



Associazione Italiana  
Information Systems Auditors



**Dicembre 2009**

### **Assemblea straordinaria dei soci AIEA**

Lo scorso 26 novembre, al termine della presentazione del Gruppo di Ricerca “Business Continuity Management e Auditing” si è tenuta l’assemblea straordinaria dei soci AIEA, indetta dopo che, ad ottobre, un numero consistente di soci aveva fatto pervenire, al Consiglio Direttivo, una mozione di richiesta di “possibilità di un eventuale ulteriore candidatura del Presidente uscente, Silvano Ongetta”. La quasi totalità dei soci presenti ha votato per la modifica allo Statuto che permetta tale possibilità.

### **Si avvicina il 2010.....**

Vi informiamo che l’iscrizione all’Associazione, anche per l’anno 2010, dovrà essere fatta via web. L’iscrizione via web, avviata l’anno scorso, è stata molto positivamente apprezzata dalla gran parte dei soci e da ISACA.

Sul sito [www.aiea.it](http://www.aiea.it) troverete tutte le istruzioni.

### **A proposito di 2010.....**

Sono cominciate le attività preparatorie al prossimo Convegno del 2010. Molto probabilmente, sarà tenuto in una città del centro Italia.

Chi volesse contribuire, segnalando argomenti di particolare interesse, è pregato rivolgersi a [aiea@aiea.it](mailto:aiea@aiea.it), specificando, nell’oggetto “ARGOMENTI DI INTERESSE”

### **AIEA parteciperà.....**

AIEA partecipa all’organizzazione del corso dell’Università Statale di Milano sull’IT Governance per promuovere e diffondere l’utilizzo di strumenti di governo dei sistemi informativi aziendali. Il nuovo Corso di Perfezionamento in IT Governance post-laurea, che si terrà nel periodo marzo-giugno 2010 e con iscrizioni entro gennaio 2010, nasce dall’idea di far crescere la figura professionale dell’esperto IT, coniugando la conoscenza delle tecnologie informatiche con le metodologie di gestione dei processi IT e di analisi delle problematiche di efficienza, rischio e misura delle performance.

Oltre ad AIEA, Deloitte ERS e Statale Milano, all’organizzazione del corso hanno collaborato Boehringer Ingelheim Italia, IBM Italia, Hewlett-Packard Italia e Opera21. (per ulteriori informazioni si consulti il sito “[itgov.dti.unimi.it](http://itgov.dti.unimi.it)”).

### **Presentati i risultati del Gruppo di Ricerca “Business Continuity Management e Auditing”**

Lo scorso 26 novembre, a Milano, sono stati presentati i risultati del Gruppo di Ricerca sul tema “Business Continuity Management e Auditing”. Al Gruppo di Ricerca hanno contribuito anche soci di ANSSAIF e AUSED. Era presente il Presidente di AUSED, dr. Erminio Seveso e alcuni soci dell’associazione.

Il coordinatore del Gruppo, Massimiliano Nulli o Rinalducci ha fatto una panoramica delle attività svolte e degli obiettivi raggiunti, lasciando, poi, la parola ad alcuni componenti del gruppo (Matteo Gritti, Sabrina Pozzi, Sergio Tagni e Claudio Telmon) i quali hanno illustrato interessanti aspetti del lavoro svolto, descrivendo il progetto ed i risultati ottenuti.



Associazione Italiana  
Information Systems Auditors



I risultati del lavoro sono stati pubblicati nella Guida AIEA n.ro 5, che è stata distribuita ai soci presenti. La guida sarà distribuita a Roma e Torino, nelle prossime Sessioni di Studio.

### **Il nuovo sito AIEA**

E' in fase di test il nuovo sito dell'Associazione. Il sito prevede un'area riservata ai soci e molte altre novità che vi illustreremo.

### **Esame CISA e CISM 12 dicembre 2009**

Questa Newsletter uscirà quando saranno staranno per iniziare gli esami. Ai soci che affronteranno l'esame, i nostri migliori auguri.

### **I nostri sponsor**

A conclusione di questo anno, particolarmente intenso per le attività svolte, vogliamo ringraziare i nostri sponsor che ci hanno supportato ed hanno contribuito, con le loro strutture e con le alte professionalità messe a disposizione, a dare un contributo qualificato ai nostri soci.

Gli sponsor sono:





### **Da PROTIVITI riceviamo**

In allegato potrete trovare la Newsletter n.ro 27 di Protiviti, che riporta la survey dal titolo "Chief Financial Officer. Una professione in continua evoluzione"

Il documento ha lo scopo di fornire una sintesi dei risultati della ricerca dal titolo "Chief Financial Officer. Una professione in continua evoluzione", condotta da Protiviti con la collaborazione di Robert Half, la più antica società al mondo di recruiting specializzato, entrambe appartenenti al network internazionale Robert Half International (RHI).

La ricerca nasce dalla volontà di condurre un'analisi in grado di coniugare gli aspetti di organizzazione e di processo in ambito Finance, che fanno parte delle competenze core di Protiviti, con i temi legati alle dinamiche retributive e di incentivazione, tipici dell'esperienza professionale di Robert Half.

### **Parlano di noi**

#### **La Newsletter di novembre di CLUSIT parla di noi.**

Infatti, nel presentare il programma del Security Summit, che si terrà a Milano dal 16 al 18 marzo 2010, è evidenziato quanto segue:

*SESSIONI SULLA GESTIONE DELLA SICUREZZA (tutte in collaborazione con AIEA):*

*- "Il ritorno dell'investimento in sicurezza informatica (ROSI)"*

*- "Frodi Interne"*

*- "COBIT, ITIL, ISO27000" (con l'intervento di itSMF e di UNINFO).*

### **Gruppi di Lavoro / Ricerca**

#### ***"Traduzione Cobit 4.1"***

In questi mesi è stato sottoscritto con ISACA un accordo per pubblicare la traduzione di COBIT 4.1 sul sito di ISACA, assieme a quelle in Spagnolo e in Russo rilasciate nel mese di luglio 2009. Stiamo pertanto rivedendo l'editing secondo le indicazioni di ISACA e completando l'attività di controllo qualità. Nell'Area Download del sito si trovano l'"Executive Summary" ed alcuni processi. La conclusione è prevista entro dicembre 2009.

