



Associazione Italiana
Information Systems Auditors



Il nostro Benvenuto al 2009

Cominciamo con un benvenuto all'anno 2009, perché, proprio l'8 ottobre di quest'anno, ricorrerà il trentennale della costituzione della nostra Associazione. Sono stati trenta anni di crescita continua e di impegno per venire incontro alle modifiche della nostra professionalità.

Guardando indietro possiamo ricordare con piacere le attività ed iniziative intraprese. Ora, la ricorrenza del trentennale diventa uno sprone per fare sempre meglio!

Passi avanti nell'organizzazione del XXIII Convegno annuale

L'organizzazione del convegno e, soprattutto l'articolazione delle relazioni e dei temi che saranno trattati, si sta sempre più delineando.

Come già anticipato nella Newsletter di dicembre, una intera sessione sarà dedicata alla Ricerca su IT Governance di SDA BOCCONI sponsorizzata da AIEA.

La scaletta della sessione prevede:

14.15 - 14.30 Introduzione – Motivazioni della Ricerca (Orillo Narduzzo – Hernan Gabrieli – Protiviti)

14.30 - 15.30 Modelli e scenario della ricerca (Severino Meregalli - SDA Bocconi)

16.00 - 16.45 Risultati della Ricerca (Elisa Pozzoli- Gianluca Salviotti - SDA Bocconi)

16.45 - 17.45 Case Study in una importante azienda nazionale

17.45 - 18.15 Dibattito

Informazione importante sui Rinnovi associativi

Per chi non avesse ancora rinnovato l'iscrizione annuale, ricordiamo che tutte le informazioni sono disponibili sul sito AIEA.

Ricordiamo ai ritardatari che le **iscrizioni** avrebbero dovuto essere fatte **entro e non oltre il 31 dicembre**. Affrettatevi, per non incorrere nelle "sanzioni" ISACA che comportano la cancellazione del socio e la necessità di provvedere ad una iscrizione ex-novo!!!

Nuovo Corso IS Audit Base

Vi ricordiamo che il prossimo appuntamento con la formazione è a Milano dal 02 al 06 febbraio, con il corso "IS Audit Base".

Questa edizione del corso è completamente rinnovata rispetto alle precedenti, sia nei contenuti, sia nell'articolazione.

Il nuovo corso è basato sul framework ITAF (IT Assurance Framework), recentemente emesso da ISACA e principale riferimento metodologico per la pratica della professione di IT Auditor.



Associazione Italiana
Information Systems Auditors



Per migliorare l'apprendimento dei contenuti, il corso è stato anche strutturato in due distinti moduli: il primo fornisce le basi e gli elementi teorici di riferimento, mentre il secondo favorisce la loro comprensione pratica, attraverso alcune esercitazioni e l'illustrazione di criteri operativi di applicazione.

Non perdetelo dunque! Ma se non siete direttamente interessati, divulgate la notizia ai vostri colleghi. Tutte le informazioni, per l'iscrizione sono sul sito www.aiea.it

Gli atti del XXII Convegno di Parma sono disponibili sul sito

Informiamo i soci che sono disponibili, sul sito www.aiea.it, le relazioni presentate al convegno.

Gruppi di Ricerca

Gruppo di Lavoro “Traduzione Cobit 4”

COBIT 4.1 – sono stati tradotti e resi disponibili nell'area Downloading del sito i seguenti processi: ME1, ME2, ME3, ME4; DS1, DS2, DS3, DS4, DS5, DS6.

Sono in corso di pubblicazione i processi: AI1, AI2, AI3, AI4

Gruppo di Ricerca “Business Continuity”

I primi risultati del processo di controllo di qualità hanno richiesto alcune sistemazioni peraltro già avviate. Il completamento del documento è previsto nel presente trimestre.

Gruppo di Ricerca “COBIT-Legge 262

Il GdR è suddiviso in 6 Focus Group. Le attività sono iniziate come da programma con il Focus Group 1 (Introduzione e normativa), che nel frattempo ha completato le proprie attività. Il lavoro procede. In particolare i Focus Group 2 (Risk based approach e Scoping) e 6 (Flussi interni di attestazione e modello di valutazione) hanno predisposto una prima bozza delle rispettive relazioni per le successive fasi di validazione e controllo di qualità. Considerata la complessità della materia, la conclusione della ricerca è prevista per fine marzo 2009.

Gruppo di Lavoro “Traduzione Val IT 2.0”

A breve partirà il Gruppo di Lavoro che si occuperà della traduzione della versione aggiornata di Val IT 2.0. Vi terremo informati sullo stato di avanzamento delle attività.

Riceviamo da PROTIVITI

In allegato l'ultima Newsletter Protiviti dal titolo: “Disclosure sui rischi. Novità normative, prassi rilevate e suggerimenti pratici”.

Con l'adozione delle Direttive Europee 2003/51/CE (c.d. “Modernizzazione”) e 2004/109/CE (c.d. “Transparency”) che hanno modificato il Codice Civile e il Testo Unico sulla Finanza, la disclosure sui rischi diventa un obbligo per tutte le società, non solo quotate, che operano in Italia. In aggiunta a ciò, per le società quotate, è prevista l'estensione dell'attestazione del Dirigente Preposto anche ai “principali rischi ed incertezze” da riportare in bilancio.



In questa Newsletter sono presentati i principali risultati di una ricerca condotta in collaborazione con l'Università di Pisa - Master Auditing e Controllo Interno, con l'obiettivo di offrire un benchmark sulle prassi di Risk Reporting diffuse a livello italiano e internazionale e di fornire alcuni spunti di riflessione per un adeguato reporting sui rischi.

Calendario Eventi AIEA

FEBBRAIO 2009

- 2 Milano – Inizio Corso Base Audit
- 11 Milano – Corso COBIT Base
- 24 Milano - Sessione di Studio
- 26 Torino - Sessione di Studio
- 27 Milano – Inizio Corso CISA

MARZO 2009

- 4 Roma - Sessione di Studio
- 6 Roma – Inizio Corso CISA
- 11 Milano – Corso COBIT Avanzato
- 20 Milano – Inizio Corso CISM
- 26 Milano - Sessione di Studio
- 27 Roma – Inizio Corso CISM

I prossimi eventi di AIEA

Calendar of Events

Dates of conferences/events are indicated in **RED**; other dates and deadlines are indicated in **BLACK**.

