



CITTÀ DI CASTELFRANCO EMILIA

PIANO TRIENNALE DI AUDIT 2018-2020

ALLEGATO AL BILANCIO DI PREVISIONE FINANZIARIO 2018-2020

PIANO TRIENNALE DI AUDIT 2018-2020

Relazione illustrativa

1. Premessa e finalità

Il sistema dei controlli interni è un elemento fondamentale del complessivo sistema di governo dell'Ente; esso assicura che l'attività sia in linea con le strategie e le politiche e sia improntata a canoni di sana e prudente gestione.

La riforma del sistema dei controlli avviata con il D.L. 10 ottobre 2012, n. 174 "Disposizioni urgenti in materia di finanza e funzionamento degli enti territoriali, nonché ulteriori disposizioni in favore delle zone terremotate nel maggio 2012", e rafforzata dalla L. 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", impone che detto sistema sia integrato e completato con gli strumenti previsti dai principi generali di revisione aziendale e, con particolare riferimento alla politica di prevenzione della corruzione, sia ispirato a modelli di *risk management* caratterizzati dalla promozione della cultura del rischio all'interno dell'organizzazione, dalla introduzione di sistemi di identificazione degli eventi rilevanti, strumenti di analisi, valutazione e trattamento del rischio, dalla previsione di strutture di auditing, di assetti di risposte al rischio, piani di comunicazione e circolazione interna ed esterna delle informazioni (trasparenza interna ed esterna).

Il presente piano rappresenta la cornice generale del sistema operativo dei controlli interni, limitatamente agli ambiti di controllo di interesse, e integra le disposizioni normative di cui al Regolamento approvato con deliberazione del Consiglio Comunale n. 5 del 16.01.2013.

Le principali finalità della disciplina sono:

- la revisione organica dei sistemi operativi di controllo interno, in attuazione delle disposizioni di cui al D.L. 10 ottobre 2012, n. 174 "Disposizioni urgenti in materia di finanza e funzionamento degli enti territoriali, nonché ulteriori disposizioni in favore delle zone terremotate nel maggio 2012" e alla L. 6 novembre 2012, n. 190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione". In tale ambito, si è tenuto conto dell'esigenza di inquadrare in modo coerente la disciplina normativa nell'ambiente di controllo dell'Ente, in applicazione delle disposizioni di cui al Regolamento approvato con deliberazione del Consiglio Comunale n. 5 del 16.01.2013;
- l'allineamento progressivo e funzionale ai principi internazionali di revisione;
- il rafforzamento della capacità dell'Ente di gestire i rischi aziendali, in linea con l'esperienza maturata nell'ambiente di controllo che ha messo in luce l'importanza del sistema dei controlli per assicurare la sana e prudente gestione delle attività e delle funzioni istituzionali;
- la definizione di un quadro applicativo che, in base al principio di proporzionalità, tiene conto della natura dell'attività svolta, della tipologia dei servizi prestati, della complessità operativa e della dimensione organizzativa dell'Ente.

2. La revisione interna

L'*internal auditing* è una funzione aziendale, normalmente posta in staff all'alta direzione, deputata al monitoraggio del sistema di controllo interno aziendale (SCI) per verificare che esso sia correttamente strutturato (architettura del SCI) e operante (funzionamento del SCI), in linea con gli obiettivi strategici definiti dall'alta direzione.

La revisione interna (*internal auditing*) rappresenta oramai una costante degli organigrammi delle aziende private di medio-grandi dimensioni, allo scopo di presidiare gli obiettivi di attendibilità

informativa, l'economicità operativa e la conformità alle norme. In funzione dei menzionati obiettivi, e dei rispettivi ambiti oggetto di verifica e delle norme a cui tali ambiti devono attenersi, l'attività di revisione svolta dagli *internal auditor* trova tradizionale distinzione nelle nozioni di *financial auditing*, *operational auditing* e *compliance auditing*.

Con l'espressione *financial auditing* si fa riferimento alla revisione contabile propriamente detta, ovvero all'insieme di verifiche aventi l'obiettivo di apprezzare l'attendibilità di un particolare insieme di informazioni, facenti parte del più ampio sistema delle informazioni aziendali.

L'espressione *operational auditing* descrive quella particolare forma di revisione che ha l'obiettivo di assicurare la compatibilità tra i risultati raggiunti e il sistema degli obiettivi ad essa assegnato. La misura del conseguimento degli obiettivi aziendali è ottenuta tramite l'apprezzamento dell'efficacia delle procedure operative, del sistema dei controlli interni e delle performance del management, intese non solo negli aspetti economico-finanziari.

Con l'espressione *compliance auditing* si fa riferimento ad una attività continuativa di confronto fra il sistema delle regole applicabili alla realtà di riferimento e i concreti comportamenti adottati in seno all'azienda, finalizzata a verificare il rispetto degli obiettivi di conformità alle normative e a prevenire il rischio di sanzioni significative.

Il principio SAS 99 (*Consideration of Fraud in a Financial Statement Audit*) e quello ISA 240 (*la responsabilità del revisore nel considerare le frodi nel corso della revisione contabile del bilancio*), hanno stabilito che l'attività di revisione interna deve fornire altresì una adeguata risposta al rischio di frodi che alterino in modo significativo il sistema dei valori dell'azienda. In applicazione dei suddetti principi si sono sviluppate tecniche di auditing specifiche finalizzate a prevenire e accertare la presenza di frodi (*fraud auditing*).

Uno dei più significativi sviluppi della metodologia di revisione interna degli ultimi anni è rappresentato dall'assunzione dell'approccio "*risk based*", che si sostanzia nella definizione, in sede di pianificazione e programmazione delle attività, delle tipologie e dell'ampiezza dei test di controllo in modo mirato rispetto alla individuazione di quelle aree di rischio (le aree critiche di revisione) nelle quali è maggiormente probabile il verificarsi di errori di rilevazione, di valutazione e di rappresentazione. L'efficacia del menzionato approccio può essere apprezzata in termini di riduzione attesa degli errori nel raggiungimento degli obiettivi di economicità, attendibilità e conformità normativa. La necessità di valutare l'efficacia dei controlli interni in termini di livello di riduzione degli errori e di coniugare l'efficacia attesa del sistema di controllo con l'economicità dello stesso in termini di costi-benefici, comporta di dover analizzare le determinanti della significatività degli errori stessi. In tale ottica, la significatività degli errori che un sistema di controllo deve ridurre può essere descritta come la risultante di due diverse variabili: la significatività dei valori economici che attraversano un processo, che a sua volta dipende dalla dimensione del processo e dalla dimensione degli errori rispetto alle operazioni, e la rilevanza rispetto agli obiettivi che caratterizza un processo, che a sua volta dipende dalla rilevanza degli obiettivi attribuiti al processo rispetto agli altri obiettivi aziendali e dalla rilevanza del contributo del processo rispetto agli obiettivi aziendali.

L'implementazione all'interno di una pubblica amministrazione della funzione di *internal auditing* e l'integrazione strutturata nel sistema di controllo dell'approccio "*risk based*", sia pure limitatamente a specifici ambiti di attività, rappresenta un obiettivo sfidante non solo per la carenza di esperienze applicative, in ambito locale e nazionale, laddove pochissime amministrazioni virtuose hanno avviato sperimentazioni in tal senso, ma soprattutto per la mancanza di professionalità interne e risorse finanziarie e strumentali adeguate.

Ulteriore significativo profilo di complessità è riconducibile alla specificità della *mission* propria della pubblica amministrazione e alle rigidità organizzative e funzionali imposte dal quadro normativo di riferimento che comportano una difficile conformazione applicativa, in chiave pubblicistica, delle *best practices* sviluppate nelle aziende private.

In termini generali, affinché la funzione di audit nel settore pubblico sia configurata in modo appropriato devono essere assicurate le seguenti condizioni:

- *Indipendenza organizzativa.* L'indipendenza organizzativa permette alla funzione di audit di condurre il proprio lavoro senza interferenze da parte dall'entità sottoposta ad audit. La funzione di audit deve avere la sufficiente indipendenza da coloro che deve sottoporre ad audit, in modo da potere, allo stesso tempo, eseguire il proprio lavoro senza interferenza e dimostrare di essere in grado di farlo. Insieme all'obiettività, l'indipendenza organizzativa contribuisce all'accuratezza del lavoro degli auditors;
- *Un mandato formale.* I poteri ed i doveri della funzione di audit devono essere fissati da un documento formale della pubblica amministrazione;
- *Accesso incondizionato.* Gli audit devono essere eseguiti con un accesso completo e senza restrizione alcuna;
- *Risorse sufficienti.* La funzione di audit deve disporre di risorse finanziarie sufficienti in relazione alla dimensione delle proprie responsabilità di audit;
- *Organico competente.* La funzione di audit necessita di personale professionale che nel suo insieme deve possedere tutte le conoscenze, capacità e competenze necessarie per svolgere la vasta gamma di incarichi di audit richiesti dal suo mandato. Gli auditor devono rispettare le esigenze minime di aggiornamento professionale continuo stabilite dalle loro rispettive organizzazioni professionali e dagli standard;
- *Standard di audit professionali.* Gli Standard di audit professionali supportano l'implementazione dei precedenti elementi ed offrono un modello per promuovere un lavoro di audit di qualità che sia sistematico, obiettivo e basato sull'evidenza.

Nell'ambito del presente piano sono illustrate le soluzioni organizzative e metodologiche assunte al fine di sperimentare, compatibilmente con la dimensione organizzativa e le risorse disponibili, un sistema di controllo interno basato su principi di audit.

3. Struttura del piano di audit

Il presente piano definisce un quadro organico di principi e regole cui deve essere ispirato il sistema di audit interno. Esso rappresenta la cornice di riferimento per l'applicazione delle disposizioni sui controlli interni di cui al Regolamento approvato con deliberazione del Consiglio Comunale n. 5 del 16.01.2013, all'interno di specifici ambiti disciplinari (ad es. in materia di gestione di singoli profili di rischio).

In quest'ambito, il piano definisce:

- i principi generali del sistema di audit (Tit. I);
- il ruolo degli organi aziendali, a cui è rimessa la responsabilità primaria di formalizzare le politiche di governo dei rischi, di istituire il processo di gestione dei rischi e di procedere al loro riesame periodico. Il piano fornisce indicazioni circa il ruolo di ciascun organo aziendale, anche al fine di chiarire i relativi compiti e responsabilità; inoltre, sono dettate specifiche disposizioni volte a promuovere il coordinamento delle diverse funzioni di controllo (Tit. II);
- le componenti essenziali del sistema di audit (Tit. III);
- la gestione della sicurezza informatica. La disponibilità di risorse I.T. adeguate alle esigenze e in grado di supportare le tecniche di gestione dei rischi si affianca e accresce l'efficacia dei controlli interni. (Tit. IV).

All'interno dell'allegato A) sono definite le disposizioni che attengono alle specifiche tipologie di rischio da trattare.

Titolo I

Principi di carattere generale del sistema di audit

1. Fonti di disciplina

1.1 Disposizioni normative:

- D.Lgs. 18 agosto 2000, n. 267 “Testo unico delle leggi sull'ordinamento degli enti locali” e ss.mm.ii;
- D.L. 10 ottobre 2012, n. 174 “Disposizioni urgenti in materia di finanza e funzionamento degli enti territoriali, nonché ulteriori disposizioni in favore delle zone terremotate nel maggio 2012” e ss.mm.ii;
- L. 6 novembre 2012, n. 190 “Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione” e ss.mm.ii;
- Regolamento del sistema dei controlli interni del Comune di Castelfranco Emilia, approvato con deliberazione del Consiglio Comunale n. 5 del 16.01.2013.

