



ENA210000871531

FONDAZIONE
ENASARCO



Servizio Internal Audit

Politica Antifrode

AZ

Sommario

| | |
|---|-----------|
| 1. DICHIARAZIONE ANTI-FRODE | 3 |
| 2. DEFINIZIONI..... | 3 |
| 3. FRAUD GOVERNANCE | 4 |
| A. RUOLI E RESPONSABILITÀ | 4 |
| i. Consiglio di Amministrazione..... | 4 |
| ii. Servizio Internal Audit | 4 |
| iii. Ufficio Controllo del Rischio..... | 4 |
| iv. Dirigenti | 5 |
| v. Servizio Analisi Organizzative e Reportistica..... | 5 |
| vi. Servizio Risorse Umane..... | 5 |
| vii. Ufficio Controllo di Conformità..... | 5 |
| viii. Ufficio Comunicazione | 5 |
| ix. Impiegati | 6 |
| B. RELAZIONE TRA ALTRE POLICY/CODICI DI CONDOTTA AZIENDALI..... | 6 |
| 4. FRAUD RISK ASSESSMENT | 6 |
| A. OBIETTIVI DEL FRAUD RISK ASSESSMENT | 6 |
| B. METODOLOGIA DEL FRAUD RISK ASSESSMENT..... | 6 |
| C. PARTECIPANTI..... | 6 |
| D. RISULTATI E REPORT..... | 6 |
| 5. ATTIVITÀ DI CONTROLLO..... | 7 |
| A. CONFLITTO DI INTERESSI..... | 7 |
| B. SEPARAZIONE DELLE FUNZIONI | 7 |
| C. ATTIVITÀ DI VERIFICA DEI CONTROLLI ANTIFRODE | 7 |
| i. Verifiche ispettive e documentali..... | 7 |
| ii. Data Analytics..... | 7 |
| D. WHISTLEBLOWING | 7 |
| E. ATTIVITÀ FORMATIVE..... | 7 |
| 6. CANALI INFORMATIVI | 7 |
| 7. ATTIVITÀ INVESTIGATIVE..... | 9 |
| A. AZIONI DISCIPLINARI | 9 |
| B. AZIONI CORRETTIVE | 9 |
| 8. MONITORAGGIO | 10 |

42

1. Dichiarazione Anti-Frode

La Fondazione Enasarco (di seguito "**Fondazione**") si impegna a contrastare qualsiasi tipo di Frode e a tal fine adotta e implementa un sistema di gestione del rischio frode (di seguito "**Fraud Risk Management**") i cui principi ed elementi costitutivi sono descritti nella presente Politica Antifrode (di seguito "**Policy**").

Tutti gli impiegati, Dirigenti e i componenti del Consiglio di Amministrazione (di seguito "**Personale**") nonché tutti i collaboratori esterni (di seguito "**Terzi Destinatari**") sono obbligati a rispettare proattivamente la Policy. La Fondazione richiede che il Personale e i Terzi Destinatari adottino una condotta conforme al Codice Etico ex D.Lgs. 231/2001 (di seguito "**Codice Etico**") ai cui principi si rimanda.

I componenti del Consiglio di Amministrazione (di seguito "**CdA**") e i Dirigenti devono essere da esempio per gli impiegati della Fondazione e per i suoi collaboratori.

Ogni violazione sarà perseguita ai sensi della normativa vigente.

Tutte le policy, le procedure, i documenti e i moduli relativi al Fraud Risk Management sono pubblicati in un'apposita sezione dell'intranet aziendale. La seguente Policy è pubblicata nella sezione *Amministrazione Trasparente* del sito istituzionale.

2. Definizioni

La **Frode**¹ è definita come "qualsiasi atto od omissione intenzionale destinato ad ingannare la controparte e che determini per la Fondazione una perdita e/o per il frodatore il raggiungimento di un guadagno" ed è identificabile nelle seguenti quattro fattispecie:

- *Corruzione*, definita come qualsiasi schema di frode in cui un impiegato abusa della sua influenza in un'operazione aziendale in modo da violare i suoi obblighi con il proprio datore di lavoro allo scopo di ottenere benefici diretti o indiretti
- *Appropriazione indebita dei beni*, definita come qualsiasi schema di frode con cui un impiegato ruba o abusa di risorse dell'organizzazione aziendale.
- *Dichiarazioni finanziarie fraudolente* intese come qualsiasi schema di frode in cui un impiegato intenzionalmente determina una dichiarazione falsa o un'omissione di informazioni nelle dichiarazioni finanziarie aziendali;
- *Dichiarazioni non finanziarie fraudolente*: intese come qualsiasi schema di frode in cui un impiegato intenzionalmente determina false rappresentazioni di informazioni non finanziarie (e.g. falsa attestazione di presenza, falso giustificativo di assenza, etc.)