February

- 11 FebruaryEarly-bird registration deadline for the June 2009 CISA, CISM and CGEIT exams
- 23-24 February...**Asia-Pacific CACS conference**, Kyoto, Japan
- 25 FebruaryEarly-bird registration deadline for North America CACS conference, Orlando, Florida, USA

March

- 2-6 March**ISACA Training Week**, Houston, Texas, USA
- 4 MarchEarly-bird registration deadline for the ISACA Training Week, Denver, Colorado, USA
- 11 MarchDeadline for contributions to April's *CobIT Focus*
- 13-18 March**Euro CACSSM Conference**, Frankfurt, Germany
- 19-20 March**IT Audit Management Forum (Europe)**, Frankfurt, Germany
- 23 MarchDeadline for contributions to volume 4, 2009, of *ISACA Journal*
- 30-31 March**Information Security Conference (Latin America)**, Bogotá, Colombia

I prossimi eventi ISACA:



Associazione Italiana
Information Systems Auditors



Riceviamo da ISACA

Leading the IT Governance Community (www.itgi.org)

ISACA Member Benefit Highlight:

IT Governance and Process Maturity: This new report, complimentary to members-only, uses the process control objectives of the COBIT framework for complete coverage of IT governance. The report includes robust benchmark information, using data from a field study, to provide a means for an organization to answer the question, 'How do we compare with our peers?' Go to www.isaca.org/downloads to request your copy now.

Avviso ai soci 1

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo, azienda di appartenenza o altro...) di comunicare i nuovi dati in segreteria aiea@aiea.it. La mancanza di tali comunicazioni potrebbero impedire, al socio, la ricezione delle comunicazioni.

Avviso ai soci 2

E' in linea, sulla homepage del sito, il calendario degli eventi AIEA.

Rinnoviamo l'invito ai soci di fornire le proprie indicazioni su argomenti o temi che desiderano vengano trattati nel corso del 2009 sia nelle Sessioni di Studio sia in Workshop.

Chi volesse dare il proprio contributo, è pregato inviare una mail a aiea@aiea.it, specificando, nell'oggetto "ARGOMENTI DI INTERESSE"

In una successiva newsletter provvederemo ad elencare tutti i temi proposti.

Partecipazione di soci ad eventi

Tutti i soci possono segnalare eventi, fatti e informazioni di possibile interesse comune da segnalare ad esempio nella newsletter.

In particolare, se partecipate ad un evento in qualità di organizzatore, relatore o chairman, valutate la possibilità di partecipare a nome AIEA. La partecipazione dell'Associazione ad un evento "deve" però essere decisa dal Consiglio Direttivo: siete quindi pregati di contattare il CD con ragionevole anticipo! In caso non fosse possibile la partecipazione a nome AIEA, vi invitiamo ad indicare, nel profilo professionale la vostra appartenenza ad AIEA, Capitolo di ISACA

Bibliografia

E' on line il nuovo numero di InterLex (<http://www.interlex.it>)

Vi informiamo che sul sito www.cnipa.it sono disponibili molti documenti di interesse per i nostri soci. Ricordiamo che alla stesura di numerosi documenti hanno partecipato diversi nostri soci e che inoltre CNIPA organizza incontri o seminari aperti anche ai soci AIEA.



Associazione Italiana
Information Systems Auditors



Le Newsletter delle altre Associazioni

E' disponibile on line, la **Newsletter CLUSIT** del 31 dicembre 2008 (disponibile in PDF all'indirizzo www.clusit.IT/newsletter_31_12_08.pdf)

Nella newsletter, oltre ai vari, interessanti articoli, vengono forniti gli aggiornamenti sull'organizzazione del Security Summit 2009, che vede, tra i patrocinatori, anche AIEA e, tra i relatori, il nostro Presidente.

Sul sito Clusit sono anche elencati i prossimi **EVENTI SICUREZZA**

La Newsletter n.ro 327 del Garante Privacy è disponibile all'indirizzo <http://www.garanteprivacy.it/garante/doc.jsp?ID=1571099>

Sono disponibili, e sono qui allegate, le Newsletter n.ro 328 e 329 del Garante Privacy



- PROTEGGERE L'IDENTITÀ DELLE DONNE VITTIME DI VIOLENZA
- STRUTTURE SANITARIE PIÙ ATTENTE ALLA PRIVACY DEI PAZIENTI
- CORTE EUROPEA DEI DIRITTI UMANI: NO A CONSERVAZIONE ILLIMITATA DNA
- CONSIGLIO D'EUROPA: PIÙ PRIVACY NELLA LOTTA AL TERRORISMO

Proteggere l'identità delle donne vittime di violenza

Occorre evitare la pubblicazione di dettagli che violino riservatezza e dignità

Occorre proteggere in modo efficace l'identità delle donne vittime di violenza. Nel riportare episodi di cronaca, i giornali devono astenersi dal pubblicare dettagli che violino la loro riservatezza e dignità.

Lo ha ribadito il Garante affrontando (con un provvedimento di cui è stato relatore Mauro Paissan) il caso di un quotidiano veneto che aveva dato notizia di un'aggressione e di una violenza sessuale subite da una donna da parte del coniuge da cui era legalmente separata. Nell'articolo venivano rese note l'identità della vittima, la sua professione unitamente all'indirizzo dove la esercitava, l'indirizzo dove la donna viveva col marito e l'attuale indirizzo con relativa fotografia.

La donna si era lamentata, segnalando al Garante, oltre alla violazione della propria dignità, anche il rischio dei danni che la pubblicazione di tali informazioni poteva arrecare alla personalità del figlio minore, nel caso in cui fosse venuto a conoscenza dei fatti tramite i mezzi di informazione.

Il Garante ha dichiarato fondata la segnalazione della donna, ribadendo preliminarmente che i giornalisti possono diffondere dati personali, anche senza il consenso degli interessati, nei limiti del diritto di cronaca, ed in particolare del principio dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico.

Nel caso specifico, l'episodio avrebbe potuto essere documentato correttamente omettendo i riferimenti in grado di portare all'identificazione della vittima del reato, anche in considerazione del fatto che le informazioni attinenti alla sfera sessuale sono soggette ad una rigorosa tutela, anche quando sono trattate nell'ambito di attività giornalistica. L'articolo è risultato quindi pubblicato in violazione della disciplina in materia di protezione dei dati personali e del Codice deontologico dei giornalisti. Il Garante ha così vietato all'editore del quotidiano l'ulteriore pubblicazione delle generalità, della professione unitamente al luogo dove viene esercitata, degli indirizzi e delle foto dell'abitazione della donna.

Strutture sanitarie più attente alla privacy dei pazienti

Le strutture sanitarie devono essere più attente alla privacy dei pazienti. Nel corso del 2008 l'Autorità è intervenuta più volte per tutelare la riservatezza dei pazienti richiamando gli organismi sanitari pubblici e privati al rispetto di una serie di misure volte ad assicurare il massimo livello di protezione dei diritti del malato, come prevede il Codice privacy. Diverse soluzioni sono state adottate dalle strutture sanitarie a seguito delle segnalazioni presentate dai cittadini al Garante.

