Internal Auditing : esperienze internazionali e prospettive evolutive "metropolitane" sui controlli antifrode in ambito Ministero della Difesa.

del Ten. Col. Sebastiano La Piscopìa, già Internal Review Officer NATO

SOMMARIO: 1. Genesi ed evoluzione del concetto e della funzione dell'*Internal Audit.* 2. Sugli standard internazionali di *Internal Audit.* 3. Uno sguardo metropolitano all'*Internal Audit* nella Pubblica Amministrazione. 4. Il controllo antifrode e l'esperienza *US Army* e *NATO*: ipotesi di studio per il Ministero della Difesa.

1. Genesi ed evoluzione del concetto e della funzione dell'*Internal Audit.*

Al fine di inquadrare storicamente e sistematicamente in ambito internazionale, l'*Internal Audit* (IA), è opportuno ricordare la nascita del concetto di *Public Internal Financial Control* (PIFC)[1], che è stato elaborato dalla Commissione Europea nel corso della seconda metà degli anni Novanta. L'acronimo nasce durante la fase iniziale dei negoziati per l'accesso all'Unione Europea dei Paesi che avevano avanzato richiesta di ingresso, allorquando la Direzione Generale *Financial Control* della Commissione Europea elaborò una strategia per diminuire la confusione che regnava in merito a una specifica questione: quale modello di sistema di controllo interno[2] dovesse essere preso in considerazione per i Paesi dell'Europa orientale (da poco usciti dall'orbita sovietica).
Ovviamente, per questi Paesi, fin dall'inizio la Commissione ha posto la sua attenzione su appositi sistemi di *audit* e di controllo volti ad eliminare ogni sorta di dubbio riguardo al PIFC e definirne in modo chiaro i contorni. In particolare la Commissione ha insistentemente posto l'accento su tre elementi cardine necessari allo sviluppo di affidabili sistemi di controllo finanziario interno:

1) rafforzamento dei sistemi di *Financial Management and Control* (FMC), quale principale responsabilità del management di ciascun centro di spesa, con particolare enfasi sui requisiti minimi del controllo interno;
2) istituzione di un servizio di *Internal Audit* (IA) "funzionalmente indipendente" (affiancato al senior management del centro di spesa) per la valutazione della qualità dei sistemi FMC e per fare raccomandazioni sul loro miglioramento;
3) identificazione di una *Central Harmonization Unit* (CHU) allocata preferibilmente all'interno del Ministero delle Finanze, a cui affidare compiti di sviluppo e implementazione della

[1] *"Il sistema di PIFC nel suo insieme va inquadrato nel contesto della più ampia area di finanza pubblica, come quelle della preparazione, approvazione ed esecuzione del bilancio nazionale, della tesoreria, della gestione tributaria e del debito pubblico, della contabilità, della rendicontazione e dell'approvvigionamento (procurement). Questo è il suo ambito di riferimento. Il sistema di controllo interno deve essere progettato come un insieme distinto ed esauriente di regole finalizzate alla trasparenza e all'efficienza nel settore pubblico. Esso, infatti, non va considerato come una semplice appendice della funzione di bilancio o di quella contabile o come uno strumento di lotta contro la frode, ma merita una sua specifica autonoma collocazione (fermi restando, naturalmente, gli ovvi collegamenti con le altre aree di finanza pubblica).*" La summenzionata definizione e parti salienti del presente articolo sono tratte liberamente, con alcune integrazioni e varianti dell'autore, da: http://www.rgs.mef.gov.it/_Documenti/VERSIONE-I/Pubblicazioni/Strumenti_e_Metodi/Il-Public-/Il-Public-Internal-Financial-Control---un-modello-evoluto-di-Controllo-Interno.pdf (di Giuseppe CERASOLI e Fabrizio MOCAVINI - Ed. 2008), pag. 7 e ss..
[2] Con particolare riferimento alla gestione dei fondi comunitari.

metodologia e dei requisiti di qualità standardizzati, riguardo ai sistemi di FMC e ai servizi di *Internal Auditing*.

In estrema sintesi il PIFC[3], può essere espresso con la seguente formula:
PIFC = CHU + IC[4]
(dove IC = FMC + IA)

Il PIFC include le attività di gestione e di controllo finanziario nel settore pubblico, *ex ante* (di approvazione) ed *ex post*, a livello centrale e periferico e si caratterizza per la netta linea di demarcazione tra le sue due funzioni principali: il *Financial Management and Control* (FMC) e l'*Internal Audit* (IA). Tale demarcazione si fonda sull'indipendenza funzionale degli *internal auditors* e assicura il corretto funzionamento del FMC, al quale sono affidati tutti i controlli *ex ante* di primo livello.

In ambito PIFC, i principali criteri di riferimento per effettuare una corretta valutazione sono la presenza di un quadro normativo primario e secondario (di applicazione), lo sviluppo della funzione di *Internal Audit*, il meccanismo di controllo per tutti i centri di entrata e di spesa e la certezza della indipendenza funzionale degli *internal auditors*. Il quadro di "controllo integrato" delineato dalla Commissione Europea per fornire ai Paesi candidati all'ammissione all'Unione europea un insieme di requisiti per la gestione delle rispettive finanze pubbliche, si ispira sia ai principi definiti nell'ambito dello *White Paper* della Commissione Europea (che ha portato alla definizione, a partire dall'anno 2000, degli standard per il Controllo Interno nella Commissione Europea) sia ai "principi d'oltre oceano" definiti nel *COSO REPORT*[5] della cosiddetta *Commissione Treadway*.

Va ricordato, infatti che il primo studio per migliorare i controlli interni "*nasce negli Stati Uniti come iniziativa delle associazioni professionali più significative "American Institute of Certified Public Accountants (AICPA), American Accountant Association (AAA), Institute of International Auditors (IIA), Instituite of Management Accountants (IMA), Financial Executive Institute (FEI) che hanno dato vita ad una commissione di studio all'interno della National Commission on Fraudolent Financial Reporting (NCFFR) conosciuta come Tradway Commission dal nome del suo presidente James C. Tradway Jr.."*[6]

Tale Commissione denominata *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), ha definito il controllo interno come:

"*un processo gestito dal management e da altre persone, strutturato per fornire ragionevole sicurezza relativamente al conseguimento degli obiettivi organizzativi nelle seguenti aree:*
1) aderenza alle regole;
2) affidabilità delle informazioni;
3) salvaguardia del patrimonio;
4) affidabilità dei bilanci;
5) efficacia ed efficienza della gestione".

Più nel dettaglio, le componenti del controllo interno individuate dal COSO sono:

A) L'ambiente di controllo, definito dalla integrità e dai valori etici presenti nell'organizzazione. Costituisce la base su cui poggiano tutti gli altri componenti. I fattori principali sono:

- l'integrità ed i valori etici; gli obiettivi ed i metodi utilizzati per realizzarli sono basati sulle priorità e sui giudizi di valore che si traducono in codici di condotta, che devono andare oltre il semplice rispetto della legge (conflitti di interessi, rapporti con gli interlocutori di riferimento, sistemi di incentivazione, ecc.);
- lo stile di direzione, che incide sulla conduzione (organizzazione, deleghe, procedure, report) e sui livelli di rischio accettati;

[3] Come indicato nell'importante pubblicazione del MEF citata in nota n.1.
[4] Internal Control.
[5] *Committee of Sponsoring Organizations of the Treadway Commission*.
[6] Alberto PESENATO, "Manuale del revisore legale", Ed. 2012, pag. 30.

- le politiche del personale, tra cui le politiche di selezione, promozione e remunerazione ed il loro livello di integrità ed etica.

B) La valutazione dei rischi, che consiste nella individuazione ed analisi dei fattori che possono pregiudicare il raggiungimento degli obiettivi, al fine di determinare come questi rischi dovranno essere gestiti.
Ovviamente, prima di poter identificare i rischi è necessario procedere all'individuazione degli obiettivi, che possono essere di tipo operativo (efficacia ed efficienza delle attività), informativo (predisposizione di bilanci attendibili) e di conformità (osservanza di leggi e regolamenti).
Successivamente si può procedere con la fase di analisi che comporta:
• la valutazione dell'importanza del rischio;
• la valutazione delle probabilità che il rischio si verifichi;
• le modalità di gestione del rischio.
Una differenza significativa sussiste tra la valutazione dei rischi (parte integrante del Sistema di Controllo Interno) e i piani di gestione dei rischi (parte integrante del processo manageriale).
È imperativo che il vertice disponga di una "mappa dei rischi", così da poter orientare la propria azione di copertura secondo criteri di priorità.
Ad avviso dello scrivente, pare significativo aggiungere alla presente digressione tassonomica del COSO (ripresa dalla pubblicazione del MEF del 2008 citata in nota 1), il dettaglio sulla "valutazione del rischio" presentato in proposito dall'*Associazione Italiana Internal Auditors* sulla "guida"[7] predisposta per la gestione del *framework* di che trattasi, ove l'*Associazione* stessa ha individuato i seguenti tre *bullets*:

- Obiettivi del *financial reporting*: il *management* determina con chiarezza gli obiettivi del *financial reporting* e adotta criteri adeguati per consentire l'identificazione dei rischi che possono pregiudicare l'attendibilità del *reporting*;
- Rischi del *financial reporting*: l'impresa identifica ed analizza i rischi che potrebbero pregiudicare il conseguimento degli obiettivi del *financial reporting*, anche al fine di stabilire come gestirli;
- Rischio di frode: l'eventualità che si verifichino errori significativi a causa di azioni fraudolente, viene esplicitamente considerata quando si valutano i rischi che influiscono sulla realizzazione degli obiettivi del *financial reporting*.
  La sopraindicata "*collocazione concettuale del rischio di frode*" è particolarmente significativa per le ragioni che saranno oggetto di approfondimento nel successivo paragrafo n.4.

C) L'attività di controllo, con politiche e procedure che garantiscano alla Direzione l'attuazione delle direttive e l'attività di contrasto dei rischi. Tipologie di attività di controllo sono ad esempio:
• analisi svolte dall'alta direzione, come il controllo sul budget o sull'andamento della gestione operativa, ecc.;
• elaborazione dei dati, per verificarne l'accuratezza e la completezza;
• controlli fisici su attrezzature e scorte mediante inventari;
• separazione dei compiti al fine di ridurre errori e irregolarità;
• controlli sui sistemi informativi (ced, *software*, applicativi, ecc.).

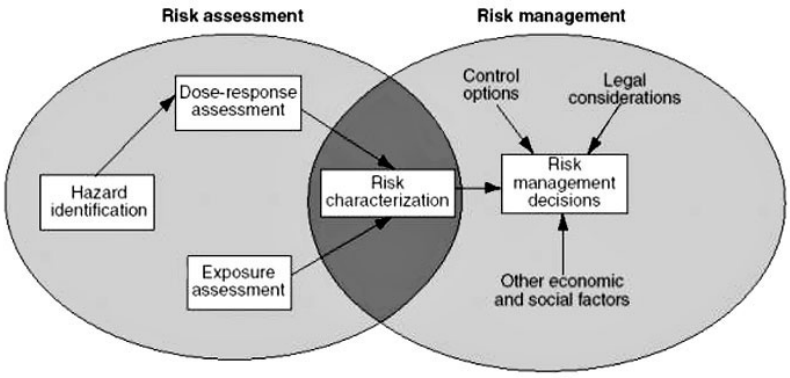
D) L'informazione e la comunicazione: le informazioni pertinenti devono essere identificate, raccolte e diffuse con modalità e tempi che consentano a ciascuno di adempiere i propri compiti.
Le organizzazioni devono poter comunicare in modo efficace e diffuso, facendo circolare le informazioni all'interno dell'organizzazione, verso il basso, verso l'alto e trasversalmente.
La qualità delle informazioni prodotte dai sistemi si valuta in base a:
• contenuto: ci sono tutte quelle necessarie?
• tempestività: possono essere ottenute nei tempi desiderati?
• aggiornamento: sono disponibili quelle più recenti?

[7] Vds. :http://www.aiiaweb.it/rivista-internal-audit/saper-maneggiare-il-framework-il-controllo-interno-lattendibilita-del

• accuratezza: sono esatte?
• accessibilità: si possono ottenere facilmente?

E) Il monitoraggio: i sistemi di controllo interno hanno bisogno di essere monitorati per valutare la qualità della loro efficacia, sia con interventi di supervisione continua, sia con valutazioni periodiche. In particolare si possono avere:
• monitoraggi continui: attività di *Internal Auditing*; confronto dei dati presenti nei sistemi con quelli esistenti fisicamente; attività di revisione contabile, ecc.;
• valutazioni specifiche: possono variare per ambito e frequenza in funzione della significatività dei rischi e dei controlli per la riduzione dei rischi. Tale attività può essere svolta attraverso *check lists*, questionari, diagrammi di flusso, *benchmarking*, ecc..

