



Presidenza del Consiglio dei Ministri
**Dipartimento della
Funzione Pubblica**

ESPERI@
ALTA FORMAZIONE SPECIALISTICA
E-LEARNING



Il risk management e le sue fasi

Formez_{PA}

Questo materiale didattico rientra nell'ambito dei Percorsi e-Learning di alta formazione specialistica del Progetto Esperia@ - Rafforzamento della capacità istituzionale ed amministrativa delle Regioni e degli Enti Locali del Mezzogiorno mediante il reclutamento di nuove figure professionali - Linea 7 Alta Formazione.

Finanziamento: Programmazione 2007 – 2013

Questo materiale è distribuito con Licenza [Creative Commons Attribuzione - Condividi allo stesso modo 4.0 Internazionale](https://creativecommons.org/licenses/by-sa/4.0/).



Autore: Maria Scinicariello

Creatore: Formez PA

Diritti: Dipartimento della Funzione Pubblica

Data: Settembre 2017

Il risk management e le sue fasi

Il concetto di rischio

Al fine di illustrare il processo di gestione del rischio (risk management), è necessario, in prima battuta, fornire dei chiarimenti terminologici sul concetto di “rischio”.

Nell’uso comune, il termine rischio è associato alla possibilità che si verifichi un fatto, una situazione dai quali si genera un danno. Tuttavia, nelle scienze economiche, il rischio assume non solo la suddetta accezione negativa, ma anche un significato positivo: in particolare, l’approccio manageriale interpreta il rischio come possibile scostamento rispetto agli obiettivi, attribuendogli sia una valenza di minaccia – scostamento negativo – che di opportunità – scostamento positivo. Tra gli standard di risk management, riconducibili all’approccio manageriale, lo standard internazionale ISO 31000:2009 definisce il rischio come “effect of uncertainty on objectives”, e di un decennio prima è la definizione che interpreta i rischi come “eventi futuri e incerti che possono influenzare il raggiungimento degli obiettivi strategici, operativi e finanziari di un’istituzione”. Un approccio simile a quello manageriale è quello definito pessimistico-manageriale, che condivide la visione del rischio come scostamento dagli obiettivi, ma vi attribuisce solo una valenza di minaccia. Tra gli standard più conosciuti e diffusi che hanno adottato tale approccio vi è il CoSO ERM, il quale sostiene che “eventi con impatti negativi costituiscono rischi che possono ostacolare la creazione di valore o erodere quello esistente”.

Definizione di rischio

Nonostante la mancanza di una visione univoca sul concetto di rischio, è possibile identificare tre elementi che lo caratterizzano:

1. il verificarsi di un evento,
2. l’incertezza sul se e sul quando l’evento si realizzerà,
3. la presenza di un effetto che origina dal suddetto evento.

Da ciò è possibile definire il rischio come la combinazione tra la probabilità che un determinato evento si verifichi e le conseguenze (impatto/danno) che questo evento provoca al suo realizzarsi.

Rispetto alle conseguenze, si è visto, dunque, che è possibile identificare due diverse dimensioni del rischio:

- il rischio nelle sue manifestazioni negative, noto anche come *downside risk*,
- il rischio nelle sue manifestazioni positive, noto anche come *upside risk*.

Gestire il rischio, quindi, significa agire sulla probabilità di accadimento di un evento e/o sulle sue conseguenze negative o positive.

Concetto di frode

Prendendo come riferimento la Convenzione relativa alla tutela degli interessi finanziari della Comunità europea, si definisce "frode", in materia di spese, qualsiasi azione od omissione intenzionale relativa:

- all'utilizzo o alla presentazione di dichiarazioni o documenti falsi, inesatti o incompleti cui consegue il percepimento o la ritenzione illecita di fondi provenienti dal bilancio generale della Comunità europea o dai bilanci gestiti dalla Comunità europea o per conto di essa;
- alla mancata comunicazione di un'informazione in violazione di un obbligo specifico cui consegue lo stesso effetto;
- alla distrazione di tali fondi per fini diversi da quelli per cui essi sono stati inizialmente concessi.

Concetto di corruzione

Il concetto di corruzione, utilizzato nell'ambito della normativa nazionale anticorruzione (legge 190/2012 e successive norme), integra alla sola accezione penalista, riconducibile allo specifico reato di corruzione e al complesso dei reati contro la pubblica amministrazione, il concetto più ampio di "*maladministration*", intesa come assunzione di decisioni devianti dalla cura dell'interesse generale a causa del condizionamento improprio da parte di interessi particolari.

