificati sulla base di un sistema basato in via prioritaria sul fattore RISCHIO, tenendo comunque in considerazione il grado di copertura temporale dei processi e delle strutture aziendali nel ciclo di audit quadriennale. In definitiva, le aree di copertura nell'orizzonte pluriennale si individuano sulla base del livello di rischio associato all'oggetto di audit, ma con la consapevolezza di dover comunque assicurare, nel tempo, una presenza costante della Funzione di IA.

Il completamento delle attività deve intendersi come la verifica di tutte le componenti rilevanti nell'ambito dei propri processi aziendali, nell'orizzonte temporale definito.

Tabella n. 1 - ciclo di audit

	STRUTTURE/PROCESSI CENTRALI/SOCIETA'	STRUTTURE RETE	STRUTTURE/PROCESSI CON RISCHI RILEVANTI	FILIALI ESTERE
Funzione IA CAPOGRUPPO	Max 4 anni	Max 4 anni	Max 3 anni	Annuale (**)
Funzione IA SOCIETÀ GRUPPO	Max 3 anni	Max 5 anni	Max 3 anni	-

(**) Dipendente comunque dalle richieste e/o impegni assunti con AA.VV. e Regulators locali.

[10] La Capogruppo ha istituito cinque Funzioni Aziendali di Controllo permanenti ed indipendenti, di seguito riportate:
- Funzione di Conformità alle Norme (Compliance);
- Funzione di Controllo dei Rischi (Risk Management);
- Funzione di Convalida Interna;
- Funzione Antiriciclaggio;
- Funzione Revisione Interna (Internal Audit).

[11] Cfr. Standard AIIA n.2010- A1: "Le indicazioni del senior management e del board devono essere tenute in debita considerazione nella formulazione del piano.

E' necessario, altresì, considerare le cosiddette **revisioni obbligatorie**, ossia quelle in adempimento a specifiche prescrizioni delle Autorità di Vigilanza, da svolgere secondo le periodicità fissate dalle disposizioni normative di riferimento.

A prescindere da quanto sopra, sia a livello di Capogruppo che di Società del Gruppo, le situazioni più critiche sono pianificate con l'obiettivo di essere analizzate con tempestività, indipendentemente dalle tempistiche massime definite. L'azione immediata della Funzione di IA rientra nelle responsabilità attribuite al Responsabile della Funzione stessa.

4.1.2 Pianificazione annuale

Relativamente ad un orizzonte temporale pari ad un esercizio ed in coerenza con quanto previsto nella pianificazione pluriennale, l'Audit Plan annuale contiene l'indicazione di:

- **attività di audit**: tipologia di attività da svolgere (es. interventi di revisione, analisi a distanza, attività di consulenza, etc. – cfr. tabella n.3);

- **unità auditabili**: riconducibili all'oggetto dell'attività di audit (possono riguardare un'unità organizzativa, un processo, ma anche un progetto, una procedura applicativa, una piattaforma hardware, etc.);

- **assorbimenti**: stima del tempo occorrente (in gg/uomo) per lo svolgimento delle medesime attività. Il calcolo degli assorbimenti deve considerare le giornate lavorative disponibili per risorsa (ottenibili con l'esclusione delle varie tipologie di assenze previste dal contratto aziendale), riservando particolare attenzione all'ottimizzazione dell'impiego delle risorse necessarie a far fronte ad eventuali indagini impreviste (interventi straordinari). Il Responsabile della Funzione di IA deve assicurare che le risorse disponibili siano adeguate, sufficienti ed efficacemente impiegate per l'esecuzione del piano approvato;

- **priorità**: nella determinazione del grado di priorità è opportuno considerare tutte le informazioni necessarie, quali:

    - prescrizioni di legge e/o di vigilanza;
    - richieste provenienti dagli Organi Aziendali, dalle Autorità di Vigilanza e dalla Funzione di IA della Capogruppo (solo per le Funzioni IA locali);
    - tempo intercorso dall'ultima attività di audit condotta sulla medesima unità e relativi risultati;
    - follow-up su interventi condotti che hanno evidenziato un significativo rischio residuo, oltre a situazioni di inadeguatezza della struttura dei controlli con mancata rimozione delle criticità;
    - andamento dello scenario economico ed evoluzione degli aggregati di natura patrimoniale, finanziaria, economica e gestionale;
    - andamento degli indicatori di anomalia utilizzati per il controllo a distanza e risultanze di Self Assessment e Scenario Operational Risk;
    - introduzione di nuovi processi/procedure dai quali potrebbero emergere nuovi rischi.

Ad eccezione delle verifiche dettate da richieste straordinarie, il processo di identificazione degli interventi da inserire nel piano e delle relative priorità è sintetizzato all'interno dell'Audit Plan, in base alla rilevanza delle aree di indagine ed al livello di rischio ad esse associato.

Tabella n. 2 - Timing Audit Plan

	INVIO ALLA FUNZIONE IA DI CAPOGRUPPO	CONDIVISIONE CON FUNZIONE IA DI CAPOGRUPPO	INVIO/APPROVAZIONE ORGANI APICALI
FUNZIONE IA CAPOGRUPPO			Entro 31 gennaio
FUNZIONE IA SOCIETÀ DEL GRUPPO	Entro 30.11	Entro 31.12	Entro 31 gennaio

Si evidenzia, infine, che durante l'esercizio la Funzione di IA di Capogruppo effettua un'attività di pianificazione operativa - con periodicità trimestrale - nel corso della quale vengono identificate, sulla base di criteri predefiniti (livello di copertura, Indicatore Sintetico di Rischio, etc.), le singole strutture periferiche di rete da auditare, in coerenza con le previsioni dell'Audit Plan annuale.

Tale pianificazione di breve periodo può, inoltre, essere condizionata dalla necessità di attivare specifici interventi conseguentemente all'osservazione, negli accertamenti a distanza, di particolari "fenomeni".

Il Responsabile della Funzione di IA deve comunicare periodicamente agli Organi aziendali lo stato di avanzamento del piano.

Il Responsabile della Funzione di IA deve, se necessario, modificare la pianificazione in risposta ai cambiamenti dell'organizzazione aziendale, dei rischi, della propensione agli stessi, dei programmi, dei sistemi adottati e dei controlli.

Il complesso delle attività di audit pianificate è riconducibile alle seguenti tipologie:

Tabella n. 3 - Tipologie attività di audit

INTERVENTI DI REVISIONE (IN LOCO O A DISTANZA)	Attività di audit da cui scaturisce anche uno specifico rapporto di audit che viene inviato agli Organi Aziendali, in base ai meccanismi relazionali definiti[12] ed alla "corporate governance" adottata.
ANALISI A DISTANZA	Attività di audit svolte senza accesso fisico alle entità owner dei processi oggetto di accertamento. Sono basate su analisi cartolari e/o su informazioni acquisite dagli archivi aziendali e possono riguardare: società, strutture organizzative, processi, fenomeni finanziari e/o bancari, un "business" oppure un suo segmento, uno o più rischi aziendali, etc.
ATTIVITÀ DI CONSULENZA	Attività di supporto e consulenza ad altre Strutture, tramite formulazione di parere non vincolante, oltreché attività connesse alla definizione/validazione di normativa interna primaria (es. Policy/Direttive di Gruppo, Regolamenti primari della Banca).
ATTIVITÀ DIREZIONALE E RELAZIONALE	Attività legate alla pianificazione e rendicontazione delle attività svolte, al coordinamento interno, alle relazioni e seguimenti per Organi di Vigilanza oltreché per i Vertici Aziendali. Si ricomprende anche l'assistenza alla Società di Revisione, per gli ambiti di competenza.
FORMAZIONE	Programmazione e partecipazione ai programmi di crescita professionale e certificazione del personale, oltre alle attività di segreteria riconducibili alla gestione della formazione stessa.
ATTIVITÀ DIVERSE[13]	Il complesso delle attività di gestione ed amministrazione del personale (ivi compresi gli aspetti logistici) e gestione della corrispondenza.

4.2 Pianificazione dell'incarico

In relazione a ciascuna tipologia di attività di audit vengono avviati nel corso dell'anno specifici incarichi, definendone: obiettivi, natura ed estensione dell'attività di verifica, tempistica e relative risorse assegnate. Per ciascun incarico gli internal auditor devono effettuare una valutazione preliminare dei rischi afferenti l'attività oggetto di audit.

Per le attività inserite nel piano di audit, gli obiettivi degli incarichi conseguono e coincidono con quelli inizialmente identificati durante il processo di *risk control assessment*. Per le attività non pianificate, gli obiettivi sono stabiliti prima dell'inizio dell'incarico e sono definiti per individuare specifiche problematiche che hanno determinato la necessità dell'incarico.

La pianificazione del singolo incarico assume particolare rilevanza qualora sia riconducibile ad interventi di revisione, come viene di seguito specificato.

[12] Cfr. Allegato n.3 – Criteri di distribuzione dei rapporti di audit e autonomie di firma e visto.
[13] In tale comparto può essere compresa l'attività di gestione dei reclami ove rientrante nelle responsabilità della Funzione di IA.

