



Published on *AiiA: Associazione Italiana Internal Auditors* (<http://www.aitiaweb.it>)

## **Guida Interpretativa 2440-2: Comunicazione di informazioni sensibili all'interno e all'esterno della catena di comando (maggio 2010)**

1. Spesso gli internal auditor entrano in possesso di informazioni sensibili che rivestono un'importanza rilevante per l'organizzazione e che, potenzialmente, possono avere conseguenze significative. Queste informazioni possono riguardare esposizioni, minacce, incertezze, frode, sprechi e cattiva gestione, attività illecite, abuso di potere, colpa grave che mette a repentaglio la salute o l'incolumità pubblica o altre infrazioni. Questi aspetti possono inoltre ripercuotersi negativamente sulla reputazione, l'immagine, la competitività, il successo, la solidità, i valori di mercato, le partecipazioni e le immobilizzazioni immateriali, nonché sugli utili dell'organizzazione.
2. Se l'internal auditor valuta che le nuove informazioni siano rilevanti e credibili, di norma le deve comunicare tempestivamente al senior management e al board, ai sensi dello Standard 2060 e della Guida Interpretativa 2060-1. In genere, questa comunicazione segue la normale catena di comando per l'internal auditor.
3. Se, dopo le discussioni del caso, il Responsabile Internal Auditing (RIA), conclude che il senior management espone l'organizzazione a un rischio inaccettabile e non intraprende le azioni opportune, egli deve sottoporre le informazioni e le divergenze di opinione al board, ai sensi dello Standard 2600.
4. Lo schema tipico della comunicazione seguendo la catena di comando può essere accelerato per determinate tipologie di fatti che risultano sensibili per effetto delle leggi, delle norme o delle prassi comuni vigenti. Per esempio, qualora si evidenzi il falso in bilancio da parte di un'organizzazione che emette titoli quotati, la normativa locale può prevedere che il board venga informato immediatamente delle condizioni di contorno che potrebbero avere condotto alla rendicontazione contabile infedele, anche se il senior management e il RIA hanno convenuto le azioni da intraprendere. Le leggi e le norme vigenti in alcune giurisdizioni impongono che il board venga informato della scoperta di eventuali violazioni del codice penale o delle leggi in materia di titoli, alimenti, farmaci o inquinamento, nonché di altri atti illeciti quali corruzione attiva o pagamento di tangenti a funzionari pubblici, fornitori o clienti.
5. In alcune situazioni, l'internal auditor può trovarsi di fronte al dilemma di decidere se comunicare le informazioni a persone esterne alla normale catena di comando o addirittura esterne all'organizzazione. In genere, questa comunicazione di denuncia di irregolarità viene designata con il termine inglese "whistleblowing". L'atto di rivelare informazioni sfavorevoli a qualcuno che fa parte dell'organizzazione, ma che si trova all'esterno della normale catena di comando dell'internal auditor, è considerato whistleblowing interno, mentre la

comunicazione di informazioni sfavorevoli a un'entità pubblica o ad altra autorità esterna all'organizzazione è considerata whistleblowing esterno.

6. In genere, chi fa questo tipo di denuncia rivela informazioni sensibili all'interno dell'organizzazione, seppur al di fuori della normale catena di comando, se ha fiducia nelle politiche e nei meccanismi predisposti dall'organizzazione per indagare sulle accuse di attività illecite o di altre irregolarità e per prendere gli opportuni provvedimenti. Tuttavia, alcune persone in possesso di informazioni sensibili possono decidere di comunicarle all'esterno dell'organizzazione se temono ritorsioni da parte del datore di lavoro o dei colleghi, se dubitano che la questione verrà sottoposta alle dovute indagini, se ritengono che verrà dissimulata o se sono in possesso di prove che dimostrano l'esistenza di attività illecite o di irregolarità che mettono a repentaglio la salute, l'incolumità o il benessere del personale dell'organizzazione o della collettività.