Va evidenziato che già prima del 2002 il COSO Report è stato individuato quale *best practise* di riferimento per l'architettura dei sistemi di controllo interno dal *Serbanex Osley Act*[8] dopo i casi Enron e Vivendi negli Stati Uniti e Parmalat in Italia.
Tuttavia il clamore di tali scandali non è stato del tutto determinante ai fini di un'applicazione generalizzata delle summenzionate regolamentazioni internazionali.
Il COSO venne successivamente integrato con la pubblicazione, nel 2004, del *framework Enterprise Risk Management* (in acronimo ERM)[9]. Tale documento, ampliando e completando i concetti e gli orientamenti contenuti nel COSO, enfatizzò la valutazione e la gestione dei rischi quale precondizione ai fini di un efficace sistema di controllo interno.
Con l'ERM venne realizzata "*una sorta di rivoluzione copernicana fra controllo interno e risk management. Nel precedente report il sistema di controllo interno era visto come il contenitore entro il quale doveva trovare spazio un'attività di identificazione e di valutazione dei rischi finalizzata ad orientare gli sforzi del controllo; nel nuovo schema interpretativo il controllo interno viene visto come elemento del più vasto sistema di risk management*"[10].



- Figura 1 -
Risk management scheme[11]

Il sistema di controllo interno divenne, così, uno dei principali meccanismi di *governance* societaria: consentì, cioè, di orientare l'attenzione dei vertici aziendali da un lato verso l'identificazione dei principali rischi relativi alle scelte strategiche ed alla gestione, dall'altro

[8] Per il testo in lingua originale vds.: https://www.sec.gov/about/laws/soa2002.pdf
[9] Per un approfondimento sull'ERM si veda Associazione Italiana Internal Auditors e Price Waterhouse Coopers, *La gestione del rischio aziendale – ERM Enterprise Risk Management: modello di riferimento e alcune tecniche applicative*, Milano, 2006.
[10] Nicola PECCHIARI e Sergio BERETTA., *Analisi e valutazione del sistema di controllo interno – Metodi e tecniche*, Milano, 2007, XV.
[11] www.learner.com

promuovendo la valutazione dell'adeguatezza delle protezioni poste in essere per contrastare i rischi individuati[12].
Il controllo interno da sistema di vincoli in capo al *management* finalizzato all'assicurazione della sola *conformance*, diventa strumento di garanzia della *performance*.
Da una visione restrittiva del sistema di controllo interno, quale mera funzione di ispettorato, si passa ad funzione di *assurance* e di consulenza.
Pertanto, il sistema di controllo interno è definibile quale insieme di strumenti e di procedure gestiti dal *management* volti a "*fornire una ragionevole sicurezza relativamente al conseguimento degli obiettivi organizzativi in termini di aderenza alle regole, affidabilità delle informazioni, salvaguardia del patrimonio e efficacia ed efficienza della gestione*"[13].
In tale quadro, l'*Internal Auditing* [14] rappresenta la "*funzione di assurance che fornisce all'organizzazione un'opinione indipendente e obiettiva sul grado con cui l'ambiente di controllo interno sostiene e promuove la realizzazione degli obiettivi prefissati*"[15].
L'*Internal Auditing*, quindi, orientando il proprio *focus* sull'attività gestionale e sul *risk management*, è chiamato ad assistere "*l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto, in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance*"[16].

2. Sugli standard internazionali di *Internal Audit*.

Prima di addentrarci nell'analisi dell'esperienza italiana descritta nel prossimo paragrafo, pare opportuno fare una panoramica dei principali *Standard internazionali* di settore applicabili all'*Internal Audit*, con particolare riferimento a quelli emanati dall'*Institute of International Audit* (IIA).
Le norme di controllo pubblicate dall'*International Organization of Supreme Audit Institutions* (INTOSAI), le norme internazionali di *audit* elaborate dal Comitato internazionale delle pratiche di controllo dell'*International Federation of Accountants* (IFAC) e gli standard internazionali per la pratica professionale dell'*Internal Auditing* elaborati dall'*Institute of Internal Auditors* (IIA), costituiscono i principali standard internazionali per la pratica professionale in materia di controllo e un importante quadro di riferimento per le attività di *audit* a cui ispirarsi per l'elaborazione della strategia e della metodologia dell'*audit* stesso.
I due documenti basilari dell'INTOSAI, la "Dichiarazione di Lima sui principi generali i controllo della finanza pubblica" (1977) e le "Regole del controllo" (*Auditing Standards* - 1992), costituiscono nel loro complesso l'originaria esposizione sistematica e coordinata delle direttive inclusive dei postulati di base del controllo, da utilizzare quale punto di partenza per tutti i Paesi che aderiscono all'osservanza in via normativa e regolamentare di tali documenti.
Le linee guida dell'INTOSAI, dopo aver chiarito il concetto e gli obiettivi dei controlli interni, enucleano poi un gruppo minimo di standard generali e particolari utilizzabili da tutti i Paesi come base per attuare un sistema di controllo interno.
Due appositi capitoli sono, infine, dedicati alle modalità normative ed organizzative di realizzazione dei sistemi di controllo interno ed alla periodica valutazione dell'efficacia di tali sistemi.

---

[12] Alessandro CAMARDA, "*La funzione di internal auditing nella Pubblica Amministrazione*", Ed. n. 2 – 2011, pag. 2 e ss.. da http://diritto.regione.veneto.it/?p=489#_ftn22. Anche nel prosieguo del presente studio si trae liberamente dal puntuale lavoro del citato autore.
[13] Associazione Italiana Internal Auditors e Ernst&Young, "*Il sistema di controllo interno nel settore pubblico – Executive Summary*", 2008.
[14] Come lucidamente osservato dal CAMARDA, op. cit..
[15] Associazione Italiana Internal Auditors e Ernst&Young, *op. cit.*, 3.
[16] Collen DITTMEIER, "*Internal Auditing – Chiave per la corporate governante"*, Milano, 2007.

Nel 1998 sono state, inoltre, elaborate, a cura della Corte dei Conti Europea, unitamente alle Istituzioni Superiori di Controllo (ISC) dell'area U.E., le "Strategie e norme di controllo" (Adattamento in ambito UE delle norme di controllo INTOSAI). Gli *International Standard on Auditing* ("ISA") emanati dall'IFAC costituiscono dei principi di revisione in ambito internazionale e rappresentano il *corpus* di riferimento nell'esercizio delle funzioni di *audit*.
Infine, gli *Standard internazionali* per la pratica professionale dell'*Internal Auditing* elaborati dall'IIA fanno parte del "*Professional Practices Framework*", approvato dal *Board of Directors* dell'IIA nel giugno del 1999. Questo documento comprende la definizione di *Internal Auditing*, il Codice Etico, gli Standard e le linee guida per l'applicazione degli stessi.
Chiaramente, l'attività di *Internal Audit*[17] è svolta in contesti giuridici e culturali diversi, all'interno di organizzazioni che variano per finalità, dimensioni, complessità e struttura, e da persone sia interne, sia esterne all'organizzazione. Tuttavia, mentre nei vari contesti ci possono essere differenze nello svolgimento dell'attività di *Internal Audit*, la conformità agli *International Standards for the Professional Practice of Internal Auditing* (gli Standard) dell'IIA è certamente essenziale per l'adempimento delle responsabilità degli *auditors* e dell'attività di *Internal Audit*. Pertanto, qualora leggi o regolamenti vietino agli *internal auditors* di operare in conformità con alcune parti degli Standard, essi dovranno tuttavia rispettarne tutte le altre parti e darne adeguata informativa.
Inoltre, se gli Standard sono utilizzati congiuntamente con standard pubblicati da altri organismi professionali riconosciuti, gli *internal auditors* possono comunicare nel modo più opportuno anche l'uso di altri standard. In tal caso, se esistono differenze tra gli Standard e altri eventualmente adottati, gli *internal auditors* devono rispettare gli Standard e possono conformarsi ad altri standard solo se questi sono più restrittivi.
Gli Standard in parola hanno lo scopo di:
1. delineare i principi base che prescrivono come deve essere svolta l'attività di *Internal Audit*;
2. fornire un quadro di riferimento per lo sviluppo e l'effettuazione di una vasta gamma di attività di *internal audit* a valore aggiunto;
3. definire i parametri per la valutazione delle prestazioni dell'*Internal Audit*;
4. promuovere il miglioramento dei processi organizzativi e operativi.

Gli Standard fissano requisiti vincolanti, basati su principi, che consistono in:
- definizioni dei requisiti fondamentali per la pratica professionale dell'*Internal Auditing* e per la valutazione dell'efficacia dell'attività, applicabili internazionalmente a diversi livelli organizzativi e individuali.
- interpretazioni che chiariscono termini e concetti contenuti nelle Definizioni.

Inoltre gli Standard utilizzano termini cui sono stati attribuiti significati specifici e che sono stati inclusi nel Glossario.
Specificamente, gli Standard usano la parola "deve" per specificare un requisito vincolante e la parola "dovrebbe" per indicare un requisito vincolante a meno di circostanze ed eventi che, sottoposti a un giudizio professionale, ne giustifichino l'inosservanza.
Per comprendere e applicare correttamente gli Standard, è necessario considerare sia le Definizioni che le loro Interpretazioni, nonché i significati specifici riportati nel Glossario.
Sotto il profilo strutturale, gli Standard si suddividono suddivisa in Standard di Connotazione e Standard di Prestazione.
Gli Standard di Connotazione precisano le caratteristiche che devono possedere le organizzazioni e gli individui che effettuano attività di *Internal Audit*.
Gli Standard di Prestazione descrivono la natura dell'attività di *Internal Audit* e forniscono criteri qualitativi in base ai quali valutarne l'effettuazione. Gli Standard di Connotazione e gli Standard di Prestazione si applicano a tutti i servizi di *Internal Audit*.

[17] Tratto da "*The Institute of International Auditors*": https://na.theiia.org/standards-guidance/Public%20Documents/IPPF%202013%20Italian.pdf (pagg. 1 e 2).

Sono inoltre previsti gli Standard Applicativi che approfondiscono l'applicazione degli Standard di Connotazione e degli Standard di Prestazione, stabilendo i requisiti relativi all'*assurance* (A) o alle attività di consulenza (C).
Più in particolare i servizi di *assurance* comportano un'obiettiva valutazione delle evidenze da parte degli *Internal Auditors* finalizzata alla formulazione di un giudizio indipendente o di conclusioni relative a un'organizzazione, all'operatività, a una funzione, a un processo, a un sistema o a un altro ambito.
E' l'*Internal Auditor* a definire la natura e l'ampiezza del servizio di *assurance*.
Tre sono le parti generalmente coinvolte nei servizi di *assurance*:
(1) il *process owner*, cioè la persona o il gruppo direttamente coinvolti nell'organizzazione, operatività, funzione, processo, sistema o altro ambito;
(2) l'*internal auditor*, cioè la persona o il gruppo che effettua la valutazione;
(3) il cliente, cioè la persona o il gruppo che utilizzerà tale valutazione.
I servizi di consulenza, invece, sono un'attività di supporto e suggerimento e sono generalmente effettuati dietro specifica richiesta del cliente committente.
Natura e ampiezza dell'intervento sono definiti in accordo con il cliente.
Due sono, in genere, le parti coinvolte in tali servizi:
(1) la persona o il gruppo che sta offrendo il servizio, cioè l'*internal auditor*;
(2) la persona o il gruppo che lo richiede, cioè il cliente. Nello svolgimento del loro compito, gli *internal auditor* dovrebbero mantenere l'obiettività e non assumere responsabilità di tipo manageriale.
Gli Standard si applicano ai singoli *internal auditors* e alle singole attività di *internal audit*.
Tutti gli *internal auditors* sono tenuti a rispettare gli Standard sotto il profilo dell'obiettività, della competenza e della diligenza professionale.
Gli *internal auditors* sono inoltre tenuti al rispetto degli Standard che si applicano alle responsabilità del loro compito. La responsabilità complessiva della conformità agli Standard ricade sui responsabili di *Internal Auditing*.

Si riportano, a seguire, i più significativi Standard emanati dall'*Institute of International Audit* (IIA):

A) Standard di connotazione:

1000: Finalità, autorità e responsabilità
Finalità, autorità e responsabilità dell'attività di *Internal Auditing* devono essere definite in un formale mandato, coerente con gli Standard ed approvato dal *Board* dell'Organizzazione (*Audit Charter*). Il mandato deve:
- definire la posizione della funzione nell'organigramma aziendale;
- autorizzare l'accesso incondizionato ai dati, alle persone, agli archivi ed ai beni aziendali, ogni volta che ciò sia necessario per lo svolgimento dell'Audit;
- definire l'ampiezza delle attività di Auditing.
E' compito del Responsabile Internal Auditing (di seguito anche "RIA") fare in modo che il vertice aziendale rilasci ufficialmente e formalizzi tale mandato. La forma scritta costituisce un formale veicolo per la revisione e l'approvazione del Management, nonché per l'accettazione da parte del *Board*.
Il Responsabile Internal Auditing deve periodicamente verificare che le finalità, l'autorità e le responsabilità definite nel mandato siano sempre adeguate a consentire alla Funzione il conseguimento dei propri obiettivi.
Il *Board* (o il Comitato per il Controllo Interno) all'interno del mandato deve autorizzare esplicitamente lo svolgimento delle attività da parte dell'*Internal Auditing*, laddove non sussistano conflitti di interesse o non si comprometta il rispetto degli impegni nei confronti del mandato stesso.