La presente Policy definisce il **Whistleblowing** (segnalazione anonima) quale "segnalazione di una condotta potenzialmente fraudolenta in danno alla Fondazione". La Fondazione riconosce il Whistleblowing quale strumento più forte e più efficiente contro la Frode e incoraggia tutto il Personale a segnalare ogni evento o comportamento potenzialmente fraudolento tramite questo strumento.

¹ La definizione di Frode e la sua tassonomia sono conformi al Fraud Risk Management Framework emanato dal CoSO. ("Committee of Sponsoring Organization of the Treadway Commission"), Commissione indipendente USA sponsorizzata dalle maggiori associazioni professionali e industriali. Ha prodotto nel 1992 il "CoSO Report - Internal Control" aggiornato nel 2013 e nel 2004 il "CoSO Report - ERM, an integrated framework" aggiornato nel 2017. Ad ottobre 2016 ha pubblicato un framework specifico per le frodi il "Fraud Risk Management Guide" (Cfr. <https://www.coso.org>)

3. Fraud Governance

A. Ruoli e responsabilità

Tutto il Personale, indipendentemente dal proprio ruolo o posizione, è responsabile del rispetto proattivo della Policy e dovrà aiutare la Fondazione a prevenire e/o individuare condotte o eventi a rischio Frode.

All'interno della Fondazione sono individuati ruoli per i quali sono previste specifiche responsabilità propedeutiche a un maggior efficienza ed efficacia del Fraud Risk Management:

i. Consiglio di Amministrazione

Il CdA è responsabile dell'attuazione del Fraud Risk Management. Nello specifico:

- a) Approva la Policy mediante apposita delibera. Si impegna a rispettare la Policy improntando le sue attività nel rispetto dei principi del Codice Etico e si assicura che essa sia rispettata dai Dirigenti
- b) Supervisiona annualmente il Fraud Risk Management attraverso specifiche informative del Servizio Internal Audit valutando eventuali modifiche alla Policy
- c) Determina il livello di rischio di Frode accettabile
- d) Supervisiona l'operato del Fraud Risk Assessment Team di cui al punto 4 attraverso comunicazioni periodiche del Servizio Internal Audit
- e) Supervisiona l'attività del Team Investigativo di cui al punto 7 attraverso comunicazioni tempestive da parte del Servizio Internal Audit

ii. Servizio Internal Audit

Il Servizio di Internal Audit fornisce un'attività di assurance e consulenza volta a valutare e migliorare il Fraud Risk Management. Nello specifico:

- a) Il Servizio Internal Audit ha pieno accesso ai dati e alle risorse della Fondazione e piena collaborazione da tutto il Personale.
- b) Avvia e dirige il Fraud Risk Assessment di cui al punto 4 e periodicamente relaziona i relativi esiti al CdA.
- c) Effettua attività periodiche di Fraud Prevention di cui al punto 5.C e periodicamente relaziona i relativi esiti al CdA.
- d) Riceve le segnalazioni di potenziali frodi attraverso i canali previsti dalla Policy.
- e) Avvia e dirige l'attività del Team Investigativo di cui al punto 7 relazionandone gli esiti al CdA.
- f) Propone al Presidente del CdA l'eventuale incarico di un consulente esterno in possesso di specifiche competenze professionali di cui al punto 7.
- g) Relaziona annualmente il CdA in merito all'andamento del Fraud Risk Management proponendo eventualmente modifiche alla Policy.
- h) Offre supporto e consulenza al Servizio Analisi Organizzative e Reportistica nella redazione di apposite procedure o altri documenti di qualità costituenti il Fraud Risk Management.

iii. Ufficio Controllo del Rischio

L'Ufficio Controllo del Rischio ha il compito di valutare il rischio Frode e le modalità con cui la Fondazione gestisce tale rischio. Nello specifico:

- a) Partecipa al Fraud Risk Assessment di cui al punto 4 e monitora l'implementazione delle azioni correttive individuate.
- b) Registra e comunica al Servizio Internal Audit i rischi di frode emersi durante il processo formalizzato dalla procedura P18.2 "Analisi e gestione dei rischi connessi con il contesto in

cui opera la Fondazione Enasarco e con i processi aziendali" (ss.mm.ii) e mappati nel Modulo P18.2-M1, ovvero di ulteriori eventuali altre procedure similari emanate.