Un'azienda sanitaria veneta ha ad esempio eliminato dai moduli utilizzati per fini amministrativi (ad es. per giustificare un'assenza dal lavoro) il riferimento al reparto che redige il certificato, evitando in questo modo che estranei possano desumere lo stato di salute del paziente attraverso l'indicazione esplicita del reparto presso cui si è recato. Per quanto riguarda la distribuzione dei referti, un ospedale ambulatoriale emiliano ha poi previsto che la cartella ambulatoriale sia inserita in un apposito contenitore con finestrella trasparente in modo tale da rendere visibili all'esterno i dati indispensabili al ritiro del referto, escludendo così l'accesso non necessario ai dati sanitari del paziente da parte dell'operatore addetto alla distribuzione. Una ditta che fornisce materiale per conto del servizio sanitario nazionale, invece, ha dal canto suo sostituito le etichette apposte all'esterno dei pacchi postali, assicurando di non indicare più informazioni circa il loro contenuto. Al fine di prevenire l'indebita conoscenza da parte di terzi di dati sensibili dei pazienti, un ospedale milanese ha invece effettuato corsi di formazione per il personale che raccoglie l'anamnesi; lo scopo è quello di garantire che le prestazioni sanitarie non avvengano in situazioni di promiscuità. Ancora, un policlinico universitario siciliano ha modificato la collocazione delle stanze dedicate alle visite e ha introdotto un codice alfanumerico al posto della chiamata nominativa dei pazienti. Infine, un'azienda sanitaria pugliese ha corretto la causale degli assegni destinati ai ragazzi con problemi e disagi psicologici eliminando il riferimento alla malattia mentale da loro sofferta.

In più di un' occasione, il Garante è intervenuto poi presso medici di base ricordando la necessità di adottare cautele durante i colloqui con i pazienti per evitare che informazioni sullo stato di salute possano essere conosciute da terzi presenti in sala d'attesa. L'Autorità ha anche ribadito che le prescrizioni mediche devono essere consegnate solo al paziente o ritirate anche da persone diverse sulla base di una delega scritta mediante la consegna in busta chiusa.

Corte europea dei diritti umani: no a conservazione illimitata Dna

Conservare senza limiti di tempo profili del Dna, campioni biologici e impronte digitali viola il diritto alla privacy, soprattutto nel caso di minori. Lo ha stabilito la Corte europea dei diritti dell'uomo, con la sentenza n. 880 del 4.12.2008, definendo il ricorso di due cittadini inglesi, uno dei quali minore, accusati rispettivamente di molestie e di tentato furto, che avevano chiesto invano alla polizia inglese la distruzione delle impronte digitali e dei campioni di Dna raccolti al momento dell'arresto e conservati anche dopo la chiusura, con assoluzione, del procedimento penale a loro carico. I due cittadini si erano visti rigettare la richiesta dalla polizia in base ad una legge nazionale che consente il prelievo e la conservazione di questi campioni senza limiti di tempo nella banca dati inglese del Dna. La Corte, all'unanimità, ha riconosciuto la violazione del diritto alla vita privata ai sensi dell'articolo 8 della Convenzione Europea dei diritti umani del 1950. I giudici di Strasburgo hanno sottolineato, in particolare, che i profili di Dna permettono di risalire all'origine etnica e ricostruire i legami familiari, il che rende la conservazione più delicata e suscettibile di ledere il diritto alla riservatezza anche di terzi. Nella sentenza, inoltre, i giudici europei hanno rilevato che Inghilterra, Galles e Irlanda del Nord sono i soli paesi in Europa a consentire la conservazione illimitata delle impronte digitali e dei prelievi di Dna di qualsiasi persona sospettata di aver commesso un reato, indipendentemente dall'età, natura e gravità del reato specifico. I giudici hanno considerato, poi, particolarmente preoccupante il rischio di stigmatizzazione, derivante dal fatto che persone innocenti siano state trattate alla stregua di criminali. Per tutti questi motivi la Corte ha considerato che la conservazione indiscriminata e senza limiti temporali dei profili del Dna e di altri elementi biometrici costituisce una violazione del diritto al rispetto della vita privata e non può ritenersi accettabile in una società democratica, né proporzionata alle finalità di tutela della sicurezza pubblica. La Corte ha chiesto alla Gran Bretagna di adottare tutte le misure necessarie per dare seguito alla sentenza.

Consiglio d'Europa: più privacy nella lotta al terrorismo

Un forte messaggio sulla necessità di non comprimere la privacy nella lotta al terrorismo è stato lanciato dal Consiglio d'Europa. E' proprio quando si combatte contro il terrorismo e la criminalità organizzata che occorre garantire il massimo rispetto dei principi che tutelano diritti umani fondamentali quali il diritto al rispetto per la vita privata, sancito nell'articolo 8 della Convenzione europea per i diritti umani. Il messaggio è contenuto nel documento pubblicato di recente dal Commissario del Consiglio d'Europa per i diritti umani, Thomas Hammarberg, dal titolo "Tutelare il diritto alla privacy nella lotta contro il terrorismo" (<https://wcd.coe.int/ViewDoc.jsp?id=1380905&Site=CommDH&BackColorInternet=FEC65B&BackColorIntranet=FEC65B&BackColorLogged=FFC679>). Il documento fa il punto sulla situazione in Europa per quanto riguarda gli sviluppi tecnologici e politici che hanno caratterizzato gli ultimi anni nel settore delle attività di contrasto al terrorismo ed alla criminalità, e sottolinea la necessità di riesaminare le politiche sinora adottate per garantire la piena tutela del diritto alla privacy ed alla protezione dei dati personali. Occorre, a giudizio del Consiglio d'Europa, ripensare tutte le proposte e le politiche sinora elaborate nella prospettiva di un reale bilanciamento con i diritti fondamentali delle persone, che non possono restare lettera morta e devono trovare eco adeguata presso tutti i governi dei Paesi che si sono impegnati, oltre mezzo secolo fa, a garantire il rispetto dei diritti umani.

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Come rottamare il pc in tutta tranquillità. Le indicazioni del Garante per la cancellazione sicura dei dati - Comunicato del 5.12.2008

Il Garante privacy vara procedure semplificate per le misure minime di sicurezza e la notificazione - Comunicato del 9.12.2008



- INFORMAZIONI COMMERCIALI: SI POSSONO TRATTARE SOLO DATI PERTINENTI
- TELECAMERE CON LE ORECCHIE: STOP DEL GARANTE
- PROTEZIONE DEI DATI PERSONALI E COOPERAZIONE GIUDIZIARIA IN EUROPA

Informazioni commerciali: si possono trattare solo dati pertinenti

A rischio la reputazione di aziende e professionisti

Nei data base di Cerved solo informazioni corrette e pertinenti che non ledano la reputazione commerciale e l'identità dei soggetti censiti. E poi: no all'uso delle liste elettorali e dei dati ricavati dai redditi del 2005 finiti on line lo scorso anno.