1100: Indipendenza e Obiettività

L'attività di *Internal Auditing* deve essere indipendente e gli *internal auditors* devono essere obiettivi nell'esecuzione del loro lavoro.

Gli internal auditors sono indipendenti quando possono svolgere la loro attività senza vincoli e con obiettività. L'indipendenza consente all'*internal auditor* di formulare una valutazione imparziale ed obiettiva, fattore fondamentale per la corretta esecuzione dell'incarico. Un'adeguata collocazione organizzativa e l'obiettività dell'*internal auditor* derivante dall'esperienza e dalla correttezza personale e professionale sono necessarie per la sua indipendenza.

1200: Competenza e diligenza professionale

Gli incarichi devono essere effettuati con la dovuta competenza e diligenza professionale.

Gli *internal auditors* devono :

- possedere le conoscenze, capacità e competenze necessarie all'adempimento delle loro responsabilità individuali. Assicurare un adeguato livello di preparazione professionale è una responsabilità sia del RIA sia dei singoli *internal auditors*;
- procurarsi l'assistenza e la consulenza specialistica se non dispongono delle conoscenze, capacità o competenze necessarie per svolgere in tutto o in parte l'incarico. Il RIA deve quindi verificare la professionalità del fornitore nell'esecuzione dell'incarico e valutare i rapporti del consulente esterno con l'organizzazione, onde assicurare il mantenimento di indipendenza e obiettività;
- possedere conoscenze sufficienti per riconoscere gli indicatori di frode, in quanto devono fornire assistenza nella prevenzione delle frodi esaminando e valutando l'adeguatezza e l'efficacia del sistema di controllo interno. Tuttavia non è loro richiesto di possedere le competenze di chi ha come responsabilità primaria l'accertamento e l'investigazione delle frodi;
- possedere una conoscenza generale dei principali rischi e controlli relativi all'IT, nonché degli strumenti tecnologici di supporto.

Gli *internal auditors* devono impiegare la diligenza e la competenza che ci si attende da un *auditor* ragionevolmente prudente e competente. La diligenza deve essere pertanto adeguata:

- alla complessità dell'incarico;
- all'ampiezza del lavoro necessario per raggiungere gli obiettivi;
- all'adeguatezza e all'efficacia dei processi di controllo, *risk management* e *corporate governance*;
- alla probabilità della presenza di significativi errori, irregolarità o non conformità;
- al costo dell'incarico in relazione ai suoi potenziali benefici;
- alle esigenze e alle aspettative del cliente.

Diligenza professionale non implica, tuttavia, infallibilità. Gli *internal auditors* devono migliorare le loro conoscenze, capacità e competenze attraverso un aggiornamento professionale continuo e sono esortati a dimostrare la loro competenza tramite appropriate certificazioni professionali.

1300: Programma di Assicurazione e miglioramento qualità

Il Responsabile Internal Auditing deve sviluppare e mantenere un programma di assicurazione e miglioramento qualità che copra tutti gli aspetti dell'attività di *Internal Auditing* e ne verifichi continuamente l'efficacia. Tale programma comprende specifiche valutazioni interne ed esterne, ed attività di monitoraggio continuo. Ciascuna di queste parti del programma deve essere strutturata in modo da aiutare l'*Internal Auditing* a fornire valore aggiunto a migliorare l'operatività dell'Organizzazione, e ad assicurare che la sua attività sia svolta in conformità agli Standard ed al Codice Etico.

B) Standard di prestazione:

2000: Gestione dell'attività di *Internal Auditing*

Il Responsabile Internal Auditing deve gestire in modo efficace l'attività al fine di assicurare che apporti valore all'organizzazione.

Il Responsabile della funzione di *Internal Auditing* deve gestire l'attività in modo appropriato così che:
- l'attività di *Audit* soddisfi le finalità generali e le responsabilità assegnate nel mandato approvato dal vertice e accettato dal Consiglio di Amministrazione;
- le risorse siano utilizzate in modo efficace ed efficiente;
- l'attività di *Audit* sia conforme agli *Standard Internazionali* per la Pratica Professionale dell'*Internal Auditing*.

2100: Natura dell'attività
L'*Internal Auditing* deve valutare e contribuire al miglioramento dei processi di *risk management*, di controllo e di *governance* tramite un approccio professionale sistematico.

2200: Pianificazione dell'incarico
Per ciascun incarico gli *Internal Auditor*s devono predisporre e documentare un piano, che comprenda, tra l'altro, obiettivi, estensione ed impiego di risorse.

2300: Esecuzione dell'incarico
L'*Internal Auditor* deve utilizzare un approccio professionale e sistematico per identificare, analizzare, valutare e registrare informazioni sufficienti al raggiungimento degli obiettivi dell'incarico.

2400: Comunicazione dei risultati
Gli *Internal Auditor* devono comunicare i risultati dell'incarico in modo appropriato.

2500: Processo di monitoraggio (*follow up*)
Il Responsabile Internal Auditing deve stabilire e mantenere un sistema di monitoraggio sul seguito dato alle risultanze segnalate al *Management*.
Deve esistere un sistema di monitoraggio che assicuri l'introduzione di efficaci misure correttive oppure l'accettazione del rischio da parte della Direzione.
Il RIA deve predisporre opportune procedure che:
- stabiliscano i limiti temporali entro i quali deve pervenire la risposta a rilievi e raccomandazioni;
- impongano una valutazione dell'appropriatezza di tali risposte;
- richiedano una verifica delle stesse, ove opportuno;
- definiscano i criteri per attivare un incarico di *follow up*, ove appropriato;
- indichino il processo da seguire per sottoporre al vertice aziendale le risposte e le azioni ritenute insoddisfacenti.

Il RIA deve istituire un processo di *follow up* per controllare ed assicurare che le azioni correttive siano state implementate, o che il *Top Management* abbia accettato il rischio di non attivare azioni correttive.

2600: Risoluzione dei contrasti in merito all'accettazione del rischio da parte del Management
Qualora il Responsabile Internal Auditing ritenga che il *Top Management* abbia accettato un livello di rischio residuo considerato eccessivo per l'Organizzazione, ne deve discutere con il Top Management. Se il disaccordo permane, il RIA e il *Top Management* devono riportare il problema al *Board*.
Il management è responsabile di decidere quali siano le azioni appropriate da intraprendere in risposta ai rilievi ed alle raccomandazioni dell'auditor.
Il RIA ha la responsabilità di valutare se le azioni del management conducano ad una tempestiva risoluzione delle anomalie rilevate. Per ragioni di costo o per altre considerazioni il *Top Management* può decidere di accettare il rischio di non intervenire con azioni correttive.
In caso di rilevanze significative ed importanti raccomandazioni di audit, il *Board* ne deve essere informato[18].

[18] I succitati Standard sono stati tratti dalla citata pubblicazione del MEF – RGS, indicata in nota n.1.

3. Uno sguardo metropolitano all'*Internal Audit* nella Pubblica Amministrazione.

In Italia, già nel 1997 venne pubblicato l'Addendum italiano del COSO Report[19] che riprende ed approfondisce le edizioni statunitensi creando i presupposti per la definizione di dettagliate *check lists* da "porre nelle mani" degli *internal auditors* "di casa nostra".
Come già accennato in precedenza, si evidenzia che quando si parla di sistemi di controllo orientati verso lo Stato, nelle sue varie articolazioni, si deve necessariamente focalizzare l'attenzione sui modelli di *governance* delle Pubbliche Amministrazioni. Con questo termine anglosassone si intende un insieme di regole, processi e sistemi tramite i quali viene esercitata e controllata l'autorità. La *governance* consiste quindi nell'insieme delle procedure connesse al processo di formulazione delle decisioni, alla *performance* e al controllo dell'organizzazione (pubblica e privata), nonché alla messa a punto da parte del management di sistemi in grado di indirizzare complessivamente l'organizzazione e soddisfare le ragionevoli aspettative degli *stakeholders*.
"Sono elementi di *governance* la struttura e l'organizzazione della funzione di indirizzo e governo dei vertici, i processi di *reporting* finanziario e di controllo interno, i codici di condotta personale.
Alcuni dei principi fondamentali a cui i modelli di *governance* di una Pubblica Amministrazione dovrebbero ispirarsi sono:

- i diritti della collettività (l'insieme di soggetti esterni portatori di interessi): le Pubbliche Amministrazioni devono sempre rispettare i diritti della collettività e assistere concretamente tutti i cittadini dell'esercizio dei loro diritti, assicurando la piena disponibilità di informazioni comprensibili e accessibili;
- l'integrità ed il comportamento etico: le Pubbliche Amministrazioni dovrebbero creare codici di condotta che promuovano processi decisionali etici e responsabili;
- la chiarezza e la trasparenza: le Pubbliche Amministrazioni devono rendere chiari e conoscibili i ruoli e le responsabilità della Dirigenza, per fornire un adeguato livello di informazione alla collettività anche e soprattutto in tema di bilancio.

La *governance* si identifica quindi in una appropriata armonizzazione di poteri, doveri e ruoli e in una ottimale combinazione di strutture e processi da implementare in una data istituzione allo scopo di definire strategie e obiettivi, monitorare le prestazioni (rispetto a obiettivi e indicatori) e garantire appropriati sistemi di controllo.
Per poter massimizzare i risultati e ridurre la variabilità del successo, anche nel settore pubblico è però necessario introdurre un sistema di valutazione dei rischi a cui sono esposte le organizzazioni e i loro obiettivi (il rischio viene definito come una potenziale minaccia o un ostacolo al raggiungimento degli obiettivi). Ulteriore compito dei *managers* è, infatti, quello di accertare se il livello di rischio della rispettiva organizzazione è accettabile e, nel caso in cui non lo sia, adottare misure appropriate.
Mappare i rischi serve, inoltre, a stabilire il grado di incidenza e prevalenza degli stessi, classificandoli in base alla loro consistenza (elevati, medi, ridotti) e ai potenziali tassi di frequenza, in modo da destinare adeguate risorse al processo di controllo.
Nel quadro della gestione dei rischi è anche necessario quantificare i rischi in termini finanziari e ordinarli secondo le priorità: i rischi ad elevato impatto, ma con scarsa incidenza, sono generalmente tollerabili laddove il costo delle misure preventive è minimo.
Lo stesso vale per i rischi ad elevata incidenza, ma ad impatto ridotto: i rischi elevati e quelli medi devono essere tenuti sotto controllo e mitigati attraverso l'applicazione di sistemi di gestione e di controllo.
Il valore della gestione dei rischi risiede nella qualità delle risposte fornite dai *managers* sotto forma di controllo interno.
La regola secondo la quale occorre implementare i controlli ovunque sussiste un rischio va soppesata rispetto al costo dei controlli stessi e all'incidenza e alla gravità dei relativi rischi.

[19] Per approfondimenti vds.: http://www.coso.org/documents/Italian_Exec-Summary_NoTrackChange.pdf

Laddove il costo ecceda i benefici, il rischio deve essere accettato dal *management* come un "rischio residuo".
La semplicità di questo approccio è indicativa del cambiamento che l'analisi dei rischi apporta alla gestione della pubblica amministrazione: la valutazione rischi/rendimento e il controllo interno rappresentano, dunque, una radicale innovazione rispetto all'ottica dei tradizionali sistemi amministrativi, incentrata su forme di controllo esaustivo.
L'analisi dei rischi solitamente richiede ai *managers*, anche pubblici, di valutare da un lato la gravità e l'incidenza del rischio e, dall'altro, l'efficacia e l'efficienza (in termini di costo) delle misure di controllo da loro attuate.
Con questo approccio, quindi, i controlli si concentrano sulle attività che presentano i più elevati fattori di rischio, mentre i rischi di minore entità vengono, in un certo senso, "accettati"".[20]
In Italia, il disegno costituzionale unitario della gestione finanziaria pubblica[21], benché difformemente strutturato, è volto a garantire le esigenze di uno Stato "funzionale" che vede l'impostazione prevalente dei controlli previsti, incentrata sui cosiddetti profili di legittimità più che su controlli di economicità, efficienza ed efficacia.
Tali ultimi controlli troverebbero del resto piena e naturale adattabilità procedurale in un contesto legislativo e bilancistico di tipo "pienamente programmatorio" che è rimasto tuttavia tale, solo nei principi finalistici individuati dai Padri costituenti. Infatti, nonostante la progressiva permeazione dei criteri e dei principi aziendali o privatistici nella Pubblica Amministrazione, e il continuo avvicinamento del nostro ordinamento ad uno spirito di efficienza anglosassone teso ad ispirare l'approccio manageriale alla gestione della cosa pubblica, i "nostri controlli interni" non paiono ancora perfettamente integrati con quelli esterni e non sembrano rispondere ad una piena efficacia operativa.
Ci si riferisce, in particolare ai controlli interni di tipo manageriale e, nello specifico, all'*Internal Audit* come individuato nella cosiddetta matrice dei controlli pubblici sottodescritta[22].

