











il secondo dalle funzioni aziendali che monitorano i tipici rischi aziendali (rischio operativo, finanziario, di mercato, di non conformità, etc.) e che potrebbe essere attribuito ad un funzione specifica di Risk Officer o a *“manager e strutture aziendali non dedicati a ciò in via esclusiva”*, il primo dai business owner che identificano, valutano e gestiscono i rischi, implementando le specifiche azioni di trattamento.

L'esempio del Codice di Autodisciplina riprende e sostanzia l'incipit di questo articolo, cioè opportunità e necessità di una governance basata sulla gestione dei rischi.

## **Bottom line**

La trasposizione del concetto nel campo dell'Information Technology mantiene tutta la sua validità a sostegno di chi pensa che l'integrazione dell'Information Risk Management con l'IT Governance, anche in periodi economici migliori, sarebbe stata essenziale per garantire la qualità degli interventi di sicurezza e la loro reale integrazione nelle attività day-by-day: la crisi economica la rende ora anche l'unica strada perseguibile. Della

serie: “non tutto il male vien per nuocere”.

Con questo il tema evidentemente non può dirsi esaurito: è recentissima la pubblicazione da parte di Banca d'Italia delle “Nuove disposizioni di vigilanza prudenziale per le banche” (15° aggiornamento del 2 luglio 2013) che introduce interessanti considerazioni in merito alla gestione dei rischi e ai ruoli aziendali; è sempre vivo il dibattito sull'Enterprise Risk management e sui framework di riferimento (es. ISO 31000); si attende una versione della ISO/IEC 27001 che dovrebbe apportare delle novità in merito al sistema di controlli e alla gestione dei rischi aziendale; si diffondono movimenti di pensiero sulla crescente necessità di considerare l'impresa come un sistema annullando la separazione tra business ed IT oltre che tra i diversi silos che per anni hanno caratterizzato i sistemi informativi (si veda il movimento *DevOps* e le implicazioni in termini di governance e rischi connessi).

Noi di HSPI proveremo – senza promettere di riuscirci - a non perderci neanche un bit e a trasferire le nostre analisi e i nostri pensieri, come al solito, su questa newsletter (stay tuned).