Il Garante privacy, intervenuto a seguito di numerose segnalazioni, ha vietato a Cerved, società che opera nel settore della c.d. *business information*, il trattamento illecito di alcune categorie di dati personali e le ha prescritto una serie di misure per conformarsi al Codice sulla riservatezza.

Cerved è la più ampia banca dati di informazioni necessarie per il mondo degli affari e fornisce a istituti bancari, finanziarie, professionisti, operatori economici ecc. informazioni sulla affidabilità dei soggetti censiti. Attualmente nei data base della società sono presenti diversi milioni di imprese e di persone fisiche.

I dati che la società tratta per realizzare i servizi che offre (dossier, report su persone fisiche o imprese) provengono in larga parte da fonti lecite, quali i registri pubblici (informazioni camerali, di conservatoria, catastali, registro dei protesti ecc.) o altre fonti accessibili (liste delle imprese certificate Iso, notizie di stampa ecc.). Tuttavia, durante gli accertamenti ispettivi effettuati dal Garante, è emerso che Cerved, oltre a dati pubblici riferiti ai soggetti censiti si serve anche di altre informazioni sulla cui base vengono strutturati i dossier e i report. Cerved, infatti, non si limita alla semplice riproposizione delle informazioni estratte da fonti pubbliche, ma vi associa altri eventi o fatti riferiti a terzi facendoli confluire in un unico contesto. In tal modo, ad alcuni soggetti censiti si associano informazioni che non li riguardano direttamente (es. partecipazioni a società in seguito fallite per responsabilità altrui), con una conseguente violazione della loro reputazione commerciale e identità personale.

Inoltre, il Garante ha accertato che tali dati, anche quelli riferiti a terzi, sono utilizzati per fornire valutazioni sintetiche che non derivano da dati personali estratti da pubblici registri, ma sono autonomi giudizi elaborati sulla base di criteri unilateralmente fissati dalla società.

Il Garante ha ritenuto tale modalità non corretta e ha vietato a Cerved l'uso di questi dati, prescrivendo anche l'adozione di ogni accorgimento per evitare il ripetersi di simili associazioni.

Nel corso degli accertamenti è emerso, tra l'altro, che la società, non solo trattava informazioni eccessive e non pertinenti, ma raccoglieva anche dati personali da fonti dalle quali non poteva attingere, come le liste elettorali, o addirittura le dichiarazioni dei redditi del 2005, acquisite in occasione delle loro messa on line da parte dell'Agenzia delle entrate (diffusione dichiarata dall'Autorità illegittima). Oltre a vietare l'uso di questi dati il Garante ha ordinato a Cerved di cancellare quelli relativi ai contribuenti.

Telecamere con le orecchie: stop del Garante

Una telecamera posta all'interno di un locale registra suoni e memorizza voci. Interviene il Garante ne vieta l'uso e ordina la cancellazione delle registrazioni. Il provvedimento inibitorio (relatore Mauro Paissan) è stato adottato a seguito delle segnalazioni di diversi cittadini che lamentavano l'installazione, da parte di un negoziante, di numerose telecamere esterne che riprendevano mezzi, persone in transito e accessi agli immobili posti nel loro angolo di visuale. I segnalanti contestavano anche l'assenza di cartelli o comunicazioni visibili che informassero dell'esistenza del sistema di videosorveglianza. Il titolare del negozio, chiamato dal Garante a dar conto del proprio operato, si giustificava affermando che le telecamere, quattro esterne e tre interne, erano state installate, con un'angolazione rivolta verso la porta e le finestre del locale, per finalità di sicurezza, dopo aver subito alcuni atti vandalici e intimidatori. Sosteneva, inoltre, che il sistema fosse adeguatamente segnalato da cartelli.

Da più accertamenti svolti sul posto è emersa invece una situazione diversa. Innanzitutto, all'epoca della prima ispezione mancavano del tutto cartelli che informassero della presenza del sistema di videosorveglianza e quelli apposti in seguito non sono risultati comunque idonei, perché non ben visibili. Ma una circostanza ha richiamato maggiormente l'attenzione degli ispettori del Garante e ha fatto scattare il divieto: una delle tre telecamere interne, collocata vicino al registratore di cassa, risultava, infatti, dotata di registratore audio. Il negoziante dovrà rimuovere la "telecamera con le orecchie" e cancellare i dati (suoni, voci) finora raccolti. L'Autorità ha ritenuto, infatti, illecita la registrazione delle voci perché non conforme al principio di finalità, secondo cui il trattamento deve essere effettuato per finalità determinate, esplicite e legittime. Finalità che non risultano ricorrere nel caso esaminato. Il Garante, inoltre, ha prescritto al titolare del negozio di designare quale responsabile del trattamento e unica persona autorizzata ad accedere alle immagini registrate, il soggetto che ha la manutenzione dell'impianto, disponendo fino ad allora il blocco della comunicazione delle immagini.

Protezione dei dati personali e cooperazione giudiziaria in Europa

Bilancio positivo per il Working Party on Police and Justice (WPPJ), il Gruppo dei Garanti europei per la protezione dei dati personali costituito nel 2007 con l'obiettivo di affrontare le problematiche connesse all'attività di collaborazione giudiziaria e di polizia (il cosiddetto "Terzo Pilastro").

Fra le questioni che più hanno impegnato nel 2008 il WPPJ, presieduto da Francesco Pizzetti, vanno segnalate innanzitutto le attività connesse al processo di adozione della Decisione quadro del Consiglio Ue in materia di protezione dati nel III Pilastro (avvenuta nel mese di novembre 2008) e le problematiche attinenti l'attuazione del Trattato di Prüm (che prevede l'obbligo per le autorità responsabili delle indagini penali negli Stati membri Ue di scambiarsi informazioni basate sull'utilizzo del Dna). In entrambi i casi il WPPJ ha richiamato la necessità di rispettare alcuni principi fondamentali e di garantire un adeguato raccordo fra le autorità nazionali di protezione dati al fine di consentire controlli realmente efficaci. In numerose occasioni nel corso del 2008 il WPPJ ha sollecitato le istituzioni europee (anche attraverso incontri bilaterali con le più alte cariche istituzionali) ad offrire chiarimenti sulla natura delle molte iniziative adottate o proposte nel settore del Terzo Pilastro, che a giudizio del Gruppo non risultavano essere sufficientemente coordinate e non tenevano nel dovuto conto le esigenze di protezione dei dati e della privacy.

Sotto la presidenza italiana, il Gruppo di lavoro europeo si è anche adoperato in un'attività di analisi per valutare le prassi attualmente in essere rispetto alle attività di controllo nel settore della cooperazione giudiziaria e di polizia, con l'obiettivo ultimo di predisporre un manuale operativo comune da utilizzare in tutta Europa. È stata, inoltre, avviata la creazione di un inventario degli accordi bilaterali in vigore fra i Paesi europei e Paesi non-europei, con lo scopo di elaborare indicazioni utili a garantire l'armonizzazione fra le disposizioni in materia di protezione dei dati, contenute in tali accordi, e quelle presenti negli strumenti vigenti e cogenti a livello europeo (in particolare, la Convenzione 108/1981 del Consiglio d'Europa).