1.1.1 Piano triennale per la prevenzione della corruzione e per la trasparenza:

- Piano triennale per la prevenzione della corruzione e per la trasparenza (PTPCT) 2017-2019, approvato con deliberazione della Giunta Comunale n. 23 del 1/2/2017. Il PTPCT 2018-2020 dovrà essere adottato entro il 31 gennaio 2018, in continuità con i contenuti del vigente PTPCT e recependo, ove rilevanti, le indicazioni di cui all'Aggiornamento 2017 al Piano Nazionale Anticorruzione in via di elaborazione da parte di ANAC.

1.2 Principi di riferimento per la revisione aziendale

La riforma della revisione contabile attuata mediante il D.Lgs. 39/2010 ha innovato anche la disciplina dei principi di revisione applicabili in Italia e le relative modalità di adozione.

L'art. 11, comma 1, del D.lgs. 39/2010 prevede tra l'altro che “La revisione legale è svolta in conformità ai principi di revisione internazionali adottati dalla Commissione europea ai sensi dell'articolo 26, paragrafo 3, della direttiva 2006/43/CE, come modificata dalla direttiva 2014/56/UE” e che “Fino all'adozione dei principi di cui al comma 1 da parte della Commissione europea, la revisione legale è svolta in conformità ai principi di revisione elaborati, tenendo conto dei principi di revisione internazionali, da associazioni e ordini professionali congiuntamente al Ministero dell'economia e delle finanze e alla Consob e adottati dal Ministero dell'economia e delle finanze, sentita la Consob. A tal fine, il Ministero dell'economia e delle finanze sottoscrive una convenzione con gli ordini e le associazioni professionali interessati, finalizzata a definire le modalità di elaborazione dei principi”.

Ai sensi dell'articolo 11 del D.lgs. 39/2010, è stato elaborato un primo set di principi di revisione, tenendo conto di quelli emanati dagli organismi internazionali, adottati con Determina dal Ministero dell'Economia e delle Finanze (Ragioneria Generale dello Stato) in data 23 dicembre 2014. Tali principi sono stati convenzionalmente definiti “principi di revisione internazionali (ISA Italia) elaborati ai sensi dell'art. 11 del D.Lgs. 39/10” (o anche solo “ISA Italia”) e sono costituiti da: (1) i principi di revisione internazionali (ISA) – versione Clarified 2009, dal principio n. 200 al n. 720 (di seguito anche “ISA Clarified”) – tradotti in lingua italiana dal CNDCEC nel corso del 2010 con la collaborazione di Assirevi e Consob e successivamente integrati dagli stessi e dall'INRL con considerazioni specifiche finalizzate a supportarne l'applicazione, nell'ambito delle disposizioni normative e regolamentari dell'ordinamento italiano. Tali integrazioni sono operate nel rispetto della Policy Position dell'International Auditing and Assurance Standards Board “A guide for National Standard Setters that

Adopt IAASB's International Standards but Find it Necessary to Make Limited Modifications" (Luglio 2006); (2) i principi di revisione, predisposti al fine di adempiere a disposizioni normative e regolamentari dell'ordinamento italiano non previste dagli ISA Clarified ed aventi ad oggetto: a) le verifiche periodiche in materia di regolare tenuta della contabilità sociale (principio di revisione (SA Italia) n. 250B "Le verifiche della regolare tenuta della contabilità sociale"); b) l'espressione, nell'ambito della relazione di revisione, del giudizio sulla coerenza delle informazioni contenute nella relazione sulla gestione e di alcune informazioni contenute nella relazione sul governo societario e gli assetti proprietari (principio di revisione (SA Italia) n. 720B "Le responsabilità del soggetto incaricato della revisione legale relativamente all'espressione del giudizio sulla coerenza").

I principi di revisione internazionali ISA, così come modificati ed integrati dal progetto "ISA Clarity" dell'IFAC, sono assunti quali punti di riferimento tecnico nell'ambito del presente piano.

Il modello di sistema di controllo proposto è inoltre basato sul framework contenuto negli standard emanati dal C.o.S.O. nel 1992 (*International Control Integrated Framework*), nel 2004 (*Enterprise Risk management Framework*) e nel 2013 (*International Control - Integrated Framework*).

2. Definizioni

Ai fini del presente piano si intendono per:

- a) *Sistema integrato dei controlli interni*: il sistema dei controlli interni del Comune di Castelfranco Emilia come disciplinato dal Regolamento approvato con deliberazione del Consiglio Comunale n. 5 del 16.01.2013;
- b) *Errore (Misstatement)* –una differenza tra un atto, una operazione o una classe di operazioni, o un procedimento e i parametri richiesti affinché l'atto, l'operazione o classe di operazioni, o il procedimento sia conforme al quadro di riferimento. Gli errori possono essere originati da comportamenti o eventi non intenzionali ovvero da frodi.
- c) *Rischi connessi all'attività*: un rischio derivante da condizioni, eventi, circostanze, azioni o inattività significative che potrebbero incidere sfavorevolmente sulla capacità dell'Ente di raggiungere i propri obiettivi e di realizzare le proprie strategie, ovvero un rischio derivante dalla definizione di obiettivi e strategie non appropriate;
- d) *Rischio di errori significativi (Risk of material misstatement)* – il rischio che un atto, una operazione o un procedimento sia significativamente errato prima di essere sottoposto a revisione. Tale rischio è costituito da due componenti, di seguito descritte:
 - Rischio intrinseco (Inherent risk) – La possibilità che una operazione o una classe di operazioni contenga un errore che potrebbe essere significativo, singolarmente o insieme ad altri, indipendentemente da qualunque controllo ad essa riferito.
 - Rischio di controllo (Control risk) – Il rischio che un errore, che potrebbe riguardare una operazione o una classe di operazioni e che potrebbe essere significativo, singolarmente o insieme ad altri, non sia prevenuto, o individuato e corretto, in modo tempestivo dal controllo interno dell'ente;
- e) *Rischio significativo (Significant risk)* – Un rischio di errore significativo, identificato e valutato, che richiede una speciale considerazione nella revisione;
- f) *Procedure di valutazione del rischio (Risk assessment procedures)*: le procedure di revisione svolte per acquisire una comprensione dell'impresa e del contesto in cui opera, incluso il suo controllo interno, al fine di identificare e valutare i rischi di errori significativi, siano essi dovuti a frodi o a comportamenti o eventi non intenzionali;
- g) *Processo di gestione dei rischi*: l'insieme delle regole, delle procedure e delle risorse volte a identificare, misurare o valutare, monitorare, attenuare e comunicare ai livelli appropriati i rischi.

3. Destinatari della disciplina

Il presente piano si applica al Comune di Castelfranco Emilia.

4. SICI - Tipologie di controllo interno - Unità organizzative responsabili dei procedimenti di controllo interno

Tipologia di controllo	Finalità	Unità organizzativa responsabile
Controllo di regolarità amministrativa nella fase preventiva	Garantire la legittimità, la regolarità e correttezza dell'azione amministrativa nella fase preventiva di formazione degli atti	Responsabili di Settore
Controllo di regolarità amministrativa nella fase successiva	Garantire la legittimità, la regolarità e correttezza dell'azione amministrativa nella fase successiva di formazione degli atti	Segretario Generale
Controllo di regolarità contabile	Garantire la legittimità, la regolarità e correttezza dell'azione amministrativa nella fase preventiva di formazione degli atti	Responsabile Settore Programmazione Economica e Bilancio
Controllo di gestione	Verificare efficacia, efficienza ed economicità dell'azione amministrativa; Ottimizzare il rapporto fra obiettivi e azioni realizzate e fra risorse impiegate e risultati ottenuti	Programmazione, organizzazione e controllo strategico
Controllo strategico	Valutare l'adeguatezza delle scelte compiute in sede di attuazione dei piani, programmi ed altri strumenti di determinazione dell'indirizzo politico, in termini di congruenza fra risultati conseguiti e obiettivi predefiniti	Programmazione, organizzazione e controllo strategico
Controllo sugli equilibri finanziari	Garantire il costante controllo degli equilibri finanziari della gestione di competenza, della gestione residui e della gestione di cassa, nonché la realizzazione degli obiettivi di finanza pubblica determinati attraverso il patto	Settore Programmazione Economica e Bilancio

Nell'ambito della letteratura della funzione di *internal auditing* i controlli interni vengono distinti in tre categorie:

1. Controlli di primo livello: diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture produttive (ad esempio, i controlli di tipo gerarchico) o incorporati nelle procedure e nei sistemi informatici, ovvero eseguiti nell'ambito dell'attività di back-office;

2. Controlli di secondo livello: affidati a strutture diverse da quelle produttive, che hanno l'obiettivo di:

- concorrere alla definizione delle metodologie di misurazione del rischio, verificare il rispetto dei limiti assegnati alle varie funzioni operative e controllare la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio rendimento assegnati (Risk Management);
- concorrere alla definizione delle metodologie di misurazione/valutazione del rischio di conformità, individuare idonee procedure per la prevenzione dei rischi rilevati e richiederne l'adozione (Compliance);
- attestare/dichiarare l'informativa contabile societaria secondo quanto previsto dalla legge;

3. Controlli di terzo livello (Attività di revisione interna/Internal audit): finalizzati alla valutazione e verifica periodica della completezza, della funzionalità e dell'adeguatezza del sistema dei controlli interni e affidati a strutture diverse da quelle che si occupano dei controlli di secondo livello.

L'art. 147 bis del D.Lgs. 267/2000 statuisce che “Il controllo di regolarità amministrativa e' inoltre assicurato, nella fase successiva, secondo principi generali di revisione aziendale”, ma all'art. 148, rubricato “controlli esterni”, il legislatore affida la verifica del funzionamento dei controlli interni non già ad una funzione interna di audit ma ad un organismo esterno: la sezione regionale della Corte dei Conti. La previsione normativa naturalmente non esclude che una funzione di revisione interna, cui siano attribuite esclusivamente attività di *assurance e consulenza*, totalmente indipendente dalla direzione, chiamata a valutare la funzionalità del complessivo sistema dei controlli interni, possa essere istituita con risorse umane, strumentali e finanziarie dedicate. La percorribilità di una tale soluzione presuppone tuttavia la compatibilità dei relativi costi con le risorse finanziarie disponibili (in una logica di bilanciamento costi-benefici) e con la dimensione e le caratteristiche della struttura organizzativa. Nell'ambito del Regolamento del sistema dei controlli interni del Comune di Castelfranco Emilia:

- le funzioni di coordinamento e di raccordo fra le varie attività di controllo sono svolte, nell'esercizio delle sue funzioni di sovrintendenza alla gestione dell'Ente, dal Segretario Generale;
- il controllo di regolarità amministrativa è posto sotto la direzione del Segretario Generale;
- è stato creato un livello di controllo finalizzato a ricondurre all'interno del sistema una verifica circa la funzionalità ed adeguatezza dei controlli interni tramite la validazione del referto annuale predisposto dal Segretario Generale, che il Sindaco deve trasmettere alla sezione regionale della Corte dei Conti, da parte di un organismo indipendente ossia il Collegio dei Revisori.

Il Segretario Generale, inoltre, è stato nominato Responsabile per la prevenzione della corruzione ai sensi della L. 190/2012 e Responsabile della trasparenza ai fini degli adempimenti di cui al D.Lgs. 33/2013.