- c) Effettua specifici risk assessment analitici su richiesta del Fraud Risk Assessment Team di cui al punto 4.

iv. Dirigenti

Tutti i Dirigenti della Fondazione hanno la responsabilità dell'adozione del Fraud Risk Management nei propri Servizi. Nello specifico:

- a) Promuovono la cultura etica e si assicurano che tutti i propri collaboratori conoscano e rispettino la Policy e il Codice Etico.
- b) Partecipano al Fraud Risk Assessment di cui al punto 4 e al Team Investigativo di cui al punto 7.
- c) Si assicurano dell'esecuzione delle attività di controllo di cui al punto 5 previste per i propri Servizi e qualora riscontrassero possibili miglioramenti provvedono a informare il Servizio Internal Audit.
- d) Si assicurano che le azioni correttive indicate a seguito del Fraud Risk Assessment siano implementate all'interno dei propri processi.

v. Servizio Analisi Organizzative e Reportistica

Il Servizio Analisi Organizzative e Reportistica è responsabile dell'analisi dei processi organizzativi operativi (attività svolte, forza lavoro, risorse dedicate) al fine di individuarne le opportunità/azioni di miglioramento, con conseguente elaborazione di documenti di qualità eventualmente propedeutici al Fraud Risk Management e partecipa al Fraud Risk Assessment di cui al punto 4.

vi. Servizio Risorse Umane

Il Servizio Risorse Umane:

- a) Promuove la cultura etica e anti Frode attraverso la promozione di appositi corsi di formazione e di aggiornamento nei confronti di tutto il Personale
- b) Periodicamente valuta la cultura anti Frode della Fondazione attraverso questionari anonimi al Personale
- c) Effettua indagini su eventuali precedenti giudiziari in fase preassuntiva della risorsa nel pieno rispetto di quanto previsto nel GDPR ed in relazione ~~alle specifiche~~ particolari mansioni cui la risorsa sarà impegnata.
- d) Effettua interviste alle risorse che lasciano la Fondazione al termine del contratto di lavoro o in seguito a dimissioni volte a raccogliere eventuali segnalazioni di sospette Frodi
- e) Partecipa al Team Investigativo di cui al punto 7

vii. Ufficio Controllo di Conformità

L'Ufficio Controllo di Conformità:

- a) Esprime pareri sulla conformità delle eventuali attività di controllo da implementare alla normativa nazionale
- b) Esprime primi pareri sulla rilevanza delle eventuali violazioni della Policy in termini di responsabilità civile e penale

viii. Ufficio Comunicazione

L'Ufficio Comunicazioni è responsabile della comunicazione del Fraud Risk Management secondo quanto stabilito dal piano di comunicazione

ix. Impiegati

Gli impiegati improntano la loro attività quotidiana sui principi della Policy e del Codice Etico. Nello specifico:

- a) Partecipano ai corsi di formazione anti Frodi promossi dal Servizio Risorse Umane
- b) Segnalano casi di sospetta Frode attraverso i canali previsti dalla Policy
- c) Partecipano al Fraud Risk Assessment di cui al punto 4 se necessario
- d) Cooperano con il Team Investigativo.

B. Relazione tra altre Policy/Codici di Condotta aziendali

Tutto il Personale e i Terzi Destinatari si impegnano a comprendere e rispettare la presente Policy che integra ed è integrata dal Codice Etico, altre policy, procedure e qualsiasi altro documento di qualità della Fondazione.

4. Fraud Risk Assessment

A. Obiettivi del Fraud Risk Assessment

Il Fraud Risk Assessment (di seguito "FRA") è l'attività con cui la Fondazione identifica i rischi di Frode di cui può essere vittima, valuta gli eventuali presidi posti in difesa da essi e determina il rischio residuo in modo da gestirlo nei termini del livello di rischio accettato dal CdA.