#### ***COBIT e legge 262***

Il Gruppo di Ricerca AIEA è articolato in 6 sottogruppi chiamati Focus Group.

I partecipanti alla ricerca sono ben 17 soci divisi in 6 Focus Group i cui Relatori sono:

Alessandro Arca (FG5)

Giuliano Flesia (FG4)

Luca Nurisso (FG1 e FG6)

Dino Ponghetti (FG3)

Luca Turri (FG2)

Le tematiche dei Focus Group sono le seguenti:

FG1: Introduzione e normativa di riferimento

FG2: Dimensionamento delle verifiche e analisi dei rischi

FG3: Controlli generali

FG4: Controlli applicativi

FG5: Campionamenti

FG6: Valutazione del sistema di controllo e attestazioni finali



---

Associazione Italiana  
Information Systems Auditors

---



La conclusione di tutte le attività è prevista per fine dicembre

### **Gruppo di Lavoro “Traduzione Val IT 2.0”**

Con il coordinamento di Guido Leone, il Gruppo di Lavoro si occupa della traduzione della versione aggiornata di Val IT 2.0. In particolare delle seguenti pubblicazioni:

*Enterprise Value: Governance of IT Investments - The Business Case*

*Enterprise Value: Governance of IT Investments - Getting Started with Value Management*

*Enterprise Value: Governance of IT Investments - The Val IT Framework 2.0*

*Sono stati rilasciati, in occasione del convegno di Pisa, i primi due documenti.*

Dopo il rilascio, in occasione del convegno di Pisa, dei primi due documenti, ora è terminata la traduzione del terzo ("The Val IT Framework 2.0").

A breve sarà attivata la fase di pubblicazione di questa **nuova Guida AIEA** che conterrà i risultati del Gruppo di Lavoro e che, all'inizio del 2010, sarà distribuita ai soci.

Al Gruppo hanno partecipato 17 soci.

### **Gruppo di Lavoro ROSI (RETURN ON SECURITY INVESTMENT)**

Lo scorso mese di settembre si è costituito un Gruppo di Lavoro sul ROSI (GdL), su iniziativa di AIEA, Clusit e Oracle, con la partecipazione di Deloitte, Ernst & Young, KPMG e PriceWaterhouseCoopers. Il GdL sta lavorando alla preparazione di un quaderno/studio che contenga indicazioni utili per le aziende per il calcolo del ROSI all'interno dei propri progetti di sicurezza. Non si pretende di ottenere uno strumento preciso, ma almeno una serie di indicazioni sulla metodologia da utilizzare e sui fattori da prendere in considerazione per calcolare il ROSI. Lo studio sarà presentato a marzo 2010 nel corso del Security Summit di Milano.



**I prossimi eventi di AIEA**

## Calendario Eventi AIEA

### Dicembre 2009

- 15.....Milano – sessione di Studio
- 16.....Roma – Sessione di Studio
- 17.....Torino – Sessione di Studio

### Gennaio 2010

- 27.....Lugano –Sessione di Studio
- 27.....Roma – Sessione di Studio

**ATTENZIONE.**

Sulla Home page del sito [www.aiea.it](http://www.aiea.it) è disponibile il calendario di tutti gli eventi programmati da AIEA nell'anno 2010

**I prossimi eventi ISACA:**

## Calendar of Events

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

### December

- 23 December .....Early-bird deadline for Information Security and Risk Management Conference, Bogota, Colombia

### January

- 13 January .....Early-bird deadline for EuroCACS, Budapest, Hungary
- 15 January .....Deadline for 2010 membership and certification renewals
- 20 January .....Deadline for contributions to volume

## ISACA Releases New Risk IT Framework

Qui di seguito è riportato un comunicato stampa di ISACA relativo al rilascio di un nuovo IT RISK FRAMEWORK, disponibile come download gratuito a [www.isaca.org/riskit](http://www.isaca.org/riskit)



---

Associazione Italiana  
Information Systems Auditors

---



### **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](mailto: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](mailto: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](http://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.

### **Le Newsletter delle altre Associazioni**

E' disponibile on line, la **Newsletter CLUSIT** del 30 novembre 2009 (disponibile in PDF all'indirizzo [www.clusit.IT/newsletter\\_30\\_11\\_09.pdf](http://www.clusit.IT/newsletter_30_11_09.pdf))

- Sono disponibili e qui allegate le Newsletter n.ro 342-2 del Garante Privacy

E' disponibile on line, la **Newsletter ANSSAIF** all'indirizzo [www.anssaif.it](http://www.anssaif.it)

- E' disponibile on line, la **Newsletter AIPSI** all'indirizzo [www.aipsi.org/newsletter](http://www.aipsi.org/newsletter)

**Sent:** Tuesday, December 08, 2009 8:16 PM

**Subject:** ISACA News: ISACA Releases New Risk IT Framework

ISACA Chapter Presidents,

Below is a news release on ISACA's brand-new Risk IT framework, available as a free download at [www.isaca.org/riskit](http://www.isaca.org/riskit).

Risk IT is a set of proven, real-world practices that helps organizations achieve their goals, seize opportunities and seek greater return with less risk. It allows enterprises to manage—and capitalize on—risk in the pursuit of their objectives. It extends COBIT, ISACA's globally recognized IT governance framework, and saves time, cost and effort by providing organizations with a way to focus effectively on IT-related business risk areas, including risks related to late project delivery, compliance, obsolete IT architecture and IT service delivery problems.

You are welcome to post this announcement on your web site, include it in your chapter newsletter and share content from it on social networking sites. If you have any questions, please feel free to contact me. For additional ISACA news, please visit [www.isaca.org/news](http://www.isaca.org/news).