4.2.1 Pianificazione intervento di revisione

La pianificazione del singolo intervento di revisione presuppone le seguenti attività:

- attività preliminari e predisposizione del compito;
- definizione del team di audit;
- scelta dell'approccio campionario;
- comunicazione apertura visita.

Attività preliminari e predisposizione del compito

Le attività preliminari consentono di effettuare una pre-analisi delle strutture, dei processi e dei relativi sottoprocessi oggetto di verifica, valutandone gli aspetti operativi nonché l'andamento dei principali fenomeni con impatto sulle strutture/processi medesimi; esse permettono di definire le principali attività che verranno svolte e predisporre i necessari supporti/strumenti (es. preparazione dei programmi di lavoro, estrazione dati relativi agli indicatori a distanza, analisi delle informazioni qualitative disponibili, etc.).

Il complesso delle informazioni acquisite nell'ambito delle attività preliminari, permette di definire e circoscrivere meglio il **compito** dell'intervento, che deve essere formalizzato in uno specifico documento e contiene i seguenti dati:

- obiettivi e limiti dell'intervento (mission, eventuale attività escluse). Gli obiettivi dell'incarico devono essere definiti secondo un approccio "top – down" basato sul rischio, coerente con la necessità di copertura, *in primis,* dei rischi più significativi;
- tipologia di intervento (in loco/a distanza; ordinario/straordinario, generale/settoriale, etc.);
- periodo di svolgimento dell'attività ed identificazione dell'assorbimento previsto in giorni uomo;
- data prevista per la finalizzazione del rapporto (nel caso di interventi di revisione)
- risorse necessarie in relazione alla tipologia di intervento ed individuazione del Responsabile del Team: è necessario che il piano del singolo intervento evidenzi il livello di adeguatezza delle risorse disponibili, in termini quantitativi e di competenza, al fine di assicurare che l'intervento stesso sia correttamente realizzato (con personale operativo e di supervisione) in relazione agli obiettivi, alla complessità ed alle competenze specifiche necessarie;
- mappatura a livello macro delle attività di processo, nonché dei rischi e delle esigenze di controllo;
- formalizzazione delle singole attività di analisi/verifica da svolgere (con indicazione della data di inizio e fine prevista dell'attività, processi e relativi sottoprocessi[14] oggetto di analisi/verifica, finestra temporale dei test e risorse referenti);

Il compito deve essere:

- predisposto su template standard per la Funzione di IA della Capogruppo
- sottoscritto e vistato, a seconda della tipologia di attività di audit, in coerenza con le previsioni dei criteri di autonomia di firma e visto della Funzione di IA (cfr. allegato n. 3b)
- archiviato nel *General Folder*;
- illustrato e, ove possibile, condiviso, ove ritenuto opportuno, con il Management della struttura auditata;
- rivisto, ove occorrano eventi che richiedono variazioni significative;
- sufficientemente dettagliato in modo da consentire la misurazione dello stato di avanzamento dell'intervento.

[14] Definiti secondo la tassonomia dell'albero dei Processi di Gruppo - ARIS

Il team di Audit

Per ogni intervento di revisione, in base alla natura ed alla complessità dello stesso, devono essere individuate le risorse che compongono il team di audit, insieme al relativo responsabile con esperienza e competenze sufficienti a supervisionare l'intervento ed assicurare il conseguimento degli obiettivi.

Nel determinare le risorse necessarie e sufficienti si devono prendere in considerazione i seguenti elementi:

- livello di esperienza;
- conoscenze, skills e altre competenze;
- disponibilità di risorse esterne , qualora siano necessarie competenze e conoscenze aggiuntive;
- fabbisogni formativi interni, poiché attraverso l'assegnazione a ciascun incarico è possibile soddisfare le esigenze formative di sviluppo professionale
- necessità di composizione di team misti con risorse appartenenti a differenzi Servizi/Settori della Funzione (*joint audit*)

Il responsabile del team, quale supervisore dell'incarico assegnato[15], ha il compito di:

- tenere i rapporti diretti con la struttura oggetto di verifica;
- supervisionare l'andamento dell'intervento, verificando il corretto svolgimento delle attività e richiedendo variazioni del *working plan* ove necessario;
- monitorare il rispetto delle tempistiche previste in relazione ai piani operativi inizialmente definiti, motivando un eventuale straordinario prolungamento delle attività;
- garantire che gli obiettivi vengano raggiunti, che siano assicurate qualità dell'azione di audit e crescita professionale delle risorse impiegate;
- identificare, analizzare e formalizzare gli eventuali usi inefficienti e/o inefficaci delle risorse;
- assicurare il contenimento dei costi;
- verificare che l'organizzazione dei fogli di lavoro sia conforme agli Standard;
- formalizzare la comunicazione dei risultati.

Scelta dell'approccio campionario

Le verifiche di internal audit sono per natura svolte, nella maggioranza dei casi, su base campionaria. A tal proposito, in assenza di Standard utilizzabili in tutte le circostanze, di seguito si delineano i principi che, nell'ambito del Gruppo, costituiscono un riferimento per la scelta del metodo e dei relativi parametri e che, ove possibile, possono essere alla base delle selezioni effettuate dagli strumenti informatici disponibili.

Il processo di campionamento è adottato di norma unitamente ad altre procedure di internal auditing (analisi di processo, informazioni quali-quantitative, altre evidenze, etc.), valutandone congiuntamente i risultati al fine di consentire la formulazione di un giudizio professionale sull'oggetto della verifica; il medesimo processo deve essere definito e tarato in funzione del grado di affidamento che l'auditor pone sulle altre eventuali procedure di internal auditing che intende utilizzare.

La selezione di una parte di elementi di una popolazione può essere effettuata sulla base di varie modalità e tecniche; la scelta dell'approccio campionario da parte dell'audit team di norma dipende dai seguenti fattori:

- conoscenza dell'oggetto dell'analisi;
- dimensione della popolazione;
- significatività della popolazione;
- grado di affidamento sul controllo interno;
- accuratezza richiesta;
- errore atteso;

[15] Cfr. Standard n. 2340 "Supervisione dell'incarico".

- altre caratteristiche della popolazione.

Basandosi sui fattori sopra indicati, l'audit team dovrà stabilire l'approccio campionario da utilizzare per le verifiche, tenendo conto che il campione selezionato dovrà essere quanto più rappresentativo possibile della popolazione indagata quanto maggiore è la dimensione di questa e quanto più alto è il rischio da presidiare.

La scelta dell'approccio campionario deve essere documentata e giustificata nelle carte di lavoro (*Working Folder*).

Comunicazione apertura visita

Nei casi di interventi di revisione è prevista la predisposizione e l'inoltro della **lettera di comunicazione di apertura della visita**[16] - salvo i casi in cui ragioni di opportunità ne suggeriscano l'iniziale riservatezza - da indirizzare (almeno 2 giorni lavorativi prima dell'arrivo in loco) al/ai Responsabile/i della/e unità da auditare.

Tale lettera deve contenere l'indicazione delle attività previste nel compito allo scopo di dare conto del perimetro e degli obiettivi dell'intervento ed è sottoscritta in coerenza con le autonomie di firma della Funzione (Cfr. Allegato n. 3b) e viene indirizzata:

- agli Organi di Vertice della Società, nel caso di accertamenti sulle Società controllate;
- al Responsabile di Direzione/Area/Struttura, per interventi sulle strutture di Direzione Generale/Rete periferica.

Per gli interventi di audit sulle strutture periferiche di Rete, la comunicazione di apertura visita può essere consegnata a mano al Responsabile dell'unità auditata.

La lettera medesima, predisposta su template standard per la Funzione di IA della Capogruppo, è archiviata nelle carte di lavoro (*Working Folder*).

4.3 Svolgimento dell'incarico

Lo svolgimento dell'incarico, ovvero l'esecuzione dell'attività di audit, avviene secondo modalità diverse, principalmente in dipendenza della tipologia stessa dell'attività (cfr. tabella n.3).

In linea generale "*Gli internal auditor devono raccogliere, analizzare, valutare e documentare informazioni sufficienti al raggiungimento degli obiettivi dell'incarico*".[17] In tale principio è connaturata la possibilità dell'internal audit di richiedere alle varie funzioni aziendali, nei tempi previsti, tutto ciò che è utile all'esecuzione dell'incarico (*need to know*).

Le informazioni da raccogliere[18] devono essere:

- *sufficienti*: ovvero concrete, adeguate e convincenti, così che in base ad esse qualsiasi persona prudente e informata giungerebbe alle stesse conclusioni dell'auditor;
- *affidabili*: quando sono fondate e sono le migliori ottenibili attraverso l'uso di tecniche adeguate all'incarico;
- *pertinenti*: ossia coerenti con gli obiettivi dell'incarico;
- *utili*: ovvero possano essere d'aiuto nel raggiungimento delle finalità aziendali.

[16] Andranno predisposte tante lettere di apertura quante sono le Strutture auditate.
[17] Standard AIIA – n. 2300 "Svolgimento dell'incarico".
[18] Standard AIIA – n. 2310 "Raccolta delle informazioni".

Per tutte le attività di audit svolte occorre garantire la necessaria **tracciabilità**, intendendo con tale termine la possibilità di ricostruire il lavoro svolto al fine di giustificare e supportare le conclusioni raggiunte (cfr. Par. 4.3.2 Organizzazione ed archiviazione dei fogli di lavoro).