Per quanto riguarda il piano d'azione 2009, il Gruppo ha come obiettivo primario quello di continuare a dare un fattivo contributo ai Paesi membri ed alle Istituzioni Europee soprattutto in vista della entrata in vigore del trattato di Lisbona, che rivoluzionerà l'architettura istituzionale dell'Unione europea e renderà necessaria un'ulteriore armonizzazione delle disposizioni in materia di protezione dei dati anche nel settore del "Terzo Pilastro".

L'attività del Garante. Per chi vuole saperne di più

Gli interventi e i provvedimenti più importanti recentemente adottati dall'Autorità

Privacy - Giovanni Buttarelli nominato Garante europeo aggiunto - Comunicato del 23.12. 2008

Persone disperse in montagna: si può localizzare il cellulare per rintracciarle - Comunicato del 24.12.2008

Dati genetici: autorizzato il trattamento per l'anno 2009 - Comunicato del 29.12.2008

NEWSLETTER

del Garante per la protezione dei dati personali
(Reg. al Trib. di Roma n.258 del 7/6/99).
Direttore responsabile: Baldo Meo.

Direzione e redazione: Garante per la protezione dei dati personali, Piazza di Monte Citorio, n.121 - 00186 Roma.
Tel: 06/69677751 - Fax: 06/69677755. Newsletter è consultabile sul sito Internet www.garanteprivacy.it

Disclosure sui rischi.

Novità normative, prassi rilevate e suggerimenti pratici

Con l'adozione delle **Direttive Europee** 2003/51/CE (c.d. "**Modernizzazione**") e 2004/109/CE (c.d. "**Transparency**") che hanno modificato il Codice Civile e il Testo Unico sulla Finanza, la **disclosure sui rischi diventa un obbligo per tutte le società, non solo quotate, che operano in Italia**. In aggiunta a ciò, per le società quotate, è prevista l'estensione dell'**attestazione del Dirigente Preposto** anche ai "principali rischi ed incertezze" da riportare in bilancio.

Dopo le specifiche disposizioni che hanno richiesto un ampliamento dell'informativa sui rischi finanziari, le nuove disposizioni estendono l'obbligo di disclosure a **tutte le tipologie di rischi aziendali**, richiedendo la **prima applicazione** a partire dai bilanci relativi agli esercizi aventi inizio dalla data successiva a quella della loro entrata in vigore (Modernizzazione il 28/3/2007 e Transparency il 24/11/2007).

Ciò significa che, per le società italiane il cui esercizio si chiude al 31 dicembre, **le nuove disposizioni si applicheranno a partire dal bilancio 2008**.

Se da un lato è chiaro l'intendimento perseguito dalle citate Direttive, ovvero quello di garantire un'informativa sempre più trasparente ed omogenea al mercato, non altrettanto si può dire sulle modalità attraverso le quali tali nuovi obblighi dovranno concretamente applicarsi: i decreti legge attuativi, infatti, riprendono le direttive europee **senza darne una concreta chiave di lettura**.

La presente Newsletter:

- A. Presenta i principali risultati di una **ricerca** condotta in collaborazione con l'Università di Pisa - Master Auditing e Controllo Interno*, con l'obiettivo di offrire un benchmark sulle prassi di Risk Reporting diffuse a livello italiano e internazionale;
- B. Fornisce alcuni spunti di riflessione sui **presupposti** necessari per un adeguato reporting sui rischi;
- C. Propone un **possibile schema di riferimento** per la predisposizione di un'informativa sui rischi completa e in linea con le migliori prassi internazionali.

* Il Rapporto completo della ricerca, predisposto a cura dell'Università di Pisa, sarà a breve reso disponibile

Gli obblighi imposti dalle Direttive "Modernizzazione" e "Transparency":

Le due Direttive in tema di Risk Reporting si inseriscono nel più ampio dibattito sul miglioramento ed allineamento alle best practice internazionali in tema di financial reporting delle Società italiane, allo scopo di garantire maggior trasparenza ai mercati di capitali e a tutti i soggetti che direttamente o indirettamente sono coinvolti nella gestione aziendale.

Il recepimento della Direttiva "**Transparency**" nell'ordinamento italiano ha comportato:

- l'ampliamento dell'informativa di bilancio per includere una "*descrizione dei principali rischi e incertezze con cui si confrontano gli emittenti*";
- la modifica dell'art 154-bis del TUF, prevedendo, di conseguenza, che l'attestazione del Dirigente Preposto (prevista da tale articolo) verta anche sulla presenza nei bilanci di una "*descrizione dei principali rischi ed incertezze*".

Il recepimento della Direttiva "**Modernizzazione**" nell'ordinamento italiano ha comportato:

- l'ampliamento del raggio d'azione dell'art. 2428 CC. prevedendo che la Relazione sulla Gestione, oltre a fornire un quadro descrittivo sulla situazione e sull'andamento della gestione della società, fornisca anche "*una descrizione dei principali rischi e incertezze cui la società è esposta*".

A. La Ricerca “Il Risk Reporting nell’informativa di Bilancio”

Nel 2008 Protiviti, in collaborazione con l’Università di Pisa - Master Auditing e Controllo Interno, ha condotto una **ricerca sull’informativa in tema di rischi e sistemi di risk management** resa, nell’ambito dei bilanci annuali, da 180 società operanti in 9 differenti settori e quotate su quattro diversi mercati finanziari, al fine di fornire alle Società italiane che per la prima volta si troveranno ad integrare o predisporre una sezione nel proprio bilancio dedicata ai rischi, una panoramica complessiva sulla disclosure e sulle prassi consolidate.

La ricerca ha avuto un **duplice obiettivo**:

- analizzare lo stato dell’arte della **comunicazione sui rischi**, al fine di comprendere quanti e quali rischi sono comunicati dalle società nell’Annual Report relativo all’esercizio 2007;
- comprendere quali sono le **azioni di prevenzione e gestione** del rischio e quali gli **attori aziendali** che prendono parte al processo di risk management.

Per la classificazione dei rischi rilevati negli Annual Report del campione analizzato, è stato utilizzato un **Business Risk Model**, ispirato al Risk Model di Protiviti, articolato nei seguenti livelli (per maggiori dettagli sui contenuti delle categorie, si rinvia all’Allegato 1 riportato in calce):

I° livello	II° livello
Rischio di contesto	Macroambientale
	Scenario competitivo
Rischio di processo	Operativo
	Finanziario
	Organizzativo
Rischio di informativa	Reporting esterno/interno

La ricerca ha fatto emergere alcune **particolarità comuni** a tutti i mercati analizzati e alcune **criticità peculiari delle società italiane**.