Best regards,

Kristen Kessinger  
Assistant Manager of Media Relations  
ISACA  
+1.847.660.5512  
[kkessinger@isaca.org](mailto:kkessinger@isaca.org)

---

**ISACA Launches Risk IT to Help Organizations Balance Risk With Profit**  
*Free Download From ISACA.org*

**Rolling Meadows, IL, USA (8 December 2009)**—ISACA today announced the release of Risk IT: Based on COBIT®, the first global IT-related risk framework to provide a comprehensive view of the business risks associated with IT initiatives. Risk IT builds on ISACA's globally recognized COBIT framework for IT governance to provide a missing link between conventional enterprise risk management and IT risk management and control.

Enterprises achieve return by taking risks, but sometimes they try to eliminate the very risks that drive profit. Available as a free download at [www.isaca.org/riskit](http://www.isaca.org/riskit), Risk IT is designed to help enterprises increase their return on opportunities by managing risks more effectively, rather than trying to eliminate them completely.

ISACA, a nonprofit association of 86,000 information technology (IT) professionals, developed Risk IT in response to member and industry demand. The framework and its supporting documentation are the result of thousands of hours of work from a team of IT and business experts and 60 expert reviewers spanning North America, Europe, the Middle East, Africa and Asia Pacific.

“Risk IT saves time, cost and effort by providing a clear method to focus on IT-related business risks such as late project delivery, compliance, misalignment, obsolete IT architecture and IT service delivery problems,” said Urs Fischer, CISA, CPA (Swiss), CIA, a developer of Risk IT. “Risk IT provides the guidance to help executives and management ask the key questions, make better risk-adjusted decisions and guide their enterprises so that risk is managed more effectively.”

Risk IT provides a single, comprehensive view of IT-related business risks, which can cost companies millions annually in lost revenues and opportunities.

“Risk and value are two sides of the same coin. Risk is inherent to all enterprises, but a balance must be struck that avoids value destruction and ensures that opportunities for value creation are not missed,” said Risk IT developer Brian Barnier, CGEIT. “Risk IT helps all levels of management manage risk for the greatest benefit and helps detect warning signs earlier.”

Risk IT complements and extends COBIT and Val IT, but also is highly effective as standalone guidance. A key aspect is that all enterprises using IT, whether one-person shops or multinational conglomerates, can benefit from Risk IT. It can also be customized for any type of enterprise in any geographic location.

*The Risk IT Framework* is available as a free download. Print versions can be purchased at [www.isaca.org/bookstore](http://www.isaca.org/bookstore).

### **About ISACA**

With more than 86,000 constituents in more than 160 countries, ISACA® ([www.isaca.org](http://www.isaca.org)) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) designations.

ISACA developed and continually updates the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

### **Contact:**

Kristen Kessinger, ISACA, +1.847.660.5512, [news@isaca.org](mailto:news@isaca.org)



- STOP A FAX SELVAGGIO
- LAVORO: ANONIMATO PER LA DIAGNOSI HIV
- NO AI DATI SANITARI SUL SITO DEL COMUNE
- A MADRID FISSATI STANDARD INTERNAZIONALI PER LA PRIVACY

## Stop a fax selvaggio

Nuovo divieto del Garante della privacy

Il Garante per la protezione dei dati personali è intervenuto nuovamente per combattere l'invio di pubblicità indesiderata via fax. Dall'inizio del 2009 sono oltre 500 le segnalazioni già pervenute al Garante da cittadini e imprese che denunciano questa tecnica di spam.

L'ultimo intervento dell'Autorità ha riguardato una società alla quale è stato vietato l'ulteriore trattamento di dati personali, utilizzati senza consenso dei destinatari per l'invio di pubblicità indesiderata. L'Autorità ha imposto, inoltre, la cancellazione di tutti i dati personali per i quali non risulti documentata la manifestazione del consenso all'invio di comunicazioni promozionali. L'azienda, nel corso dell'istruttoria, ha peraltro ammesso di aver ricevuto 20.300 richieste da parte di professionisti e imprese che chiedevano di non ricevere più pubblicità e di essere cancellati dalla loro banca dati. La mancata osservanza del provvedimento di divieto espone a sanzioni penali e al pagamento di una somma che va da trentamila a centottantamila euro.

Come altre imprese in precedenza, anche in questo caso la società ha affermato di utilizzare, per gli invii, nominativi estratti da elenchi telefonici "categorici" pubblici (come Pagine Gialle o Pagine Utili). Questo consentirebbe, ad avviso delle imprese, di poter liberamente disporre di quei numeri per comunicazioni promozionali.

Il Garante, al contrario, ha ancora una volta ribadito che l'uso di sistemi automatizzati per inviare messaggi promozionali, come è il fax (ma il discorso vale anche per sms, mms, e-mail, etc.) impone la preventiva acquisizione del consenso informato e specifico da parte dei destinatari, anche quando si tratti di dati estratti da elenchi categorici o da albi.

## Lavoro: anonimato per la diagnosi Hiv

"Idoneo" o "non idoneo" al servizio: sono le sole informazioni che possono comparire sui certificati medici legali che attestano l'idoneità al servizio di un lavoratore. Nessun riferimento a patologie sofferte è consentito e dunque ai dipendenti sieropositivi deve essere assicurata garanzia assoluta di anonimato. Questi principi sono stati ribaditi dal Garante privacy che, con un provvedimento di cui è stato relatore Mauro Paissan, ha ritenuto fondato il reclamo di un dipendente del Ministero della difesa. All'amministrazione è stato vietato far circolare al suo interno informazioni sulla salute del lavoratore, specie quelle relative all'Hiv.

Il dipendente si era rivolto all'Autorità contestando le modalità con cui i suoi dati personali erano circolati all'interno del Ministero. Nome del dipendente e diagnosi, erano infatti presenti nel verbale della visita collegiale trasmesso dalla commissione medica all'Ispettorato di sanità della marina militare. E anche la copia del verbale inviata all'ufficio del personale con la diagnosi "sbarrata e omessa", consentiva, seppur indirettamente, di risalire all'infezione Hiv, essendo l'unica patologia per la quale è prevista la "cancellazione" dai verbali di accertamento medico. Il Garante, oltre a inibire l'uso dei dati del dipendente, ha ordinato al Ministero di conformare alla normativa sulla riservatezza la circolazione dei dati sanitari al suo interno. D'ora in poi il Ministero dovrà utilizzare un attestato che riporti il solo giudizio medico legale senza diagnosi, anziché il verbale integrale della visita collegiale. Da modificare anche il modello di informativa: i lavoratori dovranno essere chiaramente informati dell'obbligatorietà o meno di fornire dati sulla propria salute e delle relative conseguenze nell'ambito degli accertamenti medico legali ai fini dell'idoneità al servizio.