Si ripercorrono di seguito i principali passaggi che caratterizzano lo svolgimento dell'incarico di audit riconducibile all'intervento di revisione.

4.3.1 Svolgimento dell'intervento di revisione

Le principali fasi che caratterizzano l'esecuzione dell'intervento di revisione possono essere così sintetizzate:

- Open meeting/entry meeting
- Esecuzione attività;
- Exit meeting.

Open meeting

Il primo atto dell'intervento di audit è l'incontro con il Responsabile della/e unità owner del processo, al fine di chiarire gli obiettivi dell'intervento, acquisire informazioni sulle attività svolte e sulle eventuali problematiche esistenti oltre ad una prima valutazione (secondo le metodologie di valutazione previste) dei rischi e dei relativi presidi nelle singole aree operative dell'unità stessa. A tal fine andranno considerate, ove disponibili, anche le risultanze degli eventuali assessment qualitativi (es. *Operational Risk)* e delle analisi/monitoraggi a distanza.

L'intervista iniziale consente di:

- aprire un confronto costruttivo con il Responsabile dell'unità auditata in materia di rischi/controlli;
- instaurare un clima di reciproca fiducia;
- focalizzare l'attenzione sugli aspetti maggiormente problematici;
- verificare la reale percezione/sensibilità del Responsabile ai rischi;
- acquisire informazioni circa eventuali modifiche operativo-procedurali e organizzative che hanno interessato l'unità auditata;
- esporre il piano di lavoro e le fasi di processo su cui si intende effettuare le verifiche;
- richiedere il primo set documentale.

Le evidenze dell'intervista con il Responsabile dell'unità auditata sono sintetizzate in apposito documento denominato "**verbale di open meeting**", standardizzato per la Funzione di IA della Capogruppo, da allegare ai fogli di lavoro (*General Folder*). Vi sono indicati oltre ai partecipanti all'incontro, gli argomenti trattati, evidenziando eventuali aspetti rilevanti da tenere in considerazione durante l'effettuazione della verifica.

Nel caso in cui il perimetro dell'intervento coinvolga più strutture/società e, conseguentemente vengano condotte più interviste, occorre predisporre un verbale di open meeting per ciascuna di esse.

Relativamente agli interventi sui processi centrali, maggiormente strutturati, per i quali l'open meeting può sovente rappresentare esclusivamente il formale annuncio dell'inizio dell'attività di verifica e non effettivamente un confronto tra auditors e funzione auditata, è preferibile effettuare successivamente un incontro di cd. **entry meeting** al fine di perfezionare eventuali lacune in sede di open. Tale incontro deve essere formalizzato in specifico verbale con le stesse modalità e caratteristiche del verbale di open meeting.

Esecuzione attività

Nell'ambito dell'esecuzione degli interventi di audit devono essere raccolte, analizzate, valutate e documentate tutte le informazioni sufficienti al raggiungimento degli obiettivi previsti; in sintesi sono percorribili le seguenti sottofasi:

- selezione/individuazione delle attività/dati oggetto di verifica con utilizzo di procedure di supporto o delle tecniche di selezione campionaria;
- applicazione delle tecniche di audit previste (test di funzionalità e conformità) e dei criteri predefiniti al fine di accertare e valutare l'esistenza, l'adeguatezza e la conformità dei processi e del sistema dei controlli interni esistente a presidio dei relativi rischi connessi all'attività oggetto di verifica, sulla base dei riferimenti contenuti nei supporti operativi adottati a livello di Gruppo (programmi di lavoro, check list di controllo, etc.), opportunamente integrati in funzione delle specifiche necessità;
- raccolta delle evidenze di sintesi e valutazione degli esiti con analisi di coerenza dei risultati stessi, in termini assoluti, e con le valutazioni iniziali;
- determinazione dell'opportunità, secondo il giudizio professionale dell'auditor, di estendere ulteriormente le verifiche al fine di giungere a valutazioni complessive documentabili e tali da supportare la solidità dei giudizi espressi.
- analisi delle principali cause (RCA – *Rout Couse Analysis*)

Durante lo svolgimento delle attività è opportuno predisporre un verbale (su template standard per la Funzione di IA della Capogruppo) per ciascun colloquio formale tenuto con il Responsabile e/o le risorse della struttura audita; tale documento deve essere - ove possibile - condiviso anche dalla struttura auditata stessa ed archiviato nelle carte di lavoro (*Working Folder)*.

Exit meeting

Le attività si concludono con il colloquio di chiusura con la funzione auditata ("**exit meeting**"), nel corso del quale devono essere rilasciate evidenze formalizzate in apposito verbale, concernenti le criticità rilevate nel corso dell'intervento nonché eventuali considerazioni che dovessero emergere da parte della struttura auditata.

Il verbale di exit meeting - redatto su template standard per la Funzione di IA di Capogruppo - da inserire nei fogli di lavoro (*General Folder*), è siglato dai partecipanti all'incontro e presenta in allegato bozza della tavola dei GAP che deve essere condivisa con la/le funzione/i auditata/e. **Devono necessariamente trovare condivisione anche le tempistiche previste per la risoluzione delle principali criticità evidenziate**. Ove, per motivi di natura logistico-organizzativa, non sia possibile acquisire la sigla sul verbale di exit meeting e sulla bozza della tavola dei gap, si procederà ad invio formale (anche via e-mail) del verbale e della tavola per condivisione con la struttura responsabile delle azioni correttive.

Per gli interventi su strutture/processi centrali, è prevista la partecipazione all'incontro di exit meeting anche del Responsabile dell'Area da cui dipende gerarchicamente la struttura auditata. Qualora le criticità rilevate abbiano impatti rilevanti e/o si prevede un giudizio negativo, è richiesta la partecipazione anche del Responsabile di Direzione e degli Organi di vertice nel caso di Società controllate.

Il documento viene tempestivamente inviato al Responsabile della struttura/processo oggetto di verifica, ovvero, ove possibile, consegnato al termine dell'incontro stesso. L'exit meeting deve essere effettuato nel rispetto della seguente tempistica:

Tabella n. 4 - Timing exit meeting

TEMPISTICA	MODALITÀ	PARTECIPANTI
Entro 15 gg. dal termine delle verifiche	Generalmente in loco (*anche videoconferenza)*	- Responsabile struttura/owner del processo auditato - Organi di Vertice della Società (problematiche rilevanti)

Nel caso in cui l'intervento interessi più Strutture/Società viene di regola condotto un incontro di exit meeting con ciascuna unità auditata, tenendo comunque in considerazione la natura/rilevanza dei GAP individuati ed i livelli di responsabilità circa l'esecuzione delle azioni correttive.

Casi particolari riconducibili agli interventi di revisione

Nel caso in cui durante un intervento di revisione si accertino potenziali comportamenti irregolari dei dipendenti[19], è necessario procedere con l'attivazione di un particolare tipologia di intervento di revisione: il cd. **Servizio Speciale** o **Indagine Interna**, che mira alla puntuale ricostruzione della dinamica degli eventi, alla valutazione delle responsabilità del/i dipendente/i con stima del danno economico, nonché alla valutazione dell'efficacia e degli eventuali fattori di debolezza del sistema dei controlli. L'intervento si conclude con la predisposizione di un apposito rapporto – standardizzato - che dovrà essere finalizzato ed inviato agli Organi aziendali[20]auspicabilmente con le attività di mitigazione già indirizzate, condivise con le funzioni aziendali competenti e, se possibile, avviate.

Al termine dell'indagine, inoltre, in presenza di rapporti di revisione con proposta di provvedimento disciplinare, sarà cura della Funzione di IA predisporre la specifica scheda riassuntiva dell'evento da trasmettere assieme al resto della documentazione disponibile alla Commissione Affari Disciplinari, ove istituita.

4.3.2 Organizzazione ed Archiviazione dei Fogli di Lavoro

Le carte di lavoro rappresentano una raccolta organica della documentazione inerente l'attività di controllo espletata, indispensabili per supportare le conclusioni che ne sono state tratte, le eventuali eccezioni rilevate ed i suggerimenti conseguentemente proposti. Esse devono consentire ad un soggetto diverso da chi ha effettuato gli accertamenti di audit, oltreché ad eventuali enti di controllo esterni, di ricostruire le attività svolte pervenendo agli stessi risultati. A tal fine la documentazione raccolta deve essere chiara, sufficientemente sintetica e deve tracciare tutte le fasi che hanno caratterizzato l'attività di audit.

Un'adeguata raccolta delle carte di lavoro deve poter consentire di:

- riscontrare la conformità delle attività svolte ai riferimenti interni ed agli strumenti adottati;
- verificare la correttezza e pertinenza della documentazione allegata e relativa allo specifico controllo;
- giustificare le conclusioni raggiunte e l'effettività dei controlli di audit eseguiti;
- facilitare il riesame dell'intervento da parte di terze parti;
- supportare il riesame del lavoro svolto in caso di frode, richieste di rimborso assicurativo, esame in giudizio, etc.;
- favorire il trasferimento di conoscenze e metodologie tra le risorse della funzione.