Con deliberazione della Giunta comunale n. 140 del 21 settembre 2013 è stata istituita la struttura di staff dedicata a controlli interni e prevenzione della corruzione, prevista dall'art. 83 del Regolamento sull'ordinamento degli uffici e dei servizi. Alla menzionata struttura è assegnato lo specifico compito di coadiuvare il Segretario Generale nello svolgimento delle funzioni di diretta pertinenza, oltre che in

materia di trasparenza e prevenzione della corruzione, anche in materia di controlli di regolarità amministrativa/audit interno.

Al fine di ricondurre a sistema, compatibilmente con le risorse finanziarie e l'assetto dell'Ente, risposte organizzative adeguate alle sollecitazioni del legislatore, si è ritenuto di sperimentare un sistema di controllo che, sebbene non preveda l'istituzione di una funzione di *internal auditing* (intesa quale controllo di terzo livello), ne recupera il valore aggiunto attraverso la combinazione di distinti e coordinati processi di controllo e l'implementazione del *risk management*.

In particolare, il presente piano, in attuazione delle disposizioni regolamentari, prevede l'integrazione di funzioni di coordinamento e di raccordo fra le varie attività di controllo, di funzioni di controllo diretto di *compliance* e *anti-fraud* e di gestione dei rischi ispirati ai principi internazionali di revisione, assegnandone la responsabilità al Segretario Generale. A detti elementi si affianca, in una logica sinergica, la verifica periodica della completezza, della funzionalità e dell'adeguatezza del sistema dei controlli interni a cura del Collegio di revisione. L'applicazione combinata dei descritti fattori ha l'obiettivo di strutturare un sistema di controllo finalizzato a valutare e migliorare continuamente i processi di controllo, di gestione dei rischi e di corporate governance, un sistema di controllo basato su principi e metodologie di *internal auditing*.

A conclusione del presente paragrafo, si evidenzia che, per i primi anni di applicazione, il sistema di audit è stato strutturato in funzione dell'esigenza di offrire, nel breve periodo, una soluzione organizzativa coerente con la *ratio* delle innovazioni legislative in materia di controlli interni e compatibile con le risorse umane, finanziarie e strumentali disponibili. L'istituzione della funzione di audit come controllo di terzo livello, in aderenza ai canoni che la contraddistinguono nell'ambito delle aziende private di medio -grandi dimensioni, presuppone necessariamente, in termini di costi-benefici, interventi di sostegno finanziario e di supporto tecnico-professionale da parte degli organismi centrali ovvero consistenti investimenti da parte del sistema delle autonomie locali in una prospettiva associativa e di economie di scala.

5. Principi generali del sistema di audit

Il sistema di audit del Comune di Castelfranco Emilia, è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, il conseguimento delle seguenti finalità:

- verifica dell'attuazione delle strategie e delle mission istituzionali;
- salvaguardia dei valori dell'Ente;
- rafforzamento del rapporto fiduciario con gli *stakeholders*;
- efficacia ed efficienza dei processi aziendali;
- prevenzione del rischio di fenomeni di *maladministration*;
- conformità delle operazioni alle normative, nonché alle politiche, regolamenti e procedure interne.

Il sistema di audit riveste un ruolo centrale nell'organizzazione in quanto:

- rappresenta un elemento fondamentale di conoscenza per gli organi di indirizzo politico-amministrativo in modo da garantire piena consapevolezza dell'andamento della gestione ed efficace presidio dei rischi aziendali e delle loro interrelazioni;
- orienta i mutamenti delle linee strategiche e delle politiche;
- consente di adattare in modo coerente il contesto organizzativo;
- presidia la funzionalità dei sistemi gestionali e il rispetto degli standards di riferimento;
- favorisce la diffusione di una corretta cultura del rischio e della legalità.

Il sistema di audit coinvolge l'intera organizzazione nello sviluppo e nell'applicazione di metodi sistemici per misurare, comunicare, gestire i rischi.

Per poter realizzare questo obiettivo, il sistema dei controlli interni deve in generale:

- consentire di identificare, valutare, monitorare, attenuare e riportare ai livelli decisionali appropriati i rischi assunti o assumibili nei diversi segmenti, cogliendone, in una logica integrata, anche le interrelazioni reciproche e con l'evoluzione del contesto esterno. Si riportano, nell'Allegato A, le disposizioni riferite alle singole tipologie di rischio da trattare;
- garantire che le anomalie riscontrate siano tempestivamente portate a conoscenza di livelli appropriati dell'Ente (organi di indirizzo politico-amministrativo, se significative) in grado di attivare tempestivamente gli opportuni interventi correttivi;
- individuare o consentire di individuare delle contromisure applicabili per ciascuno degli eventi negativi ritenuti altamente rischiosi.

Si assumono come fondamentali i seguenti principi generali di organizzazione:

- i processi decisionali e l'affidamento di funzioni al personale consentono l'univoca individuazione di compiti e responsabilità e sono idonei a prevenire i conflitti di interessi. In tale ambito, deve essere assicurata la necessaria distinzione tra funzioni di indirizzo politico-amministrativo e compiti di gestione amministrativa;
- le politiche di gestione delle risorse umane devono tendere all'arricchimento delle competenze e della professionalità per garantire l'esercizio adeguato delle responsabilità ad esse attribuite (centralità della formazione);
- le procedure operative e di controllo devono minimizzare i rischi legati a frodi o infedeltà dei dipendenti, prevenire e attenuare i potenziali conflitti d'interesse, favorire la condivisione di valori etici anche attraverso l'applicazione rigorosa dei codici di comportamento.

Titolo II

Il ruolo degli organi aziendali

1. Premessa

Nei successivi paragrafi si forniscono indicazioni minime circa il ruolo di ciascun organo nell'ambito del sistema di audit, anche al fine di chiarire i relativi compiti e responsabilità.

Tali indicazioni non esauriscono, pertanto, le azioni che possono essere adottate dai competenti organi aziendali nell'ambito della loro autonomia decisionale/gestionale.

2. Ruolo del Consiglio Comunale

Il regolamento del sistema dei controlli interni ha previsto il Piano triennale di audit quale allegato alla relazione previsionale e programmatica al fine di renderlo coerente con l'attività programmatoria di medio periodo e l'assegnazione delle risorse. A seguito della recente riforma della contabilità, per effetto della quale viene meno la Relazione previsionale e programmatica, il Piano è allegato al bilancio di previsione.

Più in dettaglio il Consiglio comunale definisce:

- in applicazione delle disposizioni normative di livello nazionale, le tipologie di controllo, i soggetti preposti, i relativi compiti e responsabilità e i flussi informativi tra tali funzioni e tra queste e gli organi aziendali (Regolamento del sistema dei controlli interni e regolamenti correlati);
- gli indirizzi strategici e le politiche di governo dei rischi e provvede al loro riesame periodico, in relazione all'evoluzione dell'attività aziendale e del contesto esterno, al fine di assicurarne l'efficacia nel tempo;
- l'assegnazione degli strumenti finanziari, assicurandone la costante adeguatezza.

Con cadenza annuale, esamina il referto predisposto dal Segretario Generale sull'adeguatezza e funzionalità del sistema dei controlli interni che il Sindaco deve inoltrare alla sezione regionale della Corte dei Conti, e, con la cadenza prevista dal presente programma, i report relativi agli esiti dei controlli in relazione alle singole tipologie di rischio.

3. Ruolo della Giunta Comunale

La Giunta Comunale, in attuazione degli indirizzi strategici in materia di controlli interni e delle politiche di governo dei rischi definite dal Consiglio Comunale, è responsabile per l'adozione di tutti gli interventi organizzativi necessari ad assicurare l'aderenza dell'organizzazione al sistema dei controlli interni.

In tale contesto:

- definisce, nel rispetto delle disposizioni regolamentari in materia di controlli interni, le componenti organizzative funzionali all'attuazione delle varie tipologie di controllo (Regolamento sull'ordinamento degli uffici e dei servizi). Le determinazioni organizzative dovranno garantire il rispetto del divieto di affidare verifiche di regolarità amministrativa e contabile a strutture addette al controllo di gestione, alla valutazione dei responsabili e al controllo strategico;
- adotta il PTPCT e i suoi aggiornamenti annuali;
- agevola lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata in relazione alle diverse tipologie di rischi ed estesa all'intera struttura organizzativa. In particolare, devono essere sviluppati e attuati programmi di formazione per sensibilizzare i dipendenti in merito alle responsabilità in materia di rischi in modo da non confinare il processo di gestione del rischio alle funzioni di controllo;
- pone in essere le iniziative e gli interventi organizzativi necessari per garantire nel continuo la complessiva affidabilità del sistema dei controlli interni. Attua i necessari interventi correttivi o di

adeguamento nel caso emergano carenze o anomalie, o a seguito dell'introduzione di nuove disposizioni normative.

La Giunta comunale inoltre adotta le misure necessarie a prevenire il rischio di conflitti di interesse (regolamento della disciplina delle incompatibilità e dei criteri per le autorizzazioni ai dipendenti comunali allo svolgimento d'incarichi esterni) e a diffondere valori etici condivisi (codici di comportamento).

4. Ruolo del Segretario Generale

Il Segretario Generale, nell'esercizio delle sue funzioni di sovrintendenza alla gestione dell'Ente, svolge le funzioni di coordinamento e raccordo fra le varie attività di controllo.

Il controllo di *compliance e anti-fraud* è svolto direttamente sotto la direzione del Segretario Generale che, a tal fine, si avvale della struttura di staff di cui all'art. 83 del Regolamento sull'ordinamento degli uffici e dei servizi.

Al Segretario generale è affidata la strutturazione e il monitoraggio dell'operatività dei processi di individuazione e mitigazione dei rischi, nel perseguimento degli obiettivi aziendali.

Nell'esercizio di tale compito il Segretario Generale:

- predispone il piano di audit in coerenza con le previsioni del piano triennale di prevenzione della corruzione;
- coerentemente con le politiche di governo dei rischi, definisce il processo di gestione dei rischi. In particolare, stabilisce le modalità e gli strumenti operativi in relazione alle varie tipologie di rischio, coerenti con il livello di rischio accettato e tenendo esplicitamente conto dei risultati emersi nel corso del processo;
- elabora i flussi informativi interni volti ad assicurare agli organi aziendali (Consiglio Comunale, Sindaco, Giunta Comunale, Nucleo di Valutazione e Collegio dei Revisori) e agli organi esterni la piena conoscenza degli esiti del processo.

Il Segretario generale svolge altresì le funzioni di Responsabile della prevenzione della corruzione.

Nell'esercizio delle attività di audit, il Segretario generale può in qualsiasi momento:

- richiedere alle strutture interne atti o notizie, effettuare interviste ecc.;
- compiere e disporre, nei confronti degli stessi uffici, anche per il tramite del personale assegnato, ispezioni e accertamenti diretti;
- formulare osservazioni e raccomandazioni, anche a seguito di eventuali segnalazioni a cura del Collegio di revisione, agli organi deputati alla gestione e richiedere comunicazione delle "misure consequenzialmente adottate";
- formulare direttive generali.

5. Ruolo dei Responsabili di Settore

Nell'ambito del processo di gestione delle diverse tipologie di rischio, identificate come tipologie da gestire, i Responsabili di Settore:

- assicurano una corretta, tempestiva e sicura gestione delle informazioni alla "funzione di audit", nonché la formalizzazione e la documentazione richiesta nelle diverse fasi del processo di gestione del rischio;
- curano che i sistemi di misurazione e mitigazione dei rischi siano integrati nei processi decisionali e nella gestione dell'operatività quotidiana delle strutture di riferimento;
- applicano, nello svolgimento dei compiti assegnati, le osservazioni/raccomandazioni/direttive elaborate in relazione al processo di audit.

