ICT Security: approcci e strumenti per una governance efficace del rischio in un'ottica integrata

Rapporto 2009 Osservatorio Information Security Management

School of Management

POLITECNICO DI MILANO

DIPARTIMENTO DI INGEGNERIA GESTIONALE

MIP

ict institute

POLITECNICO DI MILANO

DIPARTIMENTO DI ELETTRONICA E INFORMAZIONE

CEFRIEL FORGING INNOVATION POLITECNICO DI MILANO

Ottobre 2009

Indice

Indice Figure

Indice Box

Introduzione

Giunto al suo secondo anno di vita, l'Osservatorio Information Security Management, istituito e portato avanti congiuntamente dalla School of Management e dall'ICT Institute del Politecnico di Milano, si presenta quest'anno ancor più ricco di contenuti. In affiancamento all'analisi di oltre 15 casi del settore bancario, da sempre attento alla tematica dell'Information Security, la ricerca di quest'anno ha previsto due Survey, coinvolgendo più di un centinaio tra Chief Information Officer, Chief Information Security Officer e Risk Manager.

Gli obiettivi dell'Osservatorio, in linea con la missione di tutti gli Osservatori ICT & Management di diffondere cultura e best practice sull'uso strategico dell'ICT, sono di:

- analizzare e comprendere criticamente lo stato dell'arte dell'information security, con particolare riferimento ai trend e alle best practice emergenti in termini organizzativo-gestionali e ai fabbisogni, espressi e inespressi, delle imprese;
- costituire il punto di riferimento per la community di attori (studiosi, consulenti, imprese) interessati a promuovere lo sviluppo strategico dell'information security nelle imprese.

Tra i principali risultati di quest'anno c'è sicuramente l'aver analizzato a fondo l'ICT Risk Analysis, definendo un framework di riferimento che possa essere di supporto al management per una pianificazione efficace degli interventi in ambito ICT Security, nonché l'aver approfondito la complessa relazione tra ICT Security ed Enterprise Risk Management, mettendo in luce le soluzioni organizzative emergenti ed evidenziandone opportunità e rischi. Sempre più, infatti, l'ICT Security va oggi pensata e gestita come un elemento trasversale dell'organizzazione e una leva strategica che può avere un impatto rilevante sulle strategie dell'impresa.

Umberto Bertelè

Andrea Rangone

Executive Summary

Gli obiettivi della Ricerca

Nel corso del primo anno di attività l'Osservatorio Information Security Management aveva affrontato il tema della governance strategica dell'ICT Security, ovvero l'insieme di soluzioni organizzative e processi atti a garantire:

- una strategia di ICT Security ben definita e collegata agli obiettivi di business, nonché a quelli dell'ICT;
- una struttura organizzativa congruente con gli obiettivi, la tipologia di attività e il carico di lavoro previsto;
- sistemi di pianificazione adeguati;
- metodologie di Risk Analysis/ Management appropriate;
- policy di alto livello ben strutturate, che comprendano tutti gli aspetti legati alla strategia, al controllo e alla regolamentazione inerente l'ICT Security;
- processi di monitoraggio e controllo che assicurino feedback tempestivi sullo stato di implementazione dei programmi e sulla loro efficacia, in modo da consentire di attuare le opportune manovre correttive in itinere, qualora necessario;
- sistemi di apprendimento (knowledge management) che consentano un aggiornamento e un miglioramento continuo delle policy e delle procedure e, quindi, una costante riduzione del livello di rischio complessivo, nell'ottica del continuous improvement.

Riclassificando e riaggregando gli elementi sopra elencati, è possibile individuare tre macro-categorie fondamentali di leve progettuali dell'ICT Security governance, e precisamente:

- l'organizzazione, intesa nell'accezione di configurazione macro-organizzativa che consenta di mettere in atto i programmi strategici e di gestire l'operatività, nonché modalità di definizione e aggiornamento delle politiche, modalità di gestione dei progetti, definizione del processo di miglioramento continuo;
- i processi di pianificazione e controllo;
- le risorse, le competenze e la cultura organizzativa.

In continuità con il focus della Ricerca 2008, quest'anno le attività sono state articolate in due fasi distinte. In particolare, è stata svolta una prima indagine con l'obiettivo di monitorare il grado di maturità dei sistemi di governance strategica nelle imprese italiane e di evidenziare eventuali significative evoluzioni rispetto a quanto emerso dalla Ricerca dello scorso anno.
La seconda parte della Ricerca si è invece focalizzata sul tema dell'ICT Risk Analysis, che dall'analisi svolta lo scorso anno era risultata uno delle principali punti critici della governance strategica dell'ICT Security. In particolare, si è inteso analizzare:

- l'ICT Risk Analysis: il focus è stato quello di verificare la numerosità di Risk Analysis svolte dalle imprese nell'ambito dell'ICT Security, di elaborare una "tassonomia" dei diversi approcci sulla base di un insieme di variabili descrittive, nonché di mettere in relazione l'utilizzo e la diffusione di tali approcci a variabili di contesto;
- il rapporto tra ICT Security ed Enterprise Risk Management (ERM): in particolare, l'analisi ha riguardato il livello di interazione e di coordinamento tra l'unità ICT Security e l'unità che si occupa della gestione del rischio a livello integrato d'impresa. In particolare, si è cercato di capire: quali siano le informazioni che l'ERM richiede all'ICT Security ai fini della valutazione dell'esposizione complessiva al rischio dell'impresa; quale sia il livello di visibilità che l'ICT Security ha su tale pro-

cesso di valutazione integrata dei rischi (con riferimento sia alle metodologie sia ai risultati); se i risultati delle analisi svolte dall'ERM costituiscano o meno un input in sede di pianificazione delle iniziative di ICT Security.

Vista la complessità e le peculiarità settoriali che caratterizzano queste tematiche, si è scelto di focalizzare le attività di ricerca sul settore bancario, al fine di consentire un'analisi sufficientemente approfondita e completa.

La governance strategica dell'ICT Security: lo stato dell'arte

Questa fase della Ricerca è stata finalizzata a fare il punto con i Chief Information Officer (CIO) sullo stadio di maturità della governance strategica dell'ICT Security. I risultati di questa indagine mettono in luce una realtà caratterizzata da un certo livello di eterogeneità e in continua evoluzione. In particolare, per quanto concerne il posizionamento dell'unità di ICT Security all'interno dell'organigramma aziendale, nella maggioranza delle imprese rispondenti il responsabile di tale unità è un primo riporto del CIO (una percentuale sicuramente importante, e in crescita rispetto al passato). Nel contempo, in ben il 19% dei casi tale figura non è nemmeno presente nell'organigramma (né, in molti casi, è previsto il suo inserimento a breve).
Altrettanto variegata appare la situazione per ciò che concerne la dimensione dell'unità di ICT Security all'interno della Direzione ICT: se la maggioranza dei rispondenti dichiara che l'organico è composto da una persona, vi è anche un 14% di imprese in cui la dimensione supera le 10 unità.
Va sottolineato altresì che la maggioranza delle imprese (precisamente il 53%) ha modificato nell'ultimo anno l'assetto organizzativo dell'ICT Security o ritiene di farlo nel prossimo futuro, a riprova del fatto che si è ben lontani dall'aver raggiunto una situazione di equilibrio. Questo dato conferma i risultati emersi nel corso del primo anno di Ricerca sull'evoluzione dei modelli organizzativi dell'ICT Security.
Per quanto concerne gli aspetti legati ai processi di pianificazione e controllo, si conferma la crescente pervasività dell'ICT Security, tant'è che gli input per l'individuazione delle iniziative sono di natura molto diversa e provengono da numerose unità organizzative (ICT, ovviamente, ma anche Corporate Security, Internal Audit, Organizzazione, Risorse Umane, Business Unit, ecc.).
A questa estrema varietà delle fonti di input non corrisponde sempre un processo di pianificazione sufficientemente strutturato: solo poco più di un terzo delle imprese infatti redige sistematicamente un piano strategico completo, che include tutte le attività riconducibili alla sicurezza informatica. Un altro terzo delle imprese dichiara di farlo solamente per i progetti più rilevanti, mentre il 30% dei CIO non elabora alcun documento di pianificazione di questo tipo. Da questo punto di vista non sembra che le imprese abbiano fatto molti passi avanti rispetto al recente passato: questo rimane a nostro avviso un elemento di criticità piuttosto rilevante.
Nella definizione delle priorità di intervento le imprese dichiarano di fare ricorso largamente alla Risk Analysis, anche se non sempre in modo sistematico, e non sempre (o non esclusivamente) nell'ambito della fase di pianificazione annuale.
Meno eclatante appare il quadro con riferimento alla diffusione dei sistemi di misurazione delle prestazioni di tipo "direzionale" nell'ambito dell'ICT Security: solo un quarto delle imprese rispondenti ha dichiarato di avere sviluppato e di utilizzare questo tipo di strumentazione, mentre un altro 20% circa afferma che, pur non avendo un sistema "dedicato" all'ICT Security, alcuni KPI relativi a quest'area sono inseriti in sistemi "di più alto livello" (per esempio, sistemi di performance management a livello di ICT)
Infine, i dati relativi al budget allocato all'ICT Security confermano che, nonostante questo momento di crisi economica, nella maggioranza dei casi non è prevista una contrazione delle risorse dedicate a quest'area (risorse che si attestano nella maggioranza dei casi tra l'1 e il 5% del budget totale dell'ICT). Questo può essere un segnale della crescente importanza attribuita a quest'area, anche se va detto che in molti casi buona parte del budget è legato a iniziative di compliance a nuove normative, quindi, di fatto, non discrezionale.

Gli approcci alla Risk Analysis nell'ambito dell'ICT Security

Vista l'estrema varietà ed eterogeneità delle attività di ICT Risk Analysis condotte dalle aziende, è stato necessario innanzitutto definire un framework che supportasse la classificazione delle diverse tipologie di analisi e metodologie utilizzate. Tale framework intende anche essere di supporto ai manager (Chief Information Security Officer (CISO) in primis) sia per finalità di benchmarking sia nella fase di definizione degli approcci da adottare nei diversi ambiti di applicazione.

Il framework ha identificato tre macro categorie di ICT Risk Analysis ricorrenti, riconducibili alle attività di Progettazione nuove iniziative, Disaster recovery e Adempimenti normativi, sulla base del confronto tra letteratura e risultati delle interviste con i CISO.

Tale macro classificazione, però, non è sufficiente per identificare l'attività svolta, in quanto anche all'interno della stessa macrocategoria possiamo trovare approcci molto diversificati. Per tale motivo, il framework proposto prende in considerazione sia alcuni fattori che caratterizzano l'orizzonte di riferimento di una specifica ICT Risk Analysis, sia le variabili di configurazione che definiscono la specifica metodologia utilizzata. In particolare, dalle interviste effettuate i principali fattori caratterizzanti l'orizzonte di un'ICT Risk Analysis risultano essere le Finalità, l'Ambito e i Requisiti considerati. Per quanto invece concerne le variabili di configurazione della metodologia, fattori chiave risultano essere gli Input types, il Flusso logico, gli Attori, gli Input sources e gli Strumenti utilizzati.

Sulla base del framework definito si è proceduto ad analizzare in un primo momento il settore Banking, storicamente il più sensibile al tema della sicurezza, e successivamente altri settori di interesse, quali: Assicurativo, Automotive, Chimico e Farmaceutico, ICT e Telecomunicazioni, Utility.

Con riferimento al Banking, dalla Ricerca svolta emerge una copertura pressoché totale delle tre macro categorie di analisi individuate, che vengono condotte da almeno due terzi dei casi analizzati, con un picco del 90% per la categoria "Adempimenti normativi". Per quanto concerne i fattori caratterizzanti l'orizzonte dell'ICT Risk Analysis, si evidenzia come vi sia notevole eterogeneità anche all'interno della stessa macrocategoria. Ad esempio, per quanto concerne le finalità delle analisi, nel caso dell'analisi ai fini del "Disaster recovery" il panel si è distribuito in maniera omogenea tra le Stime di perdita e l'Identificazione di contromisure. L'indagine ha anche mostrato come non è sempre scontato che i requisiti di Confidenzialità, Integrità e Disponibilità siano tutti parte dell'analisi, ma che invece in talune occasioni vengano effettuate analisi molto mirate su uno o un paio di requisiti, tralasciando gli altri.

Per quanto concerne le variabili di configurazione dell'ICT Risk Analysis si può notare come molte di esse risultino essere trasversali alle tre macro categorie identificate: per esempio, per quanto riguarda l'orizzonte temporale di analisi ("gli scenari"), tutte le analisi tendono a focalizzarsi sull'"AS IS" (ovvero lo stato in essere al momento in cui viene svolta l'analisi), più che analizzare serie storiche o effettuare previsioni su scenari futuri. Similmente, si registra un utilizzo molto diffuso di strumenti di sviluppati ad hoc e basati sulla suite office a supporto dell'implementazione dell'analisi, mentre risultano poco utilizzate le soluzioni commerciali. A questo proposito, le indicazioni emerse dalle interviste fanno trasparire un'elevata attenzione a contenere la complessità delle attività di ICT Risk Analysis. Ulteriori informazioni analizzate sono la frequenza di cambiamento della metodologia utilizzata, dove emerge una sostanziale stabilità, e la possibilità di riutilizzo di semilavorati comuni per le diverse tipologie di ICT Risk Analysis, opportunità che appare sfruttata piuttosto sporadicamente, probabilmente per le indubbie difficoltà connesse.

Per quanto riguarda gli altri settori analizzati (Automotive, Assicurativo, Chimico e Farmaceutico, ICT e Telecomunicazioni, Utility), un primo dato interessante è che, contrariamente a quanto avviene nel Banking, la Risk Analysis non è diffusa in tutte le tre macro categorie identificate. In particolare in tutti i settori appare molto ricorrente l'analisi effettuata per "Adempimenti normativi". Nei settori Chimico e Farmaceutico e Utility, in-

vece, non appare diffuso l'utilizzo della Risk Analysis per "Progettazione nuove iniziative". Per quanto riguarda i fattori caratterizzanti l'orizzonte dell'ICT Risk Analysis, non si evidenzia, rispetto al settore Banking, uno scostamento così ampio come forse ci si poteva aspettare a priori.
Per quanto concerne le variabili di configurazione dell'ICT Risk Analysis, invece, vi sono alcune significative differenze, con riferimento in particolare al flusso logico dell'analisi (trasversalmente sulle tre macro categorie di Risk Analysis), nonché a diversi elementi metodologici delle analisi finalizzate alla "Progettazione nuove iniziative". Si riscontra inoltre un'elevata frammentazione degli approcci.
Sicuramente il quadro che ne emerge conferma l'interesse e l'importanza dell'ICT Risk Analysis e testimonia come probabilmente sia ancora necessaria una certa maturazione, legata all'acquisizione di maggiore esperienza in questo ambito, prima di poter giungere all'identificazione di una terminologia univoca e di approcci comuni (almeno a livello di industry).

Il rapporto tra ICT Security ed Enterprise Risk Management

I risultati della Ricerca evidenziano che l'interazione tra ICT Security ed Enterprise Risk Management nella maggioranza delle banche analizzate è ancora piuttosto limitata: oltre il 50% dei CISO rispondenti ha infatti affermato che i momenti di dialogo e di collaborazione sono di natura occasionale, e comunque non sistematici.
Scendendo più nel dettaglio, l'ERM appare relativamente poco coinvolta nella scelta delle metodologie utilizzate dall'ICT Security per le analisi dei rischi finalizzate alla definizione delle priorità di intervento: solo in un quarto dei casi partecipa attivamente alla definizione delle metodologie, mentre nella maggioranza dei casi ha un ruolo puramente consultivo.
Di converso, l'ICT Security non sembra avere un ruolo particolarmente rilevante nel processo di valutazione del livello di esposizione complessiva al rischio effettuata dall'ERM. In molti casi si limita a fornire dei dati "grezzi", che poi l'ERM elabora al suo interno, e spesso l'ICT Security non ha visibilità né sulle logiche e le metodologie utilizzate per l'elaborazione dei dati, né sui risultati.
Inoltre, solo in poco più della metà dei casi i risultati delle analisi svolte dall'ERM hanno un impatto sulle definizioni delle priorità di intervento in ambito ICT Security, mentre un terzo dei rispondenti ha dichiarato che non vi è alcun feedback di questo tipo.
In conclusione, fatta eccezione per alcuni casi di eccellenza, si ha l'impressione che vi sia un certo "scollamento" tra questi due mondi. A nostro avviso, è però opportuno che l'ICT Security eviti il rischio di isolamento e cerchi il più possibile un dialogo proficuo con l'ERM, in quanto solo in questo modo si può essere sicuri che venga data la giusta importanza al rischio ICT e che questo venga valutato con metodologie appropriate. Questo non può che aumentare la visibilità delle attività di ICT Security, accrescerne la rilevanza strategica agli occhi del Top Management, con un probabile effetto positivo anche sulle risorse allocate a queste attività.

Paolo Maccarrone

Luca Marzegalli

1. La rilevanza dell'ICT Security

L'informazione rappresenta certamente una risorsa di fondamentale importanza per le imprese: basti pensare alle organizzazioni in cui i dati rappresentano il vero e proprio core business (è il caso del settore bancario, finanziario, assicurativo, oltre ovviamente alle telecom companies e alle aziende produttrici di software). Ma, anche laddove l'output dell'impresa non sia in tutto o in parte "digitalizzato", le informazioni rappresentano comunque una risorsa critica per il corretto ed efficiente svolgimento dei processi aziendali. È quindi facile evincere come la distruzione, la compromissione o l'accesso non autorizzato al patrimonio informativo aziendale possa causare ingenti danni al business, fino a comprometterne la sopravvivenza stessa.
L'ICT Security, generalmente considerata come una parte dell'Information Security, vede il proprio focus sulla protezione di tutte le informazioni gestite dai Sistemi Informativi e trasmesse attraverso le reti aziendali. Questa definizione include:

- la protezione degli asset fisici in cui le informazioni vengono custodite (sale server, storage center, ecc.);
- la protezione delle reti aziendali e delle informazioni che viaggiano su reti pubbliche o di terze parti;
- la protezione dall'accesso non autorizzato a sistemi informativi e alle diverse applicazioni;
- la protezione dei dati aziendali sensibili/personali o regolati da normative specifiche;
- la sicurezza applicativa (protezione da errori volontari o involontari all'interno delle applicazioni);
- la protezione da errori involontari o volontari (comportamento non etico) dei dipendenti.