CONTROLLO

	INTERNO	ESTERNO
Modalità burocratica	Controllo di regolarità amministrativa e contabile	Controllo della Corte dei Conti Ispezioni esterne
Modalità manageriale	Audit interno Controllo strategico Controllo economico di gestione	Revisione e Audit esterno Certificazioni di qualità

- Fig. 2 -
Matrice dei controlli pubblici

Nell'ottica di un'appropriata gestione delle limitate risorse finanziarie della collettività, si è ormai superata l'esigenza di conoscere la rispondenza tra il corretto utilizzo delle risorse, nel senso del rispetto delle leggi e dei regolamenti, nella progressiva tensione alla conoscenza della reale capacità della amministrazioni pubbliche di raggiungere i risultati programmati in sede legislativa ed amministrativa.[23]
Ovviamente ciò deve avvenire in modo economico ed efficiente e la Comunità ha l'esigenza di disporre degli elementi di *Auditing* per valutarlo con accurata e diligente consapevolezza.

[20] Tratto liberamente da Giuseppe CERASOLI e Fabrizio MOCAVINI, Op. cit. pagg. da 21 23.
[21] Sul tema della programmazione dell'attività pubblica, vds.: Carlo CHIAPPINELLI in "Modelli di programmazione" in "*Programmazione controlli responsabilità nelle pubbliche amministrazioni*", 2010.
[22] Renato RUFFINI, "*Fondamenti di economia delle aziende e delle amministrazioni pubbliche*", 2004.
[23] Riccardo MUSSARI "*I sistemi di contabilità e bilancio dello Stato nell'Europa comunitaria*" 2005.

Si sottolinea che i controlli interni devono rappresentare strumenti capaci di garantire la correttezza delle rilevazioni contabili, ma anche l'uso efficiente delle risorse, la puntuale applicazione delle politiche adottate, la valorizzazione del patrimonio[24].
Ciò non di meno - ad avviso di chi scrive - lo *starting point* dovrebbe essere rappresentato dalla protezione del patrimonio stesso.
Non si può tuttavia affermare che fosse propriamente questo lo spirito con cui in Italia, nacque il controllo interno con la legge di contabilità 22 aprile 1869, n. 5026, poi evolutasi in una fisionomia giuridica "assestata" con il Regio Decreto del 18 novembre 1923, n. 2440, che per primo attribuisce al Tesoro, oltre al controllo di legittimità e quello contabile, anche il controllo sulla "proficuità" della spesa: una sorta di controllo che entra nel merito e valuta la convenienza della spesa.[25]
Non ci si vuol riferire, in questa sede, tuttavia, all'originario concetto di "proficuità" nell'effettuazione delle spese, il cui controllo è devoluto alla Ragioneria Generale dello Stato - Ispettorato Generale di Finanza *ex* art. 3 della legge 26 luglio 1939 n. 1037[26], o all'attività di controllo di regolarità amministrativa e contabile come riordinata e potenziata dal D.Lgs. n. 123/2011[27], modificata dalla legge n. 39/2011, alla luce della legge n. 196/2009, bensì al concetto di *Internal Audit* finalizzato alla tutela del patrimonio pubblico.
Da più parti è stato rilevato che i controlli interni di tipo burocratico, al pari di quelli esterni della Corte dei Conti, hanno storicamente rivolto il loro sguardo principalmente ad aspetti formali, ossia su atti invece che su risultati, ed in chiave sanzionatoria più che di guida: ciò ha inevitabilmente condizionato le scelte, le decisioni e le azioni dei pubblici funzionari.
Infatti, il controllo interno[28], occupandosi di organizzazione e funzionamento dell'amministrazione e, cioè, dei modi e dei tempi con i quali essa opera (le strutture, i procedimenti, le tecnologie, il personale, la gestione finanziaria), è rimasto purtroppo estraneo al dibattito sull'amministrazione come autorità-potere nei confronti dei cittadini. Inoltre, la concezione essenzialmente formalistica dell'attività amministrativa, intesa come insieme di procedimenti volti all'emanazione di atti e provvedimenti amministrativi, ha fatto passare in subordine l'importanza di organizzare nel modo più efficiente ed economico le risorse necessarie al perseguimento dei risultati che, attraverso le leggi, le pubbliche amministrazioni sono chiamate a conseguire e nei quali risiede uno dei compiti principali del controllo interno.[29]
Secondo alcuni studiosi, chi scrive incluso, l'attività dei servizi o nuclei di valutazione "interni[30] ad ogni Amministrazione" già previsti dal D.Lgs. n. 29/1993[31], se organizzata a "livello di centrale"[32], non sembra poter individuare, in caso di condotte fraudolente di dipendenti infedeli, profili di responsabilità manageriale *ex* art. 21 del D.Lgs. n. 80/1998 ed *ex* art. 4, 2° comma, del D.Lgs. n. 165/2001, o *ex* art. 7, comma 2, lett. g) della legge 15 marzo 2009, n. 15, per incapacità di organizzare un efficiente *Internal Audit*.

---

[24] Aldo PAVAN – Elisabetta REGINATO, "*Programmazione e controllo nello Stato e nelle altre amministrazioni pubbliche*", 2004, pag. 233 e ss.
[25] Cfr: V.Guccione, "*La nuova fisionomia del controllo interno. Modelli organizzativi e prime esperienze*", in Rivista Trimestrale di Diritto Pubblico, n. 3, 1998, pag. 769 e ss.
[26] Come ulteriormente potenziato dalla legge n. 94/1997 e dal D.lgs. n. 38/1998.
[27] Peraltro non completamente applicabile in ambito Ministero della Difesa (per effetto della sussistenza delle cosiddette "contabilità speciali").
[28] Per approfondimenti in chiave evolutiva dei controlli interni vds., tra gli altri,
Giuseppe BRUNI, "*Le imprese pubbliche in economia d'azienda*", 1968; Elio BORGONOVI, "*La pubblica amministrazione come sistema di aziende composte pubbliche, in introduzione all'economia delle amministrazioni pubbliche*", 1984; Giuseppe. FARNETI, "*Introduzione all'economia dell'azienda pubblica: il sistema, i principi, i valori*", 1995.
[29] Cfr: S. Cassese dal controllo sul processo al controllo sul prodotto, in "*Il nuovo sistema di controllo interno nella Pubblica Amministrazione*", Roma Istituto Poligrafico e Zecca dello Stato, 1993.
[30] Ora Organismi indipendenti di valutazione della *performance ex* art. 14, comma 8 del D.Lgs. n. 150/2009.
[31] Poi modificato dal D.Lgs. n. 470/1993.
[32] Nonostante l'esistenza degli obblighi di comunicazione alla Corte dei Conti imposti dal D.Lgs. n. 546/1993.

E ciò con buona pace del principio ISA (*Auditors International Standards*) 610 che stabilisce che "*Gli obiettivi della funzione di revisione interna sono stabiliti dalla direzione e, ove applicabile, dai responsabili delle attività di governance.*"
In altre parole, i "risultati negativi dell'attività amministrativa e della gestione", certamente presenti quando il patrimonio dello Stato è stato "depauperato", non sembrano debitamente "sanzionati" in caso di caso di *fraud*, allorquando può verificarsi, al massimo, "un mancato raggiungimento degli obiettivi", secondo il processo evolutivo che ha portato alla legge n. 15 ed al D.Lgs. n. 150/2009[33].
Se ciò sembra essere in linea con quanto affermato dalla stessa Corte dei Conti circa la "*carenza di cultura aziendalistica*" e sulla "*scarsa condivisione degli amministratori circa l'utilità dei controlli interni di gestione*"[34], è forse necessario addentrarsi nello studio di un aspetto fondamentale dell'*Internal Audit*: quello dei controlli antifrode.
Si ritiene utile effettuare tale approfondimento anche alla luce della recente normativa nazionale di settore, con uno sguardo particolare al piano triennale anticorruzione del Ministero della Difesa, tenendo in conto sia le esperienze di importanti organizzazioni internazionali, come la NATO, sia le dinamiche procedurali di Forze armate d'oltre oceano che, come abbiamo visto, vantano, al pari di altre istituzioni degli Stati Uniti d'America, un'antica tradizione di *Internal Audit*.

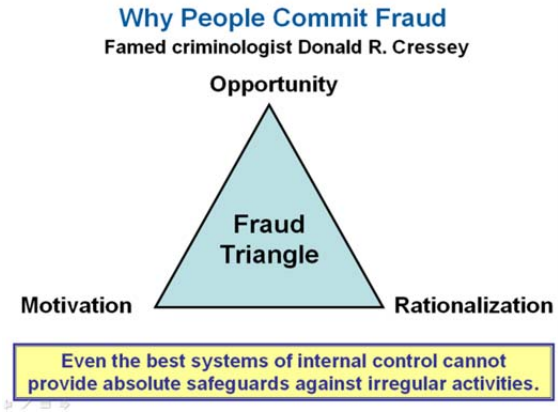
4. Il controllo antifrode e l'esperienza *US Army* e *NATO*: ipotesi di studio per il Ministero della Difesa.

Mentre l'INTOSAI ha definito il controllo interno come "*strumento manageriale usato per assicurare….che siano realizzati gli obiettivi di gestione*", la Corte dei Conti europea ha definito il controllo interno come "*l'insieme di tutte le strategie e procedure concepite ed attuate dalla direzione di un organismo al fine di garantire il raggiungimento economico, efficiente ed efficace degli obiettivi dell'organismo; l'osservanza delle norme esterne e (leggi, regolamenti ecc.) e delle politiche di gestione; la tutela dei beni e delle informazioni; la prevenzione e l'individuazione delle frodi e degli errori; la qualità dei libri contabili e la produzione tempestiva di informazioni finanziarie e di gestione affidabili*".[35] Ciò evidenzia un diverso approccio ed una diversa sensibilità in ciò che dovrebbe essere una delle principali finalità del controllo interno, ossia quella del controllo antifrode.
Tale forma di controllo è particolarmente complessa e richiede differenti competenze multidisciplinari che vanno dall'esperto contabile, al giurista d'impresa, all'analista di bilancio e revisore dei conti, all'*info-technology expert*.
Secondo i principi stabiliti dal *Governament Accountability Office*, l'ente federale di controllo negli Stati Uniti, il controllo teso ad accertare se, nel settore pubblico, le risorse sono state utilizzate in modo economico ed efficiente e nel rispetto di leggi e regolamenti è coerente con l'annuale verifica finanziaria e può essere condotto insieme al riesame dei controlli interni già effettuati dall'Amministrazione[36]che, come detto, sono anche "controlli antifrode". Ciò avviene negli Stati Uniti in piena autonomia ed indipendenza - tipiche delle funzioni anticorruzione - ed in linea con la contestuale applicazione dei principi di revisione internazionale ISA[37] 315 e 610[38].
Per addentrarci ora nell'analisi del concetto di frode, anche pubblica, e degli elementi che sottendono tale forma di truffa, per rimanere negli USA, ricordiamo che:

[33] Fabio DONATO, "*Le amministrazioni pubbliche verso logiche di governo partecipato*", 2011.
[34] Giampaolo LADU, "*Il sistema dei controlli*" in "*Contabilità dello Stato e degli Enti Pubblici*", 2013.
[35] Elena BRANDOLINI, "Il nuovo sistema dei controlli interni", http://www.univr.it/documenti/Documento/allegati/allegati406291.pdf, pag. 3.
[36] Giampaolo LADU, op. cit..
[37] Menzionati *Auditors international standards.*
[38] Rispettivamente "*Responsabilità del revisore esterno rispetto al lavoro del revisore interno*" e "*Utilizzo del lavoro dei revisori interni da parte dei revisori esterni*".

"*Donald R. Cressey* ha pubblicato, nel 1973, quella che oggi è la teoria di riferimento per spiegare i presupposi al verificarsi della frode in azienda: il *Fraud Triangle* o triangolo di Cressey.
Nel triangolo della frode, gli apici rappresentano i presupposti al verificarsi della frode:
- l'incentivo (pressione) alla commissione della frode (pressioni finanziarie, professionali, ecc.);
- l'opportunità di commettere la frode (mancanza o fallacità dei sistemi di controllo, meccanismi aziendali che permettono la commissione della frode);
- la razionalizzazione della frode, in altri termini la giustificazione che l'attore si dà per la commissione dell'evento fraudolento ("in fondo non danneggio nessuno", "l'azienda se lo merita", ecc.).

La teoria è stata sviluppata con un ardito ma efficace riferimento al triangolo del fuoco, che rappresenta, invece, i presupposti allo scoppio di un incendio e l'utilizzo di questo schema per identificare la tecnica più efficace per il suo spegnimento.
Nella teoria del triangolo del fuoco si fa riferimento ai tre elementi principali, ossia l'ossigeno, l'elemento combustibile e la fonte di calore: per spegnere un incendio è sufficiente agire su uno solo di questi tre elementi. Analogamente per agire efficacemente in chiave di prevenzione delle frodi, sarebbe sufficiente intervenire su almeno uno dei tre elementi tra motivazione, opportunità e incentivo"[39] visivamente descritti nella Fig. 3 sottoindicata.