Le carte di lavoro, siglate dall'auditor che le ha curate e sottoscritte dal Responsabile del Team che le ha supervisionate, sono archiviate in appositi dossier, preferibilmente in forma elettronica, anche mediante acquisizione/scansione elettronica dei documenti.

Con particolare riferimento agli interventi di revisione, la documentazione da raccogliere comprende:

- la pianificazione dell'intervento di audit;
- i criteri di campionamento eventualmente adottati ed il campione oggetto di approfondimento;
- i fogli di lavoro che documentano il lavoro svolto;
- le evidenze raccolte, se ritenute rilevanti ed atte a supportare le valutazioni effettuate e il giudizio finale;
- le conformità/non conformità e le anomalie rilevate, le conclusioni e le raccomandazioni;
- il rapporto prodotto a conclusione dell'intervento;
- eventuali riesami da parte dei responsabili;

[19] A tal fine rilevano sia i comportamenti operativi che risultano non conformi alla normativa di riferimento (di legge /o interna) sia le condotte eventualmente scorrette e/o poste in essere in violazione dei doveri che derivano dal rapporto di lavoro.

[20] Cfr. Allegato n. 3a per i criteri di distribuzione del rapporto.

- tutta la corrispondenza rilevante con la struttura auditata e/o con le Funzioni coinvolte a vario titolo nel corso della revisione.

La citata documentazione è di regola raccolta nei seguenti dossier:

› **General Folder** (o Fascicolo Revisione): è il dossier che riguarda la/e struttura/e owner dei processi auditati, contenente tutta la documentazione amministrativa della verifica e nello specifico il set minimale da archiviare deve comprendere:

- *compito dell'intervento*
- *verbale di open/entry meeting*
- *verbale di exit meeting*
- *rapporto di audit*
- *lettera di osservazioni*
- *lettera informativa dei risultati di audit a strutture "contributor"*

› **Working Folder** (o Fascicolo Archivio): è il dossier contenente i fogli di lavoro rappresentativi di tutte le verifiche effettuate e della documentazione acquisita durante lo svolgimento delle stesse.

Tale dossier deve essere opportunamente articolato in più fascicoli - evitandone comunque la proliferazione al fine di non far venire meno l'efficienza nella tracciabilità - contenenti i riferimenti a ciascun gap rilevato. Per ciascuna criticità devono, altresì, essere facilmente rintracciabili i test a suffragio delle conclusioni raggiunte.

Al fine di agevolare sia la gestione delle carte di lavoro che la condivisione stessa delle evidenze raggiunte e l'immediato collegamento ai gap, è preferibile predisporre, per ciascun specifico argomento/verifica, un **executive summary working folder** che sintetizzi quanto contenuto nei relativi fogli di lavoro.

Deve contenere, inoltre, tutta la corrispondenza rilevante con la struttura audita e con altre funzioni coinvolte a vario titolo nell'intervento. Nei casi di verifiche di ampio perimetro e/o su strutture complesse, è opportuna la creazione di più fascicoli, opportunamente suddivisi (es. per tematica, processo, ufficio/unità organizzativa, etc.).

Tabella n. 5 – Tempistiche di conservazione dei documenti[21]

	INTERVENTI ORDINARI (SENZA CRITICITÀ RILEVANTI)	INTERVENTI ORDINARI (CON CRITICITÀ RILEVANTI)	SERVIZI SPECIALI
GENERAL FOLDER	almeno 10 anni		
WORKING FOLDER	almeno 3 anni	almeno 6 anni	almeno 10 anni[22]

Le modalità di organizzazione ed archiviazione dei fogli di lavoro, definite in un supporto scritto a disposizione degli auditors – standardizzato per la Funzione di IA della Capogruppo - non devono in alcun modo favorire la proliferazione di documentazione cartacea (fotocopie, liste, elaborati, etc.), da limitare solo ai casi di stretta necessità e privilegiando comunque l'archiviazione elettronica.

[21] Nel caso di documentazione afferente l'analisi e la valutazione dell'operatività sospetta in materia di antiriciclaggio, l'archiviazione delle carte di lavoro deve essere effettuata in coerenza con le prescrizioni del D0892 "Gestione adempimenti operativi in materia di antiriciclaggio e contrasto al terrorismo: Operazioni Sospette.

[22] In considerazione della diversa gravità delle infrazioni trattate è comunque preferibile ottenere un parere legale sui tempi di conservazione della documentazione a supporto delle indagini sui dipendenti.

Il Responsabile dell'Audit Team ha il compito di verificare che l'organizzazione dei fogli di lavoro e di quanto archiviato elettronicamente sia conforme agli Standard.

La Funzione di IA è tenuta ad adottare appositi meccanismi di controllo sull'accesso alla documentazione prodotta ed archiviata a seguito dei singoli interventi, in considerazione della sensibilità e riservatezza delle informazioni in essa contenuti. Particolare attenzione, dovrà essere riservata ai casi di eventuali rilasci della documentazione a parti terze esterne alla Società.

4.4 Comunicazione dei risultati

La comunicazione dei risultati include le conclusioni raggiunte al termine delle complessive attività di audit svolte, insieme alle raccomandazioni ed ai relativi piani d'azione; tuttavia i relativi contenuti sono strettamente connessi alla tipologia di comunicazione (rapporto di audit, lettera all'unità auditata, etc.) oltreché ai destinatari medesimi.[23]

In linea generale la comunicazione dei risultati di audit deve essere: *accurata, obiettiva, costruttiva, completa* e *tempestiva* e deve essere indirizzata a tutti coloro che possono, nell'ambito delle proprie competenze, contribuire alla risoluzione delle criticità.

La comunicazione è efficace se chiara, concisa ed essenziale, evitando dettagli superflui e ridondanze; deve essere inoltre fedele ai fatti rilevati e scevra da pregiudizi

Nel caso degli interventi di revisione, la comunicazione dei risultati deve contenere anche il giudizio attribuito, i rilievi e le conclusioni raggiunte dagli internal auditors.

La descrizione dei rilievi, intesi come affermazioni su stati di fatto, deve essere strutturata in modo tale da prevenire malintesi e supportare le conclusioni fornite, prevedendo la comunicazione solo dei rilievi necessari a giustificare le affermazioni dell'auditor.

4.4.1 Il rapporto di audit

Gli interventi di revisione si concludono con la predisposizione di un report di audit, redatto con il contributo di tutti gli auditors che hanno partecipato all'attività, ciascuno per la parte di propria competenza, e rivisto e sottoscritto dal Responsabile del Team nonché dal Responsabile della funzione di riferimento, sulla base di un work-flow predefinito di supervisione ed approvazione[24].

Si precisa, inoltre, che per qualsiasi tipologia di audit il contenuto minimale del report ordinario è il seguente:

1. ***Obiettivi;***
2. ***Executive summary;***
3. ***Attività di verifica svolte;***
4. ***Gap e azioni correttive.***

Il report, ove necessario, può essere corredato da allegati tecnici atti a fornire le informazioni di dettaglio ritenute rilevanti.

[23] In caso di invio a terze parti esterne all'organizzazione , la comunicazione dei risultati deve espressamente prevedere limiti di utilizzo e distribuzione. Cfr. Standard AIIA n. 2410.A3

[24] Cfr: Allegato n. 3b: "Autonomie di firma e visto".

Con riferimento alle attività svolte dalla Funzione di IA della Capogruppo, è necessario che il rapporto sia predisposto con "Format Standard Rapporto Processi Centrali/Società" e sulla base delle relative "Linee Guida"(Cfr. Allegati n. 4 e 5) per gli accertamenti su processi centrali e società. Relativamente agli interventi sulle strutture della Rete commerciale il rapporto è compilato e prodotto dall'applicativo a supporto dell'attività, nel rispetto degli Standard.

La metodologia adottata dal Gruppo prevede che le valutazioni espresse siano riferite a livello di processo e sottoprocesso in coerenza con i modelli dei processi/rischi adottati[25]; ne consegue che è necessario fare riferimento agli stessi nell'individuazione degli ambiti da declinare e valutare nel rapporto, mantenendo per quanto possibile la massima aderenza a tali modelli. Il presidio dei rischi su ciascun ambito viene valutato sulla base di una scala di "grade" definita su più livelli. Tramite loro aggregazione si perviene all'espressione di un "grade/giudizio complessivo", rappresentativo della valutazione di sintesi sull'intera attività di audit effettuata.

La scala utilizzata per l'attribuzione del giudizio complessivo è composta da un numero pari di giudizi attribuibili, con stessa numerosità di giudizi negativi e giudizi positivi.

Come già in precedenza accennato, la compilazione dei report di audit è supportata da Linee Guida comprendenti scala dei giudizi e relative regole di assegnazione, che prevedono meccanismi di correlazione tra numerosità e rilevanza dei gap e giudizio di sintesi attribuito all'ambito revisionato.

Il rapporto di audit deve essere finalizzato al massimo entro 30 giorni dalla data di exit meeting.

Le modalità di inoltro dei report ai Vertici Aziendali sono basate su regole interne – condivise con l'Organo di Controllo - assoggettate a costante manutenzione (cd. Criteri di distribuzione dei rapporti di audit - All. n. 3a al presente documento). In ogni caso, le risultanze di sintesi delle verifiche sono portate all'attenzione degli Organi Aziendali in occasione della presentazione della Relazione annuale sull'attività svolta e sulla valutazione del sistema dei controlli interni di Gruppo.