6. Ruolo del Collegio dei Revisori

Nell'ambito del sistema di audit, il Collegio dei Revisori ha il compito di validare la relazione annuale del Segretario Generale sulla adeguatezza e funzionalità del sistema dei controlli interni. Nell'ambito della suddetta attività il Collegio può operare tutte le verifiche ritenute opportune, mediante accessi fisici, verifica di documentazione ecc.

Titolo III

Sistema di audit

1. Componenti del sistema di audit

In applicazione delle disposizioni normative e regolamentari, all'interno del Comune di Castelfranco Emilia, sono previste, secondo quanto di seguito indicato, linee aziendali di controllo permanenti:

- a) di controllo dei rischi (*risk management function*);
- b) anti frode (*anti-fraud audit*);
- c) di conformità alle norme (*compliance*);

Esse operano in modo integrato e fanno capo al Segretario Generale.

Per assicurare l'indipendenza delle attività aziendali di controllo è necessario che il personale che partecipa alle stesse non sia coinvolto in attività operative oggetto di controllo.

Tenuto conto che, in una logica di audit, l'adeguatezza ed efficacia delle funzioni di controllo devono essere sottoposte a verifica periodica da parte della revisione interna (controllo di terzo livello), per assicurare l'imparzialità delle verifiche, le attività di controllo saranno sottoposte alla revisione del Collegio, in funzione della validazione del referto annuale da trasmettere alla Sezione Regionale della Corte dei Conti.

Le linee guida relative alle funzioni di *anti-fraud audit e di compliance* sono contenute nell'allegato A) al presente piano. La sezione relativa al fraud audit è strettamente integrata con la politica di risk assessment elaborata nell'ambito del Piano Triennale di Prevenzione della Corruzione e suoi aggiornamenti.

Poiché il rischio frode e il rischio *compliance* sono diffusi a tutti livelli dell'organizzazione, soprattutto nell'ambito delle linee operative, l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato: è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale.

L'attività di controllo dei rischi ha la finalità di attuare le politiche di governo dei rischi, attraverso un adeguato processo di gestione dei rischi. Essa è articolata in relazione ai singoli profili di rischio.

La "funzione" di controllo dei rischi:

- è direttamente coinvolta nella definizione del livello di rischio accettato e nell'elaborazione delle politiche governo dei rischi e delle varie fasi che costituiscono il processo di gestione dei rischi nonché nella fissazione dei limiti operativi all'assunzione delle varie tipologie di rischio;
- verifica nel continuo l'adeguatezza di tali politiche, processo e limiti;
- è responsabile dello sviluppo, della convalida e del mantenimento dei sistemi di misurazione e controllo dei rischi;
- sviluppa e applica indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi;
- monitora costantemente l'evoluzione dei rischi aziendali e il rispetto dei limiti operativi all'assunzione delle varie tipologie di rischio;
- verifica l'adeguatezza e l'efficacia delle misure assunte per rimediare alle carenze riscontrate nel processo di gestione del rischio.

Nell'ambito del sistema di audit, coerentemente con il presente piano, nell'ambito della collaborazione e dello scambio di informazioni con il Collegio di revisione, individua le criticità emerse durante l'attività e si attiva affinché vengano adottati i presidi necessari per superare tali criticità.

2. Caratteri distintivi del sistema

Obiettivo del sistema di audit è quello di identificare e valutare i rischi di errori significativi, siano essi dovuti a frodi o a comportamenti o eventi non intenzionali, mediante la comprensione del contesto di

riferimento, conseguendosi in tal modo una base per definire e mettere in atto risposte di revisione a fronte dei rischi identificati e valutati di errori significativi.

Il sistema di controllo interno è basato sull'integrazione dei *framework* del C.o.S.O.IC.-IF e ERM.

Esso si articola in otto elementi complementari:

1. l'ambiente di controllo (*Control environment*);
2. il sistema degli obiettivi aziendali e le correlate attitudini al rischio (*Objective Setting*);
3. l'identificazione degli eventi negativi (*Event identification*);
4. la valutazione della probabilità e dell'impatto di ciascuno degli eventi negativi identificati (*Risk assesement*);
5. l'individuazione delle contromisure (*Risk response*);
6. le procedure di controllo (*Control activities*);
7. il sistema informativo (*Information and communication*);
8. il monitoraggio (*Monitoring*).

Nell'ambito del presente piano si assume che le componenti 3, 4, 5 e 8, più che elementi del sistema di controllo, siano principi che devono orientare i quattro elementi tecnico-operativi di cui alle componenti 1, 2, 6 e 7 in quanto:

- gli elementi che integrano la valutazione dei rischi sono un ingrediente della progettazione dei controlli interni, i quali devono essere costruiti in aderenza alle criticità di ciascuna area gestionale e nelle diverse prospettive delle funzioni di controllo;
- occorre continuamente monitorare l'adeguatezza dei controlli interni al fine di accertare l'aderenza e l'effettivo funzionamento nel tempo.

Quanto alle contromisure adottabili per mitigare un rischio significativo (componente 5), esse non consistono solo in controlli interni ma anche in azioni di tipo gestionale che possono andare nella direzione di:

- una eliminazione delle attività operative che originano i rischi individuati, ritenuti eccessivamente significativi e a fronte dei quali non si identificano contro misure adeguate;
- un trasferimento dei rischi a terzi mediante soluzioni contrattuali.

Nel biennio 2018-2019 l'attività sarà prioritariamente indirizzata alla prosecuzione, in via sperimentale anche al fine di verificarne la sostenibilità organizzativa a regime, della pianificazione del processo in relazione alla sezione compliance ed alla attuazione del piano di trattamento del rischio di cui al PTPCT in relazione alla sezione di fraud-audit. La pianificazione è una azione continua e iterativa, che inizia appena dopo il completamento del periodo di controllo precedente, per continuare fino al completamento di quello corrente.

3. Utilizzo di controlli automatizzati

L'informatizzazione dei processi consente per tutte le attività dell'amministrazione, la tracciabilità delle istanze di processo e riduce quindi il rischio di "blocchi" non controllabili con emersione delle responsabilità per ciascuna fase.

Il Comune di Castelfranco Emilia, in attuazione delle previsioni del piano triennale di audit 2013/2015, ha acquistato un software che consente di:

- gestire i piani periodici, tra cui quello della prevenzione della corruzione (L. 190/2012)
- identificare responsabili, procedure e formazione, rischi e sistema dei controlli interni

- registrare l'esecuzione degli adempimenti e dei controlli
- pianificare e condurre attività di verifica, tramite *workflow* e *checklist*
- gestire operativamente, documentare ogni processo, con consuntivi e indicatori di processo
- supportare la produzione della relazione annuale con i risultati dell'attività svolta (L. 190/2012), e un sistema di reportistica e indicatori di sintesi

Lo strumento informativo consente di gestire i controlli di *compliance* e *fraud-audit* e di tracciare il flusso delle attività degli uffici in tempo reale nel corso dell'esecuzione dei processi, rendendo possibili interventi correttivi in una prospettiva di prevenzione.

Ad oggi, il citato software gestionale è in via di progressiva sperimentazione. Tenendo conto dei processi di riorganizzazione che attualmente riguardano la struttura dell'ente, nel corso del 2018 si prevede un ulteriore sviluppo della sperimentazione in atto.

4. Modalità del campionamento

Nell'ambito del sistema di audit si assume altresì l'utilizzo del campionamento di revisione.

Le modalità del campionamento saranno condotte in base al principio di revisione internazionale ISA 530 "Campionamento di revisione"

Si introducono le seguenti definizioni:

- Popolazione – insieme completo degli elementi da cui è selezionato un campione sottoposto a revisione;
- Unità di campionamento – singolo elemento che costituisce la popolazione;
- Cardinalità della popolazione – numero (intero) delle unità di campionamento che costituiscono la popolazione;
- Campione – elementi selezionati ed estratti dalla popolazione, sui quali si applicano le procedure di revisione;
- Campionamento – procedure per la selezione degli elementi della popolazione e la costituzione del campione;
- Data di campionamento – data alla quale si riferisce la procedura di campionamento;
- Percentuale di campionamento – percentuale del numero di unità di campionamento della popolazione che costituisce il campione;
- Interferenza statistica – procedimento per cui si inducono le caratteristiche della popolazione dall'osservazione di una parte di essa, detta campione, selezionata solitamente mediante una selezione casuale delle unità di campionamento;
- Stratificazione - processo attraverso il quale una popolazione viene suddivisa in sotto popolazioni, ciascuna delle quali rappresenta un gruppo di unità di campionamento con caratteristiche analoghe;
- Generatore di numeri casuali (RNG, Random Number Generator) – software informatico che genera una sequenza di numeri aventi le stesse proprietà statistiche di una sequenza di numeri casuali;
- Sequenza (o lista) di campionamento – generazione della sequenza (o lista) delle unità di campionamento che costituiranno il campione, dopo l'applicazione del generatore di numeri casuali alla popolazione.

Prima di descrivere in dettaglio la modalità di campionamento, al fine di renderle più comprensibili, occorre fare alcune osservazioni sui generatori di numeri casuali. Lo strumento software utilizzato come RNG è quello messo a disposizione dalla Regione Emilia Romagna, sul proprio sito web, all'indirizzo <http://wwwservizi.regione.emilia-romagna.it/Generatore/default.asp>. Questo si basa su un

generatore di Lehmer, cioè un generatore congruenziale moltiplicativo, noto in letteratura, che genera una sequenza di numeri con le stesse proprietà statistiche di una sequenza casuale.

L' algoritmo, a partire dal seme identificato con X_0 , è definito in termini ricorsivi nel seguente modo:

$$X_{k+1} = (aX_k + c) \bmod m, k > 0$$

I numeri generati appartengono all'intervallo $[0, m-1]$ e

- m è un numero intero
- a e c sono numeri interi maggiori o uguali a 0 e minori di m

Di particolare importanza per la bontà della sequenza è la scelta dei valori di a , c e m (valori che scelti opportunamente assicurano sequenza a periodo completo). Nel caso di questo sito i valori scelti sono stati tratti dalla letteratura e sono: $m=2147483647$ ($2^{31}-1$), $a=1103515245$ e $c=0$.

La gestione dei casi overflow che possono capitare durante la moltiplicazione aX_k viene assicurata dall'algoritmo di Schrage, infatti dato che dopo la moltiplicazione si esegue una operazione di modulo, l'overflow può essere evitato distribuendo la moltiplicazione su più parti e eliminando i termini più significativi.

Una volta individuata la popolazione e/o la sua stratificazione la modalità di campionamento avviene secondo la seguente procedura:

- Si calcola la cardinalità della popolazione e/o di ciascuna sua stratificazione;
- Si apre la pagina web del RNG all'indirizzo <http://wwwservizi.regione.emilia-romagna.it/Generatore/default.asp>;
- Si valorizzano i campi "valore minimo", "valore massimo", "% sul totale" e "seme generatore" richiesti dal RNG, rispettivamente con i valori '1', "cardinalità della popolazione", "Percentuale di campionamento" e "Data di campionamento", dopodiché si clicca sul pulsante di conferma;
- Il RNG, restituisce una sequenza di numeri che costituisce la sequenza o lista di campionamento, utili per la costituzione del campione.

Il campione così ottenuto sarà sottoposto a revisione e per interferenza statistica fornirà le indicazioni relative alla popolazione e/o ad una sua stratificazione.