Già da questo breve elenco si nota il legame tra sicurezza informatica e gli altri domini della sicurezza (sicurezza fisica, sicurezza "logica", sicurezza organizzativa, privacy, ecc.), a testimonianza della pervasività e trasversalità di tale concetto.
Non molti anni fa la gestione dell'ICT Security era vista principalmente come un'attività molto specifica, di carattere esclusivamente tecnologico, e pertanto era spesso confinata in qualche unità all'interno della Direzione ICT. In pochi anni, però, la situazione è radicalmente cambiata a seguito della spinta di diversi driver:

- la crescente consapevolezza circa l'impossibilità, da parte delle sole soluzioni tecnologiche, di garantire l'efficacia dei sistemi preposti alla sicurezza informatica, qualora non integrate da opportune misure di tipo organizzativo;
- la progressiva digitalizzazione dei processi, che, unitamente all'utilizzo sempre più diffuso di Internet nell'ambito delle attività di business e alla crescente mobilità dei dipendenti, ha reso l'Information Security sempre più pervasiva e ha notevolmente aumentato i fattori di rischio cui sono soggette le imprese;
- la continua "escalation" degli attacchi, dovuta al progressivo innalzamento del livello di abilità di chi, per i motivi e con le tecniche più svariate, intende attentare al patrimonio informativo delle aziende. Per questo motivo le imprese e i fornitori di soluzioni sono costretti a un continuo "inseguimento";
- lo sviluppo delle teorie di management legate alla gestione integrata del rischio d'impresa (note con il termine Enterprise Risk Management, ERM), nonché il peso crescente delle normative e degli standard, che ha portato in taluni casi all'introduzione

di vere e proprie unità organizzative dedicate alla "compliance", comportano delle potenziali aree di sovrapposizione e/o di integrazione con la sicurezza, in primis l'Information/ICT Security, e che, se non ben gestite, possono portare a conflitti e a inefficienze organizzative;
- la diffusione dell'idea che la sicurezza possa essere vista come una leva strategica di business, ovvero come un fattore di differenziazione per incrementare il livello di competitività. Di conseguenza, l'interesse da parte delle unità di corporate/business strategy e del management a capo delle diverse aree di business è cresciuto notevolmente.

Da queste considerazioni emerge chiaramente la rilevanza strategica dell'ICT Security, che pertanto è necessario dotare di strumenti e risorse tali da consentirle di dialogare con il resto dell'organizzazione ai livelli che le competono e con il linguaggio corretto. In sintesi, si tratta di inquadrare l'ICT Security nell'ambito della governance complessiva dell'impresa, attribuendole la giusta importanza e garantendo il corretto livello di integrazione con le altre aree.

La governance strategica dell'ICT Security

Nella Ricerca si è preferito usare il termine governance strategica dell'ICT Security per accentuare la distinzione dalla governance operativa, che si occupa sostanzialmente delle soluzioni organizzative necessarie per il corretto funzionamento nell'operatività quotidiana. La governance strategica dell'ICT Security dovrebbe prevedere:
- una strategia di ICT Security ben definita e collegata agli obiettivi di business, nonché a quelli dell'ICT;
- una struttura organizzativa congruente con gli obiettivi, la tipologia di attività e il carico di lavoro previsto;
- sistemi di pianificazione adeguati;
- metodologie di Risk Analysis/Management appropriate;
- policy di alto livello ben strutturate, che comprendano tutti gli aspetti legati alla strategia, al controllo e alla regolamentazione inerente l'ICT Security;
- processi di monitoraggio e controllo che assicurino feed-back tempestivi sullo stato di implementazione dei programmi e sulla loro efficacia, in modo da consentire di attuare le opportune manovre correttive in itinere, qualora necessario;
- sistemi di apprendimento (knowledge management) che consentano un aggiornamento e un miglioramento continuo delle policy e delle procedure e, quindi, una costante riduzione del livello di rischio complessivo, nell'ottica del continuous improvement.

Come si è visto nel paragrafo precedente, la governance strategica dell'ICT Security non può essere vista disgiuntamente dalla governance complessiva dell'impresa. Possono essere individuate tre dimensioni fondamentali dell'ICT Security governance, e precisamente (Figura 1.1):
- l'organizzazione, intesa nell'accezione di configurazione macro-organizzativa che consenta di mettere in atto i programmi strategici e di gestire l'operatività, nonché le modalità di definizione e aggiornamento delle politiche, le modalità di gestione dei progetti, la definizione del processo di miglioramento continuo;
- i processi di pianificazione e controllo;
- le risorse, le competenze e la cultura, che agisce sugli input e, in particolare, sulle risorse umane, sulle loro competenze, sul loro sistema di valori, nonché sulla cultura organizzativa in generale.

Nel corso del primo anno di attività dell'Osservatorio, l'attenzione si era focalizzata sulle prime due dimensioni, di cui, di seguito, verranno brevemente illustrati più in dettaglio gli elementi costituenti.

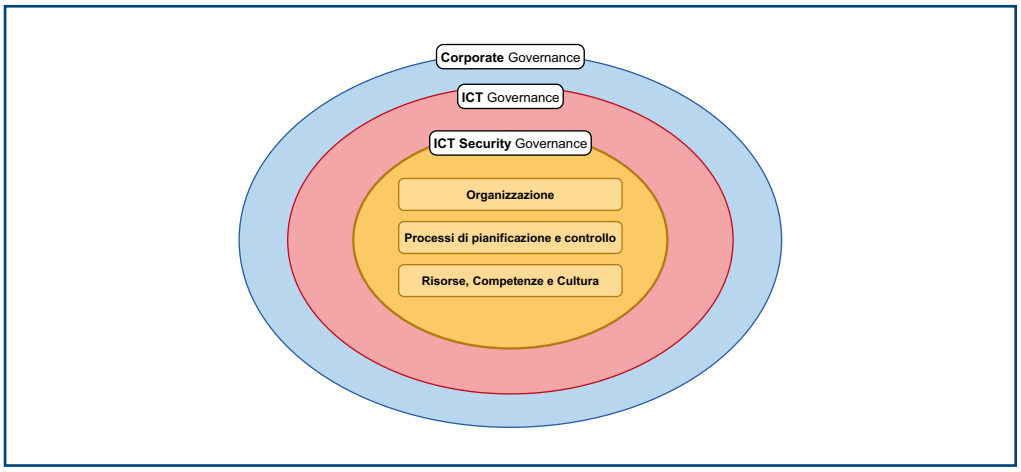


Figura 1.1
L'ICT Security governance

Gli aspetti organizzativi

Gli elementi descrittivi fondamentali che hanno avuto un approfondimento specifico sono i seguenti:

- la presenza di una o più unità organizzative dedicate all'ICT Security, la dimensione in termini di full time equivalent allocati e la posizione all'interno della macrostruttura organizzativa. A questo proposito, va sottolineato che non sempre esiste una struttura dedicata all'ICT Security. In questo caso, è opportuno capire chi è e a chi risponde il responsabile dell'ICT Security in azienda, e a quali unità/sottounità sono demandate le diverse attività;
- nel caso di più unità organizzative, la distribuzione delle responsabilità sulle diverse macro-aree di attività riconducibili all'ICT Security tra le diverse unità. Nella scelta della configurazione è necessario fare attenzione ad alcuni principi fondamentali, primo fra tutti quello noto come "segregation of duties". E' chiaro, tuttavia, che tale scelta può essere influenzata da diversi fattori (dimensione, settore di attività, ecc.);
- la strutturazione "interna" della/e unità organizzative dedicate all'ICT Security.

La Ricerca ha preso in esame anche i percorsi evolutivi di tali configurazioni organizzative (come in tutte le aree, anche in quest'ambito i modelli organizzativi adottati dalle aziende sono spesso soggetti a cambiamenti) e analizzato la presenza di trend, sia in termini di percorsi convergenti verso alcune configurazioni organizzative emergenti, sia in termini di dimensionamento delle unità organizzative.

La pianificazione strategica

Per assicurare l'allineamento tra gli obiettivi strategici di business e quelli dell'ICT Security è fondamentale pensare congiuntamente il processo di pianificazione e controllo dell'ICT Security e quello complessivo dell'impresa.

Gli input che portano alla definizione del piano strategico possono provenire dall'interno o dall'esterno dell'azienda. Tra i principali ricordiamo:

- la compliance alle normative (in particolare, in Italia abbiamo: la legge sulla privacy n. 196/2003; il Dlgs n. 231/2001 sulla responsabilità amministrativa delle persone giuridiche; la legge n. 262 del 2005 sulla tutela del risparmio e la disciplina dei mercati finanziari; legislazione a tutela del copyright in relazione alle licenze dei programmi software fino a qualunque contenuto digitale protetto);
- i risultati degli audit interni, realizzati da ICT, Corporate Security, ICT Security, Internal Audit, ed esterni, realizzati da società di revisione, organismi di controllo, enti di certificazione, ecc.;
- le nuove soluzioni proposte dai player del mercato;
- le sollecitazioni da parte delle Business Unit per l'introduzione di nuove soluzioni di sicurezza;

- lo scouting e la ricerca di soluzioni innovative interne effettuati dall'unità ICT Security.

Proprio per questo motivo le unità organizzative coinvolte nell'identificazione delle iniziative di ICT Security dovrebbero essere numerose. Oltre all'unità di ICT Security, infatti, potrebbero essere chiamate a fornire il loro contributo anche:
- ICT (o gli altri dipartimenti dell'ICT, diversi dall'ICT Security, qualora quest'ultima sia posizionata all'interno della Direzione ICT);
- Corporate Security;
- Internal Audit;
- Organizzazione e Risorse Umane;
- Line of Business;
- Enterprise Risk Management (se esistente);
- Compliance (se esistente);
- Legal.

Per garantire il pieno successo delle iniziative pianificate è opportuno ricorrere ad approcci strutturati di Risk Analysis/Risk Management, come vedremo nel dettaglio nel Capitolo 2.
A valle del piano strategico si definisce il budget corrispondente, distinto tra progetti di investimento e spese correnti. Spesso però la quantificazione delle necessità finanziarie dell'ICT Security non è di facile individuazione, a causa della definizione degli ambiti di responsabilità o delle caratteristiche legate al business o alle scelte gestionali.
Successivamente è fondamentale ricorrere a sistemi di misura delle prestazioni, per garantire l'attuazione della strategia d'impresa. Proprio per questo è interessante analizzare se ci siano all'interno delle imprese sistemi di misurazione delle prestazioni specifici per l'ICT Security, o se siano comunque presenti Key Performance Indicator (KPI) legati all'ICT Security all'interno di sistemi più ampi.
Un altro fattore fondamentale che è stato indagato sono i fattori critici di successo riguardanti i progetti legati all'ICT Security. Tra questi troviamo:
- il commitment del Top Management, che rappresenta un elemento fondamentale, se non decisivo, per il successo delle iniziative;
- il coinvolgimento da parte delle unità interessate nell'identificazione dei bisogni e nella pianificazione della soluzione;
- il coinvolgimento degli utenti fin dalla fase di design della soluzione;
- la scelta del prodotto;
- la scelta del fornitore di servizi.

Il punto di vista dei Chief Information Officer

Per l'edizione 2009, si è deciso di dedicare una prima parte della Ricerca ad approfondire e/o aggiornare alcuni dei risultati emersi dalla Ricerca dell'anno precedente.
I dati raccolti e di seguito illustrati sono rappresentativi del contributo di 105 Chief Information Officer (CIO) dei diversi settori dell'economia e toccano tematiche organizzative, progettuali e di processo.

Gli aspetti organizzativi

La prima domanda rivolta ai CIO riguardava la presenza o meno di un responsabile ICT Security all'interno della Direzione ICT. Dalle risposte emerge che nel 72% delle imprese è presente un responsabile dedicato all'ICT Security e questi è collocato all'interno della Direzione ICT. In particolare, nel 51% dei casi il responsabile riporta direttamente al CIO (a testimonianza dell'importanza strategica attribuita alla sicurezza informatica), mentre nel 21% dei casi si tratta di un secondo riporto. Il 9% dei CIO, invece, dichiara l'esistenza di un responsabile dedicato collocato al di fuori della Direzione ICT.

Ne consegue che nel 19% delle imprese rispondenti tale responsabile non è al momento presente: in particolare, va sottolineato che il 7% delle aziende pensa di introdurre a breve tale figura, mentre nel 12% dei casi questa innovazione organizzativa non è ancora prevista (Figura 1.2).

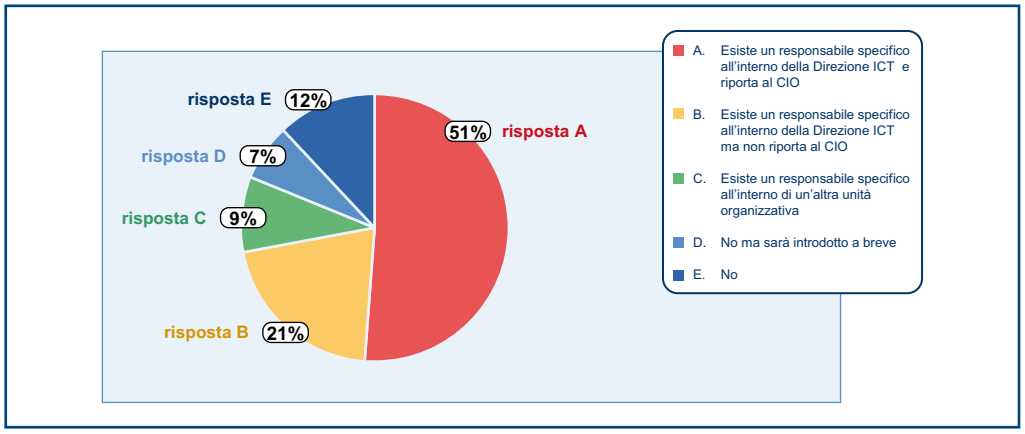


Figura 1.2
La presenza e il posizionamento del responsabile dell'ICT Security all'interno dell'organigramma aziendale

Il dato successivo riguarda il dimensionamento dell'unità di ICT Security, laddove esistente. Dalle risposte si evince che complessivamente nel 61% dei casi vi è una sola persona, perlomeno all'interno dell'ICT, che si occupa di ICT Security (Figura 1.3). Nel 22% le risorse dedicate crescono e si collocano nell'intervallo da 2 a 5. Da sottolineare, all'estremo opposto, che il 14% dei CIO ha dichiarato che la struttura di ICT Security supera le 10 unità. A questo riguardo, vanno fatte due considerazioni:

- esiste una correlazione positiva tra dimensione dell'unità ICT e dimensione dell'impresa. Tuttavia, tale correlazione è vera solamente nei settori ICT e Telecomunicazioni, Banking e Utility, mentre non sembra essere altrettanto evidente in altre industry;
- il dato sul dimensionamento dell'unità ICT Security in alcuni casi è di non facile lettura, in quanto influenzato fortemente dalle politiche di insourcing/outsourcing dell'impresa.

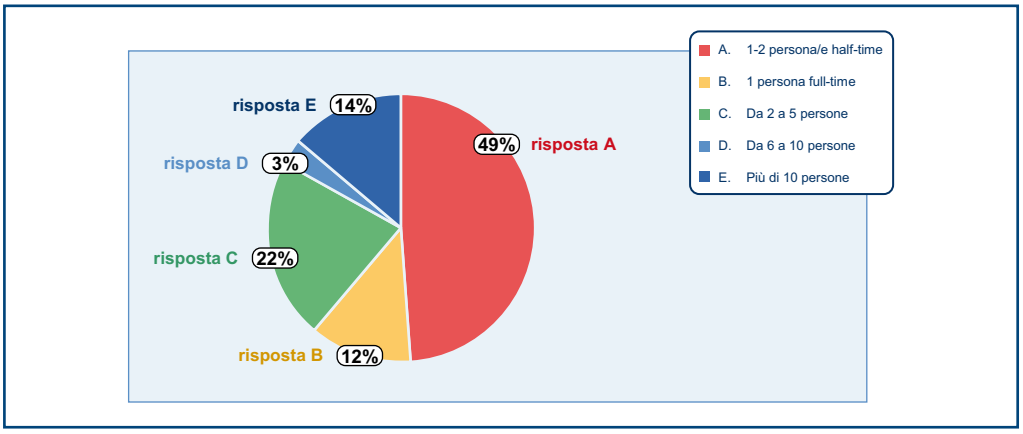
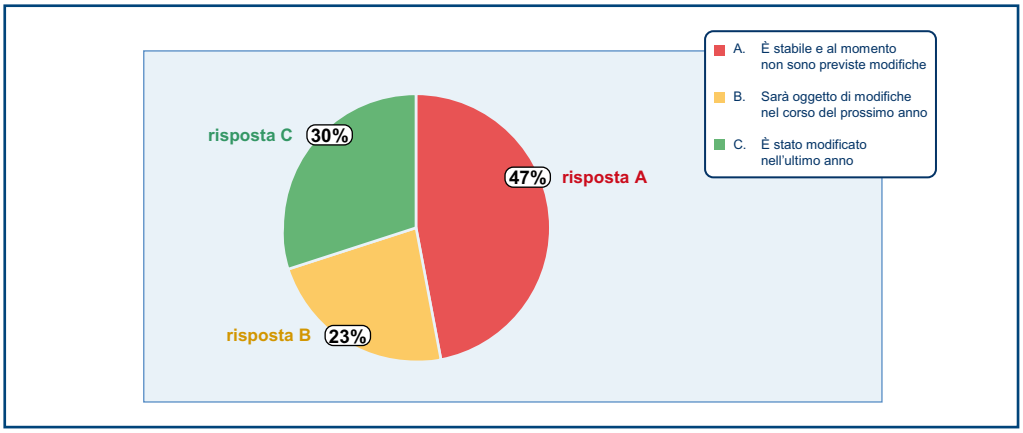


Figura 1.3
Il dimensionamento dell'unità ICT Security

L'ultima domanda relativa a questa sezione era tesa a verificare la stabilità della configurazione organizzativa, coerentemente con l'obiettivo di monitorare il grado di maturità raggiunto, nonché l'esistenza di eventuali trend, come indicato precedentemente. In questo senso, i risultati evidenziano un altro dato importante: oltre la metà dei rispondenti ha dichiarato di aver apportato o di voler apportare nel breve termine cambiamenti all'organizzazione delle attività di ICT Security: in particolare, il 30% dei modelli organizzativi dell'ICT Security delle imprese rispondenti ha subito modifiche nell'ultimo anno e il 23% sarà passibile di cambiamenti nel corso dei prossimi 12 mesi (Figura 1.4).