## No ai dati sanitari sul sito del Comune

Le amministrazioni locali non possono pubblicare sul proprio sito web il nome, il cognome e l'indicazione dello stato di salute o della condizione di indigenza dei beneficiari di contributi sociali contenuti nelle delibere.

Lo ha stabilito il Garante accogliendo la segnalazione di alcuni consiglieri comunali di minoranza che lamentavano la pubblicazione sul sito del proprio comune di una deliberazione in cui erano riportate, in forma estesa e senza *omissis*, le generalità di un cittadino in stato vegetativo di cui veniva finanziato il ricovero in una casa di cura. Lo stesso documento riportava anche il nome e cognome del padre che contribuiva al pagamento della retta. I segnalanti evidenziavano poi come in un'altra delibera, sempre visibile sul sito dell'ente, fossero riportate le generalità anche di altri cittadini indigenti e, per questo, destinatari di fondi stanziati dall'amministrazione per la loro permanenza in casa di riposo.

L'Autorità ha vietato la diffusione dei dati idonei a rivelare lo stato di salute contenuti nella prima delibera, ritenendo il trattamento illecito. Nel provvedimento (relatore Giuseppe Fortunato) l'Autorità ha ribadito che le amministrazioni locali, fermo restando il rispetto degli obblighi di legge sulla trasparenza delle proprie deliberazioni, devono compiere una selezione attenta dei dati personali da diffondere, tenendo conto non solo dei principi di pertinenza, non eccedenza e indispensabilità delle finalità perseguite dai singoli atti, ma anche del divieto di diffusione di dati idonei a rivelare lo stato di salute. L'Autorità ha prescritto inoltre al comune di attivarsi presso i responsabili dei principali motori di ricerca al fine di sollecitare la rimozione della copia web di questo provvedimento dai loro indici e memorie *cache*. All'ente è stato ordinato infine di adottare opportuni accorgimenti (diciture generiche o codici numerici) atti ad evitare che sulla seconda delibera, consultabile sul sito, siano presenti dati sulle condizioni sociali disagiate degli anziani citati.

## A Madrid fissati standard internazionali per la privacy

Le Autorità Garanti per la protezione dei dati personali di 50 Paesi, riunite a Madrid per la 31ma Conferenza internazionale, hanno approvato lo scorso 6 novembre un'importante risoluzione in materia di standard

internazionali che contiene un primo pacchetto di regole e principi condivisi a livello mondiale.

Come ha affermato Francesco Pizzetti, presidente dell'Autorità italiana, la risoluzione "consiste in una serie di prescrizioni a tutela della protezione dei dati dei cittadini che, muovendo da un impianto simile a quello della Direttiva europea, definisce principi generali in modo tale che possano essere accettati anche da Autorità di altri Paesi con una diversa cultura della protezione dei dati". "Oggi - ha proseguito Pizzetti - la protezione dei dati o è globale o non è".

Attraverso gli standard vengono definiti una serie di principi, diritti, obblighi e meccanismi procedurali che devono rappresentare l'obiettivo di qualunque ordinamento giuridico in tema di privacy e protezione dei dati, nel settore pubblico e in quello privato.

Ecco in sintesi i principi condivisi che ciascun ordinamento è chiamato ad assicurare. Liceità, correttezza e proporzionalità del trattamento di dati personali; rispetto del principio di finalità; trasparenza dei trattamenti; qualità e sicurezza dei dati; salvaguardia dei diritti di accesso, rettifica, cancellazione e opposizione da parte degli interessati; responsabilità del titolare anche per i trattamenti affidati a soggetti esterni; rafforzamento delle tutele per i dati sensibili; obbligo di assicurare il rispetto di questi standard nei trasferimenti internazionali di dati; garanzia di un controllo indipendente affidato ad autorità autonome ed imparziali provviste di adeguati poteri e risorse; potenziamento di approcci proattivi e preventivi basati sull'impiego di tecnologie, su valutazioni preventive di impatto-privacy, su controlli di qualità.

Secondo la Risoluzione, gli standard potranno costituire un'utile base di partenza per promuovere l'ulteriore armonizzazione delle garanzie in materia di privacy, soprattutto per quanto riguarda i flussi internazionali di dati.

Tra le altre significative risoluzioni approvate dalla Conferenza figurano quella sulla tutela della privacy on line dei minori e quella sulla creazione di un sito web della Conferenza internazionale per favorire la circolazione internazionale dei documenti e delle informazioni in materia di protezione dati.

Nell'ambito della Conferenza, il Presidente dell'Autorità Garante italiana, Francesco Pizzetti, ha affrontato il tema del diritto d'autore online e la imprescindibile necessità di contemperare proprietà intellettuale, diritti delle imprese e tutela della riservatezza degli utenti.

### 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: 06/6967751 - Fax: 06/6967755. Newsletter è consultabile sul sito Internet [www.garanteprivacy.it](http://www.garanteprivacy.it)



# Insight

## *Chief Financial Officer. Una professione in continua evoluzione (Survey)*

In uno scenario di business e finanziario sempre più volatile, il Chief Financial Officer (CFO) si trova oggi a dover rispondere a crescenti richieste interne ed esterne, facendo leva sull'organizzazione della funzione Amministrazione Finanza e Controllo (AFC), sui processi e sui sistemi di gestione delle informazioni al fine di:

- fornire informazioni “rilevanti” a supporto dei processi decisionali, in modo tempestivo e affidabile;
- garantire, in modo tempestivo ed economico, il reperimento delle risorse finanziarie necessarie;
- trovare soluzioni efficaci per ridurre i costi, senza compromettere i livelli di controllo;
- mantenere la stabilità della struttura organizzativa di fronte a situazioni nuove o non ricorrenti;
- garantire in via continuativa la conformità dell'organizzazione a requisiti regolamentari sempre più complessi e in perenne evoluzione.