Titolo IV

Gestione della sicurezza Informatica

Il sistema di gestione della sicurezza informatica ha l'obiettivo di garantire a ciascun insieme individuato di informazioni, ad ogni applicativo o banca dati una protezione appropriata e coerente lungo l'intero ciclo di vita, in termini di riservatezza, integrità, disponibilità, verificabilità e *accountability* (assegnazione della responsabilità di un'attività a un soggetto ben determinato). Obiettivo del sistema è anche di contribuire alla conformità delle risorse informatiche alle norme di legge e regolamenti interni ed esterni. In dettaglio, si riportano, in maniera non esaustiva alcune misure di sicurezza informatica adottate dal Comune di Castelfranco Emilia al fine di minimizzare i "rischi" informatici:

- **Antivirus:** consente di proteggere i sistemi di elaborazione da software dannosi conosciuti come virus. Per assicurarne l'efficacia e l'efficienza è aggiornato con cadenza giornaliera in modo da avere in continua esecuzione le funzioni di scansione in tempo reale. Per rendere più efficace la protezione sono pianificate scansioni settimanali di tutti i sistemi di elaborazione collegati alla rete comunale;
- **Antispyware:** software per la rimozione di "file spia" (spyware), in grado di carpire informazioni riguardanti le attività online dell'utente ed inviarle a soggetti che le utilizzeranno per trarne profitto o creare un danno;
- **Firewall:** sistema di protezione di rete hardware e/o software perimetrale che garantisce il controllo degli accessi da e verso la rete comunale, verificando tutto il traffico di rete che lo attraversa, proteggendo contro accessi indesiderati ed aggressioni provenienti da internet e bloccando eventuali programmi presenti sui sistemi di elaborazione che tentano di accedere ad internet senza il controllo dell'utente;
- **Backup:** più che un sistema di sicurezza si tratta di un utile sistema per recuperare dati eventualmente persi, cancellati accidentalmente o danneggiati. Il backup consiste nell'esecuzione di una copia di sicurezza dei dati, delle banche dati e dei sistemi di elaborazione centrale (server);
- **Ridondanza dei dischi:** tutti i sistemi di elaborazione centrali sono dotati di sistemi di ridondanza dei dischi per prevenire la perdita di informazioni in caso di rottura di un disco;
- **Aggiornamento del software:** applicazione periodica di patch, fix o service pack per la rimozione di errori, bug, malfunzionamenti o per incrementare la sicurezza contro rischi di vulnerabilità del software installato;
- **Sistema di autenticazione:** sistema di verifica della corretta "identità" di un soggetto che cerca di accedere ad una risorsa hardware o software ed usufruirne i relativi servizi ad essa associati (accesso fisico e/o logico a soggetti autorizzati);
- **Limitazione della disponibilità delle risorse:** limitazione della fruizione dei servizi previsti per un certo utente sia temporalmente sia secondo le modalità previste dal sistema di elaborazione (ambiente di rete associato ad un utente).

ALLEGATO A

Disposizioni relative alle specifiche tipologie di rischio

1. Fraud Audit

1.1 Premessa

La consapevolezza che la prevenzione delle frodi aziendali deve essere realizzata mediante un adeguato sistema di controllo interno è emersa negli Stati Uniti a seguito dei lavori della *Treadway Commission* e ha condotto alla definizione di standard in materia di controllo interno quali quelli emanati dal C.o.S.O. (*Committee of Sponsoring Organization*). Tali standard hanno in seguito influenzato numerose produzioni normative, fra le quali, in Italia il D.Lgs. 231/2001.

Secondo quanto risulta dalle indagini empiriche dell'ACFE (*Association of Certified Fraud Examiners*), l'impatto monetario della frode e l'ammontare del tempo che trascorre fino alla sua individuazione aumentano, fino a quasi raddoppiare, laddove i controlli anti-frode non sono presenti. La prospettiva legislativa che ha ispirato, in Italia, dapprima il D.Lgs. 231/2001 in materia di responsabilità amministrativa delle persone giuridiche, e più di dieci anni dopo, la L. 190/2012 in materia di prevenzione della corruzione, sposta significativamente il baricentro del contrasto dalla repressione sul piano penale (*detective controls*) alla prevenzione sul versante amministrativo (*preventive controls*).

1.2. Definizione del concetto di frode

Caratteristiche delle frodi nell'ambito del principio di revisione internazionale (ISA) 240

“2. Gli errori in bilancio possono derivare sia da frodi sia da comportamenti o eventi non intenzionali. Il fattore di distinzione tra le due categorie di errori è l'intenzionalità o meno dell'atto che determina gli errori in bilancio.

3. Sebbene il termine frode rappresenti, da un punto di vista giuridico, un concetto più ampio, ai fini dei principi di revisione internazionali il revisore si occupa di quelle frodi che determinano la presenza di errori significativi in bilancio. Per il revisore sono rilevanti due tipologie di errori intenzionali: errori derivanti da una falsa informativa finanziaria ed errori derivanti da appropriazioni illecite di beni ed attività dell'impresa. Sebbene il revisore possa sospettare, ovvero più raramente identificare, l'esistenza di frodi, non stabilisce se la frode sia effettivamente avvenuta sotto il profilo.”

Caratteristiche delle frodi nell'ambito del presente Piano di audit

In funzione del principio di proporzionalità della funzione di controllo, il concetto di frode nell'ambito del presente Piano è identificato con quello di corruzione di cui alla L. 190/2012. Ai fini del presente documento, il termine “corruzione” deve essere inteso in un'accezione ampia, ovvero come comprensivo delle varie situazioni in cui, nel corso dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati.

Le situazioni rilevanti sono quindi più ampie della fattispecie penalistica e sono tali da comprendere non solo l'intera gamma dei delitti contro la pubblica amministrazione ma anche le situazioni in cui – a prescindere dalla rilevanza penale – venga in evidenza un malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite ovvero l'inquinamento dell'azione amministrativa ab externo, sia che tale azione abbia successo sia nel caso in cui rimanga a livello di tentativo.

1.3 Obiettivi della funzione di gestione del rischio di errori significativi dovuti a frodi

- Identificare e valutare i rischi di errori significativi dovuti a frodi;
- Acquisire elementi probativi sufficienti ed appropriati riguardanti i rischi identificati e valutati di errori significativi dovuti a frodi;
- Definire le risposte appropriate;
- Fronteggiare adeguatamente frodi o sospette frodi individuate durante l'attività di controllo.

1.4 Definizioni

Ai fini del presente piano, i seguenti termini hanno il significato sotto riportato:

- Fattori di rischio di frodi – Eventi o circostanze che indicano incentivi o pressioni a commettere frodi o che forniscono un'occasione per la commissione di frodi;
- Rischio di errori significativi (limitatamente alla componente di rischio intrinseco): possibilità che un atto o una attività relativa ad una classe di operazioni contenga un errore, dovuto a frode, che potrebbe essere significativo, singolarmente o insieme ad altri, indipendentemente dai controlli ad essa riferiti.

1.5 Disposizioni normative di riferimento

- D.Lgs 231/2001;
- L. 190/2012;
- D.P.R. 62/2013.

1.5.1 Politiche attuative

- PTPCT 2017-2019 approvato con deliberazione della Giunta Comunale n. 23 del 1/2/2017 e successivi aggiornamenti;
- Codice di comportamento integrativo adottato con deliberazione della Giunta Comunale n.9 del 30.01.2014.

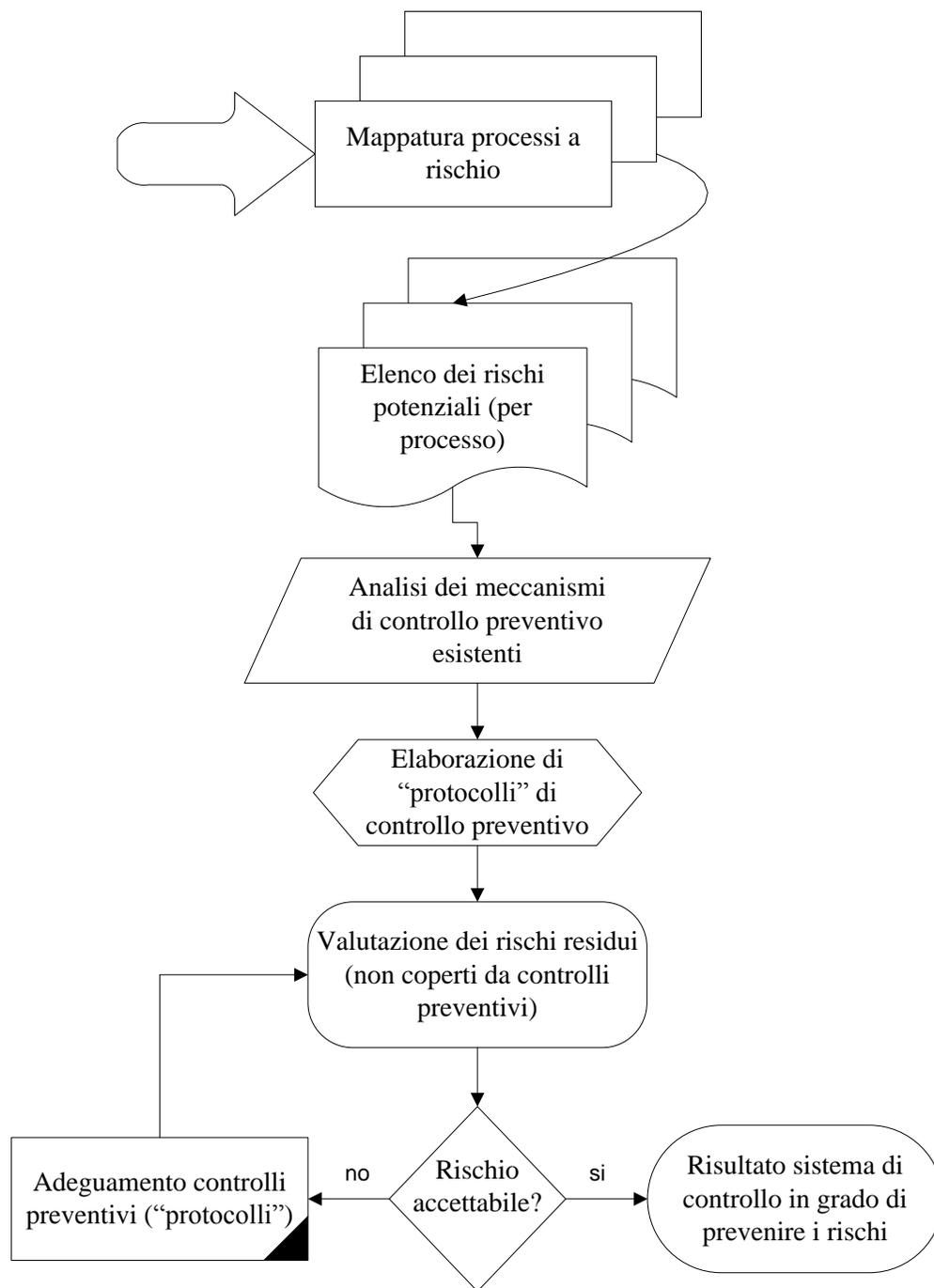
1.6 Standards internazionali di riferimento per l'attività di fraud audit

- Auditing Standard Board (ASB):
 - Statement on Auditing Standard SAS 99;
 - Consideration of Fraud in a Financial Statement Audit; October 2002;
- International Federation of Accountants (IFAC):
 - International Standard on Auditing 240;
 - The Auditors' Responsibility to Consider Fraud in an Audit of Financial Statements, February 2001;
- The Institute of internal Auditors:
 - Standard Internazionali 1210.A2;
 - Guida interpretative 1210. A2-1 Identificazione delle frodi;
 - Guida interpretative 1210. A2-2 Responsabilità per l'identificazione delle frodi;
- Confederazione Europea degli Istituti di Internal Auditing (ECIIA):
 - Position Paper, il ruolo dell'Internal Auditor nella prevenzione del controllo delle frodi;

1.7 Modello di controllo interno

Il modello di controllo interno prescelto è basato sull'integrazione strutturata dei *framework* del C.o.S.O.IC.-IF e ERM.