- Fig. 3 -
Il triangolo della frode o "di Cressey"[40]

Ciò detto vediamo come l'*Associacion of Certified Fraud Examiners (ACFE)* definisce la frode:
"*Una falsa dichiarazione effettuata conoscendo la verità o l'occultamento di un fatto materiale per indurre un altro ad agire in suo danno. Di conseguenza, per frode si intende qualsiasi atto intenzionale o deliberato commesso al fine di privare un terzo di beni o di denaro attraverso l'utilizzo di astuzia, inganno, o altri mezzi sleali.*"

L'ACFE, poi, articola e distingue i vari tipi di frode, come di seguito descritto.

Types of Fraud
"*Le frodi contro una società possono essere commesse internamente dai dipendenti, dirigenti, funzionari, o proprietari stessi, oppure esternamente da parte dei clienti, fornitori e altri soggetti. Altre tipologie di frodi possono essere rivolte verso gli individui, piuttosto che verso le organizzazioni.*"

[39] Così Umberto SACCONE su: http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/Sistema-antifrode-e-ruolo-della-security-Umberto-Saccone.pdf
[40] www.controls.ucmerced.com

Internal Fraud

"*Le frodi interne, chiamate anche frodi professionali, possono essere definite come: "L'uso della propria occupazione per l'arricchimento personale attraverso l'utilizzo improprio intenzionale o l'applicazione errata delle risorse o dell'attività dell'organizzazione" In parole povere, questo tipo di frode si verifica quando un dipendente, dirigente, o un esecutivo commette frodi contro il proprio datore di lavoro. Anche se gli autori procedono con l'utilizzo sempre maggiore di idonee tecnologie e di nuovi approcci nell'impegno e nell'occultamento di schemi di frode professionali, le metodologie utilizzate in tali frodi rientrano generalmente in chiare categorie time-tested*".

External Fraud

"*Le frodi esterne contro una società coprono una vasta gamma di sistemi. Venditori disonesti potrebbero impegnarsi in programmi di bid-rigging*[41]*, fatturazioni della società per prodotti o servizi non previsti, o richieste di tangenti da parte dei dipendenti. Allo stesso modo, i clienti disonesti potrebbero presentare assegni o informazioni sull'account falsificato per il pagamento, o potrebbe tentare di restituire i prodotti rubati o resi fuori servizio per ottenere un rimborso. Inoltre, le organizzazioni devono affrontare anche le minacce di violazioni della sicurezza e dei furti di proprietà intellettuale perpetrati da terzi ignoti. Altri esempi di frodi commesse da terzi esterni includono la truffa informatica*[42]*, il furto di informazioni riservate, la frode fiscale, la bancarotta fraudolenta, la frode assicurativa, la frode sanitaria, e la frode sui prestiti.*

Fraud Against Individuals

"*Numerosi truffatori hanno messo a punto sistemi di frode a danno individui. Il furto di identità, il metodo Ponzi*[43]*, il phishing*[44]*, e il metodo di tassazioni fraudolente, sono solo alcuni dei metodi criminali con cui si tenta di rubare denaro da vittime ignare.*"[45]

Dopo aver delineato gli ambiti operativi e fattuali delle frodi, vediamo ora, con specifico riferimento ai summenzionati standard IIA, cosa dice lo Standard di prestazione 2120.A2 relativamente al rapporto esistente tra le frodi e l'attività di *Internal Audit*: "*l'attività di internal audit deve valutare la potenziale presenza di casi di frode e come l'organizzazione gestisce tali rischi*". Tale requisito deve peraltro essere contemperato con il noto Standard di connotazione 1210.A2[46] che recita "*gli internal auditor devono possedere conoscenze sufficienti per valutare i rischi di frode e il modo con cui l'organizzazione li gestisce, senza aspettarsi che abbiano le competenze proprie di chi ha come responsabilità primaria quella di individuare e investigare frodi*".

Per quanto sopra, come lucidamente osservato da autorevole dottrina economica[47]: "*Gli Standard professionali richiedono quindi che l'internal auditor, pur svolgendo un ruolo diverso dal "fraud auditor", sia in grado di riconoscere gli indicatori di frode. In particolare, nello svolgimento del proprio incarico, dovrà prestare attenzione all'evoluzione di indicatori di frode di cui scorga evidenza nel corso delle verifiche, come per esempio dipendenti con elevate e ingiustificate ore di straordinario e/o situazioni di elevato numero di giorni di ferie non godute, scarsa job rotation,*

[41] Frodi contrattuali in parte assimilabili alla cosiddetta "turbativa d'asta".

[42] Si osservi che, come meglio chiarito nel prosieguo del presente studio, la truffa informatica può essere anche una "truffa interna" in quanto il dipendente infedele, ad esempio, può manipolare elettronicamente delle informazioni/disposizioni bancarie, al fine di perpetrare delle truffe compiute anche dall'interno dell'Organizzazione.

[43] Il metodo Ponzi (che prende il nome dal celebre truffatore italo-americano Charles Ponzi) è un'operazione di investimento fraudolento in cui l'operatore, un individuo o organizzazione, restituisce ai suoi investitori non gli interessi ma il nuovo capitale versato dai nuovi investitori, piuttosto che il profitto conseguito dal gestore.

[44] L'IISFA (di cui lo scrivente è socio) analizza puntualmente il fenomeno del *phishing* sotto il profilo tecnico e forense sull'"*International Information Systems Forensics Association (IISFA) – Memberbook 2010 Digital Forensic*" Cap. II, 2010.

[45] Liberamente tradotto dall'autore da: http://www.acfe.com/fraud-101.aspx

[46] Vds: http://www.theiia.org/guidance/standards-and-guidance/ippf/standards/full-standards/?search=risk già indicato in via generale al precedente paragrafo 2.

[47] Vds. Silvia CATALANO in "*Lezioni antifrode per l'internal audit*" 2011.

bassa tracciabilità o inadeguata segregazione dei controlli, insufficiente definizione delle responsabilità eccetera".

Ma se, come abbiamo visto, la menzionata "responsabilità primaria di investigare e individuare le frodi" non è né dell'*auditor* né del *fraud auditor*, a chi risale tale responsabilità ? Forse al revisore dei bilanci o della contabilità ?

Benché i "principi di revisione internazionale" pubblicati da *International Auditing and Assurance Standards Board di International Federation of Accountants (IFAC)* non siano direttamente applicabili alla Pubblica Amministrazione centrale e, più in particolare, alla "revisione della contabilità speciale" degli Enti militari che appartengono al cosiddetto "ramo esclusivo della Pubblica Amministrazione" (Ministero della Difesa incluso), al fine di trovare risposta al precedente interrogativo, vediamo cosa prevede il principio *(ISA) 240,* denominato "Le responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio": "*La responsabilità principale per la prevenzione e l'individuazione delle frodi compete sia ai responsabili delle attività di governance dell'impresa, sia alla direzione. E' importante che la direzione, con la supervisione dei responsabili delle attività di governance, ponga forte enfasi sulla prevenzione delle frodi volta a ridurre le occasioni che esse si verifichino, nonché introduca azioni deterrenti finalizzate a dissuadere dal commettere le frodi a causa della più elevata probabilità che queste siano individuate e punite. Ciò comporta un impegno per la creazione di una cultura aziendale ispirata al valore dell'onestà ed a comportamenti eticamente corretti che può essere rafforzata mediante un'attiva supervisione da parte dei responsabili delle attività di governance. La supervisione da parte dei responsabili delle attività di governance include la considerazione della possibilità di forzatura dei controlli o che altri fattori impropri influenzino il processo di predisposizione dell'informativa finanziaria, quali i tentativi della direzione di manipolare i risultati d'esercizio al fine di influenzare la percezione da parte degli analisti finanziari riguardo la performance e la capacità di produrre profitti dell'impresa.*"

E' molto importante, ad avviso di chi scrive, notare come per i "principi di revisione internazionali" debbano essere la Direzione ed il Management a porre la massima attenzione nell'assicurare l'attuazione di ogni azione preventiva, dissuasiva e di supervisione finalizzata a scongiurare le frodi. Ovviamente, molto importante è anche la "responsabilità operativa" dell'*internal auditor* (termine più frequentemente utilizzato "nel pubblico") in quanto egli - nel caso in cui il *management* garantisca la massima trasparenza e collaborazione - è colui che potrebbe "scoprire" le "false rappresentazioni amministrativo-contabili" della realtà gestionale.

In tal senso, infatti, va letta, ad avviso dell'autore, la definizione di "frode" fornita dal glossario delle *Guidelines for Internal Control Standards for the Public Sector*[48]*: "An unlawful interaction between two entities, where one party intentionally deceives the other through the means of false representation in order to gain illicit, unjust advantage. It involves acts of deceit, trickery, concealment, or breach of confidence that are used to gain some unfair or dishonest advantage. (XVI INCOSAI, Uruguay, 1998).*

Particolarmente utile nel delineare il concetto di frode appare poi il sotto riportato punto 6 del summenzionato principio ISA 240 sulla "responsabilità del revisore" che descrive analiticamente le possibili modalità attuative del disegno criminoso del dipendente (privato o pubblico) che pone in essere condotte fraudolente:

"*Il rischio di non individuare un errore significativo dovuto a frodi è più elevato rispetto al rischio di non individuare un errore significativo derivante da comportamenti od eventi non intenzionali. Ciò in quanto la frode può prevedere piani sofisticati ed organizzati attentamente, progettati al fine di occultarla, come ad esempio falsificazioni, omissioni intenzionali nella registrazione contabile di operazioni ovvero dichiarazioni intenzionalmente fuorvianti rilasciate al revisore. Simili atti volti ad occultare l'esistenza di frodi possono essere ancora più difficili da individuare se accompagnati*

[48] Presentate per l'approvazione al XVIII congresso del supremo organo dell'INTOSAI (INCOSAI) tenutosi a Budapest nel 2004.

da collusione. In presenza di collusione il revisore può essere indotto a ritenere che gli elementi probativi ottenuti siano persuasivi quando, in realtà, sono falsi. La capacità del revisore di individuare una frode dipende da fattori quali l'abilità di chi la commette, la frequenza e l'ampiezza delle manipolazioni, il livello di collusione, l'ammontare dei singoli importi manipolati ed il livello di autorità delle persone coinvolte. Mentre il revisore può essere in grado di identificare le potenziali circostanze per perpetrare una frode, è invece difficile che stabilisca se errori in aree soggette a valutazioni, come le stime contabili, siano causati da frodi ovvero da comportamenti o eventi non intenzionali."

Inoltre, per quanto attiene al settore pubblico, il principio di revisione internazionale n. 265 "Comunicazione delle carenze nel controllo interno ai responsabili delle attività di *governance* ed alla direzione", al punto A27 "Considerazioni specifiche per le amministrazioni pubbliche", recita: *"I revisori operanti nel settore pubblico possono avere ulteriori responsabilità di comunicare le carenze nel controllo interno identificate nel corso della revisione contabile, i cui modi, livello di dettaglio e destinatari non sono previsti nel presente principio di revisione. Ad esempio, è possibile che le carenze significative vadano comunicate all'organo legislativo o ad altri organi di governo. Leggi e regolamenti, o altre fonti normative, possono anche imporre ai revisori operanti nel settore pubblico di comunicare le carenze nel controllo interno, indipendentemente dalla rilevanza degli effetti potenziali di tali carenze. Inoltre, la normativa può richiedere che i revisori operanti nel settore pubblico comunichino aspetti più ampi relativi al controllo interno in aggiunta alle carenze nel controllo interno la cui comunicazione è richiesta dal presente principio di revisione, ad esempio, i controlli relativi al rispetto di leggi, regolamenti o previsioni contrattuali o accordi per l'erogazione di contributi.*"

Ciò lascia capire che le funzioni di chi ha l'onere di occuparsi di revisione[49] nel settore pubblico:
- includono aspetti più ampi rispetto alla semplice denuncia di carenza di controllo interno;
- prevedono anche, se del caso, comunicazioni all'organo legislativo e/o di governo.

Nei principi internazionali, vi è quindi una "maggiore responsabilità" di chi si occupa di revisione "nel pubblico" relativamente alla "segnalazione" agli organi di legislazione o di governo delle carenze, complessive e di dettaglio, riscontrate nel settore dell'*Internal Audit*.

Con particolare riferimento alla problematica della gestione del rischio antifrode, si osserva che essa è stata affrontata, a livello internazionale, da varie istituzioni internazionali, fra le quali, per citarne solo alcune, l'*American Institute of Certified Public Accountants*, l'*Association of Certified Fraud Examiners*, l'*Institute of Internal Auditors* e l'*Information Systems Audit and Control Association*.

Secondo tali organizzazioni si potrebbe sintetizzare dicendo che un efficace sistema antifrode dovrebbe articolarsi sui seguenti pilastri:
1. la creazione e il mantenimento di una cultura aziendale basata sull'etica e l'onestà;
2. l'aggiornamento continuo dei sistemi e delle procedure di mitigazione del rischio di frode;
3. il potenziamento e lo sviluppo delle strutture preposte alle attività di vigilanza e controllo.