In via ordinaria, all'unità auditata e alla rispettiva Struttura di riporto gerarchico/funzionale non viene inviato il rapporto di audit ma soltanto la lettera di osservazioni (cfr. paragrafo successivo). Possono, tuttavia, sussistere specifiche eccezioni in ragione di meccanismi relazionali instaurati con altre funzioni (es. Funzione di Compliance), in base ai quali determinati rapporti possono essere trasmessi integralmente per favorire l'organizzazione di attività idonee alla mitigazione dei rischi individuati.

In situazioni particolari, quali quelle da cui emerga l'evidenza di una possibile commissione di reato o di impatti significativi sulla struttura auditata, la Funzione di IA deve, senza indugio, fornire una pronta informativa ai propri Organi amministrativi e di controllo.

4.4.2 Comunicazione all'unità auditata

Al termine delle attività di verifica alla/e Strutture/unità oggetto auditata/e deve essere inviata una **lettera di osservazioni** contenente:

- la descrizione dei principali gap;
- il giudizio attribuito all'intervento;
- la richiesta di risposta, entro 30 giorni dalla ricezione della comunicazione, con indicazione delle azioni correttive che intende intraprendere e delle date di mitigazione dei gap rilevati;
- la tabella dei gap.

[25] Tassonomia albero dei processi di Gruppo (ARIS)

Tale lettera, da archiviare nel General Folder, è firmata in coerenza con quanto previsto dal documento che disciplina le autonomia di firma e di visto per la Funzione.[26]

In caso di interventi di revisione di durata significativa, in presenza di un ampio numero di strutture/unità auditate, è possibile - anche prima della conclusione della reportistica finale di audit - procedere alla trasmissione di una lettera di osservazioni contenente tavola dei gap (anche in bozza), affinché le unità già oggetto di accertamento possano prontamente attivarsi per la rimozione delle anomalie emerse.

4.4.3 Lettera informativa dei risultati di audit a strutture "contributor"

Unitamente alla "Lettera di osservazioni" per la/e Funzione/i auditata/e può essere prevista una lettera informativa indirizzata ad altre funzioni il cui contributo è necessario per la risoluzione delle criticità rilevate.

Con tale lettera si comunica alla funzione destinataria che sarà interessata dalla struttura oggetto dell'intervento di audit e owner della risoluzione dei gap rilevati, per contribuire a conseguire le necessarie azioni correttive.

Sono previste due tipologie di lettere informative, in relazione a:

- Ambiti di natura organizzativa/codifica normativa dei processi
  da inviare alla Funzione Organizzazione qualora nel corso della revisione emergano specifici gap attinenti il profilo normativo, affinché l'Organizzazione possa supportare la Funzione auditata nella risoluzione;

- Ambiti di natura IT (sviluppo, implementazione, evoluzione, etc.)
  da inviare alla Funzione di gestione della Demand IT, qualora nel corso della revisione emergano specifici gap attinenti profili di natura ICT, affinché la Funzione auditata venga supportata nella risoluzione attraverso il relativo processo di demand.

Il documento deve essere redatto su template standard della Funzione di IA per la Capogruppo, sottoscritto in coerenza con i criteri definiti nell'allegato n. 3b del presente documento ed archiviato nel *General Folder*.

4.5 Follow up

Il follow up, ovvero il monitoraggio delle azioni correttive[27], consiste nel verificare che i soggetti identificati come responsabili, a fronte delle criticità emerse durante le verifiche, abbiano intrapreso adeguate azioni correttive, ovvero, abbiano fatto propri i suggerimenti e le azioni indicate dalla Funzione di IA. Altrimenti il Responsabile della Funzione di IA deve avere assurance che il management e/o gli Organi aziendali abbiano accettato e si siano fatti carico del rischio di non intraprendere nessuna azione di mitigazione. Deve essere specificamente individuata la struttura responsabile della risoluzione delle criticità medesime, che di norma coincide con le Funzioni owner del/i processo/i auditato/i.

La struttura che ha effettuato l'attività di audit è responsabile del monitoraggio periodico delle azioni correttive segnalate e condivise con l'unità operativa oggetto di accertamenti e provvede ad aggiornare il follow up, anche a seguito della ricezione delle repliche da parte delle unità auditate.

[26] Cfr. Allegato n. 3b: "Autonomie di firma e visto".

[27] Cfr. Standard AIIA n.2500 – A1:"Il responsabile IA deve impostare un processo di follow up per monitorare e assicurare che le azione correttive siano state effettivamente attuate dal management oppure che il senior management abbia accettato il rischio di non intraprendere alcuna azione".

Relativamente alla gestione dei gap rilevati su processi/strutture centrali/società il Gruppo si è dotato di un approccio metodologico integrato con le altre Funzioni Aziendali di Controllo[28] (FAC) al fine della:

- adozione di un'unica base dati per la gestione delle attività di controllo svolte dalle FAC;
- individuazione delle esigenze di budget per la risoluzione dei gap;
- tracciabilità delle anomalie identificate e dei documenti di supporto;
- reportistica standardizzata verso gli Organi Aziendali;
- maggiore responsabilizzazione delle strutture coinvolte nel processo di gestione dei gap;
- automazione delle attività di monitoraggio degli interventi pianificate e gestione delle scadenze.

In relazione alla entità e tipologia delle criticità emerse, l'attività di monitoraggio potrà concretizzarsi anche mediante:

- una successiva verifica in loco, eventualmente finalizzata ad accertare la sistemazione delle criticità segnalate; tale soluzione è di norma da adottare nell'arco dei dodici mesi successivi, qualora l'intervento si sia concluso con una valutazione complessiva negativa (non favorevole o in prevalenza non favorevole) sul presidio dei rischi;
- richiesta o acquisizione degli elementi necessari ad accertarne la rimozione.

4.6 Intervento di revisione: overview fasi ed output

Nell'ottica di fornire un quadro completo delle attività da svolgere in relazione a ciascuna fase del processo di audit (pianificazione incarico, svolgimento incarico, comunicazione risultati e follow up), si riepilogano nella tabella seguente le indicazioni già fornite nei paragrafi precedenti con riferimento ad attività, output e relativi contenuti.

Tabella n. 6 – Overview fasi ed output

	FASI	ATTIVITÀ	OUTPUT	IN EVIDENZA
PIANIFICAZIONE	**ATTIVITÀ PRELIMINARI/ SCELTA APPROCCIO CAMPIONARIO**	Definizione di: - obiettivi/limiti attività di audit; - verifiche da effettuare; - audit team - durata e inizio visita	N.A.	Le informazioni preliminari acquisite, attraverso analisi di dati quantitativi, consentono di circoscrivere meglio le variabili utili alla definizione del compito.
	PREDISPOSIZIONE DEL COMPITO	Formalizzazione nel previsto documento delle informazioni emerse dalle attività preliminari	**COMPITO**	La predisposizione è a cura del Resp. Audit Team. Da rivedere al verificarsi di eventi interni/esterni che richiedano variazioni significative all'intervento.
	COMUNICAZIONE APERTURA VISITA	Predisposizione lettera di apertura da indirizzare al/ai Responsabile/i della/e unità audita/e.	**LETTERA DI APERTURA PER UNITÀ AUDITATA/E**	La lettera va indirizzata almeno 2 gg. lavorativi prima dell'arrivo in loco. Per intervento su strutture Rete può essere consegnata a mano
ESECUZIONE	**OPEN/ENTRY MEETING**	Apertura formale intervento di revisione con il Responsabile dell'unità auditata.	**VERBALE OPEN/ENTRY MEETING**	Per interventi che coinvolgono più unità si predispone un verbale di per ciascuna di esse.
	ESECUZIONE ATTIVITÀ	Svolgimento/esecuzione delle attività da parte degli Auditors	N.A.	N.A.

[28] Cfr. Circ. 285 del 17 dicembre 2013 di Banca d'Italia e successivi aggiornamenti.

	EXIT MEETING	Conclusione attività e condivisione gap con l'unità auditata.	**TABELLA GAP/ VERBALE EXIT MEETING**	Da condividere con il Responsabile dell'U.O: gap, azioni correttive e tempistiche di risoluzione (sottoscrizione tabella Gap).
COMUNICAZIONE RISULTATI	**REPORT DI AUDIT**	Massima espressione/ formalizzazione dell'attività di audit	**RAPPORTO**	Indice del report: 1.Obiettivi 2. Executive summary 3. Attività di verifica svolte 4. Gap e azioni correttive (tabella di sintesi)
	COMUNICAZIONE ALL'UO AUDITATA	Lettera chiusura con evidenza dei risultati dell'intervento (gap e azioni correttive).	**LETTERA DI OSSERVAZIONI**	La lettera contiene, tra l'altro: - richiesta di replica entri i tempi previsti; - gap; - grade dell'intervento
	COMUNICAZIONE A STRUTTURE CONTRIBUTOR	Lettera che "ingaggia" altre strutture per la risoluzione dei gap	**LETTERA INFORMATIVA A STRUTTURE CONTRIBUTOR**	A fronte di gap per la cui risoluzione debbano essere coinvolte altre strutture (es. IT, Organizzazione).
FOLLOW UP	**FOLLOW UP**	Monitoraggio circa la rimozione dei gap	*Le relative evidenze di sintesi sono formalizzate nella principale reportistica istituzionale prodotta (Relazione annuale SCI; Quarterly report)*	

4.7 Interventi di revisione "obbligatori"

La Funzione di IA è volta, da un lato a controllare, quale funzione di controllo di III livello, il regolare andamento dell'operatività e l'evoluzione dei rischi e, dall'altro, a valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità della struttura organizzativa e delle altre componenti del Sistema dei Controlli Interni, portando all'attenzione degli Organi aziendali i possibili miglioramenti al processo di gestione dei rischi nonché agli strumenti di misurazione e di controllo degli stessi.