1. Si rileva una **generale carenza**, comune a tutti i mercati analizzati, di **disclosure sui rischi operativi**, ovvero sugli eventi incerti di origine interna che possono impattare negativamente sull’efficacia, efficienza ed economicità delle attività aziendali.
2. In Italia, solo un **numero limitato di società** (13%) dedica una sezione della Relazione sulla Gestione alla disclosure sui rischi “a 360°” e sui relativi sistemi di risk management in essere.
3. Sempre in Italia, l’**Internal Audit** emerge quale attore principale coinvolto nel processo di risk management, sostituito dal **Risk Manager** se previsto in azienda.
4. L’Italia ha il **minor numero di aziende** (3 su 45) che dichiara di aver adottato un modello integrato di gestione dei rischi, di tipo “*enterprise-wide*”, preferendo, invece, il sistema di fronteggiamento dei rischi specifici.

Il campione analizzato

Il campione selezionato per la ricerca è composto da 180 società quotate, 45 per ognuno dei quattro mercati di quotazione presi in considerazione:

- New York Stock Exchange (Stati Uniti)
- London Stock Exchange (Regno Unito)
- Deutsche Börse (Germania)
- Borsa Italiana (Italia)

Per ogni Paese sono state identificate 5 società per ciascuno dei nove settori riportati nella tabella seguente:

Basic Materials
Consumer Goods
Consumer Services
Health Care
Industrials
Oil & Gas
Technology
Telecommunications & Media
Utilities

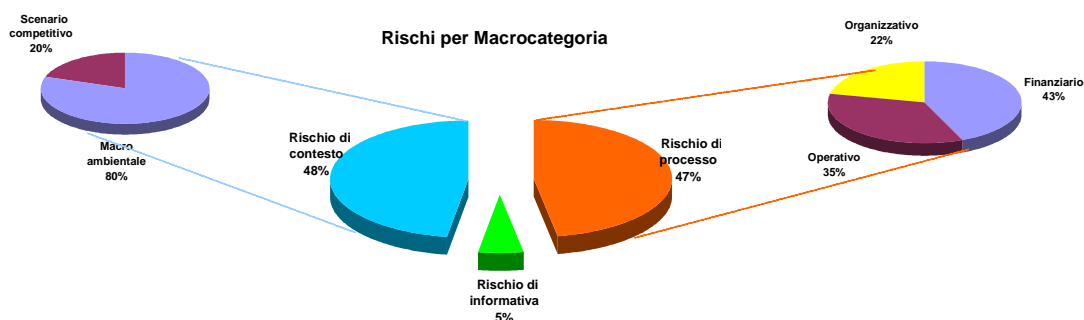
La classificazione utilizzata riprende il primo livello dello standard *Industry Classification Benchmark (ICB)* definito da Dow Jones e FTSE.

È stato inoltre volutamente escluso il settore finanziario, per poter dare un maggior grado di omogeneità al campione.

1. Aspetto generale: Carente disclosure sui rischi operativi, organizzativi e di informativa

Analizzando gli Annual Report delle società selezionate, si sono rilevati 3.768 rischi, con una media di quasi 21 rischi per società. Guardando alla distribuzione percentuale dei rischi fra le macrocategorie individuate, si osserva un sostanziale bilanciamento fra l'informativa riferita ai **rischi di contesto** (48%), cioè quelli derivanti da variabili esterne all'impresa e quella relativa ai **rischi di processo** (47%), cioè originati da variabili interne. I **rischi di informativa**, ovvero quelli relativi alle informazioni a supporto dei processi decisionali e ai sistemi di reporting, costituiscono invece solo una percentuale marginale (5%).

Grafico n. 1 - La comunicazione sui rischi per macrocategoria

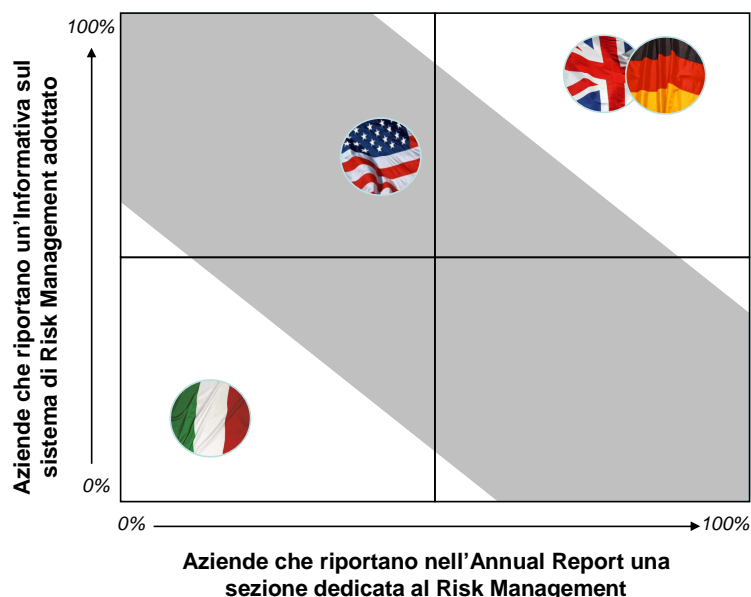


Scendendo al secondo livello di classificazione, i più diffusi nel campione sono i **rischi macroambientali** (38%). Seguono, a distanza, i **rischi finanziari** (21%), i **rischi operativi** (16%), i **rischi organizzativi** (10%) e quelli riferiti allo **scenario competitivo** (9%). È interessante evidenziare come la categoria dei **rischi operativi** originati da variabili interne sia poco comunicata all'esterno, pur trattandosi di rischi sempre presenti e spesso rilevanti per le aziende. Ciò potrebbe dipendere dalla politica di comunicazione seguita dalle società, spesso avverse, per ragioni di riservatezza, alla comunicazione verso l'esterno di certi tipi di minacce e vulnerabilità.

2. Italia: Le società comunicano poco

L'Italia è il Paese con il minor numero di aziende che dedicano una parte specifica dell'informativa annuale all'analisi dei rischi (13%). Le società italiane dimostrano anche **una bassa propensione alla divulgazione di informazioni circa i processi di risk management in essere**, quale elemento caratterizzante di un efficace modello manageriale e di governo. Al contrario, le società quotate sui mercati britannico e tedesco forniscono sempre informazioni, oltre che sui fattori di rischio, anche sui processi di risk management implementati.