Tali Istituzioni internazionali confermano dunque come la prima esigenza sia quella di migliorare l'ambiente di lavoro, cioè la cultura aziendale. Infatti, proprio una cultura aziendale incentrata sull'etica e sul "fare la cosa giusta" sembrerebbe rappresentare la misura più idonea ad inibire o ad interrompere sul nascere comportamenti non corretti, o fraudolenti. Tuttavia, anche se in un certo qual modo una struttura permeata da buoni principi, aiuta una diligente attuazione dei compiti da parte dei dipendenti, non può ignorarsi che l'intero *management* debba per primo:
- evitare ogni forma di pur tacito assenso a condotte eticamente scorrette;
- assicurare e garantire il più "dissuasivo" *Internal Audit* possibile.

"Tra i mezzi a disposizione per raggiungere lo scopo possono annoverarsi il Codice di Comportamento o il Codice Etico, da diffondere tramite gli strumenti più opportuni a tutti i livelli aziendali. Un ambiente di lavoro positivo, sereno e corretto in cui il lavoratore non si senta abusato,

[49] In ambito nazionale vds. concettualmente il riferimento alla revisione legale dei conti (degli enti locali), a norma dell'articolo 16, comma 25, del decreto legge 13 agosto 2011, n.138, convertito in legge 14 settembre 2011, n.148.

sfruttato o semplicemente ignorato, è già una buona garanzia di successo nella lotta alle frodi aziendali interne. In questo ambiente favorevole i dipendenti, solitamente quelli più produttivi, diventano vere e proprie "sentinelle antifrode" rispettando in prima persona le regole ed esigendo che queste vengano rispettate anche dai colleghi meno disciplinati.
Il secondo pilastro dei modelli antifrode riguarda il complesso delle procedure e dei controlli adottati dall'azienda. Il primo passo da compiere consiste nell'individuare i punti di debolezza del sistema in essere e capire se da questi possano scaturire potenziali danni all'azienda privata come per un Ente statale.
Questa attività è chiamata "*Fraud Risk Assessment*" e risulta essere lo strumento più adatto ad effettuare la valutazione del complesso dei processi, delle procedure e delle attività aziendali al fine di individuarne i punti di debolezza. Solitamente questa attività è svolta da professionisti esterni, in quanto è necessaria una valutazione autonoma, indipendente e critica sulle reali vulnerabilità dei sistemi antifrode. Una volta identificati i punti di debolezza occorre adeguare il modello di prevenzione, individuazione e deterrenza in modo da renderlo idoneo a gestire efficacemente un rischio, quale quello di frode, mai del tutto eliminabile e potenzialmente letale per l'azienda. Il sistema così implementato non deve essere statico bensì deve evolvere nel corso degli anni. Il sistema economico è infatti dinamico, pertanto anche un sistema antifrode che si vuole mantenere in efficienza, seppur adeguato alle esigenze del momento, deve essere costantemente monitorato e migliorato. L'ultimo pilastro sul quale poggia un valido programma di prevenzione del rischio di frode, riguarda le strutture preposte all'attività di vigilanza e controllo. Tale compito può essere assunto da vari organismi sia interni che esterni all'azienda, quali a titolo esemplificativo, il Comitato di *Internal Audit*, il Consiglio di Amministrazione, i *fraud auditor*."[50]
Con specifico riguardo al *Fraud Risk Assessment* di cui sopra, al fine di delinearne finalità e obiettivi (in prevenzione di "frodi governative") vediamo ora a seguire, in lingua originale, come descrive il fenomeno l'ACFE (*Associacion of Certified Fraud Examiners*).
"*Fraud risk assessment is a process aimed at proactively identifying and addressing an organization's vulnerabilities to internal and external fraud. As every organization is different, the fraud risk assessment process is often more an art then a science. What gets evalueted and how it gets assessed should be tailored to the organization – there is no one-size-fits-all approach.*
Additionally, organizational fraud risks continually change. It is therefore important to think about a fraud risk assessment as an ongoing, continuous process rather then just an activity.
The objective of a fraud risk assessment is to help an organization recognize what makes it more vulnerable to fraud. Through a fraud risk assessment, the organization is able to identify where fraud is most likely to occur, enabling proactive measures to be considered and implemented to reduce the chance that it could happen.
Government fraud
Asset misappropriation schemes (cash schemes / non – cash schemes).
1) Cash schemes

- *Fraudolent disbursements – are on book fraude schemes, meaning that cash (checks) leaves the entity fraudulently, but is recorded on the books, and thus an audit trail exists.*
  Fraudolent disbursements are broken down into the following types: check tampering schemes, register disbursement schemes, billing schemes, expense reimbursement schemes, and payroll schemes.
- *Cash larceny – is an occupational setting, may be defined as the intentional taking away of an employer's cash without the consent and against the will of the employer.*

[50] Così Stefano MARTINAZZO, Simone MIGLIORINI, in "*Sistemi antifrode: i pilastri fondamentali*" su http://www.diritto24.ilsole24ore.com/avvocatoAffari/professioneLegale/2012/02/sistemi-antifrode-i-pilastri-fondamentali.php
Sulla necessità di implementare i sistemi antifrode vds. anche Mauro DI GENNARO su http://www.ecnews.it/2013/10/approccio-aziendale-alle-frodi/

Cash larceny schemes involve the theft of money that has already appeared on a victim company's book.

- *Skimming – is the theft of cash that has not been recorded in the accounting system.*
  The way in which an employee extracts the cash for a skimming scheme may be the same for a cash larceny scheme; the difference however is the timing. Skimming occurs before the cash is recorded as received on the accounting records ò thus, it is known as an off - book scheme whereas cash larceny occurs after the cash receipt transaction is recorded. The most common places for the skimming schemes to occur are in sales and accounts receivable.

2) *Non – cash schemes (inventory and other assets)*
   Non cash schemes involve the theft or misuse of inventor, equipment, supplies, and other physical assets of the company. In particular inventory theft is a very common and costly form of fraud, and there are four categories of inventory fraud: unconcealed larceny, falsified receiving reports, fraudulent shipments and fraudulent materials requisitions."[51]

Dopo tale puntuale approccio tassonomico di respiro internazionale, vediamo che in ambito nazionale, la sempre maggiore attenzione alla prevenzione dei fenomeni corruttivi nell'Amministrazione, ha portato all'approvazione della legge 6 novembre 2012, n. 190[52], recante disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella P.A., che ha disciplinato in modo organico un piano di azione, coordinato su tutto il territorio nazionale, volto al controllo, prevenzione e contrasto della corruzione e dell'illegalità.

Non potendo, per ovvie ragioni di sinteticità, affrontare analiticamente la citata legge 6 novembre 2012, n. 190, ci si limita, ai fini del presente studio, a segnalare l'articolo 31[53] del D.Lgs. 14 marzo, 2013, n. 33[54] predisposto in attuazione dei principi e criteri di delega previsti dall'articolo 1, comma 35 della suddetta norma anticorruzione. Il predetto art. 31 sancisce il dovere per la P.A. di pubblicare, unitamente agli atti cui si riferisce l'obbligo di pubblicità, anche i rilievi non recepiti degli organi di controllo interno, degli organi di revisione amministrativa e contabile e tutti i rilievi, ancorché recepiti, della Corte dei Conti riguardanti l'organizzazione e l'attività dell'amministrazione o di singoli Uffici.[55] Sarà di straordinaria rilevanza, monitorare la reale applicazione da parte della P.A. della norma *de qua*, anche al fine di far luce su quelli che potremmo definire i "*coni d'ombra amministrativi*" della P.A..

Tali "zone grigie" possono essere "illuminate" anche con il cosiddetto *whistleblowing* da qualsiasi dipendente che nell'esercizio delle proprie funzioni scopra e denunci un fatto illecito.

Molto importante al riguardo appare l'Art. 54-bis, comma 1, del D.Lgs. 165/2001 (Tutela del dipendente pubblico che segnala illeciti), articolo introdotto dalla summenzionata norma anticorruzione e precisamente dall'art.1, comma 51, della legge n. 190 del 2012: "*1. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile, il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti o all'Autorità nazionale anticorruzione (ANAC), ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o*

[51] www.acfe.com

[52] In attuazione dell'articolo 6 della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 e ratificata ai sensi della legge 3 agosto 2009, n. 116, e degli articoli 20 e 21 della Convenzione penale sulla corruzione, fatta a Strasburgo il 27 gennaio 1999 e ratificata ai sensi della legge 28 giugno 2012, n.110.

[53] Denominato "*Obblighi di comunicazione concernenti i dati relativi ai controlli sull'organizzazione e sull'attività dell'amministrazione*".

[54] Per il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, mediante la modifica o l'integrazione delle disposizioni vigenti, anche prevedendo nuove forme di pubblicità.

[55] Vds. relazione illustrativa al provvedimento su:
http://www.tuttocamere.it/files/pamministrazione/2013_33_Relazione.pdf

indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia."[56]

Il mondo cambia e con esso l'assetto normativo del mondo dell'anticorruzione: ci si augura che presto anche la giurisprudenza di settore recepisca unanimemente la *ratio* di questa fondamentale norma di civiltà giuridica.

Il dipendente onesto che contribuisce alla tutela della *cosa pubblica*, ha diritto all'anonimato e va tutelato e difeso.

Inoltre, particolarmente significativi appaiono i contenuti della relazione illustrativa del disegno di legge che ha portato all'emanazione della prefata "norma anticorruzione", in quanto l'obiettivo della prevenzione e repressione del fenomeno corruttivo viene "mirato" attraverso un approccio multidisciplinare o forse per meglio dire multisettoriale, nel quale gli strumenti sanzionatori si configurano solamente come alcuni dei fattori per la lotta alla corruzione e all'illegalità nell'azione amministrativa. Più in dettaglio si nota che tale relazione illustrativa pone a sostegno del provvedimento legislativo, motivazioni di trasparenza e controllo proveniente dai cittadini stessi[57] e di adeguamento dell'ordinamento giuridico italiano agli *Standards internazionali* di riferimento.

La predetta relazione illustrativa precisa, inoltre, come la corruzione[58] porti danni alla credibilità del sistema Paese[59] che si traducono anche in danni di ordine economico, per effetto del potenziale calo degli investimenti, anche stranieri, frenando così lo sviluppo economico.

Infatti, "la Commissione per lo studio e l'elaborazione di proposte in tema di trasparenza e prevenzione della corruzione nella pubblica amministrazione, istituita il 23 dicembre 2011 dal Ministro per la pubblica amministrazione e la semplificazione col doppio mandato di formulare emendamenti al disegno di legge in materia di corruzione e di predisporre un Rapporto in materia, diretto ad identificare politiche, modalità e misure di prevenzione della corruzione del settore pubblico, nella propria analisi ha ricondotto le motivazioni che possono indurre alla corruzione ai seguenti due ordini di ragioni:

- economiche, derivanti dal bilanciamento tra l'utilità che si ritiene di poter ottenere, la probabilità che il proprio comportamento sia scoperto e la severità delle sanzioni previste;
- socio- culturali: la corruzione è tanto meno diffusa quanto maggiore è la forza delle convinzioni personali e di cerchie sociali che riconoscono come un valore il rispetto della legge; infatti, dove è più elevato il senso civico e il senso dello Stato dei funzionari pubblici, i fenomeni corruttivi non trovano terreno fertile per annidarsi.

La corruzione, e più in generale il malfunzionamento dell'amministrazione a causa dell'uso a fini privati delle funzioni attribuite, ha un costo per la collettività, non solo diretto (come, ad esempio, nel caso di pagamenti illeciti), ma anche indiretto, connesso ai ritardi nella conclusione dei procedimenti amministrativi, al cattivo funzionamento degli apparati pubblici, alla sfiducia del cittadino nei confronti delle istituzioni, arrivando a minare i valori fondamentali sanciti dalla Costituzione: uguaglianza, trasparenza dei processi decisionali, pari opportunità dei cittadini.

Sulla base di tali presupposti, la legge n. 190 del 2012 ha introdotto un "nuovo concetto di corruzione", inteso in senso lato, comprensivo altresì di quelle ipotesi in cui, nell'esercizio dell'attività amministrativa, si riscontri l'abuso da parte di un soggetto del potere affidatogli al fine di ottenere vantaggi privati. Le situazioni rilevanti sono, quindi, più ampie delle mere fattispecie penalistiche di cui agli artt. 318, 319 e 319 ter del codice penale, e ricomprendono non solo l'intera

[56] Comma così modificato dall'art. 31, comma 1, legge n. 114 del 2014.

[57] Anche dipendenti: vds. la "procedimentalizzazione" del fenomeno di *whistleblowing.*

[58] Vds. per un approccio multidisciplinare al fenomeno: Sergio SEMINARA, *"La riforma dei reati di corruzione e concussione come problema giuridico e culturale*", in Diritto penale e processo, fascicolo n. 10/2012, da pag. 1235 a pag. 1245.