In tale ambito e coerentemente con il proprio piano di audit, la Funzione di IA deve sottoporre a verifica le funzioni aziendali di controllo dei rischi e di conformità alle norme; deve, inoltre, verificare, la regolarità delle attività aziendali esternalizzate e l'evoluzione dei relativi rischi. La frequenza di tali ispezioni è coerente con l'attività svolta e la propensione al rischio.

Le disposizioni di vigilanza e la normativa interna/esterna prescrivono, altresì, che la Funzione di IA di effettui, con cadenza definita, attività di audit cd "obbligatorie" (*Mandatory Audit*), ossia previste da disposizioni regolamentari, la cui specificità, in primo luogo per l'obbligo di legge da cui derivano, ne giustifica una trattazione separata (Cfr. Allegato n. 8 "Mandatory Audit").

4.8 Focus su altre tipologie di attività di audit

Come già accennato, le altre tipologie di attività di audit (cfr. Tabella n.3), seguono in linea generale lo stesso iter di realizzazione previsto per gli interventi di revisione, sebbene con caratteristiche, formalizzazioni ed output diversi.

In altri termini, per ciascuna attività di audit occorre: pianificare il singolo incarico, eseguire l'attività, evidenziare/comunicare i risultati e monitorare il seguimento circa la rimozione delle eventuali criticità riscontrate. Particolare attenzione va sempre riservata alla formalizzazione ed archiviazione delle carte di lavoro, ovvero di tutta la documentazione concernente l'attività svolta (es. relazioni, note, o qualsiasi altro documento, che evidenzi i risultati raggiunti e le considerazione finali).

Di seguito si evidenziano le principali caratteristiche (modalità operative, obiettivi, reportistica) che contraddistinguono l'attività di analisi a distanza e l'attività di consulenza della Funzione di IA.

4.8.1 Attività di analisi a distanza

L'analisi a distanza è configurabile come attività di audit svolta senza accesso fisico diretto alle entità owner dei processi oggetto di accertamento. E' pertanto basata su analisi cartolari e/o su informazioni acquisite dagli archivi aziendali e possono riguardare: una società, una struttura organizzativa periferica o centrale, un processo oppure una sua componente, un fenomeno finanziario e/o bancario, un "business" oppure un suo segmento, uno o più rischi aziendali, etc.

Tale tipologia di attività di audit è finalizzata a valutare sia il livello di presidio dei rischi dell'ambito auditato che l'idoneità del relativo sistema dei controlli interni. La medesima consente, inoltre, di:

- indirizzare le attività di pianificazione operativa degli interventi di revisione;
- individuare eventuali ambiti meritevoli di ulteriori approfondimenti;
- segnalare situazioni anomale (compresi casi outlier) o potenziali tali, sia alle strutture owner dei processi che alle strutture che svolgono attività di audit "on site" per l'esperimento di idonee attività.

L'analisi a distanza si traduce nella redazione di uno specifico report, che contempla elementi di natura quantitativa (analisi parametriche, di specifiche variabili, trend spazio-temporali etc.) e qualitativa (morali, fattori causali, criticità osservabili a distanza) utili per la realizzazione degli obiettivi sopra enunciati. In linea generale, oltre al report di analisi a distanza, devono essere resi disponibili i dati al massimo livello di dettaglio a disposizione (es. per ndc, unità commerciale, etc.).

Qualora nel corso dell'attività di analisi a distanza si rilevino particolari elementi di attenzione/criticità la Funzione di IA, ove ne ravvisi la necessità sulla base della valutazione del rischio, può avviare un intervento di revisione.

4.8.2 Attività di Consulenza

L'attività di consulenza della Funzione di IA è sostanzialmente riconducibile ad un'attività di supporto ed assistenza, per lo più espletata attraverso suggerimenti e raccomandazioni che hanno l'obiettivo di apportare valore aggiunto e migliorare i processi di governance, gestione dei rischi e controllo.

La Funzione di IA finalizza l'attività di consulenza nell'individuazione di soluzioni idonee a garantire il superamento dei punti di debolezza del sistema dei controlli interni, in conformità con le linee guida definite e le policy di Gruppo. Tale contributo si manifesta sia nel momento in cui emergono disallineamenti tra il sistema stesso e il modello di business e di governo adottato dall'azienda, sia nella fase di impianto/revisione di processi e procedure, con l'obiettivo di garantire coerenza e linearità all'intero impianto dei controlli a presidio dei rischi.

Fondamentale è il coordinamento con le altre Funzioni Aziendali di Controllo, non solo nell'ottica di efficientamento del sistema di controlli interni, ma anche con l'obiettivo di individuare sinergie nella realizzazione dei controlli, eventuali ambiti non presidiati e limitare gli impatti sulle strutture auditate.

La consulenza dell'audit si esplica altresì nella valutazione sulla rischiosità connessa a nuove iniziative, riconducibile al giudizio indipendente e critico circa la profittabilità in termini di rischio/rendimento sull'ingresso in nuovi business o attività, sullo sviluppo di nuovi prodotti, altro.

In questi termini, l'attività di consulenza della Funzione di IA si focalizza sulla necessità che l'iniziativa risulti coerente con le strategie di business e di governo e che risponda al generale obiettivo di contenimento dei rischi aziendali.

È opportuno che l'attività venga realizzata durante la fase di studio/ingegnerizzazione e dovrebbe concludersi antecedentemente alla valutazione finale da parte della Capogruppo/Società del Gruppo con una relazione di audit o altro documento che evidenzi la fattibilità dell'iniziativa e proponga gli eventuali correttivi (rilascio del parere non vincolante).

In particolare, la valutazione sulla rischiosità delle nuove iniziative viene effettuata dalla Funzione di IA sulla base dei seguenti elementi d'analisi:

- impatti sul sistema dei controlli interni
- rischiosità dell'iniziativa;
- valutazione risk assessment;
- conformità interna alle politiche e/o strategie di Gruppo;
- adeguatezza dei profili organizzativi e degli strumenti di supporto;
- conformità alla normativa esterna
- impatti ai fini del D.Lgs. 231/01;

Tali valutazioni consentono alla Funzione di esprimere un giudizio finale sintetico in ordine alla rischiosità, complessità e importanza della nuova iniziativa, che considera tra l'altro i pareri delle Società/strutture coinvolte.

Le attività di consulenza possono concludersi anche senza la predisposizione di un report; è comunque necessario consentire la tracciabilità documentale dell'attività svolta e delle eventuali indicazioni fornite (es. relazioni, verbali, lettere, etc.).

L'attività di affiancamento/validazione svolta con riferimento alla definizione di nuove procedure, norme primarie (Regolamento sull'Organizzazione della Banca MPS - cd. Regolamento n.1 - solo per le parti di competenza - e Policy/Direttive ad alto impatto sullo SCI) e presidi di controllo, nonché al rilascio di nuovi sistemi informativi, rappresenta un'attività mediante la quale la Funzione IA esercita il proprio ruolo di "consulente", rilasciando pareri consultivi che non minano l'indipendenza della stessa. Tra le attività di affiancamento rientrano inoltre tutte le attività di supporto agli Organi ed alle altre funzioni di controllo, nonché alla società di revisione del bilancio ovvero le consulenze a favore delle altre strutture di Direzione Generale. In tali attività possono rientrare, altresì, la gestione, il coordinamento ovvero il monitoraggio di progetti sui quali alla Funzione è richiesto un coinvolgimento diretto.

5. REPORTING PERIODICO ISTITUZIONALE

Il reporting rappresenta la sintesi formale dell'attività di controllo e deve essere sviluppato in relazione alle esigenze informative degli Organi destinatari[29] ed alle previsioni normative di riferimento (es. relazioni obbligatorie), contemperando requisiti di essenzialità e completezza. La frequenza ed il contenuto delle relative comunicazioni sono definiti di concerto agli Organi Aziendali e variano a seconda della rilevanza delle informazioni stesse e dell'urgenza dei relativi provvedimenti eventualmente connessi.

[29] Cfr.Standard AIIA n. 2060 - Informativa periodica al Senior Management e al Board - "*Il Responsabile Internal Auditing deve informare periodicamente il senior management ed il board in merito a finalità, poteri e responsabilità dell'attività di internal auditing, nonché comunicare lo stato di avanzamento del piano. Tale comunicazione deve comprendere inoltre i rischi significativi, inclusi quelli di frode, i problemi di controllo, i problemi di governance ed ogni altra informazione necessaria o richiesta dal senior management e dal board*".