7. Nei casi in cui si opti per il whistleblowing interno, l'internal auditor deve valutare modi alternativi per comunicare il rischio rilevato a persone o a gruppi esterni alla normale catena di comando. A causa dei rischi e delle implicazioni di questi metodi, l'internal auditor deve procedere con cautela nel valutare l'evidenza e la ragionevolezza delle sue conclusioni, oltre a esaminare i meriti e gli svantaggi dei singoli interventi potenziali. Il ricorso a questa soluzione potrebbe essere adeguato se serve a provocare un intervento responsabile da parte di componenti del senior management o del board.

8. Le leggi o la normativa vigenti in molte giurisdizioni impongono ai dipendenti pubblici che siano a conoscenza di atti illeciti o contrari all'etica di informarne un ispettore generale, un altro funzionario pubblico o un difensore civico. Alcune leggi in materia di denuncia delle irregolarità (whistleblowing) tutelano i cittadini che decidono di farsi avanti per denunciare determinati tipi di attività scorrette. Le attività elencate in dette leggi o normative comprendono:

- reati penali e altre violazioni degli obblighi legali;
- atti ritenuti errori giudiziari;
- atti che mettono a repentaglio la salute, l'incolumità o il benessere delle persone;
- atti che danneggiano l'ambiente;
- attività che dissimulano o nascondono qualsiasi delle attività sopra elencate.

Alcune giurisdizioni non forniscono orientamenti né tutele, oppure prevedono tutele soltanto per i dipendenti pubblici (per esempio, i dipendenti di enti statali).

9. L'internal auditor deve conoscere le leggi e le normative delle varie giurisdizioni in cui opera l'organizzazione. Gli internal auditor che devono affrontare questa problematica possono consultare un legale esperto in materia di whistleblowing. L'internal auditor deve sempre richiedere consulenza legale nei casi in cui non sia certo dei requisiti o delle conseguenze legali connessi alle denunce interne o esterne di irregolarità.

10. Molte associazioni professionali sanciscono che la denuncia di attività illecite o scorrette rientri tra le responsabilità dei loro soci. Un tratto distintivo di una professione è rappresentato dall'assunzione di un'ampia responsabilità nei confronti del pubblico e dalla sua capacità di tutelare il benessere generale. Oltre a esaminare i requisiti legali, i soci IIA e tutti i professionisti CIA (certified internal auditor) devono attenersi a quanto previsto dal Codice Etico dell'IIA.

11. L'internal auditor ha il dovere professionale e la responsabilità etica di valutare con cura le evidenze e la ragionevolezza delle sue conclusioni, nonché di decidere se siano necessari ulteriori interventi per tutelare gli interessi e i portatori di interesse dell'organizzazione, la collettività o le istituzioni. Inoltre, l'auditor deve prendere in considerazione il dovere di riservatezza imposto dal Codice Etico dell'IIA al fine di rispettare il valore e la proprietà delle

informazioni e può divulgarle soltanto se debitamente autorizzato, salvo ove sia tenuto a farlo in virtù di un obbligo legale o professionale. Nel corso di questo processo di valutazione, l'auditor può chiedere la consulenza di un legale ed eventualmente di altri esperti. Queste discussioni potrebbero contribuire a porre le circostanze in un'ottica diversa e a procurarsi pareri sui potenziali effetti e conseguenze di possibili interventi. Il modo in cui l'internal auditor tenta di risolvere questo tipo di situazione delicata e complessa potrebbe dare luogo a ritorsioni e a una potenziale responsabilità.

12. In definitiva, spetta all'internal auditor prendere una decisione professionale circa i propri obblighi nei confronti del datore di lavoro. La decisione di comunicare all'esterno della normale catena di comando deve poggiare solidamente sulla certezza che l'infrazione è sostenuta da evidenze sostanziali e credibili e che è necessario intervenire sulla scorta di un imperativo normativo o di un obbligo professionale o etico.

AIIA - Via Santa Tecla, 5 - 20122 Milano - Tel. 02.36581500 Fax 02.86995492 - C.F. e P.I.  
02893990156 | [Note legali](#) | [Privacy policy](#)