Figura 1.4
La stabilità del modello organizzativo inerente l'ICT Security



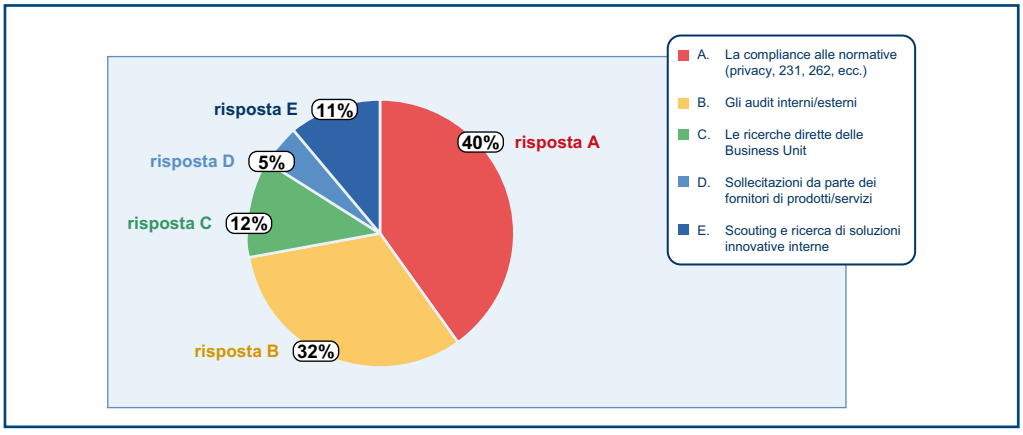
La pianificazione strategica

Nella seconda sezione della Survey rivolta ai CIO ci si è focalizzati sui seguenti aspetti legati alla strutturazione dei processi di pianificazione e controllo delle attività di ICT Security:

- le principali fonti di input per la pianificazione delle attività di ICT Security;
- il grado di coinvolgimento delle altre unità organizzative nella fase di definizione del piano di ICT Security;
- la presenza e il livello di "comprensività" del piano strategico di ICT Security, che dovrebbe includere gli obiettivi, i piani d'azione e i progetti ad essi connessi in un orizzonte temporale pluriennale;
- l'intensità del ricorso ad attività di Risk Analysis per l'individuazione delle priorità d'intervento e quindi per la costruzione del piano strategico;
- il budget allocato all'ICT Security e il relativo trend;
- l'esistenza di sistemi di monitoraggio delle prestazioni di tipo direzionale o strategico, volti a misurare l'efficacia dell'Information Security Management System e a evidenziare eventuali aree di criticità e di miglioramento;
- i fattori critici di successo dei progetti di ICT Security.

Con riferimento al primo punto, dalla Figura 1.5 si evince come la compliance alla normativa (40%) e i risultati degli audit interni o esterni (32%) siano le due maggiori determinanti delle iniziative. Complessivamente, quindi, il 72% degli input deriva dalla necessità di adeguamento a nuove leggi e/o da non conformità a standard, policy e/o normative già vigenti. Non va comunque trascurato il 12% di imprese che dichiarano di ricevere input anche dalle aree di business, a riprova di un crescente coinvolgimento di queste ultime nelle attività legate alla sicurezza ICT. L'11% raggiunto dallo scouting e dalla ricerca di soluzioni innovative da parte degli specialisti di ICT Security interni conferma che l'innovazione tecnologica esercita un ruolo importante, ma probabilmente non fondamentale. Rilevanza ancora minore viene, infine, attribuita ai provider di prodotti e servizi ICT, che i CIO hanno dichiarato incidere solo per il 5%.

Figura 1.5
Gli input per l'individuazione delle iniziative di sicurezza ICT



Si è quindi chiesto quali siano le funzioni/unità organizzative più attive nell'individuazione delle iniziative di ICT Security (Figura 1.6) . Il ruolo principale spetta all'ICT con il 36%, seguita dall'Internal Audit con il 24%, e dalla Corporate Security che si attesta al 18%. Meno influenti sono la Direzione Organizzazione all'8%, le Line of Business al 7% e la Direzione Risorse Umane al 7%.

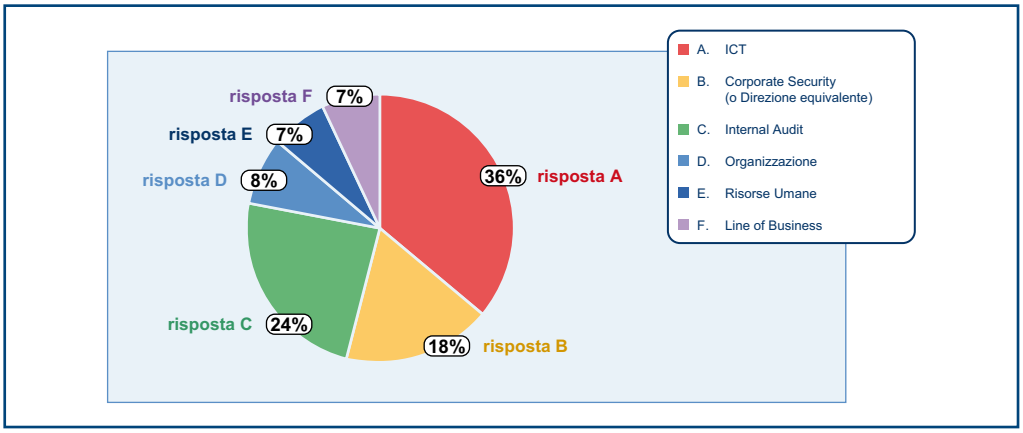


Figura 1.6

Le unità organizzative maggiormente coinvolte nell'individuazione delle iniziative di ICT Security

Incrociando le risposte a questa domanda con quelle ottenute al punto precedente è possibile concludere che, qualsiasi sia la fonte originaria del problema di sicurezza ICT, nell'individuazione delle contromisure il ruolo principale è esercitato dalla Direzione ICT (il che è piuttosto plausibile, visto che alcuni degli audit sono di natura "tecnologica" – si veda per esempio i vulnerability assessment o gli ethical hacking). Tuttavia, emerge il ruolo importante della Corporate Security, spesso in quanto tale unità si occupa proprio degli aspetti di governance della security, e dell'internal Audit, coinvolto massicciamente per gli aspetti legati a compliance a normative – già in essere o nuove – e ai vari standard quali ad esempio ISO17799, ISO27001, SOX, ecc.

Il punto successivo riguardava la formalizzazione del processo di pianificazione strategica delle iniziative in ambito ICT Security. Come si può notare in Figura 1.7, le risposte si sono divise piuttosto equamente: il 36% delle imprese rispondenti prevede un processo formale di pianificazione che copre tutti gli aspetti legati all'ICT Security. Il 34% attiva invece il processo di pianificazione solo in concomitanza all'avvio di grandi progetti o in caso di promulgazione di nuove normative con forte impatto sulla sicurezza ICT; in ultimo, il 30% dei CIO dichiara che non esiste in azienda un Master Plan ICT che riguardi l'ICT Security.

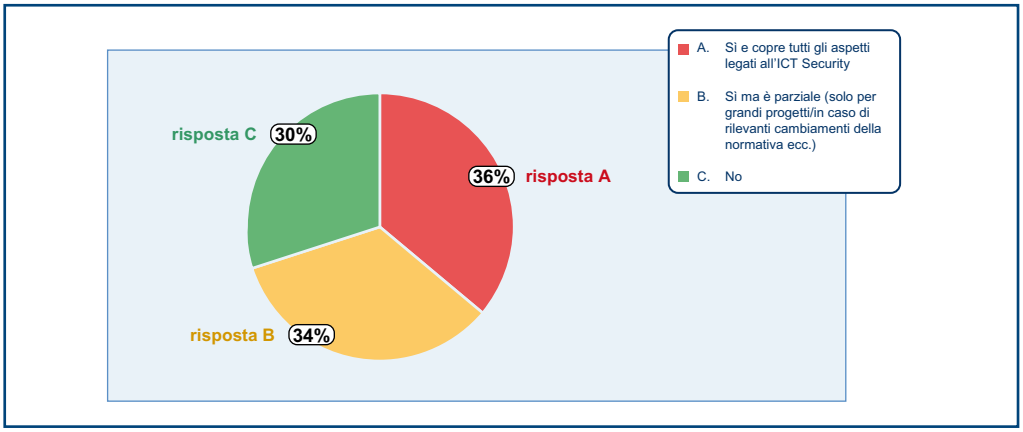


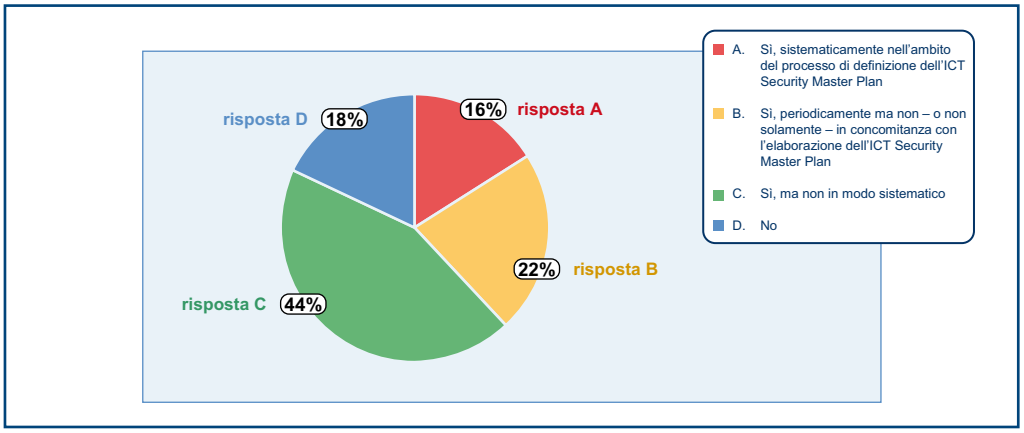
Figura 1.7

Il ricorso a un processo formale di pianificazione strategica delle iniziative in ambito ICT Security (Master Plan ICT/Information Security)

I risultati ottenuti su questo aspetto non sono proprio "esaltanti". L'assenza di un momento di formalizzazione e condivisione di un piano integrato e "omnicomprensivo" rappresenta un elemento di debolezza, che rischia di riflettersi anche sull'entità del budget, oltre che sul corretto dimensionamento delle unità organizzative e, quindi, sulla successiva gestione efficiente delle attività.
In Figura 1.8 sono invece riportate le risposte dei CIO relativamente al ricorso ad approcci di Risk Analysis per l'individuazione delle aree di criticità e, quindi, delle iniziative da includere nel piano strategico di ICT Security. Dai dati emerge che l'82% dei CIO ricorre a metodologie di Risk Analysis; tuttavia, solo il 16% le utilizza sistematicamente (in modo strettamente strumentale all'elaborazione del piano di security o anche nell'ambito di altre analisi periodiche), mentre ben il 66% delle Direzioni ICT si avvicina in modo episodico, o comunque non sistematico.

Figura 1.8

Il ricorso ad approcci strutturati di Risk Analysis/Risk Management per la definizione delle iniziative

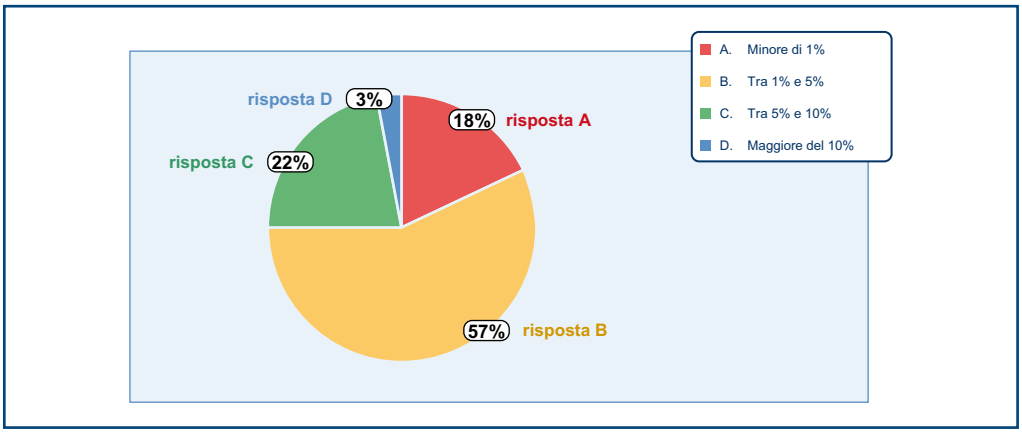


La domanda successiva era volta ad analizzare l'entità del budget dedicato alle attività di ICT Security. Considerato il ruolo ricoperto dai destinatari della Survey, si è deciso di chiedere una quantificazione in termini relativi, in particolare rispetto al totale del budget ICT. E' opportuno però sottolineare che:

- il budget ICT Security gestito dall'ICT non è rappresentativo della spesa complessiva in sicurezza informatica, in quanto alcuni progetti che prevedono importanti attività di sicurezza ICT sono in capo ad altre unità organizzative (Corporate Security, Organizzazione, Risorse Umane tra le principali);
- pur rimanendo all'interno dei confini della Direzione ICT, non è sempre facile individuare tutti i costi riconducibili alla sicurezza ICT, in quanto alcuni sono "annegati" all'interno di altri dipartimenti ICT (si pensi, ad esempio, alla determinazione e alla verifica di sicurezza nello sviluppo applicativo).

Figura 1.9

La percentuale del budget di ICT Security in relazione al budget complessivo ICT



In ogni caso, nella maggioranza dei casi (il 57%) il valore dichiarato dai CIO rispondenti è compreso nel range tra 1% e 5% del budget ICT complessivo (Figura 1.9). Il 22% dei CIO asserisce che il budget ICT Security si assesta in un valore compreso tra il 5% e il 10%, mentre il 3% rivela che la strategicità dell'ICT Security porta l'azienda a stanziare un budget annuale che supera il 10% del budget complessivo ICT. All'estremo opposto, solo il 18% degli intervistati dichiara un budget ICT Security minore dell'1% del budget ICT.
Inoltre, il 48% dei CIO dichiara un trend in crescita dello spending in ICT Security, mentre nei restanti casi non si registrano variazioni rilevanti (Figura 1.10). È importante sottolineare, comunque, che solo il 6% delle imprese rispondenti ha dichiarato un trend in calo, a conferma del fatto che, nonostante l'attuale momento di significativa recessione economica e le conseguenti difficoltà incontrate da molte imprese, l'attenzione sul tema della sicurezza rimane sempre elevato.

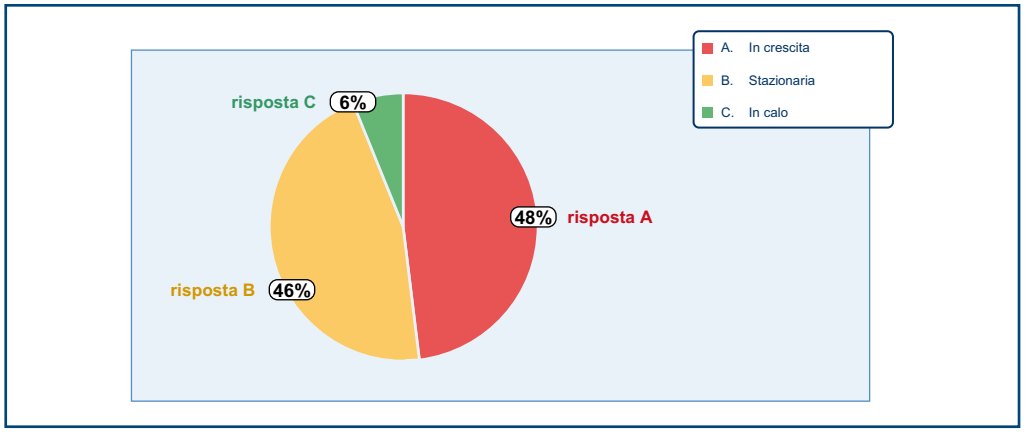


Figura 1.10
I trend del budget di ICT Security

Per quanto riguarda la formalizzazione dei sistemi di misurazione delle prestazioni specifici per l'area ICT Security, i risultati non sono particolarmente entusiasmanti: come riportato in Figura 1.11, infatti, sistemi di misurazione sviluppati ad hoc per l'area ICT Security sono infatti presenti solo nel 25% dei casi, mentre per un altro 22% dei casi alcuni KPI relativi all'ICT Security sono inclusi in sistemi di misurazione a più ampio spettro, quali quelli della Direzione ICT. Ben il 53% delle aziende, invece, non ha al momento implementato sistemi di rilevazione delle performance in quest'ambito.