Nell'ambito della complessiva informativa predisposta dalla Funzione di IA, oltre ai già citati report ordinari, predisposti a margine di una specifica attività di revisione (rapporto di audit) rilevano i cosiddetti report consuntivi/periodici, concernenti l'attività di audit svolta in un arco temporale definito.

Nella tabella seguente si evidenziano i principali report istituzionali prodotti dalla Funzione di IA della Capogruppo, avendo riguardo all'oggetto, alla periodicità ed ai relativi destinatari[30].

TABELLA N.7 PRINCIPALI FLUSSI ISTITUZIONALI INTERNAL AUDIT

OGGETTO	SINTESI CONTENUTO	PERIODICITÀ	ORGANI DESTINATARI	AAVV DESTINATARIE
AUDIT PLAN	Pianificazione attività	Annuale	Collegio Sindacale Comitato Rischi CdA	JST (BCE)
RELAZIONE SULL'ATTIVITÀ SVOLTA E VALUTAZIONE DEL SISTEMA DEI CONTROLLI (RELAZIONE SCI)	Espressione del giudizio complessivo sul Sistema dei Controlli di Gruppo e sulle singole componenti (ambiente di controllo, controllo rischi, assetto controlli, informazione e comunicazione, follow up)	Annuale	Collegio Sindacale Comitato Rischi CdA	Banca d'Italia JST (BCE)
REPORT TRIMESTRALE INTERNAL AUDIT	Rendicontazione trimestrale su attività svolta	Trimestrale	Collegio Sindacale Comitato Rischi Presidente CdA AD	JST (BCE)
RELAZIONE SUGLI ACCERTAMENTI EFFETTUATI PRESSO LE SOCIETA' CONTROLLATE DEL GRUPPO MPS (ALLEGATO RELAZIONE SCI)	Focus su verifiche in loco condotte presso le Società controllate	Annuale	Collegio Sindacale Comitato Rischi CdA	Banca d'Italia JST (BCE)
RELAZIONE SUI CONTROLLI SVOLTI SULLE FUNZIONI OPERATIVE ESTERNALIZZATE (ALLEGATO RELAZIONE SCI)	Controlli svolti sulle funzioni operative importanti o di controllo esternalizzate	Annuale	Collegio Sindacale Comitato Rischi CdA	Banca d'Italia JST (BCE)
SISTEMA DEI CONTROLLI SUI METODI AVANZATI (AIRB, AMA - ALLEGATO RELAZIONE SCI)	Attività svolte in materia di revisione dei sistemi di gestione e misurazione dei rischi nonché del processo di convalida interna dei rischi di credito ed operativi (AIRB, AMA).	Annuale	Collegio Sindacale Comitato Rischi CdA	Banca d'Italia JST (BCE)
RELAZIONE SUI SERVIZI DI INVESTIMENTO CON LA CLIENTELA (ALLEGATO RELAZIONE SCI)	Attività di audit in materia di prestazione dei servizi di investimento ed accessori e di distribuzione dei prodotti finanziari	Annuale	Collegio Sindacale Comitato Rischi CdA	Banca d'Italia JST (BCE) Consob

[30] "Per le banche facenti parte del Gruppo BMPS (MPS Leasing & Factoring, Widiba e MPS Capital Services) la Capogruppo coordina e trasmette a Banca d'Italia o BCE, la stessa documentazione richiesta alla medesima ad eccezione delle relazioni delle funzioni aziendali di controllo delle società controllate. In luogo di queste la Capogruppo invia annualmente la Relazione sugli accertamenti effettuati presso le società controllate." Cfr. Circ. 285 del 17 dicembre 2013 di Banca d'Italia e successivi aggiornamenti .

6. RELAZIONI CON ORGANI E FUNZIONI DI CONTROLLO

6.1 Rapporti con gli Organi Aziendali

La definizione di Internal Auditing prevede tra l'altro che la Funzione assista l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale e sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di governance. Il raggiungimento di detti obiettivi richiede necessariamente la presenza e la costanza di rapporti e relazioni della Funzione di IA con gli Organi di Vertice dell'Azienda, pur nel mantenimento della necessaria autonomia ed indipendenza connaturata nella specifica attività di audit.

Con particolare riferimento alla Funzione di IA della Capogruppo, la relativa autonomia e l'indipendenza sono assicurate da meccanismi relazionali e di raccordo con gli Organi di Vertice, tra cui:

- diretto riporto della Funzione al CdA;
- nomina/revoca del Responsabile da parte del CdA, sentito il Collegio Sindacale, su proposta del Comitato Rischi, avvalendosi del contributo del Comitato Nomine e Remunerazione; assetto retributivo del Responsabile deliberato da parte del CdA, sentito il Collegio Sindacale, su proposta del Comitato Nomine e Remunerazione che acquisisce il parere del Comitato Rischi
- determinazione dell'Audit Plan da parte del CdA su proposta della Funzione di IA e previo esame del Collegio Sindacale;
- possibile richiesta di attivazione di revisioni interne da parte del Collegio Sindacale, del Comitato Rischi , e ODV 231/2001 e dal Presidente del CdA.;
- rendicontazione periodica dell'attività agli Organi Aziendali (es. Quarterly Report) e almeno annualmente una relazione sull'attività svolta e sulla valutazione sul sistema dei controlli al Consiglio di Amministrazione;
- composizione e dimensionamento della struttura deliberato da parte del CdA., sulla base della relazione della Funzione, previo parere dell' Organo di Controllo;
- disposizione delle risorse (anche economiche eventualmente attivabili in autonomia con rendicontazione periodica al CdA e all'AD) e delle competenze necessarie per lo svolgimento del proprio compito;
- criteri di remunerazione delle risorse definiti dal CdA su proposta della Funzione HR sentito il parere del Comitato Rischi

I principi che consentono di garantire il corretto livello di autonomia ed indipendenza, a presidio di un'operatività della Funzione di IA non condizionata da alcunché, devono in ogni caso risultare coerenti con le norme di legge e con le disposizioni di vigilanza.

6.2 Coordinamento con le altre Funzioni di Controllo

"Il corretto funzionamento del sistema dei controlli interni si basa sulla proficua interazione nell'esercizio dei compiti (d'indirizzo, di attuazione, di verifica e di valutazione) fra gli Organi Aziendali, gli eventuali comitati costituiti all'interno di questi ultimi, i soggetti incaricati della revisione legale dei conti e le funzioni di controllo".[31]

Le nuove disposizioni di vigilanza prudenziale sul sistema dei controlli interni regolamentano la necessità di un approccio integrato al processo di gestione dei rischi ed al relativo sistema dei controlli tra le Funzioni Aziendali di Controllo.[32]

[31] Circ.285 del 17 dicembre 2013 di Banca d'Italia e successivi aggiornamenti .
[32] Cfr. Nota n.10

In ottemperanza al Codice di Autodisciplina delle Società quotate il Gruppo MPS ha istituito la figura dell'Amministratore Incaricato del Sistema di Controllo Interno al quale viene attribuita la responsabilità dell'istituzione e del mantenimento di un efficace sistema di controllo interno e di gestione dei rischi.

La Capogruppo ha, inoltre, istituito il Comitato per il Coordinamento delle Funzioni con Compiti di Controllo[33] che si configura come l'organismo aziendale cui spetta il compito di assolvere e dare concreta attuazione nel continuo al tema del coordinamento tra le funzioni di controllo.

In particolare tale coordinamento si esplicita, in particolare, attraverso i seguenti fattori:

- flussi informativi
- linguaggio comune nella gestione dei rischi
- coordinamento ai fini della pianificazione delle attività
- gestione integrata delle aree di miglioramento
- job rotation

Flussi informativi.

Le norme primarie del Gruppo in materia di controlli interni e gestione dei rischi[34] - in ottemperanza alle prescrizioni della normativa della Vigilanza - disciplinano le relazioni esistenti tra le Funzioni Aziendali di Controllo, individuando un complesso di flussi informativi strutturato tra le funzioni stesse e tra queste e gli Organi Aziendali al quale la Funzione di IA si attiene.

E' evidente come i flussi informativi rappresentino un fattore da cui nessuna struttura può prescindere per assicurare il corretto ed esaustivo espletamento delle proprie funzioni, in particolar modo all'interno del sistema dei controlli. Infatti, le relazioni che intercorrono tra gli attori coinvolti rappresentano uno dei fondamentali meccanismi atti a consentire il funzionamento dello SCI, la cui inadeguata attuazione può condurre a fenomeni di sovrapposizione, presidio incoerente, incompleto e ridondante. I flussi devono preservare gli appropriati livelli e posizionamenti organizzativi delle Funzioni interessate, oltreché l'assoluto mantenimento dei requisiti di indipendenza della Funzione di IA quale unica Funzione Aziendale di Controllo (di seguito FAC) di 3° livello.

Linguaggio comune nella gestione dei rischi.

La scelta di definizioni univoche per tutte le funzioni di controllo del Gruppo, inserite in policy o documenti di coordinamento non lascia margine ad interpretazioni dissonanti, per tematica e/o funzione aziendale, e indica la volontà di ricondurre ad unità la gestione del sistema dei controlli.