Il riferimento, pertanto, è ad atti e comportamenti che, anche se non consistenti in specifici reati, costituiscono una deviazione intenzionale dal perseguimento e dalla tutela dell'interesse pubblico.

Il parametro di riferimento rispetto al quale si può valutare la deviazione del comportamento è costituito non solo da "regole giuridiche", ma anche da "regole etiche e morali" ritenute rilevanti in un determinato contesto.

Anche la definizione di corruzione utilizzata dalla Commissione europea – riportata nelle "Linee guida EGESIF sulla valutazione dei rischi di frode e misure antifrode efficaci e proporzionate" del giugno 2014 –, ha un'accezione ampia e coincide con "l'abuso di potere (pubblico) ai fini di un profitto privato".

Il concetto di corruzione così inteso ricomprende il concetto di frode e, allo stesso tempo, include tutti quei comportamenti prodromici alla frode stessa.

Il rischio di frode e corruzione

Alla luce dei concetti suddetti, il rischio di frode e corruzione può essere definito come il possibile verificarsi di una intenzionale violazione di norme e regole etiche/morali dalla quale derivano il mancato o ridotto perseguimento dell'interesse pubblico e una perdita o spreco di risorse pubbliche.

Pertanto, il concetto di rischio applicato ai concetti di frode e corruzione assume inevitabilmente una valenza negativa (*downside risk*) e la sua gestione richiede innanzitutto l'identificazione e analisi di tutti quegli eventi di natura corruttiva e fraudolenta, intesi nel senso sopra riportato, al fine di ridurre la probabilità di realizzazione e gli impatti negativi, non solo economici.

Definizione di risk management

In linea generale, il risk management è inteso come un insieme coordinato e sistemico di azioni, iterative e continuamente aggiornate, funzionale al rispetto degli obiettivi di un'organizzazione, volto a identificare e gestire rischi di diversa natura, con lo scopo di creare e preservare valore per l'azienda e per gli stakeholder.

Un aspetto interessante che emerge dagli standard e dalla letteratura è il collegamento con gli obiettivi di una organizzazione, per cui la gestione del rischio è tesa proprio ad evitare o minimizzare gli ostacoli e, quindi, gli eventi dolosi o accidentali, frapposti al raggiungimento dei suddetti obiettivi. Obiettivi che possono essere di diversa natura: strategici, operativi, economici, di sicurezza, di compliance.

I principali standard di risk management

La gestione del rischio ha impegnato diverse istituzioni e operatori nella definizione di sistemi in grado di guidare le organizzazioni nella identificazione, valutazione e gestione dei rischi e nell'integrazione del risk management nei processi strategici, di programmazione e controllo. Tra i principali standard riconosciuti e applicati a livello internazionale si annoverano: l'Enterprise Risk Management Framework - ERM prodotto e pubblicato nel 2004 dal Committee of Sponsoring Organizations of the Treadway Commission; l'ISO 31000:2009, emanato dall'International Organization for Standardization. Quest'ultimo, nella sua versione italiana, UNI ISO 31000:2010, è stato scelto come standard di riferimento, anche se non vincolante, per la predisposizione dei piani di prevenzione della corruzione nelle pubbliche amministrazioni, introdotti con la legge 190/2012.

A tali standard di taglio generale, si affiancano una serie di linee guida specifiche per la gestione del rischio di frode e corruzione, tra le quali: "Fraud Risk Management: A Guide to

Good Practice”, emanata nel 2002 dal CIMA - Chartered Institute of Management Accountants, e aggiornata nel 2009; “Managing the Business Risk of Fraud: a practical guide”, emanata nel 2008 dall’Institute of Internal Auditors, dall’American Institute of Certified Public Accountants e dall’Association of Certified Fraud Examiners. Infine, di recente pubblicazione è lo standard ISO 37001:2016 sui sistemi di gestione anticorruzione.

Infine, come già ricordato, la Commissione europea ha elaborato delle linee guida specifiche per la gestione dei rischi di frode nell’ambito dei Fondi strutturali e di investimento europei, note come “Linee guida EGESIF sulla valutazione dei rischi di frode e misure antifrode efficaci e proporzionate”.