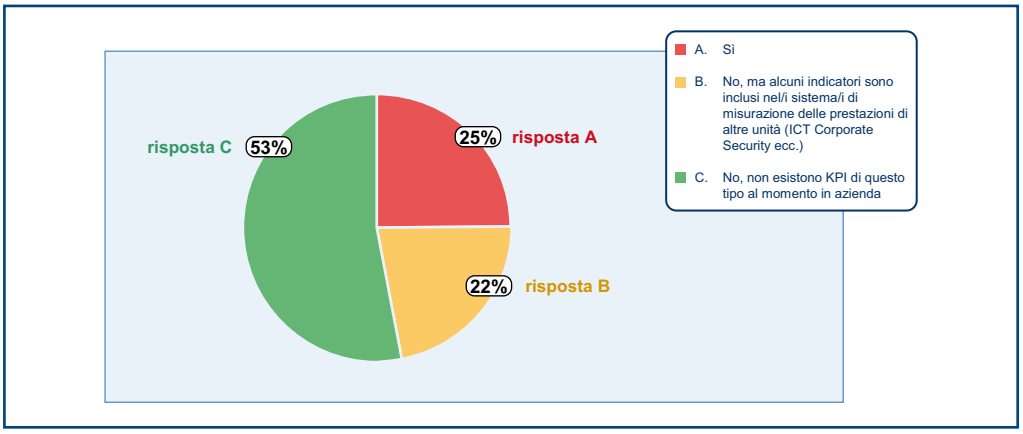
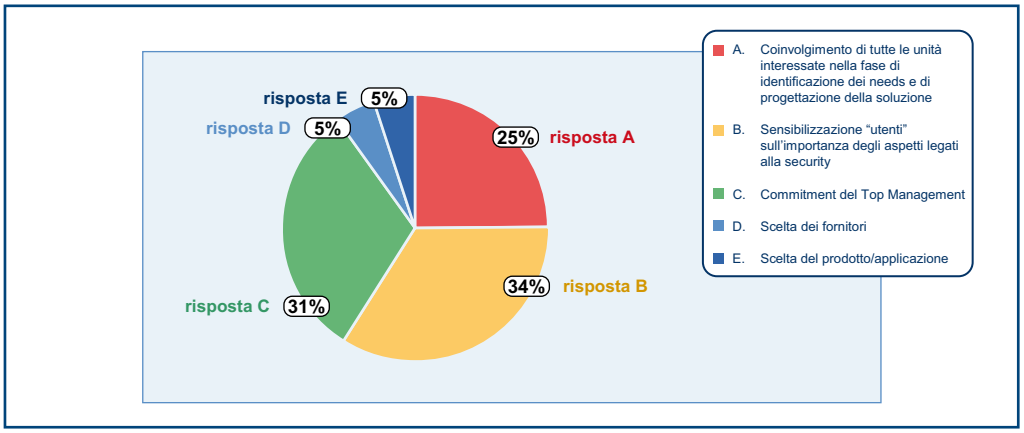


Figura 1.11
La diffusione dei sistemi di misurazione delle prestazioni specifici per l'ICT Security

L'ultimo quesito riguardava i fattori critici di successo (figura 1.12) di progetti legati all'ICT Security. Si nota come la sensibilizzazione degli utenti e il commitment del Top Management raggiungano, insieme, il 65%. Un altro fattore critico di successo considerato dal 25% dei CIO è il coinvolgimento delle unità interessate nell'identificazione dei bisogni e nella pianificazione delle soluzioni, mentre il restante 10% si divide tra la scelta del prodotto e la scelta del fornitore di servizi.

Figura 1.12
I principali fattori critici di successo nella gestione dei progetti di ICT Security



Box 1.1

Credem

Il Gruppo Credem, presente in 19 regioni italiane, opera sul territorio nazionale, sia sul mercato retail sia su quello corporate con particolare attenzione alle piccole e medie imprese. Conta circa 6.000 dipendenti, 630 unità tra filiali e centri imprese, 58 negozi finanziari e una rete di oltre 1.000 promotori finanziari. Il gruppo è presente inoltre in Svizzera e Lussemburgo con filiali specializzate nel private Banking ed è composto da società specializzate nei settori del Banking, dell'investment Banking, dell'asset management e della bancassurance.
La Direzione ICT riporta a un Centro Servizi Corporate, che include Sistemi Informativi, back office e logistica; questa struttura dipende direttamente dalla Direzione Generale. Al suo interno la Direzione ICT era storicamente articolata in tre funzioni: "Sviluppo applicativo", "Servizio Presidio, Governo outsourcing e Help desk clienti interni" e "Pianificazione, Controllo e Sicurezza". Nel corso del 2008 sono stati creati all'interno della prima unità due uffici: il Demand Management, che funziona da interfaccia tra le funzioni business e il Sistema Informativo (discute delle priorità, dei progetti da portare avanti, dei piani trimestrali) e l'ufficio "Architetture Applicative", che sovrintende l'evoluzione e l'innovazione dell'architettura applicativa. Dalla funzione "Pianificazione Controllo e Sicurezza", parzialmente inglobata nell'unità di "presidio e governo outsourcing", è stata creata la funzione Sicurezza Logica che si occupa del governo della sicurezza ICT.
Al momento l'analisi del rischio di sicurezza ICT viene ancora condotta utilizzando un processo basato sull'esperienza personale dell'analista. E' stata pertanto sviluppata un'iniziativa che ha portato alla formalizzazione di un completo sistema di information security management, in fase di progressiva introduzione.
La relazione tra ICT Risk Management e Enterprise Risk Management non prevede, ancora, momenti di collaborazione definiti.

Box 1.2

Intesa Sanpaolo

Intesa San Paolo è il gruppo bancario nato, il 2 gennaio 2007, dalla fusione di Banca Intesa e San Paolo IMI. Leader in Italia grazie ad una rete distributiva molto capillare, ha una forte presenza internazionale. Grazie alla sua rete con 8.119 filiali, Intesa San Paolo offre i propri servizi a circa 19,6 milioni di clienti nel mondo.
All'interno della Direzione Organizzazione e Sicurezza è stato costituito l'Ufficio Progettazione e Standard di Sicurezza Informatica con lo scopo, tra gli altri, di presidiare i livelli di rischio IT e di svolgere le necessarie attività di Risk Analysis.
L'analisi del rischio è lo strumento principale mediante cui si intende garantire l'adeguatezza delle misure di sicurezza, obiettivo che risulta tra gli indirizzi di cui il Gruppo Intesa Sanpaolo si è dotato per governare il proprio operare. Secondo tale principio, il patrimonio fisico e informativo deve esser protetto mediante la predisposizione e il mantenimento di adeguate contromisure e i sistemi, le reti e gli apparati mediante i quali è gestito il patrimonio fisico e informativo devono essere tutelati al fine di preservare la riservatezza, l'integrità e la disponibilità delle informazioni.

In questo, l'Ufficio Progettazione e Standard di Sicurezza Informatica opera per coordinare ed aggiornare la valutazione dei rischi IT, valutandone il grado di esposizione e la corretta gestione delle tecnologie di sicurezza, tramite l'integrazione dei monitoraggi forniti dagli Enti realizzatori, nonché identificando con gli stessi le contromisure più opportune. Parimenti, nell'ambito delle iniziative progettuali, assicura la definizione dei requisiti di sicurezza informatica, verificando la rispondenza ai requisiti delle contromisure e/o specifiche identificate dall'ente realizzatore, accertando la coerenza dei relativi sviluppi sia con i requisiti sia con le linee guida e gli standard di sicurezza informatica di Gruppo.

2. L'ICT Risk Analysis: approcci e metodologie

Alla luce dei risultati emersi nel Capitolo 1, con riferimento in particolare all'importanza che l'ICT Risk Analysis riveste all'interno del processo di pianificazione delle iniziative, si è deciso di approfondire il tema, esaminando le metodologie e gli approcci maggiormente utilizzati per l'analisi dei rischi ICT.

Oggi, infatti, si parla spesso di Risk Analysis in azienda, ma dietro questo termine si celano significati e interpretazioni differenti e si corre il rischio di identificare con difficoltà quale sia l'insieme degli obiettivi che spinge ad attivare il processo di analisi e soprattutto quali siano le metodologie più adatte e le sorgenti di informazioni più appropriate per ciascuna tipologia di analisi.

Grazie al contributo di Chief Information Officer, Chief Information Security Officer (CISO) e Risk Manager che hanno partecipato alla Ricerca si è quindi cercato di fare un po' di chiarezza sul tema. A tale scopo, è stato innanzitutto elaborato un framework di riferimento per la classificazione dei diversi approcci alla Risk Analysis in ambito ICT. Si è poi proceduto a verificare il grado di adozione delle diverse "configurazioni" all'interno delle organizzazioni, anche con riferimento agli specifici ambiti di applicazione.

L'analisi si è focalizzata in un primo momento sul settore del Banking, storicamente il più sensibile al tema della sicurezza e successivamente è stata estesa ad altri settori di interesse, quali: Assicurativo, Automotive, Chimico e Farmaceutico, ICT e Telecomunicazioni, Utility. Nei successivi paragrafi verranno inizialmente illustrati gli elementi del framework di riferimento, per poi procedere all'esposizione dei risultati dell'indagine nel settore Banking, che verranno infine confrontati con le evidenze empiriche raccolte negli altri settori analizzati.

Un framework di riferimento per la categorizzazione delle attività di ICT Risk Analysis

La Ricerca ha fatto emergere che le metodologie utilizzate per l'ICT Risk Analysis sono numerose e di difficile categorizzazione. Ciò che è stato da subito evidente è la complessità di ricondurre le metodologie utilizzate a modelli di riferimento noti. Per tale motivo, di seguito sarà proposto un framework che è stato elaborato per supportare la classificazione delle diverse tipologie di analisi e metodologie utilizzate. Tale framework vuole anche essere di supporto ai decisori (CISO in primis), in quanto permette di dotarsi di uno strumento di classificazione delle iniziative intraprese.

Dalle interviste con gli ICT Manager emergono, in particolare, tre macro categorie di analisi ricorrenti, che saranno descritte a seguire.

- *Progettazione nuove iniziative:* l'analisi nell'ambito di una nuova iniziativa viene svolta tipicamente nelle fasi preliminari, come ad esempio la progettazione. Lo scopo è quello di identificare i punti di attenzione per un singolo dominio applicativo e verificare che il livello di rischio permetta la messa in esercizio dell'applicazione.

- *Disaster recovery*: l'analisi nell'ambito Disaster recovery viene solitamente effettuata per stabilire quali siano, in base ai rischi identificati e alla loro rilevanza, le iniziative da intraprendere per tutelarsi da un'eventuale indisponibilità dei sistemi.
- *Adempimenti normativi*: alcune normative prevedono esplicitamente lo svolgimento di un'ICT Risk Analysis. Ad esempio, la legge sulla privacy prevede tale attività e stabilisce che i risultati debbano essere riportati nel Documento Programmatico sulla Sicurezza, al fine di evidenziare quali contromisure siano idonee per il particolare contesto.

All'interno delle diverse macro categorie sopra elencate si possono tuttavia riscontrare numerose differenze di approccio. Per ovviare alla molteplicità di metodologie, il framework prenderà in considerazione sia alcuni fattori che caratterizzano l'orizzonte di una specifica ICT Risk Analysis, sia le variabili di configurazione che definiscono la specifica metodologia utilizzata.

In particolare, dalle interviste effettuate, i principali fattori caratterizzanti l'orizzonte di un'ICT Risk Analysis sono risultati i seguenti:
- Finalità
- Ambito
- Requisiti

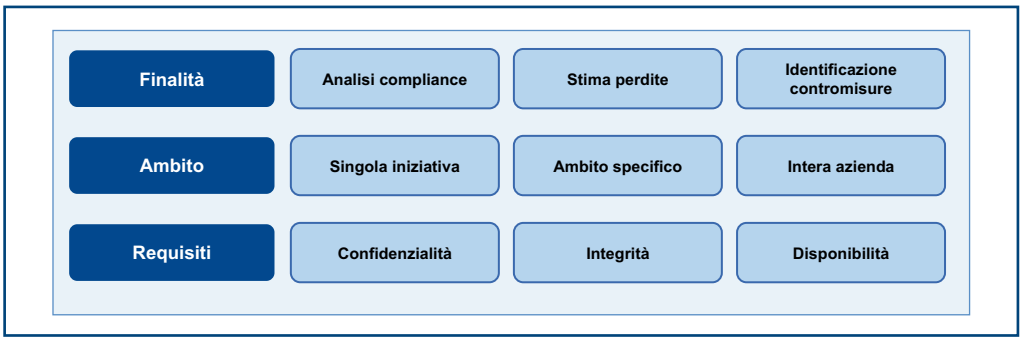
Di seguito sono invece elencate le variabili di configurazione della metodologia:
- Input types
- Flusso logico
- Attori
- Input sources
- Strumenti

Nel corso dei due paragrafi successivi saranno analizzate nel dettaglio queste due classi di variabili, che verranno poi utilizzate per la costruzione del framework di riferimento dell'ICT Risk Analysis.

I fattori caratterizzanti l'orizzonte dell'ICT Risk Analysis

Un primo insieme di variabili serve per "contestualizzare" la specifica attività di Risk Analysis, e deve essere definita puntualmente, in quanto la scelta caratterizzante la metodologia di analisi dipende da tali fattori, che saranno approfonditi di seguito (Figura 2.1).

Figura 2.1
Il framework di riferimento – I fattori caratterizzanti l'orizzonte di analisi



Le finalità

Un primo elemento fondamentale, che si riscontra nell'ambito dell'ICT Risk Analysis, è il fatto che solitamente all'interno dello stesso modo di chiamare questo processo si fa riferimento ad attività che hanno scopi diversi. Di seguito sono descritte nel dettaglio le finalità per cui una ICT Risk Analysis può essere compiuta.

- *Analisi compliance:* una prima finalità che può guidare un'ICT Risk Analysis consiste nell'identificazione di eventuali difformità rispetto a uno standard di riferimento che, a seconda dei casi, può essere una normativa nazionale o internazionale, oppure un regolamento interno all'azienda.
- *Stima perdite:* un'altra delle finalità che può guidare un'attività di ICT Risk Analysis è la valutazione del grado di esposizione dell'azienda, espresso come stima di possibili perdite conseguenti all'eventuale accadimento di determinati eventi. La conoscenza di tale stima rappresenta un valore per il management, in quanto permette di valutare se l'attuale posizionamento dell'azienda sia accettabile o se sia necessario prevedere ulteriori interventi. Tali stime possono essere di tipo quantitativo, inteso come riferito a indicatori di carattere economico, o di tipo qualitativo, cioè riconducibili a una scala che permette unicamente un posizionamento relativo dei rischi (ad esempio alto-medio-basso).
- *Identificazione contromisure:* un'ulteriore finalità che può motivare un'attività di ICT Risk Analysis è l'individuazione delle contromisure necessarie al raggiungimento di un livello di rischio definito a priori dall'organizzazione e ritenuto accettabile. Tale livello tipicamente è stabilito sulla base di common practice. Un'ICT Risk Analysis con questa finalità spesso presenta notevoli somiglianze con una gap analysis volta a identificare gli interventi necessari per l'allineamento con i riferimenti individuati.

L'ambito

Un altro importante fattore riguarda lo spettro di copertura delle ICT Risk Analysis. L'orizzonte di focalizzazione può variare dalla *Singola iniziativa*, a un *Ambito specifico* (una Country, un processo, ecc.), fino a riguardare l'*Intera azienda*. La scelta dell'ambito può essere influenzata non solo dalle finalità dell'attività, ma anche dal grado di complessità che si intende gestire. Riduzioni di ambito possono avvenire anche sulla base di prime valutazioni di rischio non strutturate e formalizzate.

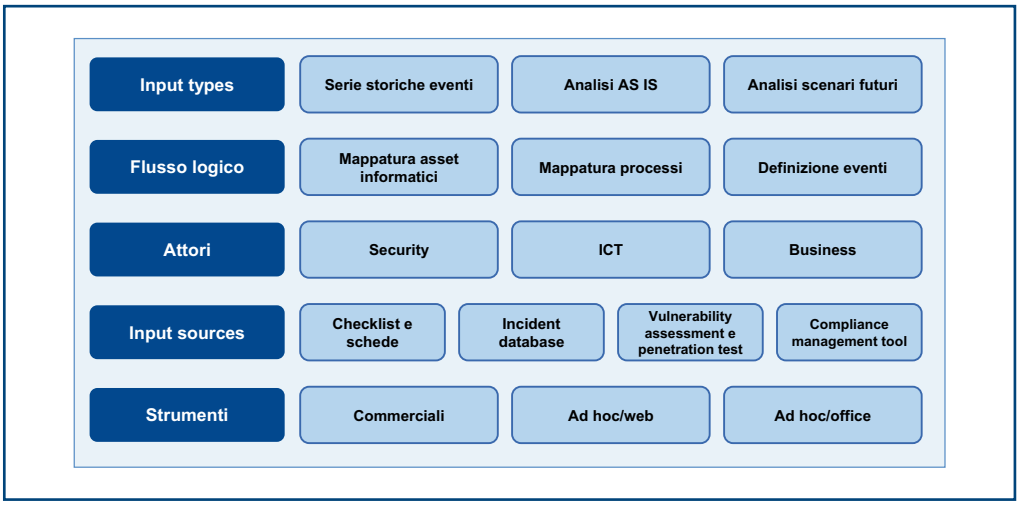
I requisiti

La terza importante spinta da considerare per classificare l'analisi è costituita dai requisiti considerati. I tre requisiti fondamentali, definiti anche dalla letteratura, sono *Confidenzialità*, *Integrità* e *Disponibilità* dei dati. Quando si analizzano i rischi connessi ai sistemi informativi non è sempre detto che occorra tener presente e basarsi su tutti i requisiti elencati. Ad esempio è possibile condurre un'analisi dei rischi unicamente orientata alla disponibilità, che tenga in considerazione solo eventi che possano portare all'indisponibilità del dato, trascurando invece altre tipologie di rischi quali la diffusione non autorizzata di informazioni. Tale focalizzazione su un sottoinsieme di requisiti di sicurezza può essere giustificata da particolari finalità di analisi o dalla necessità di ridurre la complessità delle attività.