Il presente documento ha lo scopo di fornire una sintesi dei risultati della ricerca dal titolo **“Chief Financial Officer. Una professione in continua evoluzione”**, condotta da Protiviti con la collaborazione di Robert Half, la più antica società al mondo di recruiting specializzato, entrambe appartenenti al network internazionale Robert Half International (RHI).

La ricerca nasce dalla volontà di condurre un'analisi in grado di coniugare gli aspetti di organizzazione e di processo in ambito Finance, che fanno parte delle competenze *core* di Protiviti, con i temi legati alle dinamiche retributive e di incentivazione, tipici dell'esperienza professionale di Robert Half.

In tal senso, la presente ricerca rappresenta un'integrazione dei contenuti della **Global Financial Salary Guide 2009**, analisi condotta ogni anno da RHI sui livelli retributivi di 16 profili professionali in area Amministrazione, Finanza e Controllo (AFC) di 21 Paesi (tra Europa, Nord e Sud America, Medio Oriente e Asia-Pacifico), disponibile sul sito di Robert Half nella sezione [Notizie e Eventi](#).

La ricerca, rivolta ad un'ampia platea di professionisti, ha visto la partecipazione di oltre 100 CFO.

I risultati della ricerca sono stati sintetizzati e aggregati in funzione delle seguenti aree tematiche:

- Il profilo professionale del CFO;
- Il pacchetto retributivo;
- Il CFO e la Governance societaria;
- Organizzazione e sviluppo della funzione AFC;
- L'agenda del CFO.

### **I risultati in pillole**

*Il CFO è confermato tra le figure di Top Management dell'azienda: spesso viene richiesto il suo ingresso nel Consiglio di Amministrazione.*

*Il CFO si trova ad affiancare il Vertice nella definizione e nell'implementazione della strategia, vedendosi riconosciuta la profonda conoscenza dell'azienda e del business maturata attraverso la “visione dei numeri”.*

*Il controllo dei costi, la gestione e l'efficiamento dei processi, il monitoraggio dei flussi finanziari restano i temi fondamentali sul tavolo del CFO.*

*La crescita aziendale, la pianificazione strategica e operativa e il Risk Management sono invece gli aspetti su cui è attesa una crescente focalizzazione da parte del CFO.*

# Il profilo professionale del CFO

**Il CFO è uno specialista il cui percorso di carriera richiede esperienza e mobilità.**

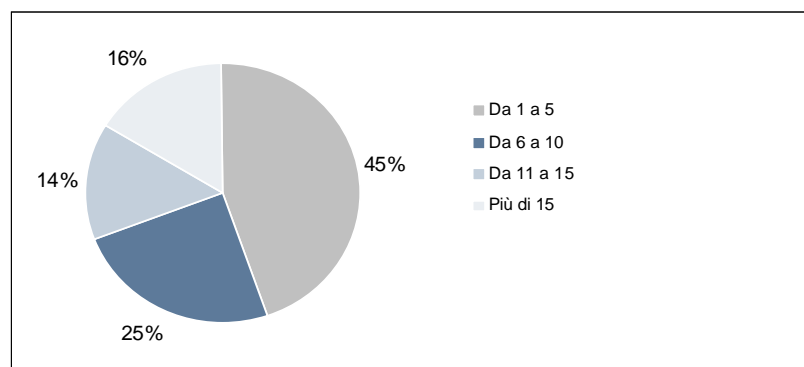
La quasi totalità dei CFO intervistati è rappresentata da uomini (96%) e laureati/e (85% del totale).

Con riferimento all'età anagrafica, il 58% degli intervistati si colloca tra 41 e 50 anni, il 16% oltre 51 anni, mentre solo il 26% tra 30 e 40 anni.

Solo il 35% dei CFO intervistati ha raggiunto l'attuale posizione a seguito di un percorso di carriera sviluppatosi all'interno della stessa azienda o dello stesso Gruppo.

Nei rimanenti casi, la carriera professionale si è sviluppata prevalentemente in società appartenenti ad altri settori (94%), denotando, nel campione analizzato, una significativa mobilità richiesta per lo sviluppo di carriera verso posizioni di vertice, nonché la generale multi-settorialità dell'esperienza maturata.

**Fig. 1 - Anni di esperienza maturati nell'attuale posizione**



## Il pacchetto retributivo

**La retribuzione media annua di un CFO varia significativamente in funzione delle dimensioni dell'azienda e degli anni di esperienza. Il pacchetto retributivo prevede una parte variabile che può anche avvicinarsi o superare il 40%.**

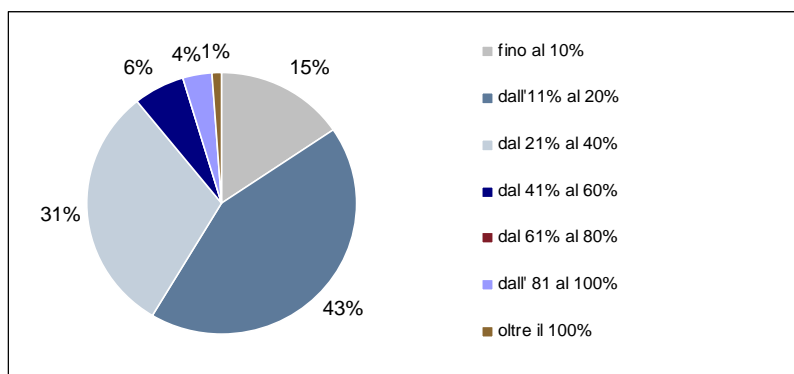
Integrando i risultati della ricerca con i trend retributivi evidenziati nella *Global Financial Salary Guide 2009*, emerge che la retribuzione annua lorda dei CFO delle società italiane (Tab. 1) risulta mediamente più bassa rispetto agli altri Paesi europei, soprattutto nei primi anni di esperienza nel ruolo, per andare ad allinearsi al mercato nel corso dello sviluppo professionale.