Il processo di gestione del rischio si sviluppa attraverso le seguenti fasi:



Lo sviluppo del sistema di controllo interno, basato sul framework contenuto negli standard emanati dal C.o.S.O. nel 1992 (*International Control Integrated Framework*), nel 2004 (*Enterprise Risk Management Framework*) e nel 2013 (*International Control - Integrated Framework*), è gestito attraverso le riflessioni e adattamenti imposti dall’ottica *anti-fraud*. Sotto questo profilo si assumono quali principi – guida le indicazioni contenute nel documento del 2004 *A Framework for Evaluating Control Exceptions and Deficiencies*. In particolare si assume che:

- solo quando i controlli sono esaminati a livello di singolo processo operativo ne è possibile una valutazione quantitativa;
- l'affidabilità dei controlli va esaminata non in relazione alle diverse componenti del sistema di controllo interno, secondo il modello del C.o.S.O., ma in relazione agli errori/frodi che possono verificarsi in uno specifico processo.

La valutazione dei rischi implica l'esplicita identificazione degli eventi negativi nonché la valutazione di probabilità e impatto a questi ascrivibile. Nella individuazione dei comportamenti attuativi un riferimento metodologico imprescindibile è costituito dai c.d. *fraud schemes*, che esplicitano le tipiche modalità attuative dei comportamenti fraudolenti. E' proprio con riferimento a tali elementi che si deve valutare chiaramente l'eventualità che siano poste in essere azioni illecite.

1.8 Criteri di identificazione e valutazione dei rischi di errori significativi

Il PTPCT 2017-2019 ha proseguito e aggiornato il processo di gestione del rischio già impostato in origine dal PTPC 2014-2016.

Il processo di identificazione, analisi e ponderazione del rischio è stato impostato sulle seguenti metodologie di *risk assessment*:

- 1) utilizzare le informazioni già in possesso dell'ambiente di controllo:
 - esperienza organizzativa acquisita
 - risultati degli audit annuali
 - relazioni degli organismi di controllo, con particolare riferimento ai pareri del collegio di revisione
 - precedenti giudiziari (procedimenti avviati e sentenze di condanna della Corte dei conti e della giurisdizione civile e penale)
 - precedenti disciplinari (procedimenti avviati e sanzioni irrogate)
 - reclami e segnalazioni interne ed esterne
 - documentazione prodotta in sede di elaborazione del PTPC precedente
- 2) utilizzare l'esperienza e le competenze del personale:
 - creazione di una *task force* multidisciplinare in grado di coordinare le attività di analisi e di sistematizzarne i risultati
 - discussioni di gruppo condotte dal Responsabile della prevenzione della corruzione con il coinvolgimento di Responsabili di Settore
 - interviste individuali di Responsabili di settore condotte dal Responsabile della prevenzione della corruzione
- 3) utilizzare le esperienze di altre pubbliche amministrazioni e le analisi di organismi nazionali e internazionali:
 - rapporti e relazioni quali, ad esempio: il Rapporto della commissione per lo studio e l'elaborazione di proposte in tema di trasparenza e prevenzione della corruzione nella pubblica amministrazione; le Relazioni della Corte dei Conti; le relazioni dell'AVCP (oggi ANAC); i Rapporti di *Transparency International*
 - per gli appalti pubblici: *Procurement Toolbox* (cassetta degli attrezzi) elaborato dall'OECD (*Organisation for Economic Co-operation and Development*); Manuale dell'OCSE sulla sensibilizzazione alla corruzione ad uso dei verificatori; "*Most common Red Flags of Fraud and Corruption in Procurement*" elaborato dalla *World Bank*; altre metodologie di *Public Procurement Risk assessment*

Le fasi principali del processo di gestione del rischio, sviluppate nel PTPCT, recependo le indicazioni di ANAC, sono le seguenti:

1. Analisi del contesto esterno ed interno (quest'ultima comprensiva della mappatura dei processi)
2. Valutazione del rischio di corruzione per processi e dei rischi specifici di corruzione
3. Trattamento dei rischi

A regime, sono destinati a essere sottoposti al sistema di controllo - *risk assessment anti fraud* i processi individuati nel PTPCT come “a rischio rilevante e critico”, con specifico riferimento alle fasi per le quali siano emersi livelli di rischio netto “Medio” o “Alto”.

1.9 Sistema di controllo interno anti-fraud

Lo sviluppo di un sistema di controllo interno, basato sul framework contenuto negli standard emanati dal C.o.S.O. nel 1992 (*International Control Integrated Framework*), nel 2004 (*Enterprise Risk Management Framework*) e nel 2013 (*International Control - Integrated Framework*), ma orientato specificamente a finalità di *crime prevention*, presuppone l'implementazione delle seguenti azioni strategiche:

- applicare meccanismi informativi e organizzativi tali da garantire elevati livelli di tracciabilità delle operazioni aziendali, mediante sistemi di documentazione delle attività che siano il più possibile delegati ai sistemi informatici e, in quanto tali, meno facilmente manipolabili;
- la necessità di orientare i controlli interni in modo rilevante verso una attività di prevenzione al compimento delle frodi e strutturare controlli successivi o *detective controls* con carattere di efficacia segnaletica e tempestività molto elevate; ciò impone di definire meccanismi e protocolli di mitigazione del rischio specifico assai stringenti e attributi informativi dei processi o fasi di processo molto puntuali, in modo da “blindare”, ex ante, l'operatività aziendale entro parametri ritenuti accettabili e consentire, ex post, l'immediata segnalazione di operazioni che possiedono caratteristiche anomale;
- utilizzare in modo massivo controlli automatizzati (*automated controls*) in quanto questi possiedono tassi di eccezioni molto bassi e sono quindi tali da garantire standard di adeguatezza nel funzionamento dei controlli molto elevati; i controlli svolti dal management e dal personale aziendale (*manual controls*) devono essere ridotti al minimo indispensabile, tipicamente là dove non esistono alternative di possibile automazione;
- utilizzare indicatori (*Key risk indicators*) le cui logiche di costruzione e di interpretazione siano tali da garantire una elevata efficacia segnaletica dei *red flag* rispetto ad anomalie che possono rivelare la presenza di una frode; in questa prospettiva, tali indicatori devono essere il più possibile “vicini” ai processi aziendali, essere raccolti e monitorati con tempestività ed essere agevolmente interpretabili, in modo che il loro valore segnaletico non si presti ad eccessiva discrezionalità.

Negli anni 2018-2019 l'attività di fraud audit sarà prioritariamente orientata alla realizzazione dei seguenti obiettivi:

- prosecuzione dell'attuazione del piano di trattamento del rischio secondo il vigente PTPCT;
- prosecuzione della prima sperimentazione del software dedicato;
- elaborazione di banche dati che consentano di sviluppare controlli automatizzati;
- sviluppo dei *Key risk indicators* e dei *red flag*.

Le disposizioni operative del processo di fraud audit saranno definite con provvedimenti del Responsabile della prevenzione della corruzione.

Nelle more della implementazione del software, il Responsabile della prevenzione della corruzione potrà avvalersi delle evidenze documentali risultanti dai controlli di Compliance.

1.10 Reporting (a regime)

Periodicità	Termine	Destinatari
Annuale	Entro il 15 dicembre di ogni anno, in occasione della predisposizione della relazione sull'efficacia delle misure di prevenzione definite dal PTPCT	Responsabili di Settore Giunta Comunale Consiglio Comunale Collegio dei Revisori Nucleo di valutazione

Sezione 2 Compliance

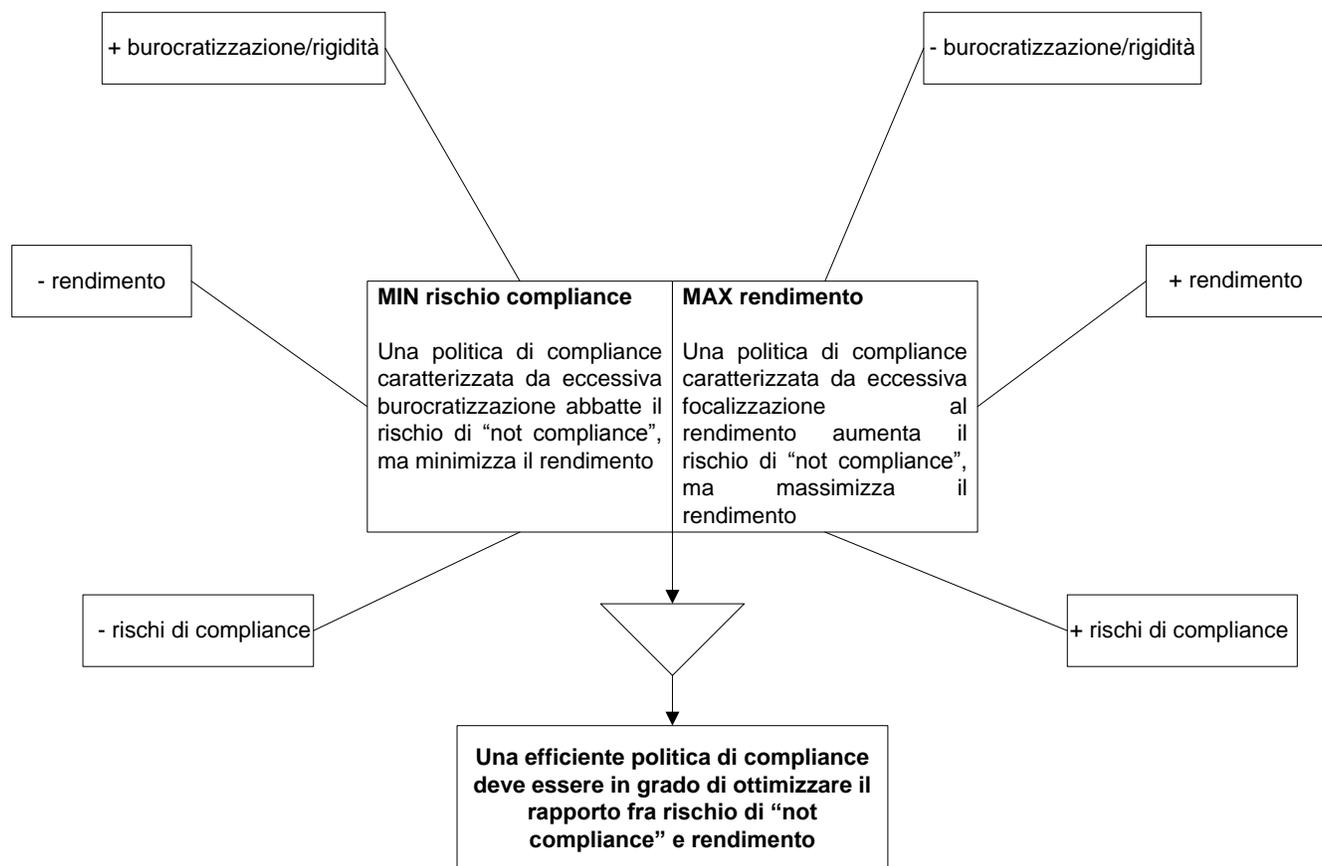
2.1 Premessa

“*Compliance*” è la conformità delle attività aziendali alle disposizioni normative, ai regolamenti, alle procedure, ai codici di condotta e alle *best practices*.