Le variabili di configurazione dell'ICT Risk Analysis

Le diverse dimensioni rilevate nell'esame dei fattori caratterizzanti l'orizzonte d'analisi danno evidenza delle numerose declinazioni in cui può prendere forma un'ICT Risk Analysis. È inoltre possibile identificare molteplici elementi che caratterizzano la specifica metodologia utilizzata (Figura 2.2.), che verranno di seguito analizzati.

Figura 2.2
Il framework di riferimento – Le variabili di configurazione dell'analisi



Gli input types

Una prima classificazione della metodologia è volta a definire l'origine dei dati analizzati al fine di costruire gli indicatori utili per l'analisi. Quando si attiva un processo di ICT Risk Analysis, le tipologie di informazioni considerate possono essere di diversa natura.

- *Serie storiche:* la frequenza di accadimento delle diverse classificazioni di eventi passati può essere una base per la determinazione del livello di rischio previsto per il futuro. Tale approccio è tipicamente usato per fenomeni stabili nel tempo e caratterizzati da un'elevata frequenza.
- *Analisi AS IS:* in questo caso vengono analizzati rischi legati ad asset e a processi. La numerosità e la gravità di minacce e vulnerabilità identificate costituiscono un indicatore fondamentale per l'analisi del rischio.
- *Analisi scenari futuri:* quest'analisi tenta di prevedere quali potrebbero essere gli scenari di rischio prossimi futuri, legati in particolare all'emergere di nuove minacce, che potrebbero mettere in luce vulnerabilità attualmente non note o non rilevanti. La gravità delle conseguenze associate all'accadere di tali scenari rappresenta un indicatore che guida l'analisi.

Il flusso logico

Un altro importante fattore che caratterizza le diverse metodologie è il punto di partenza dell'analisi, da cui derivano diversi flussi logici conseguenti.

- *Mappatura asset informatici:* queste analisi hanno inizio da una mappatura degli asset informatici a cui segue l'individuazione delle eventuali vulnerabilità presenti. A ogni asset identificato e per ciascun processo supportato si procede con l'analisi del livello di criticità associato.
- *Mappatura processi:* queste analisi partono da una mappatura dei principali processi svolti in azienda. Per ciascun processo identificato si procede quindi con l'identificazione degli asset informatici sui cui tali processi "insistono".
- *Definizione eventi:* queste analisi partono dalla definizione degli eventi che si intende prendere in considerazione nel perimetro di gestione del rischio. La scelta di tali eventi può essere guidata da normative o da scelte effettuate a priori dell'azienda. Una volta definiti gli eventi considerati oggetto d'analisi, per ciascuno di essi si procede col verificare su quale asset o processo abbia impatto. Gli eventi tipicamente si classificano attraverso la probabilità di accadimento e l'impatto che ne conseguirebbe nel caso si verificassero.

Gli attori

La decisione di quali interlocutori interpellare all'interno dell'azienda ha un impatto sui risultati dell'analisi. Si possono considerare figure che appartengono a diversi ambiti di responsabilità e a diverse aree funzionali. Gli attori più frequentemente coinvolti ap-

partengono alle seguenti aree: *Security* (CISO, Security manager, ecc.), *ICT* (CIO, ICT Executives, ecc.) e *Business and functional manager.*

Gli input sources

Dopo aver definito l'origine dei dati di input, è necessario individuare le sorgenti da cui ricavare gli input stessi. La natura della fonte può incidere sull'output della metodologia.

- *Checklist e schede:* una prima fonte di input consiste nella raccolta e compilazione di checklist o schede informative, che vengono redatte direttamente dai soggetti coinvolti o compilate tramite interviste. I destinatari dell'intervista possono essere il responsabile di un singolo ambito organizzativo, un progettista o gli utenti dell'applicazione in esame.
- *Incident database:* esistono delle basi dati che contengono tutti gli eventi accaduti e riportano, per ciascun evento, la categoria e talvolta l'impatto. Ad esempio, in ambito bancario esistono database anonimi, a cui gli iscritti attingono e su cui mettono a disposizione informazioni relative agli eventi dannosi di cui sono stati oggetto. Questo strumento è una modalità di condivisione e trasferimento della conoscenza in ottica di benchmarking non competitivo.
- *Vulnerability assessment e penetration test:* questa tipologia di sorgente è sfruttabile qualora nelle aziende vengano periodicamente svolte attività finalizzate a identificare le vulnerabilità di sistemi o applicazioni. L'output è tipicamente un report in cui sono evidenziati i rischi a cui ogni asset è soggetto.
- *Compliance management tool:* si possono utilizzare strumenti di monitoraggio che rilevano se un determinato asset o comportamento è difforme da quanto stabilito come regola all'interno dell'impresa. Tipicamente, questi strumenti rilevano la mancata attuazione di una contromisura prevista. Dalle analisi condotte è emersa la crescente diffusione di questo tipo di soluzioni.

Gli strumenti

A supporto del processo di analisi dei rischi, data la sua complessità, vengono normalmente utilizzati degli strumenti informatici. Tali strumenti possono essere ricondotti alle seguenti tre categorie descritte in seguito.

- Commerciali: sul mercato sono presenti soluzioni appositamente sviluppate per supportare l'analisi dei rischi. Tali soluzioni sono tipicamente molto strutturate e guidano il processo di analisi.
- Ad hoc/web: sono strumenti evoluti, sviluppati appositamente per il particolare contesto dell'azienda e implementano una propria metodologia. Sono utilizzati per la gestione di alcune attività connesse all'analisi, partendo dalla raccolta delle informazioni online, fino ad arrivare, in taluni casi, alla condivisione dei risultati.
- Ad hoc/office: sono strumenti sviluppati tipicamente all'interno dell'organizzazione e si basano su semplici fogli Excel o database Access o equivalenti. Spesso permettono la memorizzazione e l'elaborazione delle informazioni. Tali strumenti sono tipicamente più flessibili rispetto alle tipologie precedentemente indicate.

Le principali evidenze del settore Banking

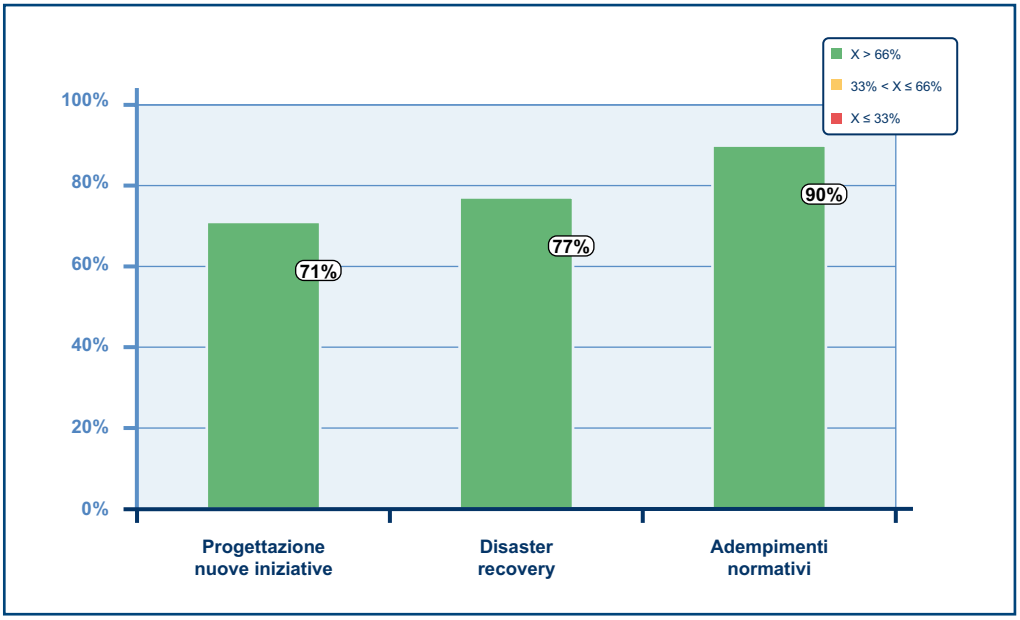
Per approfondire l'analisi delle relazioni tra fattori caratterizzanti e variabili di configurazione delle metodologie e appurare l'esistenza di alcune configurazioni "emergenti" (date dalla combinazione delle variabili di progettazione) si è proceduto a un'indagine empirica, che si è inizialmente focalizzata sul settore Banking. Storicamente, infatti, questo settore è tra i più sensibili alle tematiche di sicurezza, sia per via della particolarità dei servizi forniti, sia per via della normativa particolarmente "corposa" su questo tema. L'analisi si è basata su interviste dirette ai Chief Information Security Officer, Risk e Operational Risk Manager delle Banche, cui ha fatto seguito una Survey erogata a Chief Information Officer e Chief Information Security Officer.

Per chiarezza di rappresentazione sono stati utilizzati i colori rosso, giallo e verde per rappresentare le diverse fasce di adozione. In particolare si è usata la seguente convenzione:

- *Rosso:* laddove l'indicazione di adozione abbia riguardato meno di un terzo degli intervistati (≤ 33%).
- *Giallo:* nel caso in cui la scelta sia stata espressa da un numero di intervistati compreso tra un terzo e due terzi (> 33% e ≤ 66%).
- *Verde:* qualora la scelta sia stata indicata da più di due terzi degli intervistati (> 66%).

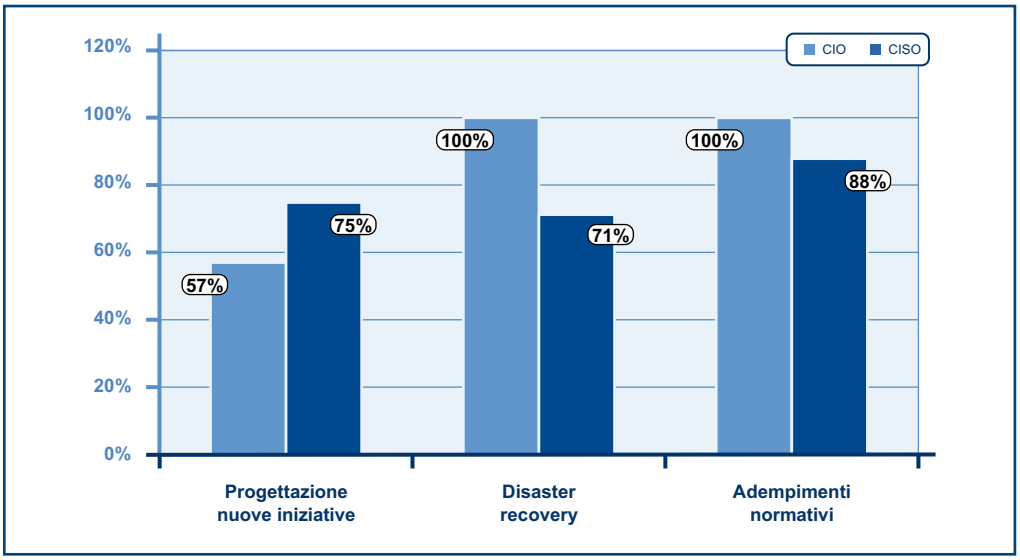
Per quanto riguarda le macro categorie di analisi condotte all'interno del mondo del Banking, quello che emerge dai risultati (Figura 2.3) è una copertura pressoché totale delle tre macro categorie di analisi individuate, tutte realizzate da almeno il 71% dei rispondenti, con un picco del 90% per la categoria "Adempimenti normativi".

Figura 2.3
Le tipologie di ICT Risk Analysis nel Banking



Scendendo nel dettaglio, separando e confrontando le risposte di CIO e CISO (Figura 2.4), emerge una differenza sostanziale. In particolare si può notare come tutti i CIO abbiano affermato di fare analisi del rischio ICT sia per "Disaster recovery" sia per "Adempimenti normativi", fatto non confermato dai CISO. È possibile ipotizzare che talune Risk Analysis in questi due ambiti siano di visibilità esclusiva dell'ambito ICT. Le risposte dei CISO mostrano un sostanziale equilibrio tra le tre macro categorie di ICT Risk Analysis.

Figura 2.4
Le tipologie di ICT Risk Analysis nel Banking: il confronto CIO/CISO



I fattori caratterizzanti l'orizzonte dell'ICT Risk Analysis nel Banking

I risultati della Survey e le interviste svolte hanno permesso di mappare e quantificare le finalità, l'ambito specifico di applicazione e l'importanza dei diversi requisiti di sicurezza per le tre fondamentali macro categorie di Risk Analysis.

Le finalità

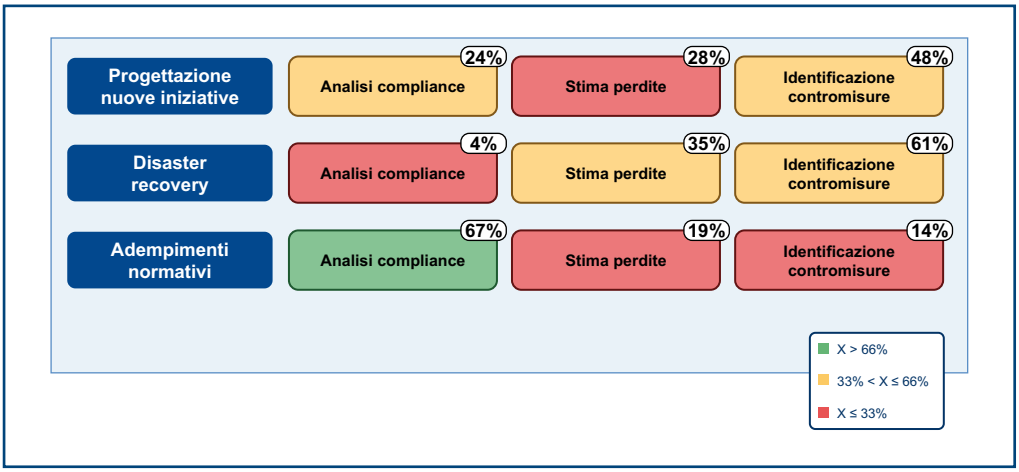


Figura 2.5
Le finalità prevalenti per le ICT Risk Analysis nel Banking

Per quanto riguarda la finalità (Figura 2.5), per "Progettazione nuove iniziative" e per "Disaster recovery" la più frequentemente indicata consiste nell'Identificazione delle contromisure. Nel caso di Risk Analysis finalizzate agli "Adempimenti normativi", invece, in ben il 67% dei casi il fine consiste nella Verifica della compliance. Questo può essere connesso al fatto che numerose normative fissano dei riferimenti per le contromisure da adottare. La finalità meno considerata, infine, risulta essere la Stima delle perdite, probabilmente a causa della complessità a essa associata. Tale motivazione può anche giustificare il fatto che, nel caso in cui si menzioni la Stima delle perdite, ci si riferisca prevalentemente a una stima di tipo quantitativo e non qualitativo, come si può vedere nel dettaglio in Figura 2.6.

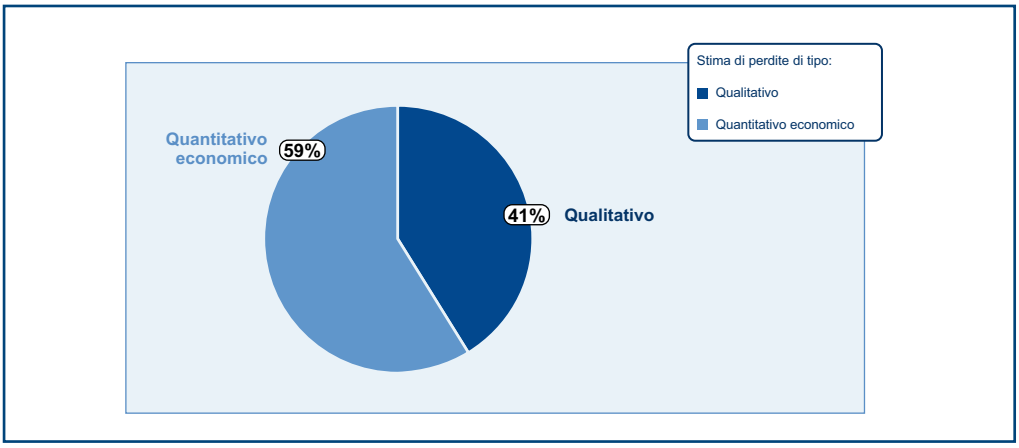
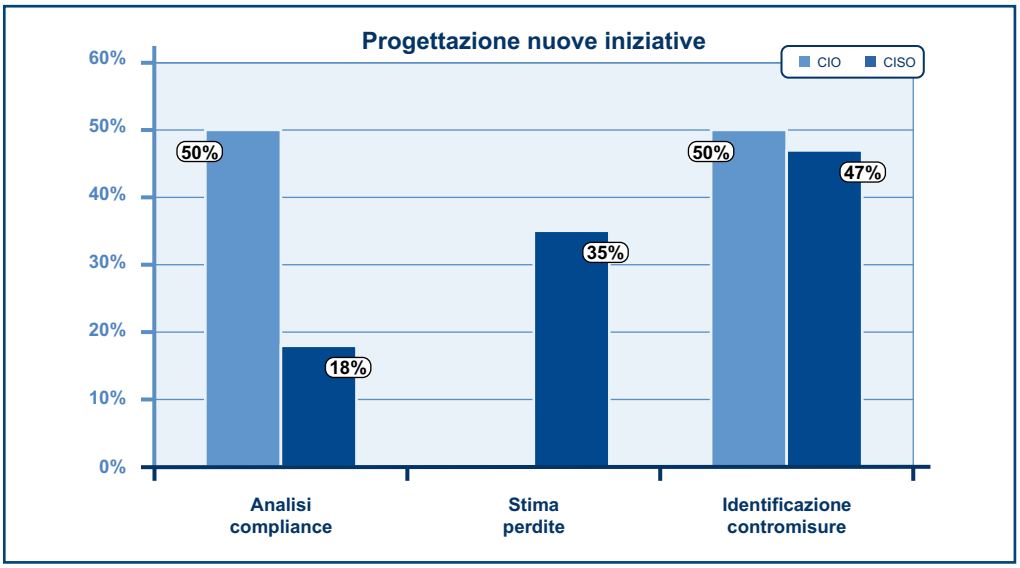


Figura 2.6
Le finalità: il dettaglio della stima delle perdite

Per quanto riguarda, in particolare, le finalità per la macro categoria "Progettazione nuove iniziative" (Figura 2.7), CIO e CISO sembrano avere idee piuttosto diverse: i CIO si dividono tra Analisi della compliance e Identificazione di contromisure, entrambe al 50%, mentre le Stime delle perdita qualitative/quantitative non vengono citate da nessun CIO. I CISO privilegiano invece l'Identificazione delle contromisure (47%), ma citano come seconda finalità la Stima delle perdite (35%).