Grafico n. 2 - Informativa sul Risk Management per Paese

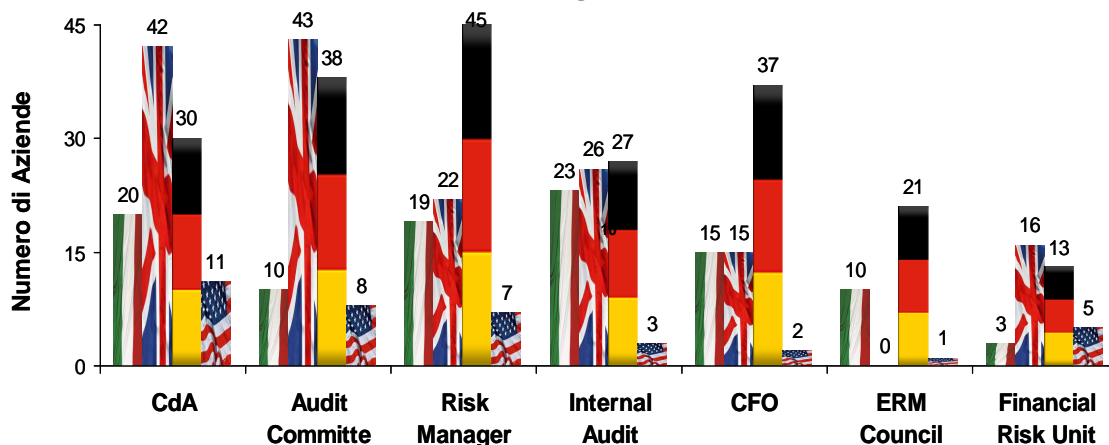


3. Italia: Internal Audit il soggetto maggiormente coinvolto nel Risk Management

In UK e in Germania si rileva un maggiore coinvolgimento di organi di governo societario, quali Consiglio di Amministrazione e Audit Committee rispetto agli altri Paesi, denotando la volontà di considerare il risk management parte integrante dei processi di gestione strategica delle aziende ed elemento fondante della creazione del valore.

In Italia e negli Stati Uniti, l'informativa sembra mettere in evidenza che le aziende tendono a non considerare gli organi di governance aziendale come parte in causa nell'attività di risk management. In questi casi la gestione dei rischi pare essere percepita più come un fatto tecnico di competenza di organi/funzioni specifiche come l'internal auditing o, dove esistente, il risk manager, piuttosto che come attività integrata nel processo di definizione/indirizzo delle strategie aziendali.

Grafico n. 3 - Attori coinvolti nel Risk Management secondo l'informativa delle società

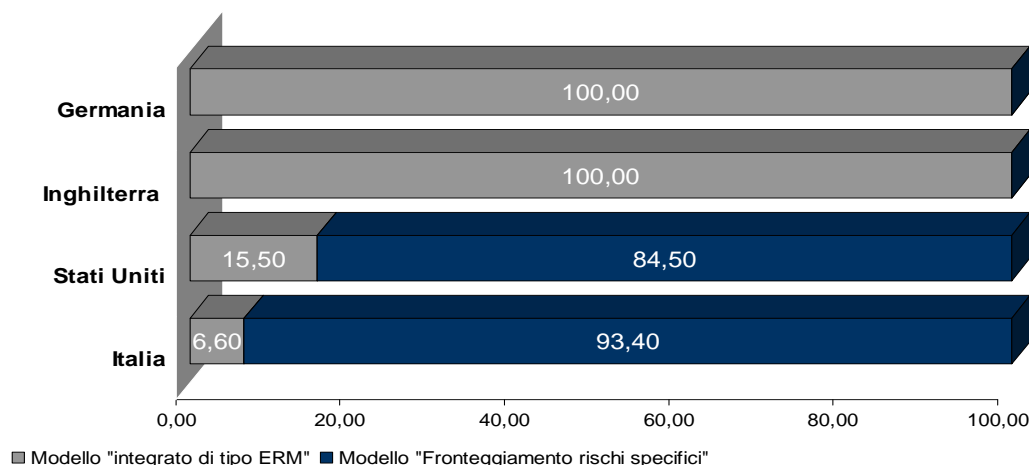


4. Italia: Enterprise Risk Management (ERM) poco diffuso

Per ciò che concerne l'approccio di Risk Management adottato dalle aziende, si rileva che a livello aggregato il 73% delle società fa menzione del sistema di risk management nell'informativa obbligatoria e che, di queste, l'88% dichiara di adottare un approccio al risk management di tipo *enterprise-wide*.

Tuttavia, mentre tutte le società tedesche e britanniche dichiarano, nell'ambito dell'informativa di bilancio, di avere un sistema di gestione integrata dei rischi (es. ERM), in Italia e negli Stati Uniti l'informativa in tema di risk management si concentra prevalentemente sulle modalità di gestione di rischi specifici (es. strumenti di copertura per fronteggiare i rischi di variazione tasso, cambio, commodity) e soltanto poche società (rispettivamente 3 per l'Italia e 7 per U.S.A) comunicano di aver adottato un modello che riguarda l'azienda/il gruppo nel suo complesso e si riferisce alle varie tipologie di rischi che caratterizzano la catena del valore dell'azienda.

Grafico n. 4 - Grado di diffusione di un sistema di risk management di tipo Enterprise wide



B. I presupposti necessari per un adeguato Risk Reporting

Prendendo spunto dai risultati della ricerca, riportiamo di seguito alcune riflessioni sui presupposti che sarà necessario adottare per consentire un Risk Reporting trasparente e allineato alle *best practice* internazionali.

In primo luogo, per disporre delle informazioni necessarie al Risk Reporting, occorre provvedere all'implementazione di un **processo sistematico di risk management** che consenta di:

1. Definire e classificare l'universo dei rischi di riferimento della società, che potrà ispirarsi a quelli adottati da aziende analoghe che già forniscono questo tipo di informativa (come contemplata negli Annual Report delle società UK, USA e tedesche, nonché i prospetti informativi degli emittenti italiani), ma che dovrà poi essere adattato per tener conto delle peculiarità organizzative e di business.
2. Valutare sistematicamente l'esposizione ai rischi rilevanti per la società.
3. Definire le strategie, le tecniche e le azioni di contenimento/gestione dei rischi.
4. Monitorare costantemente quanto rilevato a cura del Top Management.

Il secondo passo consiste nel prevedere un **maggiore e diretto coinvolgimento** nel processo di risk management di attori quali il **Dirigente Preposto e/o il Direttore Amministrativo-Finanziario**.

Il terzo passo richiede l'inclusione nel bilancio di **uno schema per la descrizione qualitativa e quantitativa dei rischi** cui è esposta l'azienda (vedi "un possibile schema di riferimento per il Risk Reporting").

Perché l'Enterprise Risk Management (ERM)?

La crescente attenzione alla *disclosure* sui rischi da parte degli investitori istituzionali è dimostrata anche dall'iniziativa avviata dall'agenzia di rating **Standard & Poor's** (S&P) di includere nelle analisi finalizzate all'emissione del *rating* anche approfondimenti sul profilo di rischio aziendale e sull'approccio adottato nella gestione dei rischi, in ottica di *Enterprise Risk Management*.