Il rischio di *not compliance* o di non conformità alle norme è il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite finanziarie rilevanti o danni reputazionali in conseguenza della violazione di norme imperative o di autoregolamentazione.

La compliance aziendale è quindi un’attività che si preoccupa di prevenire il rischio di non conformità dell’attività aziendale alle Norme, suggerendo, ove si riscontrino disallineamenti, le più opportune soluzioni. Essa è, pertanto, funzionale a prevenire il rischio di non conformità dell’attività aziendale alle norme “*laws, rules and procedures*” e a implementare e consolidare il rapporto fiduciario con gli *stakeholders*.

In termini generali, obiettivo della funzione di *compliance* è l’ottimizzazione di due fattori:



Ad una prima riflessione può apparire singolare introdurre l’approccio della *compliance* e della funzione di conformità in un Ente pubblico, che deve essere necessariamente “*compliant*” in quanto l’azione amministrativa persegue, per sua natura, l’interesse pubblico. In realtà, nonostante si sia assistito, soprattutto nell’ultimo decennio, ad un autentico proliferare di disposizioni normative,

peraltro spesso poco chiare e incoerenti quando non addirittura contraddittorie, e ad un potenziamento dei controlli esterni e degli obblighi informativi, preoccupanti fenomeni di *maladministration*, negligenza e inefficienza hanno interessato la pubblica amministrazione italiana. Occorre quindi sperimentare una nuova logica del controllo, da intendersi non quale meccanismo teso a individuare errori e a sanzionare i responsabili ma come strumento utile per migliorare le strutture organizzative e le risposte alle esigenze degli *stakeholders*, in una logica sistemica di promozione della qualità dell'azione amministrativa. Spostare, quindi, il baricentro dal "controllo per il verdetto" al "controllo per la prevenzione".

Nel nuovo sistema dei controlli delineato dal D.L. 10 ottobre 2012, n.174 un rilievo decisivo assume il controllo di regolarità amministrativa, la cui rinnovata disciplina prevede, nella fase successiva, che esso venga svolto secondo i principi di revisione aziendale. Il novellato art. 147 "Tipologia dei controlli interni" del D.lgs. 267/2000, al comma 1, stabilisce che "Gli enti locali, nell'ambito della loro autonomia normativa e organizzativa, individuano strumenti e metodologie per garantire, attraverso il controllo di regolarità amministrativa e contabile, la legittimità, la regolarità e la correttezza dell'azione amministrativa". L'art. 147 bis "Controllo di regolarità amministrativa e contabile" del D.Lgs. 267/2000, al comma 2, stabilisce che "Il controllo di regolarità amministrativa è inoltre assicurato, nella fase successiva, secondo principi generali di revisione aziendale e modalità definite nell'ambito dell'autonomia organizzativa dell'ente, sotto la direzione del segretario, in base alla normativa vigente. Sono soggette al controllo le determinazioni di impegno di spesa, i contratti e gli altri atti amministrativi, scelti secondo una selezione casuale effettuata con motivate tecniche di campionamento". L'art. 147 bis del D.Lgs. 267/2000, al comma 3, stabilisce che "Le risultanze del controllo di cui al comma 2 sono trasmesse periodicamente, a cura del segretario, ai responsabili dei servizi, unitamente alle direttive cui conformarsi in caso di riscontrate irregolarità, nonché ai revisori dei conti e agli organi di valutazione dei risultati dei dipendenti, come documenti utili per la valutazione, e al consiglio comunale".

Il legislatore, sebbene la nuova tipologia di controllo, sotto il profilo oggettivo, interessi, non già l'attività complessivamente intesa, ma singoli atti, conferma l'abbandono del modello del "controllo di legittimità", sancendo così quanto rappresentato dalla Ragioneria Generale dello Stato nell'ambito del documento "Principi di Revisione per il controllo di Regolarità Amministrativa e Contabile negli Enti Pubblici Istituzionali": "il semplice adempimento delle norme di legge comporta solo il rispetto delle modalità con le quali si deve manifestare l'azione pubblica, non necessariamente il raggiungimento dell'obiettivo che lo stesso legislatore pone a quella amministrazione". Il parametro generale di riferimento del controllo pare quindi propriamente individuabile non già nel concetto di "legittimità", ma in quello di "legalità" intesa come rispetto sostanziale, non meramente formale, della norma, come capacità di raggiungere i fini che la norma indica ed estesa alle norme tecniche di "corretta amministrazione". Si assume pertanto che il modello di controllo successivo di regolarità amministrativa cui tendere debba essere funzionale a garantire che l'Ente risponda effettivamente al modello ideale tracciato dall'art. 97 della Costituzione, quello di un apparato pubblico realmente operante sulla base dei principi di legalità, imparzialità ed efficienza.

La nuova tipologia di controllo si avvicina, sotto molteplici e rilevanti aspetti, al perimetro dei controlli sulla gestione:

- la finalità (e quindi il parametro) del controllo è quella di garantire la legittimità, la regolarità e la correttezza dell'azione amministrativa;
- è un controllo ex post;
- la "risposta/reazione", normativamente codificata, che il sistema di controllo deve assicurare, a fronte di riscontrate irregolarità, consiste nell'elaborazione di "direttive cui conformarsi",

laddove la direttiva è atto a carattere generale, che non può riguardare singoli affari e che ha ad oggetto la definizione di indirizzi unitari riguardanti l'attività amministrativa;

- misura del controllo è il referto periodico del Segretario da trasmettere ai responsabili dei servizi, ai revisori dei conti, agli organi di valutazione dei risultati dei dipendenti e al Consiglio Comunale.

Alla luce delle evidenziate connotazioni esso non può che consistere nel confronto ex-post tra la situazione effettivamente realizzata con l'attività amministrativa e la situazione ipotizzata dal legislatore come obiettivo da realizzare, in modo da verificare, ai fini della valutazione del conseguimento dei risultati, la qualità dell'azione amministrativa sotto il profilo della legalità, imparzialità ed efficienza.

La ricostruzione offerta del quadro normativo induce a ritenere che il controllo successivo di regolarità amministrativa non sia prioritariamente destinato ad incidere sull'efficacia giuridica dei singoli atti e non abbia primaria funzione sanzionatoria bensì finalistica e referente, essendo diretto a stimolare nell'Ente processi di "autocorrezione" ed evoluzioni virtuose sul piano delle decisioni strategiche, dell'organizzazione amministrativa e delle attività gestionali. Tutto ciò, ovviamente, non esclude che, in conseguenza di notizie o elementi raccolti nel corso del controllo successivo, debbano essere attivati, in relazione a singoli atti di gestione, interventi in autotutela o possano essere formalizzate responsabilità di singoli funzionari laddove gli scostamenti dai parametri di riferimento risultino censurabili.

Occorre peraltro ribadire l'esigenza di perseguire un equilibrio fra gli obiettivi che la pubblica amministrazione si dà, i rischi che possono mettere in forse la realizzazione di tali obiettivi e i controlli chiamati a presidiare il rispetto delle procedure attivate in risposta ai vari rischi identificati. Quando i controlli non sono legati ai rischi e agli obiettivi si scivola nella burocrazia; viceversa se i controlli sono troppo pochi o sono inadeguati rispetto ai rischi da presidiare, si scivola nell'inefficienza. Alla luce delle considerazioni svolte, sebbene possa apparire un paradosso, l'obiettivo del presente piano è quello di strutturare il controllo "successivo" di regolarità amministrativa come "controllo per la prevenzione" del rischio di "not compliance".

La finalità di creare, attraverso il percorso delineato, valore per l'Ente, sia in termini di contenimento del rischio di sanzioni da non conformità che in termini di rafforzamento della fiducia degli *stakeholders* nella legalità ed efficienza dell'azione amministrativa, consente di mettere a sistema il quadro delle azioni previste dal D.L. 174/2012, dalla L. 190/2012 e dal D.Lgs. 33/2013.

Il triangolo virtuoso declinato in termini di "responsabilizzazione, controllo e comunicazione/trasparenza" si pone come la via per creare una amministrazione che costi di meno e sappia lavorare meglio.

2.2 Definizione del concetto di non conformità

Definizione del concetto di "non conformità" ai fini del principio di revisione ISA 250

11. Ai fini del presente principio di revisione, il termine seguente ha il significato sotto riportato:

Non conformità – Atti di tipo omissivo o commissivo, sia intenzionali sia involontari, compiuti dall'impresa, contrari alle leggi o ai regolamenti vigenti. Tali atti includono operazioni compiute dall'impresa, o in nome o per conto dell'impresa, dai responsabili delle attività di governance, dalla direzione o dai dipendenti. La non conformità non include comportamenti non corretti personali (cioè non connessi alle attività dell'impresa), da parte dei responsabili delle attività di governance, della direzione o dei dipendenti dell'impresa.

Definizione del concetto di "non conformità" ai fini del piano di audit

Ai fini del presente piano, il termine seguente ha il significato sotto riportato:

Non conformità: Atti o procedimenti contrari alle leggi, regolamenti (esterni e interni), direttive/circolari interne, codici di condotta ecc. ma anche a disposizioni "non normative" in senso stretto, quali regole tecniche e principi di buona amministrazione.

2.3 Obiettivi della funzione di gestione del rischio di errori significativi di compliance

- Identificare nel continuo le norme applicabili;
- Tradurre le norme in processi e procedure;
- Misurare/valutare l'impatto delle norme su processi e procedure;
- "Educare" la struttura sulle disposizioni normative e regolamentari di riferimento e "addestrare" sulle attività operative messe a disposizione;
- Proporre modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati;
- Predisporre flussi informativi diretti agli organi ed alle strutture coinvolte;
- Verificare l'efficacia degli adeguamenti organizzativi (strutture, processi, procedure) suggeriti per la prevenzione del rischio di non conformità.

2.4 Definizioni

Ai fini del presente piano, i seguenti termini hanno il significato sotto riportato:

- Fattori di rischio di non conformità – Eventi, condizioni o circostanze che generano un rischio di non conformità;
- Rischio di errori significativi: possibilità che un atto o una attività relativa ad una classe di operazioni contenga un errore, dovuto a non conformità, che potrebbe essere significativo, singolarmente o insieme ad altri, indipendentemente da qualunque controllo ad essa riferito.