Con riferimento alla componente variabile del proprio pacchetto retributivo, il 15% dei professionisti interpellati dichiara che tale componente rappresenta un valore inferiore al 10%, per il 43% un valore compreso tra l'11% e il 20%, per il 31% tra il 21% e il 40%, mentre solo per l'11% degli intervistati, concentrati principalmente presso società di grandi dimensioni, incide per un valore superiore al 40% (Fig. 2, pagina successiva).

**Tab. 1 – Retribuzione Annua Lorda media per i CFO italiani**

|                                | anni di esperienza |                   |                |
|--------------------------------|--------------------|-------------------|----------------|
|                                | 6-9 anni           | 10-15 anni        | più di 15 anni |
| <i>piccole e medie imprese</i> | 50.000 - 80.000    | 75.000 - 120.000  | 130.000+       |
| <i>grandi imprese</i>          | 70.000 - 110.000   | 100.000 - 160.000 | 180.000+       |

**Fig. 2 - Incidenza (%) della retribuzione variabile all'interno del pacchetto retributivo**



Analizzando gli obiettivi quantitativi utilizzati per il calcolo della retribuzione variabile, il risultato operativo (40%) rappresenta il parametro economico - finanziario maggiormente diffuso.

Esaminando invece obiettivi qualitativi ai quali la componente variabile risulta correlata, il miglioramento del Sistema di Controllo Interno e la Gestione delle Risorse sono gli indicatori di maggior peso, confermando

l'importanza e l'attenzione data alla gestione dei processi aziendali e dell'organizzazione.

Benché il Risk Management rappresenti un obiettivo su cui lavorare solo per il 10% del campione, è interessante notare come tale elemento sia presente non solo presso società quotate e/o di grandi dimensioni, ma anche presso realtà medio-piccole, a testimonianza di una sempre più diffusa percezione dell'importanza della gestione dei rischi in ambito aziendale.

## Il CFO e la Governance societaria

**Le recenti evoluzioni ispirate dalle Best Practice di Corporate Governance hanno ampliato notevolmente gli ambiti di responsabilità e intervento dei CFO (soprattutto con riferimento al risk management e ai sistemi di controllo interno).**

Nella maggioranza dei casi il CFO è un riporto diretto dell'Amministratore Delegato.

Il ruolo di vertice del CFO, nonché la sua partecipazione sempre più attiva alla gestione aziendale, è testimoniata oltre che dalla diffusa presenza all'interno di comitati di direzione o di indirizzo, dalla sua inclusione anche all'interno del Consiglio di Amministrazione o del Consiglio di Gestione (51% del totale).

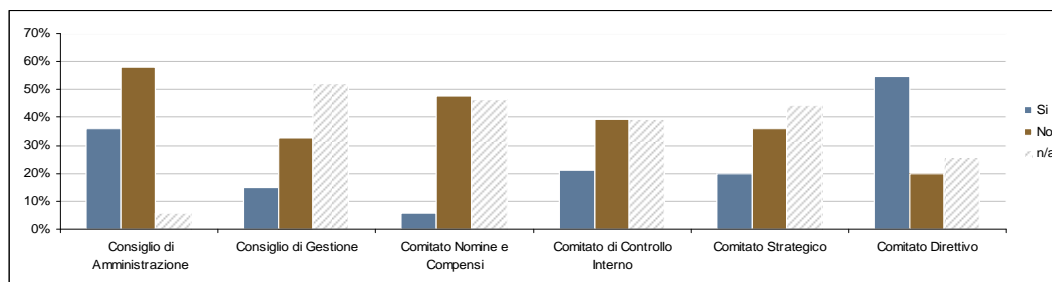
Contrariamente a quanto ci si potrebbe attendere, invece, il 21% degli intervistati dichiara di essere membro del Comitato di Controllo Interno e il 6% del Comitato Nomine e Compensi (Fig. 3).

Inoltre, il 38% degli intervistati ha assunto la carica di Preposto al Controllo Interno.

In tali casi, presenti anche presso società quotate, si può presupporre che vi sia la tendenza a privilegiare la necessità di conoscenza dell'operatività e degli eventi aziendali, piuttosto che il mantenimento dell'indipendenza rispetto a ruoli e responsabilità operative definite all'interno dell'organizzazione.

Infine, analizzando le ulteriori cariche ricoperte dai CFO, emerge che il 79% del campione dipendente di società quotate ricopre, come è lecito attendersi, anche il ruolo di Dirigente Preposto alla redazione dei documenti contabili e societari.

**Fig. 3 – Presenza negli organismi collegiali**



# Organizzazione e sviluppo della funzione AFC

**In un contesto di stabilità o contrazione degli organici, il ricorso all'Outsourcing e al lavoro temporaneo costituiscono le principali leve di sviluppo organizzativo della Funzione. Le priorità, in termini di sviluppo delle competenze, riguardano le tematiche della gestione dei rischi e dei sistemi informativi a supporto dei processi decisionali.**

In relazione al dimensionamento della funzione AFC, il 46% degli intervistati ha dichiarato che l'organico non ha subito variazioni negli ultimi 2 anni e quasi il 50% prevede che rimarrà invariato per i prossimi 12 mesi. Tendenze queste ultime legate, da un lato, al contesto economico-finanziario attuale, dall'altro alla possibilità di avvalersi di servizi in outsourcing.

Infatti, l'83% delle società appartenenti al campione dichiara di avvalersi di fornitori esterni di servizi amministrativi (out-sourcing) o di strutture/società di servizi interne al gruppo di appartenenza (in-sourcing).

In relazione alla tipologia di servizi, si rileva che le attività relative alla gestione del Costo del Personale (78% dei casi), Fiscalità (37%) e Information Technology (24%) risultano essere le più esternalizzate.