Tutte le funzioni aziendali di controllo, ciascuna per le proprie competenze, devono attenersi ad un'unica mappa dei processi aziendali [35] nonché ad una libreria comune dei rischi.[36]

Coordinamento ai fini della pianificazione dell' attività

Le funzioni aziendali di controllo si devono dotare di approcci volti a garantire la coerenza dei propri *Risk Assessment* mediante meccanismi di coordinamento quali:

- comitati o incontri periodici durante la fase di predisposizione dei piani annuali/pluriennali di attività;
- scambi formali dei rispettivi documenti di pianificazione e degli eventuali aggiornamenti.

Il coordinamento nel processo di pianificazione – antecedente alla presentazione dei rispettivi Plan agli Organi Aziendali – è finalizzato a:

[33] Cfr. D00751 - Regolamento n. 1 "Organizzazione della Banca MPS.
[34] D00793 "Policy di Gruppo in materia di Sistema dei Controlli Interni" e l'allegato D01915 "Flussi Informativi
[35] Albero dei Processi di Gruppo ARIS
[36] D01308 "Direttiva di Gruppo in materia di Processo Interno di Valutazione dell'Adeguatezza Patrimoniale.

- evitare eventuali aree di sovrapposizione;
- sviluppare sinergie ed individuare ambiti di verifica di comune interesse;
- garantire un'adeguata copertura dei fattori che compongono il sistema dei controlli interni, nell'ambito dei rispettivi piani di lavoro.

L'approccio integrato alla pianificazione deve comunque garantire l'autonomia di ciascuna FAC ed il rispetto degli specifici ambiti di competenza.

Gestione integrata delle aree di miglioramento.
Una maggiore integrazione nella rilevazione e gestione delle anomalie segnalate dalle funzioni di controllo, nonché nel successivo monitoraggio accresce l'efficacia nella rimozione delle criticità rilevate che espongono l'azienda ad un rischio.

Sotto il profilo applicativo il consolidamento delle anomalie rilevate da ciascuna FAC nell'esercizio delle proprie attività si realizza mediante l'adozione di un unico repository integrato per la tracciatura dei dettagli dei gap e delle relative azioni di rimedio (Cfr. Par.4.5).

In ogni caso la Funzione di IA è dotata di processi di escalation verso gli Organi Aziendali finalizzati a risolvere le criticità individuate entro tempi congrui rispetto alla significatività delle stesse.

Job rotation.
All'interno del Gruppo sono istituiti programmi di rotazione annuale delle risorse tra le FAC volti a favorire sia la crescita professionale che eventuali sinergie.

Possono, inoltre, essere promosse iniziative al fine di incrementare il *training on the job* quali affiancamenti temporanei tra le risorse appartenenti alle funzioni aziendali di controllo e progetti interfunzionali.

6.3 Rapporti con le Autorità di Vigilanza

La nuova regolamentazione bancaria ha apportato importanti cambiamenti per gli istituti di credito dal punto di vista di:

- *Soggetto regolamentare di riferimento*: la BCE ha assunto il ruolo di supervisore unico coordinando le *National Competent Authorities (NCA),* in collaborazione con EBA.
- *Approccio di supervisione*: in ottica "*forward looking*", più articolato e svolto da un Joint Supervisory Team (JST).
- *Contesto normativo:* numerose nuove normative fra cui lo SREP (*Supervisory Review and Evaluation Process*), nuovo approccio di valutazione del regolatore, e la BRRD (*Bank Recovery and Resolution Directive*) volta a migliorare la gestione delle crisi finanziarie sistemiche.

La Funzione di IA, quale funzione di controllo di 3°livello continua a rivestire il ruolo di interlocutore privilegiato nei confronti delle Autorità di Vigilanza di riferimento (BCE, Banca d'Italia, Consob, Isvap).

I rapporti con le medesime Autorità devono essere improntati a criteri di trasparenza, correttezza e piena collaborazione; tutte le segnalazioni, le informazioni, anche di natura valutativa, e i dati indirizzati a tali autorità devono essere trasmessi tempestivamente ed essere rispondenti al vero, completi ed accurati.

Rilevante risulta il ruolo della Funzione di IA nel processo di replica alle osservazioni formulate dalle Autorità di Vigilanza a seguito delle verifiche condotte, laddove la medesima Funzione:

- supporta i Vertici aziendali nella stesura delle controdeduzioni relative ai rilievi mossi dall'Autorità di Vigilanza a seguito di ispezioni presso le strutture della Capogruppo; le repliche fornite all'Autorità di vigilanza sono sottoposte di norma all'approvazione del Consiglio di Amministrazione;

- in occasione di ispezioni presso Società del Gruppo supporta la medesima società nella predisposizione delle controdeduzioni, supervisionando il complessivo processo di replica alle Autorità di Vigilanza.

Ferme restando le esistenti relazioni tra le funzioni aziendali di controllo e le predette autorità per i rispettivi perimetri di competenza, il Gruppo BMPS ha previsto l'istituzione di apposita funzione, a diretto riporto dell'Amministratore Delegato, cui compete la responsabilità di presidiare in accentrato a livello di Gruppo, quale univoco punto di coordinamento regolamentare, le relazioni con le Autorità di Vigilanza Europea (BCE/JST) e locali (Banca d'Italia).

6.4 Rapporti con la Società di Revisione

In generale, i rapporti con la Società di Revisione attengono lo scambio di informazioni relative alle attività autonomamente svolte, al fine di consentire una più ampia valutazione del livello di presidio del rischio.

Con riferimento all'incarico di revisione contabile dei bilanci d'esercizio e consolidato della Banca, come previsto dai principi di revisione internazionali (ISA), la Società di Revisione esterna effettua lo studio e la valutazione dei controlli interni, con particolare riguardo a quelli relativi al processo di informativa finanziaria, al fine di stabilire l'estensione e l'approfondimento delle verifiche dei dati contabili per l'espressione di un giudizio sul bilancio; a tal fine il revisore considera il controllo interno pertinente alla predisposizione del bilancio, al fine di definire le procedure di revisione appropriate alle circostanze e non per esprimere un giudizio sull'efficacia del controllo interno dell'impresa.

L'attività di assistenza e supporto alla società di revisione da parte della Funzione di IA ai fini del lavoro di certificazione del bilancio di esercizio, deve essere concordata con il revisore ogni anno, all'inizio del processo di revisione contabile. Le attività in questione si inseriscono all'interno della programmazione annuale al fine di consentire un'efficiente gestione ed un continuo monitoraggio delle stesse. La Funzione di IA supporta, inoltre, nell'ambito e nei limiti delle proprie responsabilità, determinate tipologie di richiesta di conferma di saldi e altre informazioni da parte del revisore esterno.

D'altra parte la Circ. n. 285 del 17 dicembre 2013 di Banca d'Italia prevede che il corretto funzionamento del sistema dei controlli interni si basi sulla proficua interazione nell'esercizio dei compiti (d'indirizzo, di attuazione, di verifica, di valutazione) fra gli organi aziendali, gli eventuali comitati costituiti all'interno di questi ultimi, i soggetti incaricati della revisione legale dei conti, le funzioni di controllo.

La Circolare prevede in particolare che, la Funzione di IA, qualora nell'ambito della collaborazione e dello scambio di informazioni con il soggetto incaricato della revisione legale dei conti venga a conoscenza di criticità emerse durante l'attività di revisione legale dei conti, si attivi affinché le competenti funzioni aziendali adottino i presidi necessari per superare tali criticità.

Un generale coordinamento tra le attività svolte dal revisore esterno e la Funzione di IA è inoltre richiamato dalla Guida interpretativa allo Standard dell'AIIA n. 2050[37] che sottolinea l'opportunità di specificare le attività dei due soggetti per garantire un'adeguata copertura delle materie oggetto di analisi, puntando ad una

[37] Coordinamento delle attività: "Il responsabile internal auditing dovrebbe condividere le informazioni e coordinare le diverse attività con i diversi prestatori, esterni e interni, di servizi di assurance e consulenza, alfine di assicurare un'adeguata copertura e minimizzare le possibili duplicazioni."

minimizzazione delle duplicazioni. Presupposto di un'efficace collaborazione tra le due funzioni è, ovviamente, uno scambio informativo continuo e puntuale su tutte le tematiche che possono influenzare il reciproco operato.

Un rapporto efficace fra internal ed external audit, consentendo una maggiore comprensione reciproca dei rispettivi ruoli e responsabilità, può quindi condurre ad una comunicazione regolare di informazioni reciprocamente utili nell'ambito delle funzioni di rispettiva competenza.

Premesso quanto sopra la Funzione di IA e la Società di Revisione Esterna hanno predisposto un protocollo di interazione che disciplina e scadenza lo scambio di informazioni utili alle rispettive funzioni di cui siano venute a conoscenza nell'ambito e nello svolgimento del loro lavoro.

Resta inteso che l'elencazione dei flussi è da intendersi come minimale e non esaustiva, e potrà pertanto essere oggetto di modifiche ed integrazioni sia in relazione all'effettivo ambito del lavoro di revisione (e dei suoi limiti), con l'ulteriore documentazione che si renderà necessaria ed utile per entrambi i soggetti nell'esercizio dei rispettivi compiti.