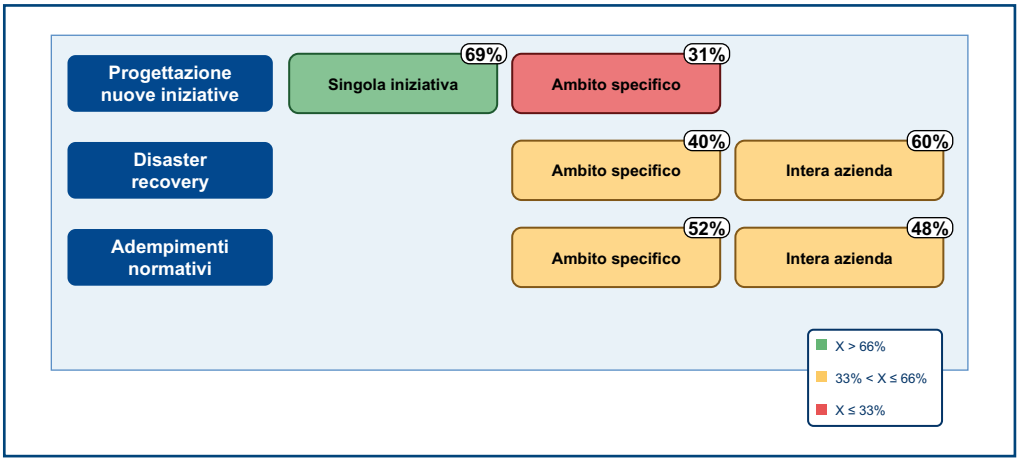
L'ambito

Figura 2.7
Le finalità prevalenti per le ICT Risk Analysis nel Banking – Il confronto CIO/CISO



Come riportato in Figura 2.8, per la "Progettazione Nuove Iniziative" l'ambito specifico di riferimento dell'analisi risulta essere in oltre due terzi dei casi la Singola iniziativa (come peraltro facilmente prevedibile). Per quanto riguarda l'analisi di "Disaster recovery" e di "Adempimenti normativi", la situazione risulta essere più equilibrata, sebbene per il "Disaster recovery" vi sia una certa prevalenza dell'estensione dell'analisi all'Intera azienda, mentre per "Adempimenti normativi" vi è una prevalenza per l'Ambito specifico.

Figura 2.8
L'ambito di copertura delle ICT Risk Analysis nel Banking



I requisiti

In Figura 2.9 è illustrata l'importanza relativa dei diversi requisiti di sicurezza per le diverse tipologie di ICT Risk Analysis. Come si può notare, Confidenzialità, Integrità e Disponibilità si posizionano sostanzialmente allo stesso livello. Emerge una leggera predominanza dell'attenzione dedicata a Confidenzialità e Integrità nella tipologia "Adempimenti normativi". Per "Disaster recovery", invece, la Confidenzialità è il requisito di minore importanza.

In conclusione, è possibile riassumere i dati raccolti per i diversi fattori caratterizzanti l'analisi per le diverse macro categorie di ICT Risk Analysis e costruire così il quadro sinottico riportato in Figura 2.10, che fornisce una panoramica dei fattori caratterizzanti l'orizzonte delle ICT Risk Analysis nel settore Banking.

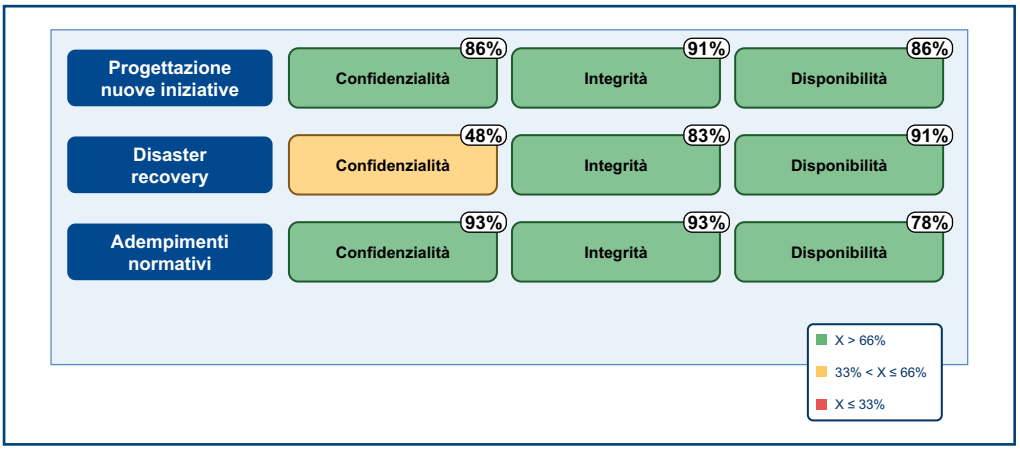


Figura 2.9
I requisiti di sicurezza considerati nelle ICT Risk Analysis nel Banking

La figura 2.10 evidenzia in modo immediato come ciascuna macro tipologia di Risk Analysis in ambito ICT presenta delle peculiarità evidenti, a riprova della eterogeneità degli approcci e della complessità del tema.

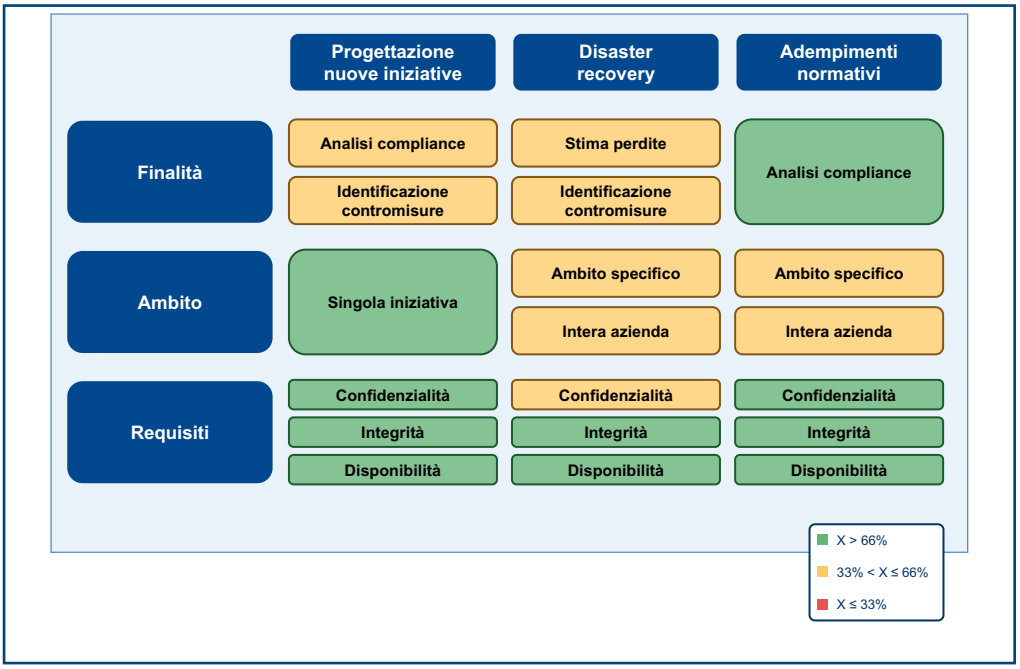


Figura 2.10
Il quadro sinottico dei fattori caratterizzanti l'orizzonte delle ICT Risk Analysis nel Banking

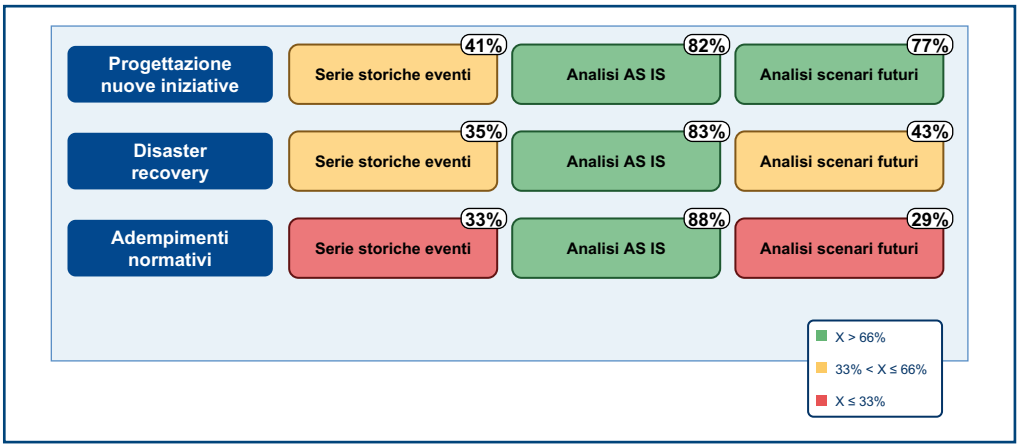
Le variabili di configurazione dell'ICT Risk Analysis nel Banking

Anche le variabili atte a definire la metodologia di analisi sono state oggetto di un'indagine empirica nel settore bancario, i cui risultati verranno qui di seguito illustrati.

Gli input types

Analizzando le tipologie di input che vengono impiegate per realizzare le ICT Risk Analysis (Figura 2.11), si nota come l'Analisi AS IS sia la più utilizzata, essendo stata segnalata da più dell'80% del campione per tutte le tre macro categorie di analisi. Le Serie storiche, invece, risultano essere di gran lunga la scelta meno ricorrente. Probabilmente una delle motivazioni alla base di questa risposta sta nella mancanza di dati, spesso derivante dalla difficoltà di tenere traccia di ciò che avviene in appositi database. L'Analisi degli scenari futuri, invece, assume una certa rilevanza solo per la macro categoria "Progettazione nuove iniziative", per la quale si può ipotizzare che tale tipo di analisi sia meno complessa, anche grazie alla limitatezza dell'ambito.

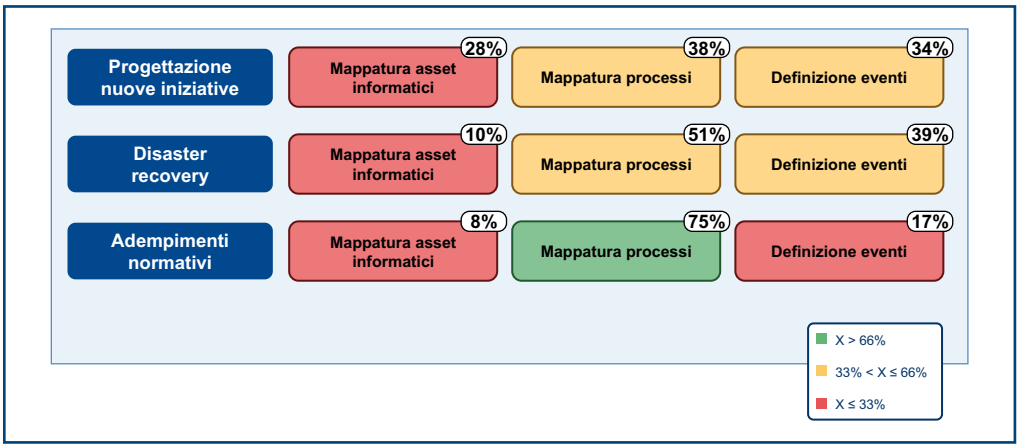
Figura 2.11
La tipologia di input su cui sono basate le ICT Risk Analysis nel Banking



Il flusso logico

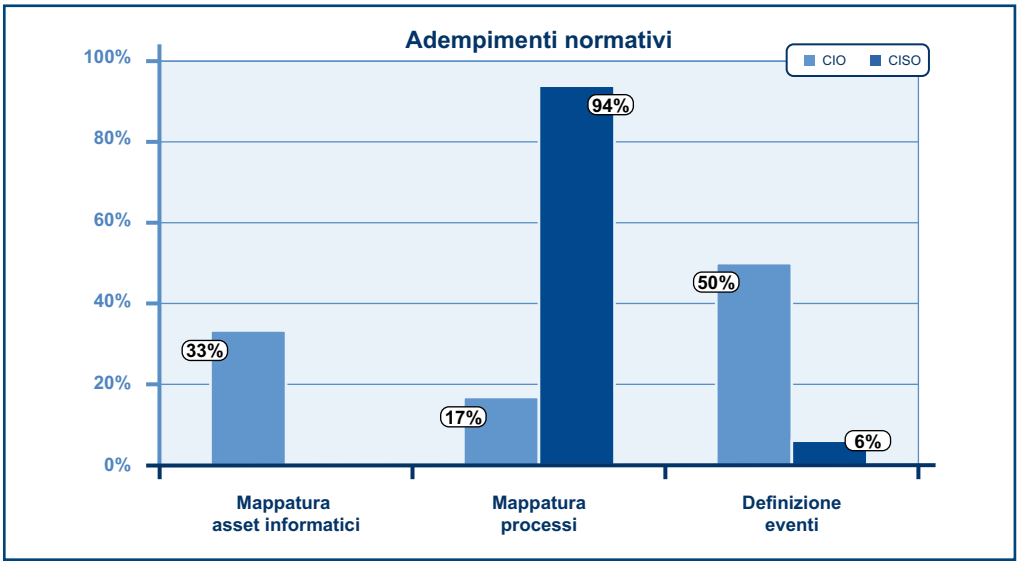
La logica che tipicamente caratterizza le ICT Risk Analysis nel Banking è quella per processi, come si evince dalla Figura 2.12, mentre la Mappatura degli asset informatici ha un livello di adozione limitato.

Figura 2.12
Il flusso logico che caratterizza le ICT Risk Analysis nel Banking



Confrontando le risposte di CIO e CISO si nota una profonda differenza, soprattutto nella tipologia "Adempimenti normativi" (Figura 2.13). I CISO, infatti, indicano la Mappatura processi come la soluzione più idonea e perseguita (94%), mentre per i CIO è la logica con minor rilevanza (17%).

Figura 2.13
Il flusso logico che caratterizza le ICT Risk Analysis nel Banking – il confronto CIO/CISO



Gli attori

Nei processi di ICT Risk Analysis la Direzione ICT e la/le unità di Security sono coinvolte in maniera pressoché analoga, mentre i Business e functional manager in misura minore (Figura 2.14), fatta eccezione per la categoria "Progettazione nuove iniziative", in cui sono menzionati al pari delle altre due tipologie di attori. Un risultato di non facile interprestazione risulta essere, invece, il minor coinvolgimento di Business e functional manager nelle ICT Risk Analysis ai fini del "Disaster recovery". Infatti, secondo la letteratura, nella valutazione dell'impatto di un'eventuale non disponibilità dei sistemi informativi coinvolti dovrebbero essere proprio loro a fornire una valutazione dell'impatto sui processi di business.

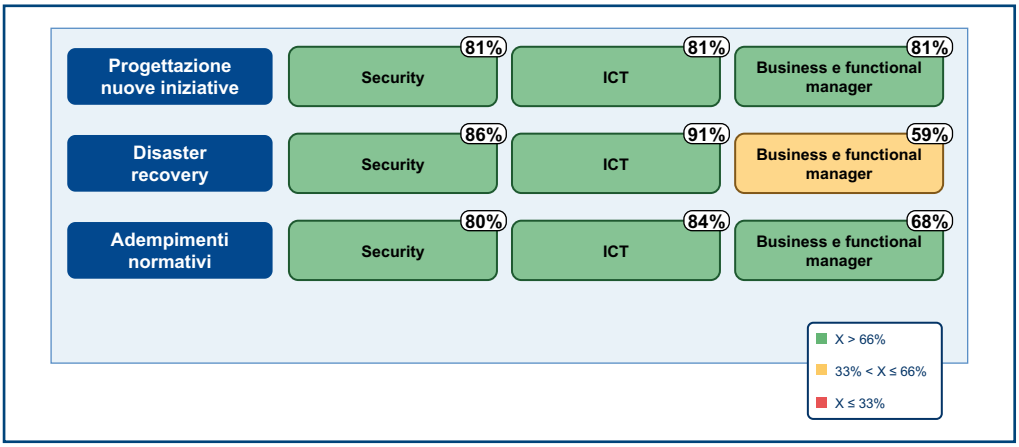


Figura 2.14
Gli attori coinvolti nel processo di ICT Risk Analysis nel Banking

Scendendo, invece, nel dettaglio dell'analisi per "Adempimenti normativi" rappresentata in Figura 2.15, si nota una singolare discordanza nelle risposte di CIO e CISO. Mentre i CIO indicano che è la Security ad essere maggiormente coinvolta, i CISO indicano proprio l'opposto, il che potrebbe far supporre l'esistenza di qualche difficoltà nell'attribuzione delle responsabilità specifiche dell'analisi. Risulta interessante anche la discrepanza tra la percezione del riscorso ai Business e functional manager tra CIO e CISO.