2.5 Disposizioni legislative di riferimento

- D.L. 174/2012 e ss.mm.ii;
- L. 190/2012 e ss.mm.ii;
- D.lgs. 33/2013 e ss.mm.ii;
- L. 241/1990 e ss.mm.ii;
- D.Lgs. 267/2000 e ss.mm.ii;

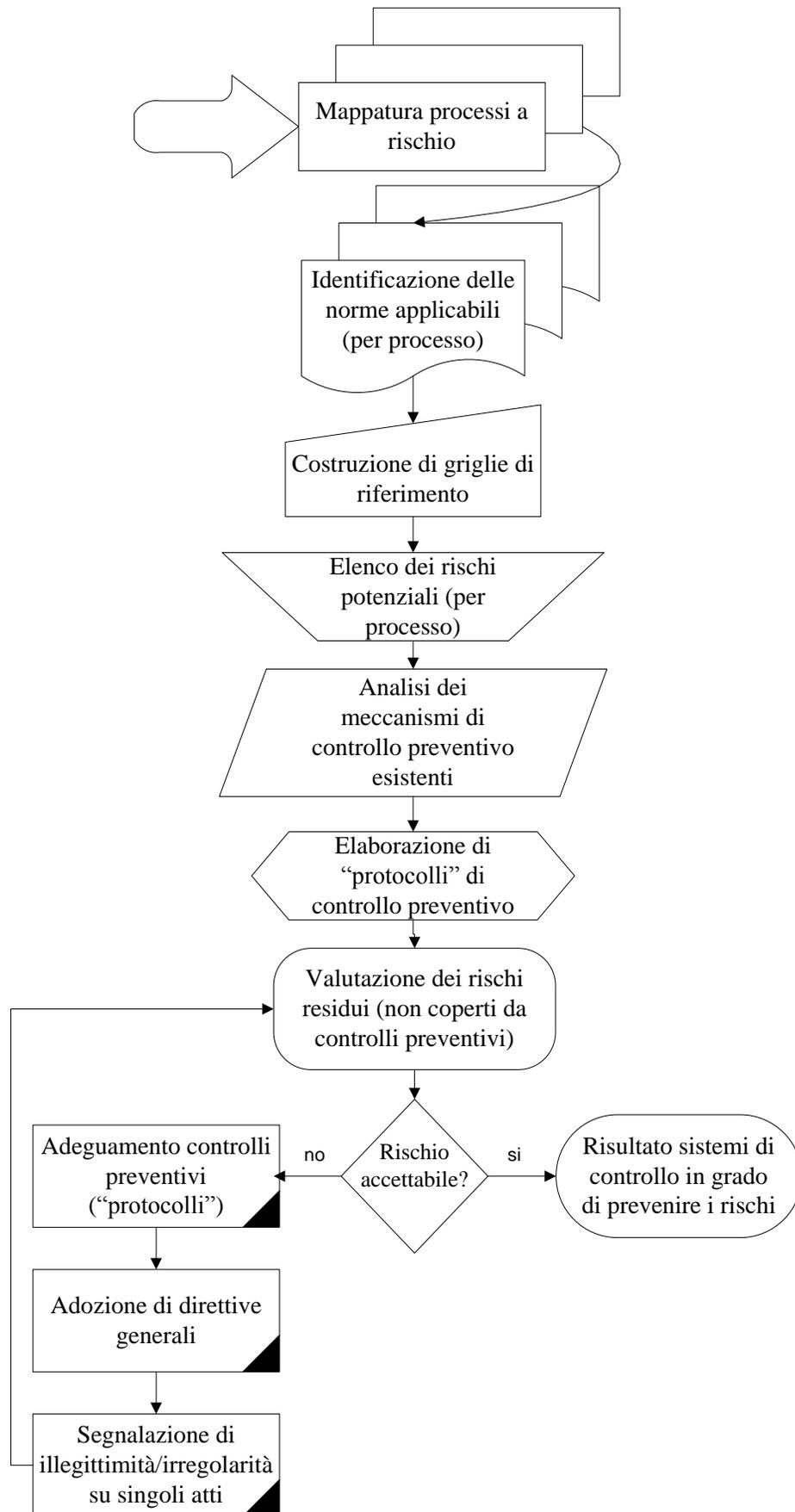
2.6 Standards internazionali di riferimento

- International Federation of Accountants (IFAC):
 - International Standard on Auditing 250.

2.7. Modello di controllo interno

Il modello di controllo interno prescelto è basato sull'integrazione strutturata dei *framework* del C.o.S.O.IC.-IF e ERM.

Il processo di gestione del rischio sarà sviluppato attraverso le seguenti fasi:



2.8 Criteri di identificazione e valutazione dei rischi di errori significativi

L'attività di *risk assessment* implica la definizione dei livelli di tolleranza (le cd. *risk tolerance*) associati alle diverse fattispecie di non compliance.

Al proposito risultano essenziali quegli indicatori (KPI, Key Performance Indicator e KRI, Key Risk Indicator) elaborati allo specifico scopo di garantire una elevata efficacia segnaletica dei c.d. *red flag*, cioè di quelle anomalie che possono rivelare la presenza errori significativi.

La progettazione degli indicatori, la definizione dei livelli di tolleranza e dell'elenco dei rischi potenziali per processo, costituirà il fulcro dell'attività dell'unità deputata al controllo e i relativi esiti confluiranno negli aggiornamenti del presente piano.

Tali attività verranno realizzate sulla base del metodo già sviluppato per il *risk assessment anti fraud*. Nel caso specifico dei controlli di conformità si tratterà, pertanto, di applicare l'approccio sviluppato sull'analisi dei rischi nella progettazione dei controlli riguardanti le disposizioni (normative, regolamenti, procedure, ...) alle quali il Comune adempie su base obbligatoria o volontaria.

Nell'esercizio 2018, nelle more esiti del completamento della elaborazione ed applicazione della metodologia di *risk assessment* all'area *compliance*, la identificazione dei processi a rischio è operata assumendo quale criterio la predeterminazione del grado di rischiosità delle classi di attività di competenza dell'amministrazione, operata dalla Corte dei Conti - Sezione Autonomie nell'ambito delle linee guida per il referto semestrale del Sindaco per i Comuni con popolazione superiore ai 15.000 abitanti sulla regolarità della gestione e sull'adeguatezza ed efficacia del sistema dei controlli interni (linee guida allegate alla delibera n. 4/2013/SEZAUT/INPR). Nel menzionato documento la Corte dei Conti stabilisce che "*nelle linee - guida, alle quali i vertici politici degli enti dovranno informare le proprie relazioni semestrali, è necessario prendere in considerazione la regolare osservanza delle norme che disciplinano il settore degli appalti pubblici, le spese di funzionamento, la gestione del patrimonio immobiliare e gli altri ambiti di gestione di maggior rilievo finanziario*".

In considerazione del fatto che:

- gli appalti pubblici (intesi in senso ampio) sono individuati, nelle menzionate linee guida, come la prima delle aree sulle quali le autonomie locali dovranno concentrare il controllo;
- gli appalti pubblici (intesi in senso ampio) rappresentano l'ambito di gestione di maggior rilievo finanziario nel bilancio comunale;
- in una logica di economie di scopo derivanti dall'integrazione dei diversi ambiti di controllo (compliance integrata), le attività di controllo interno con finalità di *compliance* sono complementari alle attività di controllo interno con finalità *anti - fraud*

si conferma prioritariamente quale processo sottoposto a controllo *risk assessment compliance* per l'anno 2018 "Approvvigionamento di lavori, servizi e forniture".

Al fine di rendere maggiormente incisiva l'attività di controllo e di razionalizzare l'impiego delle relative risorse, si concentrerà l'attenzione sui processi di approvvigionamento maggiormente significativi, e quindi: da un lato si escluderanno dal controllo i processi di approvvigionamento di valore meno significativo (micro-affidamenti) che vengono qui definiti come gli affidamenti di importo inferiore a 5.000 €; dall'altro lato si agirà sulle percentuali di campionamento, che – per i restanti processi di approvvigionamento – saranno differenziate in ragione del valore dell'importo (cfr. § 2.10). Inoltre, al fine di acquisire risultanze significative, si ritiene opportuno, nelle more del completamento della elaborazione ed applicazione della metodologia di *risk assessment* all'area *compliance*, proseguire l'attività di controllo sui processi già individuati nell'ambito dei precedenti piani triennali di audit, sulla base delle check list elaborate dal Segretario Generale.

Processi sottoposti a controllo - *compliance* – anno 2018:

1. Approvvigionamento di lavori, servizi e forniture di importo pari o superiore a 5.000 €;

2. Concorsi e prove selettive per l'assunzione del personale;
3. Concessione ed erogazione di sovvenzioni, contributi, sussidi e ausili finanziari e attribuzione di vantaggi economici di qualunque genere a persone, enti pubblici e privati;
4. Permessi di costruire.

2.9 Campionamento

In termini generali la prospettiva compliance nelle pubbliche amministrazioni richiede che le conclusioni cui si perviene siano assai rigorose e dotate di un livello di affidabilità molto elevato. Ciò implica la preferenza per due direzioni significative ma diverse:

- effettuazione di campionamenti mediante parametri statistici assai stringenti, con la conseguenza di progettare dimensioni campionarie importanti;
- l'impiego di controlli automatizzati che possono essere svolti sull'intera popolazione, rinunciando ad un approccio campionario.

In relazione alle attuali potenzialità dell'ambiente di controllo, si ritiene l'approccio campionario (con stratificazione della popolazione) maggiormente efficiente in termini di costi - benefici attesi. Si applicano le disposizioni di cui al Titolo III par.3.

Quanto all'entità delle dimensioni campionarie si richiama inoltre quanto precisato al paragrafo precedente in merito alla esigenza – parimenti fondamentale – di razionalizzazione delle risorse disponibili, da perseguire anche mediante la selezione dei processi economicamente più significativi e la differenziazione del campionamento in base al valore del relativo importo.

La periodicità del campionamento è definita su base trimestrale a decorrere dal 01.01.2018.

2.10 Individuazione della popolazione e suddivisione in sotto-popolazioni – Percentuale di campionamento

Anno 2018

Processo	Popolazione	Sotto-popolazione	Percentuale di campionamento
Approvvigionamento di lavori, servizi e forniture di importo pari o superiore a 5.000 €.	Determinazioni dirigenziali	- Determinazioni a contrarre, ivi comprese proroghe ed eventuali rinnovi; - Determinazioni di aggiudicazione definitiva; - Determinazioni di approvazione dei SAL, di atti di collaudo e certificati di regolare esecuzione; - Determinazioni di approvazione di varianti, ivi comprese quelle riguardanti la "revisione prezzi in corso d'opera" e quelle riguardanti "maggiori/ opere ad integrazione dell'aggiudicazione iniziale autorizzate"; - Determinazioni di autorizzazione ai subappalti; - Determinazioni in autotutela.	40% della Sotto-Popolazione relativamente ad affidamenti di importo superiore a 40.000 €; 20% della Sotto-Popolazione relativamente ad affidamenti di importo compreso fra 20.000 € e 40.000 €; 10% della Sotto-Popolazione relativamente ad affidamenti di importo fino a 20.000 €.
	Contratti	- Contratti in forma di scrittura privata.	40% della Sotto-Popolazione
Concorsi e prove selettive per l'assunzione del personale	Determinazioni dirigenziali	- Determinazioni di approvazione dei bandi di concorso;	10% della Sotto-Popolazione

		- Determinazioni di approvazione delle graduatorie.	
Concessione ed erogazione di sovvenzioni, contributi, sussidi e ausili finanziari e attribuzione di vantaggi economici di qualunque genere a persone, enti pubblici e privati	Determinazioni dirigenziali/decisioni direzione Istituzioni	Determinazioni di Concessione ed erogazione di sovvenzioni, contributi, sussidi e ausili finanziari e attribuzione di vantaggi economici di qualunque genere a persone, enti pubblici e privati.	10% della Sotto-Popolazione
Permessi di costruire	Permessi di costruire	Permessi di costruire	10% della Sotto-Popolazione

In relazione a ciascun elemento campionato, verrà esaminato l'intero processo, limitatamente alle operazioni compiute nel corso dell'anno di riferimento e fino alla data di campionamento.

Anno 2019

Da definirsi in sede di aggiornamento del presente Piano.

2.11 Reporting

Periodicità	Termine	Destinatari
Trimestrale	Entro il terzo mese successivo al trimestre di riferimento	Responsabili di Settore Giunta Comunale Consiglio Comunale Collegio dei Revisori Nucleo di valutazione