[59] Per approfondimenti di taglio penalistico sulle tipologie dei fenomeni criminali *de quibus* Vds.: Emilio DOLCINI e Francesco VIGANÒ, *"Sulla riforma in cantiere dei delitti di corruzione"*, in *Dir. pen. cont. – Riv. trim.*, 1, 2012, 232 ss.; Paola SEVERINO, *"La nuova Legge anticorruzione"*, in *Dir. Pen. e Proc.*, 2013, 7 ss. (la quale evidenzia l'ampliamento della gamma dei beni attinti dal delitto di corruzione, per la necessaria inclusione, ora, anche della concorrenza).

gamma dei delitti contro la pubblica amministrazione (disciplinati nel Titolo II, Capo I, del codice penale), ma anche tutte quelle situazioni in cui, pur non verificandosi una situazione penalmente perseguibile, si realizzi una distorsione dell'azione amministrativa dovuta all'uso a fini privati delle funzioni pubbliche attribuite, in dispregio ai principi di trasparenza e di imparzialità cui l'azione pubblica deve costantemente ispirarsi. Il fenomeno corruttivo può compromettere il buon andamento e l'imparzialità della pubblica amministrazione. Esso, infatti, nel momento in cui dà rilievo agli interessi privati estranei alla pubblica amministrazione, tende a inquinare e distorcere il corretto esercizio delle pubbliche funzioni, potendo comportare un vero e proprio esercizio disfunzionale dei poteri. Un pregiudizievole inquinamento dell'esercizio funzionale, a rigore, si ha soltanto quando il vantaggio privato svolge in termini immediati e diretti una pressione motivazionale sul comportamento del pubblico funzionario contrario ai doveri d'ufficio."[60]
In particolare, il Piano Nazionale Anticorruzione 2015 - 2017 del Ministero della Difesa, che ad avviso di studiosi come chi scrive, e non solo, rappresenta un esempio di eccellenza in ambito P.A., ha ad oggetto l'individuazione delle iniziative necessarie, nonché degli adeguati assetti organizzativi e gestionali, per prevenire, rilevare e contrastare i fenomeni corruttivi e di malfunzionamento negli ambiti interessati da potenziali rischi di corruzione nell'esercizio delle attività amministrative e gestionali ed è stato elaborato nel rispetto delle seguenti finalità:

- individuare le attività nell'ambito delle quali è più elevato il rischio di corruzione;
- prevedere meccanismi di formazione, attuazione e controllo delle decisioni, idonei a prevenire il rischio di corruzione;
- prevedere obblighi di informazione nei confronti del Responsabile della prevenzione della corruzione, chiamato a vigilare sul funzionamento e sull'osservanza del Piano;
- monitorare il rispetto dei termini previsti dalla legge e/o dai regolamenti per la conclusione dei procedimenti amministrativi;
- individuare obblighi di trasparenza nel rispetto delle disposizioni di legge.

Tuttavia, come detto, l'obiettivo del presente lavoro non è quello di analizzare nel dettaglio il menzionato Piano Nazionale Anticorruzione 2015 - 2017 del Ministero della Difesa, per cui ci si limita ad osservare che stante l'attuale l'assetto ordinativo ed organizzativo dei "controlli interni" delle Amministrazioni centrali[61] a cui si è fatto cenno, il PNA-Difesa non fa un espresso richiamo agli *Standard di Internal Audit*.

Alla luce di ciò, al fine di meglio comprendere come il collaterale Ministero della Difesa Americano abbia recepito i più volte citati *Standard internazionali* in materia di *Internal Audit*[62], pare molto interessante andare ad analizzare alcuni aspetti dell'*Army Internal Review Program*[63] dell'Esercito Americano, di cui si riportano alcuni passaggi ritenuti significativi a fini del nostro studio.

---

[60] Così la premessa del Piano Nazionale Anticorruzione 2015 2017 del Ministero della Difesa, di cui all'art. 1, comma 5, lett. a) della legge 6 novembre 2012, n. 190, è stato emanato anche sulla base del decreto legislativo 14 marzo 2013, n. 33 (recante riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni), del Codice di comportamento dei dipendenti pubblici adottato con decreto del Presidente della Repubblica 16 aprile 2013, n. 62, del D.Lgs. 8 aprile 2013, n. 39 (recante disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190) e ovviamente, del Piano Nazionale Anticorruzione (PNA), oltre che del decreto-legge 24 giugno 2014, n. 90 (convertito con modificazioni dalla legge 11 agosto 2014, n.114, recante misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari).

[61] Come il Ministero della Difesa.

[62] Spesso espressamente menzionati nei "Codici di comportamento" emanati dai Ministeri (adottati ai sensi dell'art. 54 del decreto legislativo 30 marzo 2001, n. 165 e secondo le linee guida del D.P.R. 16 aprile 2013, n. 62). Vds. MARTINAZZO – MIGLIORINI, *op. cit.*, in nota n. 42.

[63] Reperibile *open sources:* http://www.apd.army.mil/pdffiles/r11_7.pdf. Tale documento "non classificato" cita espressamente gli *American Institute of Certified Public Accountants (AICPA) Standards*, .gli *Institute of Internal Auditors (IIA) Internal Audit Standards*, *i Government Auditing Standards*, ecc..

Concetto di revisione interna

a. Il principio fondamentale della filosofia di gestione dell'Esercito è che i Comandanti a tutti i livelli sono responsabili della realizzazione delle loro missioni e dell'efficace gestione delle risorse messe a loro disposizione per la realizzazione della missione. I Comandanti sono responsabili del rispetto delle leggi, delle politiche e delle procedure, di realizzare il programma assegnato per il raggiungimento degli obiettivi e sono responsabili della precisione, correttezza, legalità e affidabilità delle loro azioni. Nell'esercizio della loro responsabilità, i Comandanti potranno usare la loro capacità di *Internal Review* (d'ora in avanti IR) e altri aspetti del loro sistema di controllo interno per garantire la conservazione e l'uso corretto delle risorse.
b. I *report interni* sono basati sulla legge e sui requisiti normativi di comando (…);

Obiettivo del programma

a. L'IR è un'organizzazione indipendente, obiettiva, che garantisce l'attività di consulenza all'interno del Comando progettata per aggiungere valore e migliorare le operazioni del comando. L'obiettivo del programma IR dell'Esercito è quello di fornire ai Comandanti e al loro personale, con una gamma completa di servizi di revisione interna, decisioni professionali che siano tempestive e che sostengano i responsabili delle decisioni locali al fine di garantire una gestione efficace.
b. L'IR è uno strumento primario del sistema di "comando e controllo" del Comandante, progettato per ridurre i rischi e per aumentare la garanzia dell'efficacia ed efficienza delle operazioni di comando.

Requisiti legali e normativi, clausole contrattuali, e convenzioni di sovvenzione.

a. I valutatori determineranno quali leggi, regolamenti e disposizioni di contratti o convenzioni di sovvenzione sono significativi nel contesto degli obiettivi di revisione e valuteranno il rischio che le violazioni di tali leggi, regolamenti e disposizioni di contratti o convenzioni di sovvenzione potrebbe verificarsi. Sulla base di tale valutazione del rischio, i valutatori dovranno progettare ed eseguire procedure per fornire una ragionevole garanzia di rilevare casi di violazione dei requisiti legali e normativi o violazioni delle disposizioni di contratti o convenzioni di sovvenzione che sono rilevanti nel contesto degli obiettivi di recensione.
b. La valutazione del rischio da parte dei valutatori può essere influenzata da fattori quali la complessità o la novità di leggi, regolamenti e disposizioni di contratti o convenzioni di sovvenzione. Tale valutazione può esaminare le misure dei controlli esistenti per verificarne l'efficacia nel prevenire o individuare violazioni di leggi, regolamenti e disposizioni di contratti o convenzioni di sovvenzione. Se i valutatori ottengono sufficienti prove di un'adeguata efficacia di questi controlli, possono ridurre la portata dei loro test di conformità.

Frode

a. Nel pianificare la revisione, gli *Internal Review Officers* valuteranno i rischi di frode esaminando ciò che è significativo nel contesto del obiettivi di recensione. I membri del team di recensione discuteranno sui rischi di frode, inclusi i fattori quali le persone, gli incentivi o le pressioni che possano indurre a commettere delle frodi, la possibilità che le frodi si verifichino e le razionalizzazioni o gli atteggiamenti che potrebbero consentire agli individui di commettere delle frodi. I revisori dovranno raccogliere e valutare le informazioni per identificare i rischi di frode che sono significativi nell'ambito degli obiettivi di revisione o che potrebbero influenzare i risultati e le conclusioni. Per esempio, i valutatori possono ottenere informazioni attraverso la discussione con i funzionari dell'Ente revisionato o attraverso altri mezzi volti a determinare la vulnerabilità del programma antifrode, lo stato dei controlli interni dell'Ente che ha stabilito di rilevare e prevenire le frodi o il rischio (leggasi l'eventualità) che i funzionari dell'Ente esaminato potessero ignorare il controllo interno. Un atteggiamento di scetticismo professionale nel valutare questi rischi deve assistere i revisori nel valutare quali fattori o rischi potrebbero significativamente influenzare gli obiettivi di revisione.

b. Quando i valutatori identificano alcuni fattori o rischi di frode verificatasi o potenzialmente verificabili nel contesto degli obiettivi di revisione, saranno definite le procedure per garantire una ragionevole certezza di individuare tali frodi.
   "Valutare il rischio di frode" è un processo *ongoing* durante tutta la revisione ed è finalizzato non solo alla pianificazione della revisione, ma anche alla valutazione delle prove ottenute durante la revisione.
c. Quando le informazioni acquisite richiamano l'attenzione dei valutatori perché la frode potrebbe essersi verificata, i valutatori estenderanno i passi e le procedure di ricorso, se necessario, a determinare se:
   (1) si è verosimilmente verificata in concreto una frode;
   (2) si è verificata la frode, il suo effetto complessivo da inserire nel *report*. Se la frode che può essersi verificata non è significativa nel contesto degli obiettivi di revisione, i valutatori possono svolgere un lavoro di revisione supplementare, con un impegno aggiuntivo e separato, o adire ad altre parti con responsabilità di supervisione o giurisdizione.

Frode, atti illegali, violazioni delle disposizioni di contratti o convenzioni di sovvenzione, e abusi.

a. Quando i revisori/valutatori concludono, in base a sufficienti prove del caso, che la frode, o atti illeciti, o significative violazioni delle disposizioni di contratti o convenzioni di sovvenzione, o abusi importanti si sono verificati o è probabile che si siano verificati, essi sono tenuti a denunciare il fatto come una scoperta.
b. Quando i valutatori rilevano violazioni delle disposizioni di contratti o convenzioni di sovvenzione, o abusi che non sono significativi, essi comunicano tali constatazioni per iscritto ai funzionari dell'Ente esaminato a meno che i risultati siano irrilevanti nel contesto degli obiettivi di revisione, considerando fattori sia qualitativi che quantitativi. (…)
c. Quando la frode, gli atti illegali, ecc. si sono verificati o è probabile che si siano verificati, i valutatori possono consultarsi con le Autorità preposte al fine di valutare se segnalare pubblicamente tali informazioni che potrebbero compromettere i procedimenti investigativi o giuridici. I valutatori possono limitare la loro comunicazione pubblica su questioni che non comprometterebbero tali procedimenti, e, per esempio, possono limitare i contenuti della relazione alle sole informazioni che sono già in possesso della pubblica informazione.