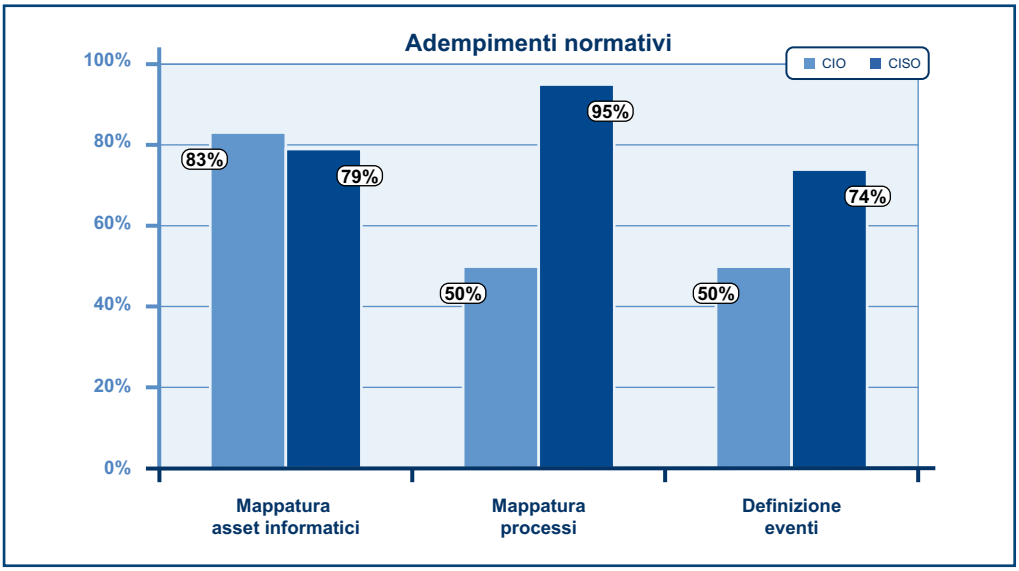
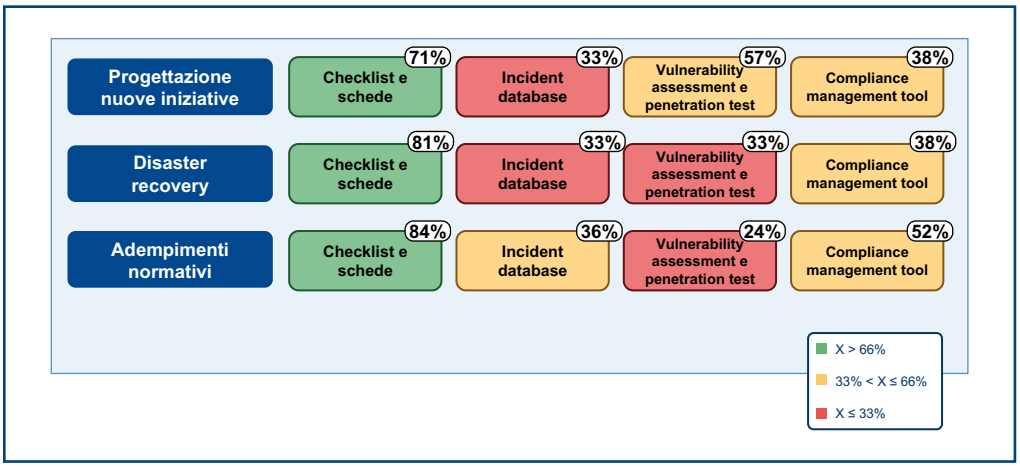


Figura 2.15
Gli attori coinvolti nel processo di ICT Risk Analysis nel Banking – il confronto CIO/CISO

Gli input sources

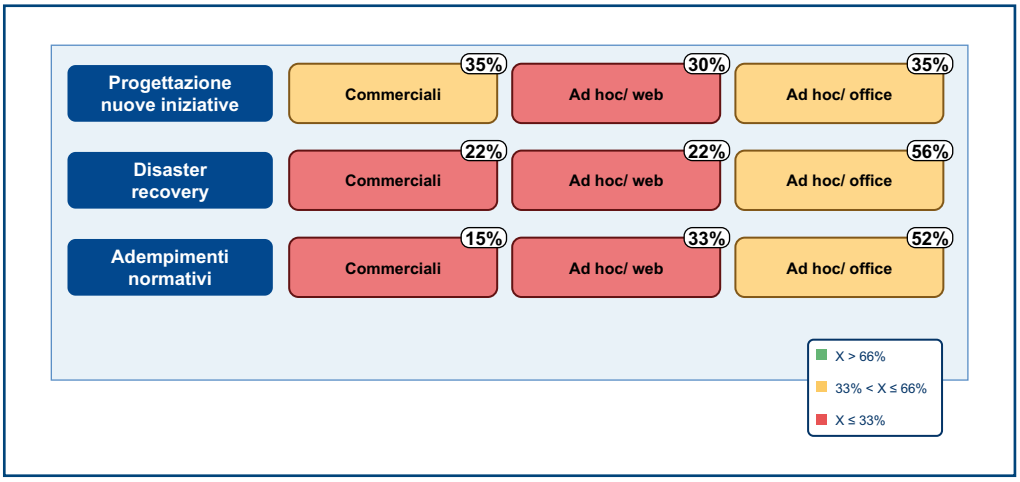
Figura 2.16
Le fonti di input utilizzate per le ICT Risk Analysis nel Banking



Come emerge dalla Figura 2.16, le fonti di informazioni in input utilizzate per le analisi sono in particolar modo basate su Checklist e schede. Il dato riguardante lo scarso utilizzo dell'Incident database può essere direttamente collegato allo scarso utilizzo di analisi di Serie storiche. Le sorgenti Vulnerability assessment e penetration test e Compliance management tool appaiono aver conquistato una certa rilevanza. Dalle interviste emerge che tali strumenti in futuro si affermeranno anche in maniera più significativa.

Gli strumenti

Figura 2.17
Le tipologie di strumenti informatici utilizzati per le ICT Risk Analysis nel Banking



Gli strumenti adottati sono per lo più di tipo Ad hoc/office, cioè sviluppati in casa e di semplice utilizzo (Figura 2.17). Il limitato utilizzo di strumenti Commerciali è stato motivato da una quota significativa di intervistati dalla complessità riscontrata nel loro utilizzo.

Si possono riassumere i dati raccolti per le variabili di configurazione dell'analisi costruendo il quadro sinottico riportato in Figura 2.18, che offre una panoramica delle scelte operate dalle banche intervistate sulle diverse variabili di configurazione con riferimento alle tre macro categorie di ICT Risk Analysis.

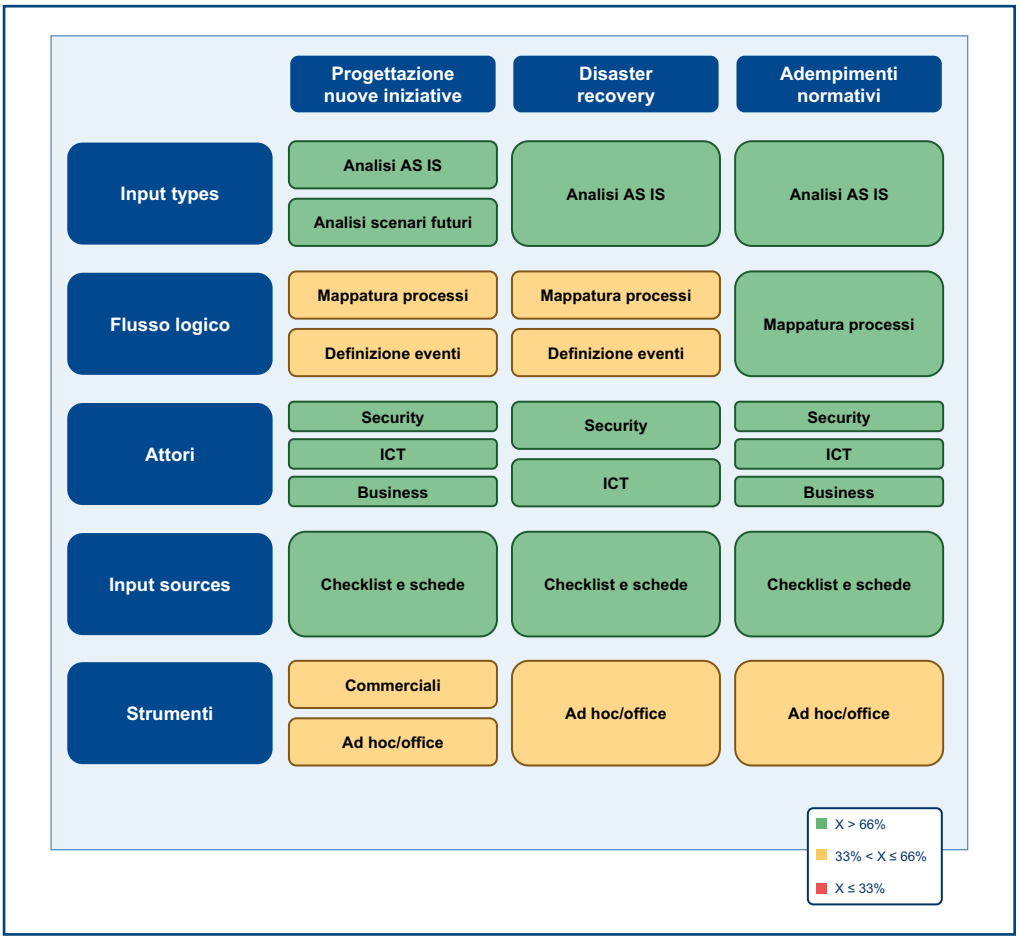


Figura 2.18

Il quadro sinottico delle variabili di configurazione delle ICT Risk Analysis nel Banking

Si può notare come molte delle variabili risultino essere trasversali alle tre macro categorie identificate, sebbene vi siano delle peculiarità, che riflettono le specificità delle diverse tipologie di Risk Analysis (evidenziate anche dai fattori caratterizzanti). A questo proposito, le indicazioni emerse dalle interviste fanno trasparire un'elevata attenzione a contenere la complessità delle attività di ICT Risk Analysis, limitando il più possibile la proliferazione degli approcci.

Ulteriori informazioni utili per comprendere la gestione del processo di ICT Risk Analysis all'interno di un'azienda sono costituite dalla frequenza di cambiamento della metodologia utilizzata e dalla possibilità di riutilizzare, almeno in alcuni casi, semilavorati comuni per le diverse tipologie di ICT Risk Analysis.

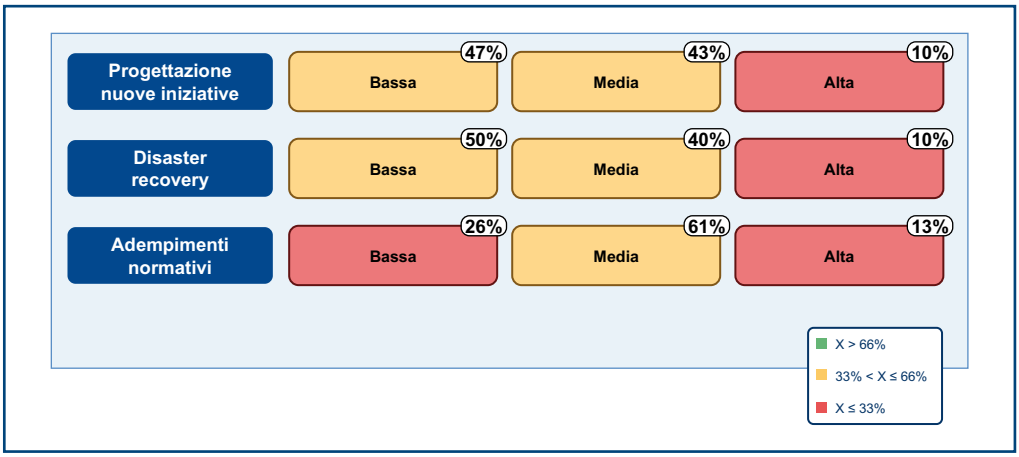
Frequenza di cambiamento e riutilizzo dei risultati

In riferimento alla frequenza di cambiamento è stata scelta la seguente scala:

- *Alta*: la metodologia è cambiata praticamente ogni anno.
- *Media:* la metodologia è cambiata più volte negli ultimi anni.
- *Bassa:* la metodologia è invariata da diversi anni.

Figura 2.19

La frequenza di cambiamento della metodologia utilizzata per le ICT Risk Analysis nel Banking

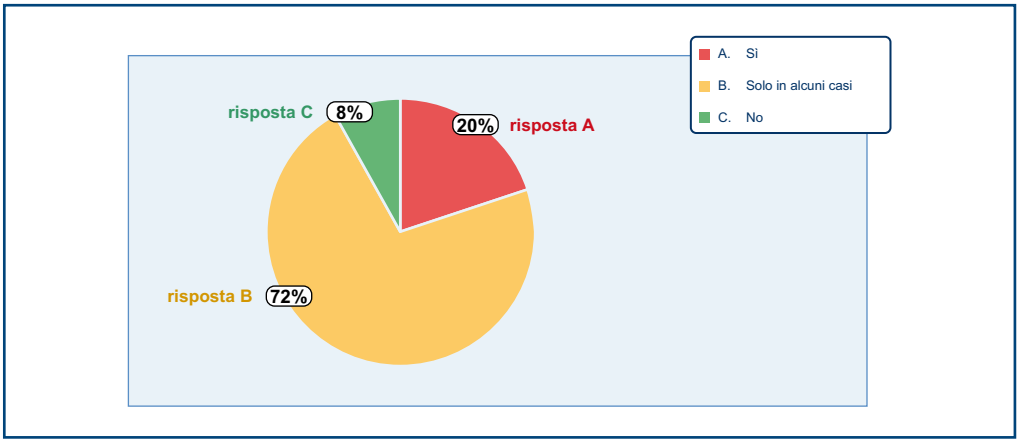


Le risposte (figura 2.19) evidenziano una certa stabilità delle scelte effettuate in passato riguardo l'ICT Risk Analysis. Infatti per nessuna delle tre macro categorie è stata indicata un'alta frequenza di cambiamento superiore al 13%. Per quanto riguarda le macro categorie "Progettazione nuove inziative" e "Disaster recovery" la situazione tra bassa e media risulta essere molto equilibrata, mentre per "Adempimenti normativi" emerge un orientamento a una frequenza di cambiamento media.

Per quanto riguarda la possibilità di utilizzare semilavorati comuni per le diverse ICT Risk Analysis, solo l'8% dei CIO e CISO dichiara di non riutilizzare parti comuni, a testimonianza dell'attenzione all'efficienza, in termini di tempo e di risorse spese delle diverse attività di ICT Risk Analysis (Figura 2.20). Questo è anche sintomo di un elevato livello di knowledge sharing tra le diverse unità organizzative dell'azienda.

Figura 2.20

L'utilizzo di semilavorati comuni per diverse metodologie di ICT Risk Analysis nel Banking



Box 2.1

Credit Suisse

Fondata nel 1856, Credit Suisse vanta una lunga tradizione nel panorama bancario internazionale. Oggi Credit Suisse è uno dei principali gruppi bancari internazionali, riconosciuta a livello globale come banca leader nell'ambito dei servizi di consulenza, soluzioni omnicomprensive e prodotti innovativi dedicati alla clientela Private, Corporate e Istituzionale. Credit Suisse ha sede a Zurigo ed è presente in 50 paesi con circa 40.000 dipendenti. In Italia Credit Suisse è presente con varie entità legali, e oltre 600 collaboratori.

La funzione di Information Technology di Credit Suisse a livello world wide è molto articolata e a livello Italia è presente con circa 30 persone.

In particolare, il dipartimento IT Risk è la principale unità di gestione del rischio, cui spetta il compito di proteggere la banca attraverso l'individuazione e la segnalazione di rischi connessi all'ambiente IT, di approvare i piani di contenimento del rischio e di garantire la gestione del rischio residuo.

In Credit Suisse la Risk Analysis è in continua evoluzione. Le metodologie e i tool utilizzati permettono di effettuare analisi sia ad ampio spettro, che specifiche sul singolo progetto. L'attenzione è rivolta a tutti e tre i requisiti fondamentali di sicurezza: disponibilità, integrità e riservatezza.

Il riferimento principe per il Risk Assessment è un documento (Risk Profile Document), che raccoglie i risultati dell'intero processo e che viene sottoposto alla singola area di business per la formale accettazione. L'analisi dei rischi è parte integrante del processo di gestione dei progetti, inoltre viene effettuata annualmente una valutazione dal dipartimento centrale IT Risk a livello Italia, a cui se ne aggiunge una seconda realizzata dalla funzione locale (Local Information Security).

L'aggiornamento e la formazione sono fondamentali, infatti Credit Suisse è impegnato a realizzare corsi di formazione interattivi, con esame di valutazione finale e con la finalità di mantenere elevato il livello di attenzione e continuare a promuovere la conoscenza e la consapevolezza dei diversi fattori di rischio.

L'attenzione dell'Operational Risk Manager è rivolta anche ai rischi legati all'ICT, in quanto proprio su tali tecnologie è basata la gran parte delle operations della banca. Per questo, l'Operational Risk Management di Credit Suisse Italy, ai fini dell'individuazione dei possibili profili di rischio operativo, si affida pesantemente alle analisi di sicurezza effettuate dal dipartimento IT, facendole proprie.