I principi di attuazione del risk management

I principi di sviluppo e attuazione del risk management, definiti dai principali standard, riassumono l’approccio, le finalità e le caratteristiche con cui un’organizzazione deve adottare un sistema di gestione del rischio affinché questo risulti efficace. In linea generale, i principi prevedono che il risk management sia collegato agli obiettivi dell’organizzazione e ne favorisca il perseguimento; sia parte integrante di tutti i processi dell’organizzazione e del processo decisionale, supportando i vertici e il management nelle scelte e nelle priorità delle azioni; tratti in maniera sistematica, strutturata e tempestiva l’incertezza e sia basato sulle migliori informazioni disponibili; sia costruito su misura per l’organizzazione; sia dinamico, iterativo e si adatti al cambiamento; faciliti il miglioramento continuo e il rafforzamento dell’organizzazione.

Il processo di risk management

Dalla sintesi dei principali standard indicati precedentemente è possibile identificare un nucleo di fasi e azioni ricorrenti e caratterizzanti un processo di risk management:

- analisi del contesto, finalizzata alla definizione della struttura del processo di risk management (ruoli e responsabilità), dell’ambito di applicazione, della cultura del rischio, e alla rilevazione dei fattori di rischio interni ed esterni, attraverso l’osservazione dell’organizzazione, dei suoi processi, degli individui e delle dinamiche che li caratterizzano, del contesto socio-economico in cui opera;
- identificazione degli eventi di rischio, finalizzata alla mappatura degli eventi potenziali che possono pregiudicare il conseguimento degli obiettivi dell’organizzazione e all’analisi delle modalità operative e delle cause determinanti gli eventi rischiosi;

- analisi del rischio, finalizzata alla stima della probabilità di accadimento e dell'impatto generato sulla base di tecniche quantitative e/o qualitative;
- valutazione del pressing dei controlli sui rischi, finalizzata a valutare l'adeguatezza e l'efficacia del sistema di controllo esistente in relazione ai rischi identificati, al fine di evidenziare il rischio residuo;
- ponderazione del rischio, finalizzata a supportare l'organizzazione nel decidere quali rischi trattare e con quali priorità, attraverso la comparazione tra livelli di rischio rilevati e criteri di rischio predefiniti;
- trattamento del rischio, finalizzato ad individuare e scegliere le soluzioni per modificare il rischio e all'implementazione delle stesse;
- monitoraggio e valutazione, finalizzati sia a verificare l'attuazione e valutare l'efficacia delle soluzioni di trattamento del rischio definite, sia a verificare il funzionamento e valutare l'efficacia del sistema di risk management e la sua tenuta nel tempo;
- reporting e comunicazione, finalizzati sia alla rendicontazione agli organi di vertice e al management delle informazioni prodotte ed elaborate dal sistema di risk management per il supporto delle decisioni e delle azioni, sia alla comunicazione interna ed esterna delle policy di risk management al fine di creare una cultura del rischio condivisa e un atteggiamento funzionale all'efficacia del sistema.

Il processo di gestione del rischio di frode e corruzione

L'applicazione del risk management ai fenomeni di frode e corruzione, pur mantenendo la stessa articolazione, richiede un necessario adeguamento tenuto conto della natura dei fenomeni indagati.

Un atto di frode e di corruzione è determinato, innanzitutto, da una volontà individuale a compiere il fatto, volontà che è condizionata da fattori ambientali e culturali. Ciò ad esempio, in termini di gestione del rischio, richiede una particolare attenzione all'analisi del contesto culturale interno ed esterno, sia quale elemento determinante i fattori di rischio, sia quale elemento incidente sull'efficacia delle misure di risposta al rischio.

Inoltre, un atto di frode e di corruzione si può verificare ma non necessariamente essere scoperto e, quindi, tracciato e registrato come tale. Ciò complica il processo di valutazione del rischio, poiché l'utilizzo di tecniche quantitative, basato principalmente sulla rilevazione e osservazione di dati storici, risulta non pienamente adeguato; pertanto occorre inserire alcuni correttivi nel sistema di valutazione della probabilità e dell'impatto, basandosi su un mix di tecniche quantitative, qualitative, ma anche di analisi di scenari futuri.

Infine, la natura sommersa dei rischi in oggetto rende sicuramente più efficaci politiche di

gestione del rischio che agiscono sulla riduzione della probabilità piuttosto che sul contenimento degli impatti, quali, ad esempio, le politiche di prevenzione e di investigazione.