Anche in ambito NATO, l'impostazione di massima del servizio di *Internal Audit* e la filosofia che sottende tale attività è fondamentalmente analoga, per cui, pur tralasciando di entrare nel merito di direttive "classificate" per chiare ragioni di riservatezza delle stesse, l'autore può tuttavia esporre - avendo svolto un mandato pluriennale all'estero presso la predetta Organizzazione internazionale nell'incarico di *Internal Review Officer* - alcune consapevoli considerazioni di carattere generale mirate ad evidenziare delle possibili criticità dell'attuale organizzazione di *Internal Audit* in ambito Ministero della Difesa.
Stando alla tipologia di attività svolta dall'*internal auditor* NATO, la sua *job description* evidenzia[64] come egli sia responsabile, tra l'altro, di condurre un'attività di IA su tutta la gestione e rendicontazione dei fondi internazionali e sulle attività operative, inclusa la gestione dei sistemi contabili informatizzati. In particolare, le aree di *Internal Audit* includono: *"financial management and accounting, risk management, corporate governance, performance management and measurement, material, transportation, communication and ADP systems, base engineering, and aircraft maintenance management, purchasing and contracting, as well as civilian personnel entitlements and administration, and NATO Security Investment Programme funding. Conducts audits of services being provided by other NATO Forces and Host Nations in accordance with relevant Memoranda of understanding/Agreement."*

[64] http://www.aco.nato.int/resources/20/vacancies/shape/A3,AUDITOR(FINANCIAL%20SYSTEMS),A25_0913,20DEC13,WEB.pdf

Inoltre, è significativo notare come, in ambito internazionale, oltre ad un'esperienza pluriennale nel settore dell'*auditing* serva anche una comprovata conoscenza degli *International Standards* di cui abbiamo avuto modo di accennare nella prima parte del presente lavoro.
Infatti, la *job description* dell'*Internal Auditor NATO* richiede: "*experience with the interpretation (to include auditing) and/or application of International Public Sector Accounting Standards (IPSAS) and/or International Accounting Standards/International Financial Reporting Standards (IAS/IFRS).*"
Ciò in quanto, l'*Internal Auditor NATO* "*assesses compliance of accounting transactions, operational and logistics activities, and accounting reports in accordance with NATO accepted accounting standards (IPSAS) and/or appropriate commercial standards*."
Tra i compiti aggiuntivi dell'*internal auditor* vi è poi quello di condurre "investigazioni speciali" ove richiesto ed eventuali "studi ad hoc".
Va da se, infatti, che ove l'analisi del *risk assessment* dovesse far emergere – in presenza di controlli gestionali sui *key control points* individuati – problemi particolari legati, ad esempio, all'esistenza di eventuali frodi, sarebbe necessario procedure con apposite "investigazioni speciali".
Al riguardo, si osserva che, al fine di assicurare l'indipendenza della funzione di *audit* da quella finanziaria, le predette attività non dovrebbero essere affidate a chi è normalmente assegnato a "*direct operational or financial function responsibilities*".
In altri termini vi è una netta distinzione tra responsabilità di *audit* e responsabilità di gestione amministrativo-contabile.
Questo principio che in ambito internazionale è piuttosto chiaro e che, come abbiamo visto, è in linea anche con la necessità di garantire l'indipendenza (e non l'interdipendenza[65]) della funzione di *audit*, non pare essere stato recepito del tutto in ambito metropolitano.
Più in particolare, nella NATO l'*Internal Review Officer*[66] si occupa di "audit interno al Comando NATO", essendo completamente svincolato dalla gestione e dipendendo dal Capo Divisione Finanziaria[67] (in qualità suo *deputy*), senza però avere alcun tipo di responsabilità gestionale, mentre negli Enti del Ministero della Difesa, il Capo Ufficio Amministrazione[68] non ha alle dipendenze alcun *Internal Review Officer*, per cui di fatto ogni controllo – compreso quello antifrode – viene ad essere affidato, per quanto possibile, "solo" a controlli interni[69] al Ministero ed a controlli esterni allo stesso[70].
Tuttavia, chi si occupa di controlli interni di tipo "burocratico"[71] nell'Amministrazione della Difesa, sia di natura ispettiva, sia di revisione[72], difficilmente ha l'"*ability to recognize potential fraud indicators and develop steps to expand fiscal oversight scope to evaluate whether investigative referral is appropriate*"[73] e, peraltro, non necessariamente il predetto controllo antifrode fa chiaramente parte del relativo mandato ispettivo o di revisione.
E ciò in quanto non esiste - a differenza di quanto accade in ambito NATO, o in ambito ONU, con le figure di *Professional* con l'incarico di *Inspectors* - un vero e proprio servizio di *Internal Audit* che sia effettivamente presente "con un suo uomo[74]" all'interno dell'Ente/Comando militare.
Questo rappresenta un *focal point* in quanto, ad avviso dello scrivente[75], la presenza di un *internal auditor* effettivamente presente che ha modo in qualsiasi momento, per tutto il tempo necessario e

[65] Dalla funzione *financial* o, più in dettaglio, *fiscal*.
[66] Si chiarisce che l'*Internal Auditor* NATO si occupa, appunto, di *Internal Audit* in ambito NATO, mentre l'*Internal Review Officer* si occupa di *Internal Audit* all'interno dei singoli Headquarters.
[67] Denominato *Financial Controller*.
[68] Equiparabile al predetto Capo Divisione Finanziaria (o *Financial controller*). Tale figura è stata recentemente ridefinita dal D.P.R. 24 febbraio 2012, n. 40.
[69] Di revisione e ispettivi.
[70] Principalmente del MEF – RGS – Ispettorato Generale di Finanza e Corte dei Conti.
[71] Ossia di regolarità amministrativa e contabile (nel senso della "matrice dei controlli pubblici" in fig. 2).
[72] Non in senso anglosassone, bensì in senso di revisione della contabilità del danaro e patrimoniale.
[73] Vds.: http://www.mlkstroy.ru/news/navy-financial-management-intern-program-283.html
[74] In divisa o non.

senza *caveats*[76] di condurre ispezioni (in linea o non con l'*internal review program*), rappresenta un deterrente fortissimo al compimento di truffe anche di natura informatica che potrebbero essere poste in essere da dipendenti infedeli.
Infatti l'*Internal Review Officer* si occupa di revisione sia delle attività, sia delle procedure in ambiti come *purchasing* o *fiscal* (ossia di gestione contabile), ma anche delle relative *info technology procedures* per valutare nell'ambito delle competenze di *risk assessment* le eventuali "falle del sistema".
Ciò può contribuire ad eliminare almeno la punta del menzionato triangolo di *Cressey*, ossia "l'opportunità", e con essa, per tale affermata teoria, il rischio stesso di frode.
La suddetta frode, infatti, molto spesso si annida in opache ed interconnesse procedure informatiche, in cui la responsabilità del singolo operatore, unita alle sue specifiche (e talvolta esclusive) competenze, sia lavorative che tecniche, rendono quasi impenetrabile la "cortina fumogena che nasconde la frode" che, come visto, per l'*Associacion of Certified Fraud Examiners (ACFE)*, si compie con "*una falsa dichiarazione effettuata conoscendo la verità"* o, appunto, con "*l'occultamento di un fatto materiale"*.
In tal senso ci preme chiarire che, ad esempio, anche una semplice distinta di versamento bancario, se falsificata, rappresenta l'occultamento di un fatto materiale, ove lo stesso è costituito dall'effettuazione "di bonifici differenti".
Talvolta, in altri casi diversi dalla "truffa contabile"[77] si manifesta, invece, la "frode informatica" *ex* art. 640 *ter* del C.P., certamente molto più difficile da controllare, a causa dei differenti contorni della fattispecie delittuosa[78].
Al riguardo, va osservato che per la Suprema Corte "*il reato di frode informatica ha la medesima struttura e i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona, di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui"*[79].
Ciò detto, andando ad analizzare il requisito dell'"indipendenza" di quello che forse un giorno potrebbe essere un "Auditor dell'Esercito Italiano", di estremo interesse, appare un passaggio della summenzionata *U.S. Army Regulation 11-7* , la quale è perfettamente in linea con il citato Standard di connotazione n. 1100 emanato dall'*Institute of International Audit*[80].
Tale passaggio recita: "*<u>Commanders at all levels</u>, heads of HQDA activities, and U.S. Property and Fiscal Officers (USPFOs) <u>will</u>:*
(1) Establish and adequately resource an IR program as part of the command and control process.
(2) <u>Ensure IR offices are organizationally aligned as independent offices, which are located outside the typical staff structure that reports directly to the commander, principal deputy commander, or chief of staff of installation/garrison, division, district, or separate activity</u>.
As an independent office, the IR office will not be aligned under another directorate or staff section."

---

[75] Che ha esperienza sia come *Internal review officer NATO*, sia come Amministratore pubblico (anche ispezionato), sia come Ispettore del Nucleo ispettivo centrale, sia come membro tecnico di Commissione d'inchiesta amministrativa.
[76] Vds. a pag. 5 del presente lavoro, lo Standard 1000 IIA ove si prevede che il mandato deve "*autorizzare l'accesso incondizionato ai dati, alle persone, agli archivi e ai beni aziendali, ogni volta che ciò sia necessario per lo svolgimento dell'Audit*".
[77] Che quando ingegnata per distrarre danaro pubblico direttamente gestito configura l'ipotesi del reato di peculato.
[78] La Sentenza n. 18909 in data 30 aprile 2013 (II Sezione penale) precisa che "*la frode informatica è un'ipotesi speciale di truffa della quale conserva tutti gli elementi costitutivi fra cui proprio la condotta fraudolenta (artifizi e raggiri) finalizzata ad ottenere un ingiusto profitto con altrui danno (…) l'unica differenza (soggetto passivo) fra le ipotesi di reato di cui agli artt. 640 e 640 ter cod. pen. non influisce sui criteri che servono a distinguere il peculato dalla truffa aggravata"*.
[79] Cass. Pen. n. 3065 / 1999.
[80] Menzionato al paragrafo n. 2 del presente lavoro.

Per quanto sopra, non sembrerebbe ultroneo notare che un possibile "*Internal Auditor* con le stellette", dovrebbe essere considerato "*special staff*"[81], ossia dovrebbe dipendere direttamente dal Comandante/Direttore dell'Ente militare, al fine di assicurare l'indipendenza di un ruolo che, per natura e competenze, potrebbe essere certamente ricoperto da Ufficiali del Corpo di Commissariato dell'Esercito. All'autore preme evidenziare[82] che sarebbe molto proficuo imparare delle esperienze internazionali e, perché no, "copiare" da chi ha dimostrato, con i fatti, di essere più avanti di noi.
Sì, perché dopo tutto quanto abbiamo pur *pindaricamente* descritto, per ovvie ragioni di malriuscita sinteticità espositiva, non vi è chi non veda che non può confondersi un controllo interno burocratico - vuoi di "alta vigilanza" o amministrativo-contabile, vuoi di revisione o ispettivo - con un controllo interno manageriale antifrode. Si osserva, infine, che nonostante il soccorso di consolidata giurisprudenza contabile in tema di "valore esimente delle responsabilità patrimoniali sussidiarie in presenza di dolo specifico del dipendente infedele" [83], sarebbe una grave "compressione concettuale" cadere nell'equivoco di compiere delle pur comode semplificazioni e generalizzazioni[84] delle responsabilità antifrode in ambito Amministrazione della Difesa, riducendo ad un unico *genus* ogni forma di controllo [85], a causa dell'assenza ordinativa [86] di figure professionali[87] esistenti in altri Eserciti o in altre importanti Organizzazioni internazionali[88].
In conclusione, al fine di non lasciare solo sulla carta i menzionati *Standard internazionali* in materia di *Internal Audit*, anche antifrode, e considerando che "*Litterae non intrant sine sanguine*"[89], speriamo che anche questa "goccia d'impegno" di un modesto studioso[90], irrighi il germe del cambiamento dell'Organizzazione militare, creando i moderni presupposti per la realizzazione di un "controllo interno di qualità" che sia in grado di aumentare la deterrenza contro le truffe di dipendenti corrotti ed infedeli.

"*Scire leges non esta verba earum tenere, sed vim ac potestatem !*"[91]

---

[81] Al pari di quanto dovrebbe sempre accadere per il *legal advisor*.
[82] Nell'espressione di una convinzione personale che non rappresenta in alcun modo il pensiero ufficiale della Forza Armata o del Ministero della Difesa.
[83] Cfr. Sebastiano LA PISCOPIA "*Sulla responsabilità amministrativo patrimoniale negli Organismi tipici del Ministero Difesa*" su www.contabilita-pubblica.it, a pag. 8 e ss. (vds. anche approfondimenti sul *principio di causalità efficiente*, desumibile dall'art. 41, comma 2, c.p.).
[84] *"Si possono distinguere, nel diritto, diversi livelli o momenti della generalizzazione; (…) si è preferito usare il termine "momenti", laddove il latino momentum è la sincope di "movimentum" e si riferisce a un'indicazione temporale di un potenziale dinamico, essendo l'attimo in cui si condensa una forza, una pulsione a risalire su un livello differente poiché quello in cui ci si trova non è più sufficiente a raccogliere le complessità del reale. I momenti della generalizzazione sono dunque dei passaggi da un piano a un altro del discorso, passaggi che rilevano tanto per la spiegazione logica della struttura del sistema giuridico, quanto per mostrare il carattere epistemico del linguaggio giuridico, avvicinando così il diritto – quantomeno in una prospettiva filosofica – alle scienze sociali.*" Così Angela CONDELLO, in "*Il poliformismo nella generalizzazione del diritto: una prospettiva filosofico-giuridica*" su http://www.juscivile.it/contributi/2014/10_Condello.pdf.
Ad avviso dell'autore del presente studio, il contesto di attualità giuridica in cui andrebbe inquadrato l'auspicato *Internal Audit* in ambito Ministero Difesa, non consente più tale forma di storica generalizzazione epistemica di linguaggio.
[85] Seppure esclusivamente in via *gergale*.
[86] Ci si riferisce agli organici che individuano posizione e *job description* delle risorse umane dell'Ente.
[87] Che dovrebbero avere, ad avviso dell'autore, i requisiti di professionalità e onorabilità *ex* art. di cui al regolamento adottato ai sensi dell'articolo 39, comma 1, del decreto legislativo 8 luglio 1999, n. 270.
[88] *Inter alia* NATO e ONU.
[89] La conoscenza richiede sangue (impegno).
[90] Con esperienze metropolitane di amministratore pubblico e di Ispettore interno.
[91] "*Conoscere le leggi non consiste nel sapere solo le loro parole, bensì nell'interpretarne il loro spirito e la loro forza*" del giureconsulto *Publio Giovenzio Celsio* in Digesto Giustinianeo.