Questo tipo di analisi, prevista già dal 2005 per le società finanziarie, sarà estesa dal 2008 a tutte le società non finanziarie soggette al giudizio di S&P.

L'analisi proposta dall'agenzia di rating verterà sostanzialmente sui seguenti aspetti:

- *Risk-management culture and governance*
- *Risk controls*
- *Emerging risk preparation*
- *Strategic risk management*

In questo contesto ben si può apprezzare quale sarà il valore che la sezione sui rischi e contemplata nell'ambito del reporting finanziario potrà assumere arricchendosi di informazioni circa le modalità di gestione ed i processi di *risk management*.

Per ulteriori informazioni su "**Implementazione ERM**" e "**S&P ERM rating**" si consulti l'archivio sul sito www.protiviti.it

C. Un possibile schema di riferimento per il Risk Reporting*

In concomitanza con la concreta applicazione dei nuovi obblighi informativi nell'ambito della Relazione sulla Gestione per il Bilancio 2008, sarebbe auspicabile e quanto mai opportuno che le aziende italiane migliorassero la disclosure sui rischi, creando un'apposita sezione all'interno della Relazione, in cui esporre un insieme di elementi di interesse per gli stakeholder così come, ad esempio, avviene da tempo in UK e Germania.

La sezione dedicata al Risk Reporting potrebbe essere articolata nei seguenti tre paragrafi:

- Fattori di rischio cui la società è esposta
- Politiche e strumenti di gestione adottati
- Modello organizzativo di risk management in essere

L'introduzione di tale sezione permetterebbe agli Stakeholder aziendali una più agevole ricognizione delle varie tipologie di rischio cui risulta essere esposta l'azienda, nonché delle politiche di gestione intraprese.

Tra questi, in primo luogo, potrebbero essere rappresentati i fattori di rischio che connotano il modello di business dell'azienda e che possono impattare sulle performance economico-finanziarie.

Potrebbe essere, inoltre, opportuno riportare in questa sezione anche informazioni sulle politiche, gli strumenti e le azioni adottate o intraprese dalla società per far fronte ai rischi e alle incertezze descritti, per consentire ai destinatari dell'informativa di valutare l'atteggiamento nell'azienda al trattamento dei rischi.

Infine, in presenza di un modello formalizzato di gestione dei rischi, gli amministratori potrebbero darne informativa, evidenziando le soluzioni organizzative adottate e i ruoli e le responsabilità attribuite.

* Sul tema, si rinvia all'articolo "Reporting sui rischi: un approccio sistematico" pubblicato sul n. 3 (Luglio 2008) della rivista "ANDAF" Magazine e predisposto a cura di A. Cencioni (Managing Director Protiviti), F. De Gennaro (Manager Protiviti), R. Mannozi (Responsabile Amministrazione e Bilancio Gruppo FS), E. Pattumelli (Assistente Dirigente Preposto Gruppo FS).

Caratteristiche del Risk Reporting

Sulla base del benchmark condotto, si riportano di seguito alcune best practice rilevate in materia di Risk Reporting.

1. Costituisce una sezione separata dell'*Annual Report*.
2. Copre un arco temporale prospettico adeguato alla tipologia di business (1-2 anni).
3. Classifica i rischi in base alle caratteristiche rilevanti da un punto di vista organizzativo e/o funzionale, in coerenza con il processo di risk management adottato, ad esempio:
 - Rischi di ambiente/contexto
 - Rischi strategici
 - Rischi operativi
 - Rischi finanziari
 - Rischi di compliance
4. Fornisce informazioni quantitative e qualitative circa la probabilità di manifestazione dei rischi e l'impatto potenziale sulla situazione economico-patrimoniale e finanziaria.
5. Rappresenta i rischi in ordine di priorità e rilevanza per la società.
6. Fornisce evidenza delle azioni di mitigazione in atto.
7. Prevede la descrizione del sistema di risk management in essere, sia con riferimento alle politiche perseguite, sia con riguardo agli aspetti e soluzioni organizzative implementate.

Conclusioni

In attesa di poter verificare come le società italiane si comporteranno di fronte al nuovo obbligo, le esperienze internazionali costituiscono un primo utile elemento di confronto da utilizzare come riferimento operativo dei direttori amministrativi e finanziari.

Un ulteriore, atteso, contributo potrebbe arrivare dagli standard setter nazionali ed internazionali (n.d.r. OIC e IASB), laddove decidessero non solo di definire uno standard di riferimento, ma anche di sviluppare (ad esempio attraverso le Associazioni di Categoria) le apposite “verticalizzazioni” dell’universo dei rischi specifici per settore di business, garantendo contemporaneamente l’aderenza alla realtà operativa e la loro comparabilità.

Allegato 1 – Il Business Risk Model utilizzato nella ricerca per la classificazione dei fattori di rischio

Rischio di contesto	<i>Macroambientale</i>	<ul style="list-style-type: none"> Andamento economico generale Cambiamenti demografici Catastrofi ambientali - Cambiamenti climatici Leggi e regolamenti Rischio Paese - Instabilità politico-sociale Oscillazione tassi di interesse Oscillazione tassi di cambio valutari Variazione prezzo delle commodities
	<i>Scenario competitivo</i>	<ul style="list-style-type: none"> Concorrenti del settore Potenziali entranti Prodotti sostitutivi Fornitori - Approvvigionamento materie prime Clienti - Mercati di sbocco Approvvigionamento commodities strategiche per il settore
Rischio di processo	<i>Operativo</i>	<ul style="list-style-type: none"> Problematiche relative al processo produttivo Mancata vendita di prodotti/servizi Interruzione/Mancata realizzazione di progetti interni Difficoltà nello sviluppo del prodotto Interruzione dell’attività dovuta a cause gestionali Reperimento di risorse umane qualificate Relazioni con i dipendenti Protezione della proprietà intellettuale Mancata realizzazione della strategia
	<i>Finanziario</i>	<ul style="list-style-type: none"> Insolvenza clienti Concentrazione del credito Incagli finanziari - Problemi di liquidità Scelte di struttura finanziaria
	<i>Organizzativo</i>	<ul style="list-style-type: none"> Alleanze e joint venture Fusioni e acquisizioni Contenziosi legali e contrattuali Ristrutturazioni aziendali Scioperi Contenziosi legali e contrattuali Danni di immagine - reputazione Ripercussioni sociali e ambientali
Rischio di informativa	<i>Informativo</i>	<ul style="list-style-type: none"> Sistema di controllo sull’affidabilità del reporting Stime di voci in bilancio “Forward-Looking and Cautionary Statements”

* * *

Per ulteriori informazioni sui Servizi di Risk Management offerti da Protiviti, rivolgetevi all’ufficio Protiviti più vicino o contattate Alberto Carnevale o Emma Marcandalli al numero 02 6550 6301.