Oggetto del FRA dovranno essere i rischi di Frode di cui al punto 2 compreso il rischio di aggiramento dei controlli anti Frode.

B. Metodologia del Fraud Risk Assessment

Il FRA è effettuato da un apposito Team periodicamente e comunque ogni volta che si reputerà necessario in seguito al manifestarsi di una frode, al mutamento delle caratteristiche organizzative della Fondazione o a specifica richiesta inoltrata al Servizio Internal Audit.

La metodologia di analisi di tipo risk based coincide con le metodologie utilizzate dall'Ufficio del Controllo del Rischio (approccio bottom-up o top-down).

La direzione del Team è affidata al Servizio Internal Audit.

C. Partecipanti

Il Team è composto almeno dal Servizio Internal Audit, dal Servizio Analisi Organizzative e Reportistica, dall'Ufficio Controllo del Rischio e dal Dirigente del Servizio oggetto di FRA.

A seconda delle esigenze e dall'ampiezza del FRA può essere coinvolto personale del Servizio oggetto di FRA nonché altri Servizi/Uffici della Fondazione così come eventuali consulenti esterni.

D. Risultati e report

Al termine del FRA è compilata una matrice dei rischi contenente l'identificazione dei rischi di Frode, loro quantificazione, le attività di controllo anti Frode esistenti, il rischio residuo e le eventuali azioni correttive individuate. Tale documento:

- a) Costituisce lo strumento mediante cui l'Ufficio Controllo del Rischio effettua il monitoraggio dell'adozione delle azioni correttive
- b) Costituisce lo strumento mediante cui il Servizio Internal Audit effettua verifiche di fraud prevention e/o fraud detection ossia verifiche preventive o investigative.
- c) Costituisce il punto di partenza per il successivo FRA

Periodicamente il Servizio Internal Audit relaziona sulle attività svolte al CdA.

5. Attività di controllo

Al termine di ogni FRA il Team individua per ogni rischio di Frode le attività da implementare per gestire il rischio residuo, coerentemente con le indicazioni del CdA.

Le attività di controllo sono classificate in due categorie:

- *Fraud Prevention* (preventive) se sono finalizzate a prevenire l'insorgenza della frode. Possono essere di molteplici tipologie: separazione dei ruoli e delle deleghe, presidi per gli accessi fisici e accessi logici, questionari anonimi al personale, alert automatici bloccanti e non, etc.
- *Fraud Detection* (investigative) se sono volte a scoprire la frode dopo che essa ha avuto origine e sono disegnate per identificare le tentate frodi o individuare quelle ancora in essere.

Ogni Struttura organizzativa durante il FRA collabora con il Team alla valutazione dell'efficacia dei presidi di controllo esistenti e all'individuazioni di nuove tipologie di meccanismi di controllo.

A. Conflitto di interessi

La Fondazione si è dotata di un Regolamento per la Gestione dei Conflitti di Interesse al quale si rinvia

B. Separazione delle funzioni

La Fondazione riconosce l'importanza di un'attenta separazione dei ruoli e delle deleghe.

Ogni cambiamento dell'organizzazione aziendale deve assicurare il rispetto di questo principio.

C. Attività di verifica dei controlli antifrode

i. Verifiche ispettive e documentali

Il Servizio Internal Audit effettua verifiche ispettive e documentali volte a valutare e migliorare i presidi di controllo antifrode esistenti.

ii. Data Analytics

Il Servizio Internal Audit effettua periodicamente attività di data analytics sia in ottica di Fraud Prevention sia in ottica di Fraud Detection.

La Fondazione implementa all'interno dei processi sensibili attività di data analytics come controlli di primo livello sia in ottica di Fraud Prevention sia in ottica di Fraud Detection.

D. Whistleblowing

Il processo di segnalazione mediante whistleblowing è disciplinato da apposita policy alla quale si rimanda.

E. Attività formative

La Fondazione adotta specifiche attività formative verso il Personale aventi come scopo la descrizione del Fraud Risk Management e della cultura antifrode.