Oltre il 70% del campione dichiara di fare ricorso a forme di collaborazione temporanea in area AFC, che però incidono meno del 5% sul totale delle risorse impiegate all'interno della funzione stessa. In questo caso è verosimile pensare che il lavoro temporaneo sia

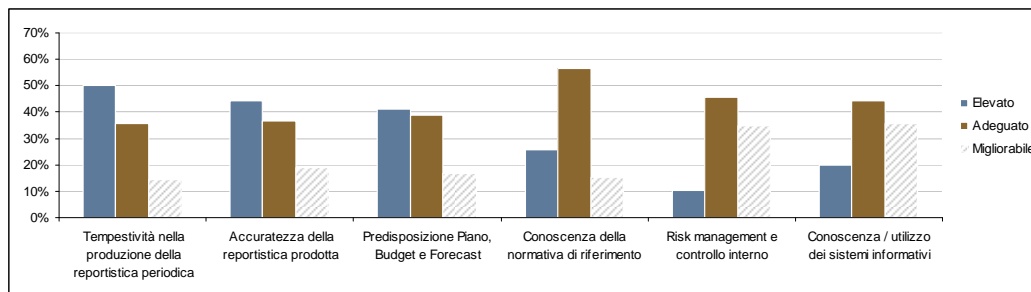
principalmente utilizzato per coprire picchi di lavoro specifici.

Tra i fattori significativi per un'efficace gestione del personale e per riuscire ad attrarre/trattenere i talenti, il 40% del campione ha individuato, come maggiormente rilevante, il poter garantire un adeguato sviluppo professionale, mentre l'offerta di un pacchetto retributivo competitivo si rileva solo nel 20% dei casi.

Tra le aree operative direttamente gestite dai CFO (Fig. 4), più del 40% degli intervistati ritiene che la propria struttura possieda capacità e conoscenze consolidate circa la produzione della reportistica a valori consuntivi e previsionali, mentre il 57% circa ritiene che sia adeguatamente preparata su tematiche relative alla conoscenza della normativa di riferimento.

Le aree che invece presentano i maggiori margini di miglioramento, risultano essere il Risk Management e il Controllo Interno, nonché la conoscenza e l'utilizzo dei Sistemi Informativi a supporto delle attività operative.

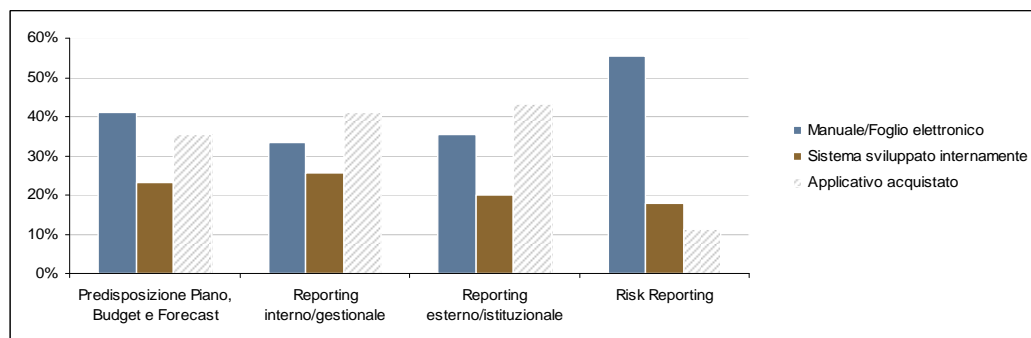
**Fig. 4 – Livello di confidenza verso le aree operative della funzione AFC**



Con particolare riferimento ai sistemi informativi adottati (Fig. 5), emerge che, soprattutto per le attività di budgeting e reporting gestionale verso la Direzione, il 40% delle strutture AFC utilizza fogli elettronici, nonostante sia presente una sempre più ampia parte di professionisti che si avvale del supporto di applicativi dedicati.

In generale, il ricorso ad applicativi di budgeting e reporting sembra rappresentare un trend destinato ad affermarsi ulteriormente, in quanto per molti professionisti rappresenta un valido supporto per ottenere analisi affidabili ed effettuare simulazioni tempistiche di scenari alternativi, in base alle quali prendere decisioni di business, soprattutto in momenti di crisi.

**Fig. 5 – Sistemi informativi utilizzati**



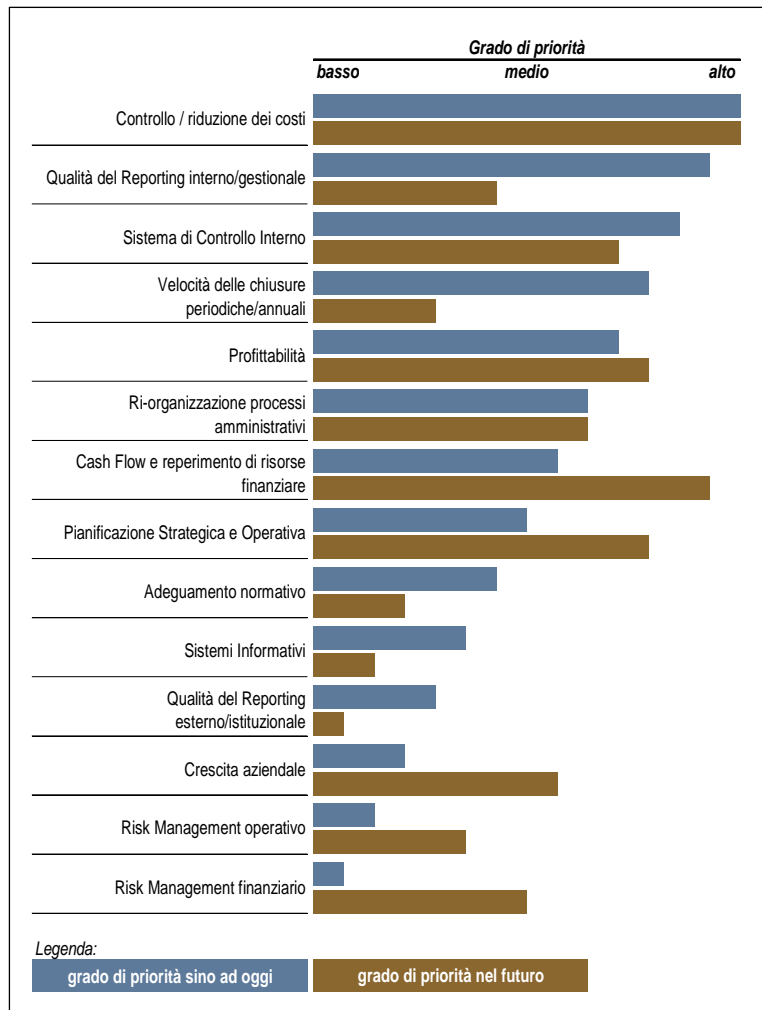
# L'agenda del CFO

**L'agenda del CFO è stata profondamente modificata dai recenti eventi legati alla crisi economico/finanziaria.**

Il confronto tra priorità passate e future del CFO (Fig. 6) fa emergere le seguenti considerazioni:

- un ridimensionamento dell'importanza relativa delle tematiche legate alla qualità dei numeri, al controllo e alla compliance normativa che negli ultimi anni (grazie anche all'ondata di novità normative intervenute) ha costituito un particolare ambito di attenzione<sup>1</sup>. Questa tendenza non deve tanto leggersi come manifestazione di disinteresse verso tematiche che restano prioritarie nella quotidianità della funzione, ma piuttosto come riconoscimento degli sforzi e degli investimenti fatti in passato;
- la permanenza, al top delle priorità del CFO, dei temi legati all'efficienza e al controllo dei costi. A testimonianza di una figura del CFO sempre più focalizzata al monitoraggio delle performance in un'ottica previsionale;
- una rinvigorita attenzione ai temi del risk management e della gestione/controllo finanziario. A conferma che uno degli insegnamenti che i CFO hanno tratto dagli eventi degli ultimi anni è che le nuove sfide si giocheranno proprio sulla capacità di implementare processi di controllo finanziario ispirati alle migliori prassi di risk management.

Fig. 6 – Le tematiche affrontate dal CFO



<sup>1</sup> Tuttavia occorre notare che la lettura dei dati rispetto alle società quotate/controlate da quotate e operanti in settori fortemente regolamentati (ad esempio Servizi Finanziari) restituisce un quadro sostanzialmente differente in quanto sia il Reporting, in particolare gestionale, che la Normativa resteranno temi significativi su cui lavorare.

## Il campione analizzato

La ricerca è stata portata a termine grazie alla collaborazione di circa 100 professionisti che ricoprono ruoli di responsabilità nel settore Amministrazione Finanza e Controllo di società italiane appartenenti principalmente al settore Manifatturiero industriale (25%), al Terziario/Servizi (18%) e alla produzione di Beni di largo consumo (12%).

La distribuzione geografica delle aziende campione è prevalentemente concentrata nel Nord Italia (Nord Ovest per l'83% e Nord Est per il 5%). Solo il 12% del campione è rappresentativo di realtà aziendali presenti nel Centro e Sud Italia.

La maggioranza delle società facenti parte del campione (71%) si contraddistingue per un fatturato annuo inferiore ai 500 milioni di euro.

In relazione al dimensionamento, il 29% delle aziende analizzate impiega meno di 100 dipendenti, il 21% da 100 a 250 (con una media di 170), mentre nel 14% dei casi possono essere considerate come medie imprese (tra 251 e 500 dipendenti, con una media di 280). Il restante 36% rappresenta aziende di grandi dimensioni, con più di 500 dipendenti.

Sul totale delle società che hanno partecipato alla ricerca, il 35% risulta essere quotata in un mercato regolamentato o appartenente a gruppi quotati in Italia o all'Estero.

## Il Protiviti Governance Portal (PGP)

La raccolta e l'elaborazione delle informazioni sono state realizzate attraverso l'applicazione "Assessment Management" della suite "Protiviti Governance Portal", piattaforma informatica sviluppata da Protiviti in grado di supportare e facilitare l'implementazione di un approccio integrato alle attività di Governance, Risk & Compliance (GRC). Il Protiviti Governance Portal si compone dei seguenti moduli:

- **Internal Audit** - Supporta la gestione dei processi di Internal Audit, dalla definizione del Piano di Audit, di tipo "risk-based", fino al reporting e al follow-up;
- **Risk Management** - Consente di gestire le attività di identificazione e valutazione dei rischi aziendali, anche per finalità di compliance;
- **Control Management** - Supporta la mappatura, la valutazione e l'eventuale testing dei controlli per finalità di business e/o di compliance.
- **Incident Management** - Consente la raccolta e l'analisi dei dati, interni, esterni o "virtuali", di perdite operative;
- **Assessment Management** - Consente di gestire in modo sostenibile survey o programmi di auto-valutazione a supporto delle esigenze di governance e compliance.

\* \* \*

Per approfondimenti sulla ricerca o per ricevere la **Global Financial Salary Guide 2009**, rivolgersi a:



### Siro Tasca

Director

E-mail: [siro.tasca@protiviti.it](mailto:siro.tasca@protiviti.it)

### Fabrizio Rubegni

Manager

E-mail: [fabrizio.rubegni@protiviti.it](mailto:fabrizio.rubegni@protiviti.it)

[www.protiviti.it](http://www.protiviti.it)



### Erika Perez

Senior Manager

E-mail: [erika.perez@roberthalf.it](mailto:erika.perez@roberthalf.it)

[www.roberthalf.it](http://www.roberthalf.it)

Scopo della ricerca è quello di fornire informazioni di carattere generale e agevolare la discussione rispetto alle principali tematiche connesse al ruolo e alla professione del CFO (Chief Financial Officer).

I dati raccolti sono stati trattati in forma aggregata e conseguentemente le informazioni di cui al citato documento non intendono fare riferimento ad alcuna specifica situazione.

Protiviti e Robert Half, pur adoperandosi per fornire informazioni accurate e tempestive, non sono responsabili per qualsiasi errore o omissione né per i risultati ottenuti attraverso la ricerca.

In nessun caso Protiviti e Robert Half saranno responsabili per danni conseguenti, indiretti, incidentali o speciali di qualsiasi natura derivanti dall'utilizzo di qualsiasi informazione contenuta nel presente documento.