6. Canali informativi

La Fondazione invita il Personale e i Terzi Destinatari a segnalare ogni anomalia potenzialmente riconducibile a comportamenti fraudolenti e assicura la loro protezione da eventuali azioni di ritorsione: ogni eventuale azione di ritorsione nei confronti del soggetto segnalante sarà oggetto di sanzioni disciplinari

La segnalazione può avvenire tramite i seguenti canali:

- Comunicazione diretta al proprio Responsabile che provvederà a inoltrare la segnalazione al Servizio Internal Audit
- Via posta utilizzando il seguente indirizzo: Fondazione Enasarco – Riservata Servizio Internal Audit, via Antoniotto Usodimare 31, 00154 Roma.
- Via email al Servizio Internal Audit alla seguente casella di posta elettronica accessibile esclusivamente dal personale in forze al Servizio Internal Audit: internal.auditing@pec.enasarco.it
- Whistleblowing

Indifferentemente dal canale scelto, qualsiasi segnalazione sarà oggetto delle tutele previste per il whistleblowing. La Fondazione comunica al segnalatore i progressi relativi all'analisi della segnalazione, eventuali investigazioni e conclusioni ed eventuali azioni correttive intraprese.

La Fondazione comunica al Personale e ai Terzi Destinatari i principi stabiliti dalla presente Policy.

7. Attività investigative

Qualora si rendesse necessaria un'investigazione essa sarà effettuata da un Team coordinato dal Servizio Internal Audit al quale partecipa almeno il personale appositamente individuato del Servizio Risorse Umane.

Qualora la natura della segnalazione lo richieda, ovvero siano presenti delle concrete ipotesi di reato, il Dirigente del Servizio Internal Audit propone al Presidente del CdA la partecipazione di un consulente esterno in possesso di specifiche competenze professionali.

Qualora l'investigazione riguardi una figura dirigenziale ovvero si rilevino dei profili di particolare riservatezza il Dirigente del Servizio Internal Audit può chiedere al Presidente del CdA che essa sia svolta direttamente da un consulente esterno.

Il Presidente del CdA fornirà successiva informativa al CdA.

La supervisione di un consulente esterno in possesso di specifiche competenze professionali diventa necessaria qualora l'indagine riguardi membri del CdA

La disciplina dell'azione investigativa è inclusa nel Fraud Response Plan al quale si rinvia.

A. Azioni disciplinari

Al termine dell'investigazione il Servizio Risorse Umane valuta l'adozione di azioni disciplinari che sono sottoposte alla Direzione Generale per l'approvazione e la successiva erogazione, così come previsto dallo Statuto della Fondazione e dalla contrattazione collettiva.

Al termine dell'investigazione la Direzione Generale valuta e propone al Presidente del CdA l'avvio di azioni legali volte ad accertare eventuali responsabilità civili e penali a tutela della Fondazione

B. Azioni correttive

Il Team investigativo propone al Direttore Generale o se necessario al Presidente un piano di azione contenente una o più azioni che sono reputate opportune in seguito alla conclusione dell'indagine. Esse possono consistere in:

- **Correzione dei controlli interni** aventi lo scopo di mitigare il rischio che simili Frodi accadano in futuro
- **Correzione dei processi aziendali** attraverso una loro reingegnerizzazione allo scopo di ridurre l'opportunità del compimento di Frodi simili
- **Formazione** sul Fraud Risk Management allo scopo di aumentare la cultura anti Frode
- **Nuove azioni investigative** aventi lo scopo di individuare se frodi simili sono in corso in altre aree della Fondazione
- **Azioni di risarcimento civile**
- **Denuncia penale alle Autorità competenti**

La Fondazione adotterà in maniera chiara e netta qualsiasi azione reputi adeguata alle circostanze.

8. Monitoraggio

La Fondazione implementa varie attività di monitoraggio del Fraud Risk Management volte a garantirne la sua esecuzione e la sua efficienza. Tali attività sono svolte sia in maniera continua, attraverso controlli informatici o attività di data analytics, sia periodicamente, attraverso le attività di cui al punto 5.B

La Fondazione adotta criteri semplici e oggettivi per misurare l'efficacia del Fraud Risk Management. Essi possono includere:

- Ratio tra numero di segnalazioni ricevute e numero di segnalazioni meritevoli di investigazione
- Ratio tra potenziali frodi investigate e frodi scoperte
- Numero di segnalazioni ricevute tramite i vari canali informativi
- Numero di dipendenti oggetto di corsi di formazione

Periodicamente, e comunque almeno una volta l'anno, il Servizio Internal Audit relaziona al CdA l'andamento e l'efficacia del Fraud Risk Management.