Deutsche Bank

Box 2.2

Deutsche Bank opera nel settore bancario sui mercati Retail, Small Business, Private e Corporate. Il Gruppo costituisce oggi una delle principali banche d'investimento a livello globale, con un'importante rete di clienti privati. Con 81.308 dipendenti in 75 paesi (dati al 30 giugno 2008), Deutsche Bank si posiziona come leader globale nella fornitura di soluzioni finanziarie per una clientela di standing elevato e con le sue attività crea valore per gli azionisti e il personale.
Per la gestione dei servizi ICT in Italia, Deutsche Bank si avvale di una società di servizi (la DB Consorzio) che conta più di 600 dipendenti, e di cui è unico cliente. In essa sono confluite la maggior parte delle attività di servizio, quali l'ICT, il Global Sourcing e il CRES. Il 75% delle risorse di DB Consorzio si occupa dell'ICT e fa capo al GTO (Global Technologies and Operations), suddiviso in tre unità operative: Operations, che rappresenta il back office centralizzato, Information Enterprise Services (IES), che si occupa della parte infrastrutturale e della sicurezza logica, e ICT applicativo.

Nell'ultimo anno è stata avviata un'attività di assessment del Rischio Operativo e Normativo, che ha cominciato a produrre alcuni risultati interessanti. L'input a questa analisi è stato dato dalla normativa Basilea 2, dalle disposizioni di Banca d'Italia e dalle policy di gruppo.

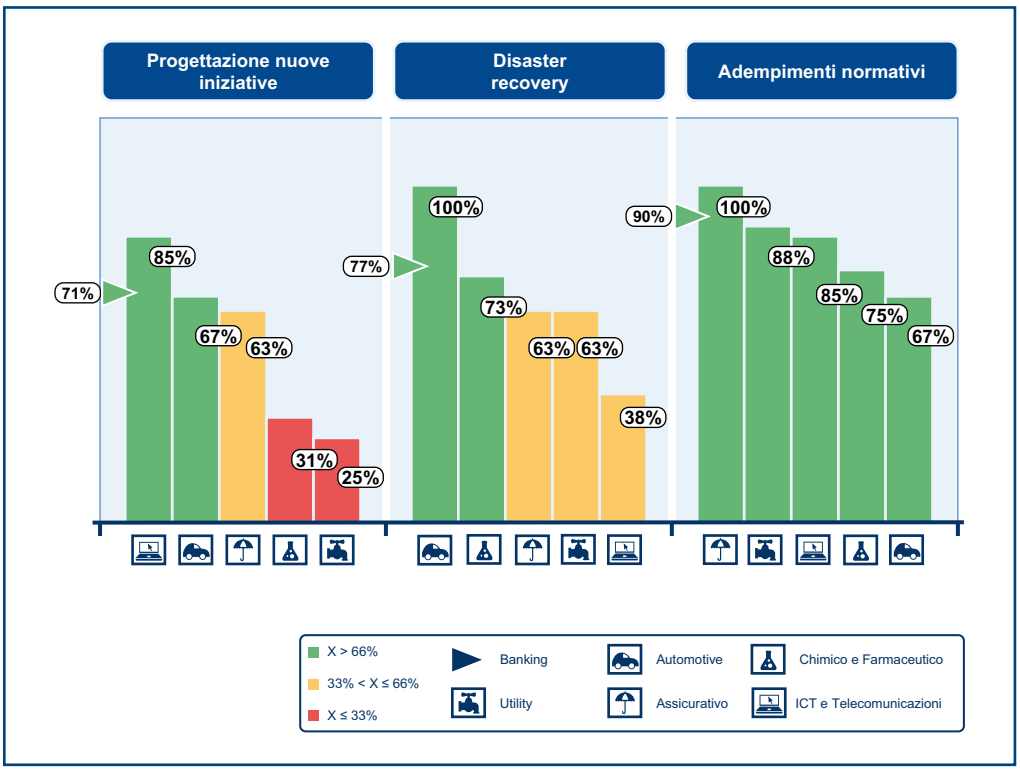
L'attività di Risk Analysis prevede una prima mappatura del rischio potenziale, valutato con un approccio quali-quantitativo sulla base di probabilità e impatto. Alla matrice di esposizione al rischio così ottenuta viene applicata una valutazione di adeguatezza dei controlli e di efficacia degli interventi di mitigazione per il calcolo della matrice di propensione al rischio residuo. Diversi coefficienti di rischio consentono di disporre in ordine di priorità la necessità di ulteriori azioni di monitoraggio o di mitigazione. Sia gli eventi negativi occorsi sia gli esiti delle attività di controllo sia il completamento delle misure di mitigazione comportano una revisione continua della mappatura del rischio.

Grazie alle novità introdotte dalle iniziative di Risk Analysis, la collaborazione tra l'ICT Risk Manager e l'Operational Risk Manager e l'interazione con le singole Funzioni Operative, owner del rischio, è stata periodica e frequente. Durante gli incontri viene messa a punto la metodologia e si analizzano i risultati raggiunti. Questo avviene anche grazie alla struttura organizzativa di Deutsche Bank, che prevede l'Operational Risk Management a stretto contatto con il Consorzio.

Oltre il Banking: i risultati degli altri settori

Visto l'interesse dei risultati ottenuti nel Banking, si è deciso di procedere anche all'analisi di altri settori, caratterizzati anch'essi da un'elevata strategicità dell'ICT Security. Per questo sono stati selezionati i seguenti settori: Automotive, Assicurativo, Chimico e Farmaceutico, ICT e Telecomunicazioni, Utility.

Figura 2.21
Le tipologie di ICT Risk Analysis



Un primo risultato interessante consiste nel fatto che, contrariamente a quanto avviene nel Banking, la Risk Analysis negli altri settori, a eccezione di quello Automotive, non è diffusa in tutte le tre macro categorie identificate (Figura 2.21). In particolare in tutti i settori appare molto ricorrente l'analisi effettuata per "Adempimenti normativi". Nei settori Chimico e Farmaceutico e Utility, invece, non appare diffuso l'utilizzo della Risk Analysis per "Progettazione nuove iniziative". Lettura attenta deve essere invece fatta per il settore ICT e Telecomunicazioni dove il 38% di CIO dichiara di non ricorrere a Risk Analysis per "Disaster recovery". Questo dato potrebbe essere collegato al fatto che le infrastrutture di ICT e Telecomunicazioni devono garantire ridondanza globalmente, senza necessitare di un'analisi di questo tipo.

I fattori caratterizzanti l'orizzonte dell'ICT Risk Analysis

Le finalità

Dalla figura (2.22) si evidenzia come il ricorso a metodologie che puntino alla stima del livello di esposizione sia più elevato nei settori non Banking, specie in relazione alla tipologia "Disaster recovery". Tale risultato potrebbe essere legato al fatto che l'esperienza su metodologie per la Stima dell'esposizione sia maggiore nel settore bancario, e tali esperienze abbiano evidenziato un livello di complessità e di costi tale da far orientare le banche verso metodologie a minor impatto.

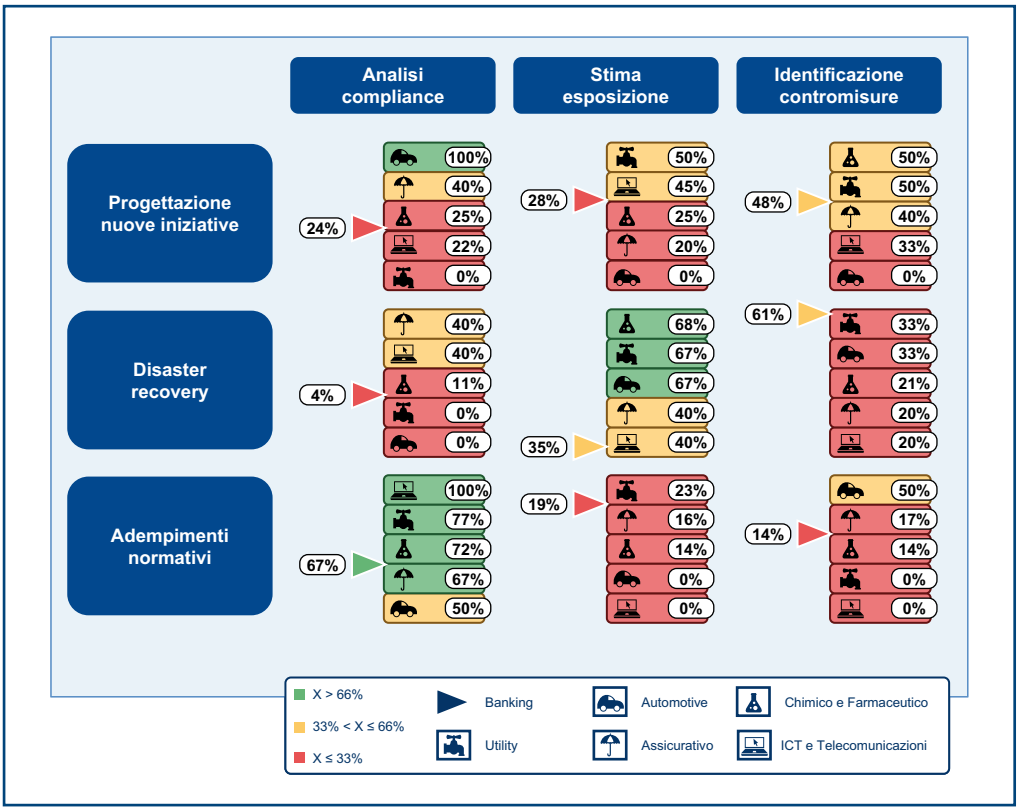


Figura 2.22

Le finalità prevalenti per le ICT Risk Analysis

L'ambito

Per quanto riguarda l'ambito di copertura delle analisi, non emergono particolari scostamenti rispetto al settore bancario, se non una maggior propensione degli altri settori nell'effettuare Risk Analysis con ambito esteso all'Intera azienda (Figura 2.23).

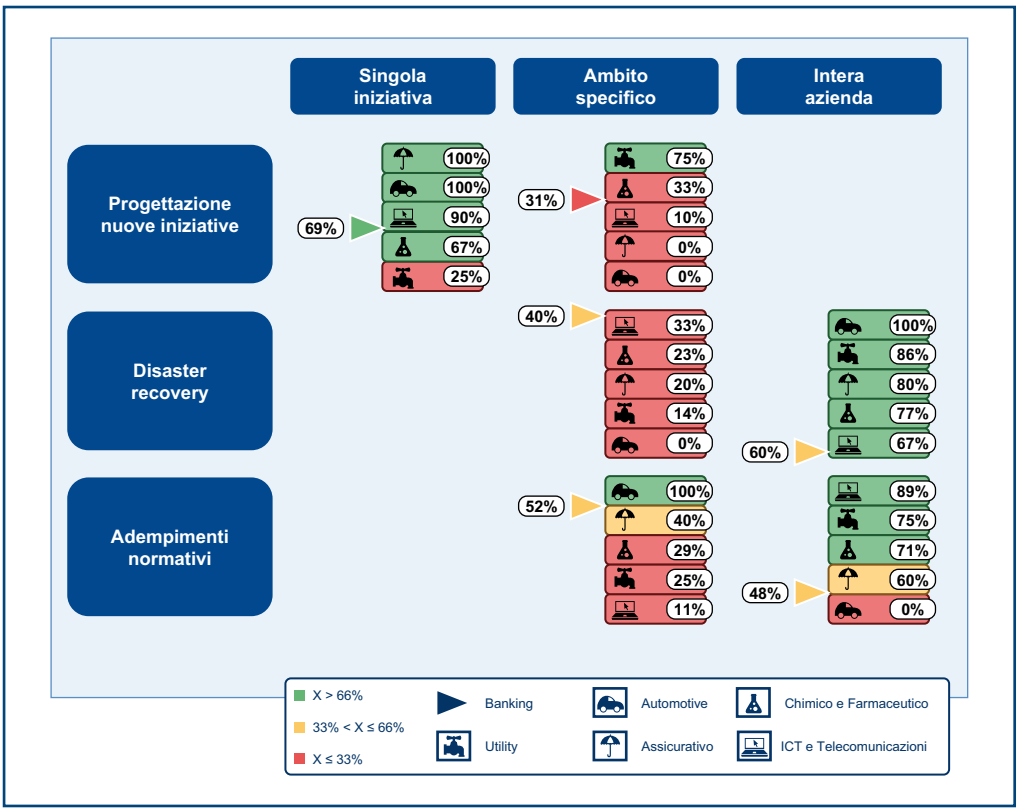


Figura 2.23

L'ambito di copertura delle ICT Risk Analysis

I requisiti

Per quanto concerne i requisiti di sicurezza da considerare nelle ICT Risk Analysis, si evidenzia come in molti casi vi sia una minore attenzione ad alcuni dei requisiti. In particolare, a parte per il settore ICT e Telecomunicazioni, che sono ICT intensive, spesso la Confidenzialità non viene presa in considerazione nella Risk Analysis ai fini dell "Disaster recovery", e la stessa sorte tocca alla Disponibilità nelle analisi per "Adempimenti normativi" (Figura 2.24).

Figura 2.24
I requisiti di sicurezza considerati nelle ICT Risk Analysis

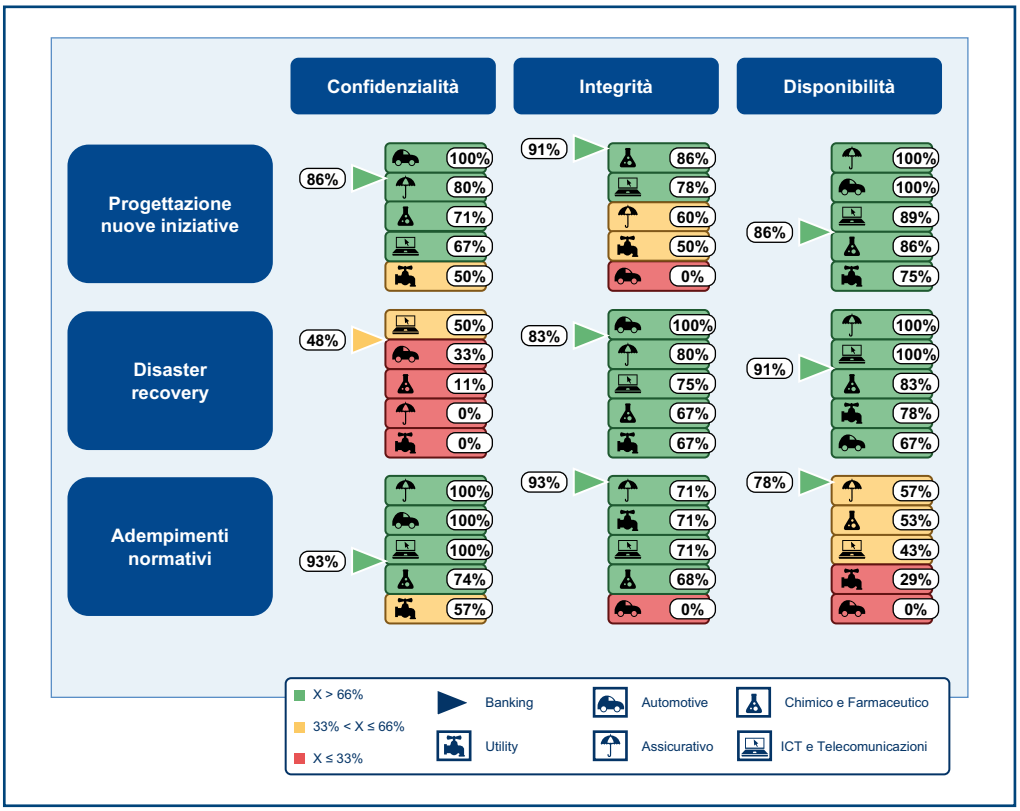
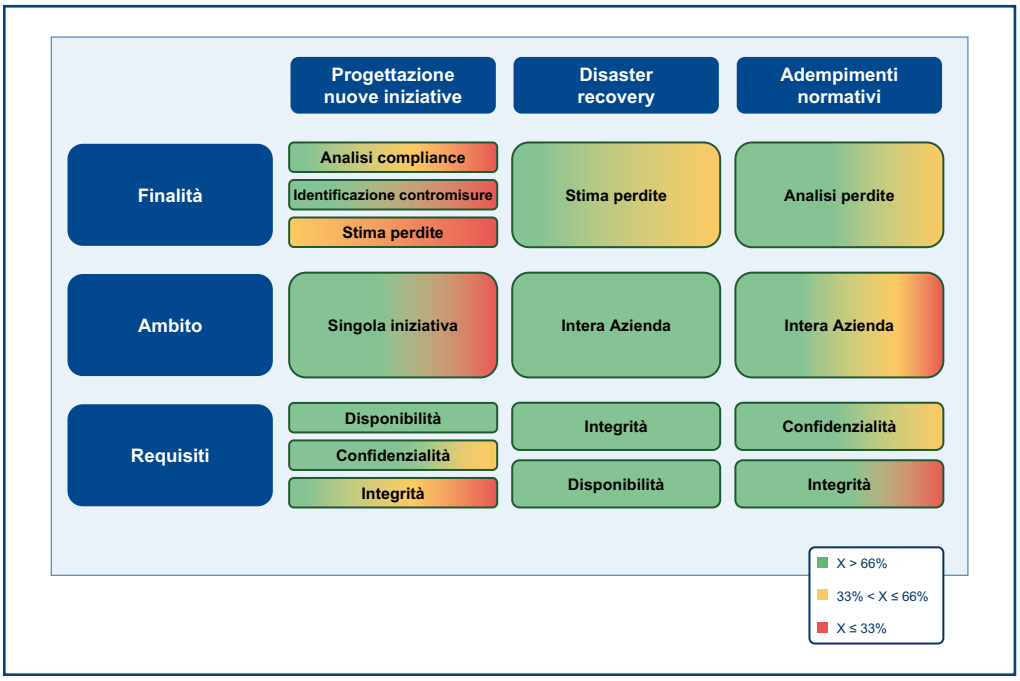


Figura 2.25
Il quadro sinottico dei fattori caratterizzanti l'orizzonte dell'ICT Risk Analysis



I risultati ottenuti, riassunti nel quadro sinottico riportato in Figura 2.25, evidenziano sostanzialmente che lo scostamento rispetto al settore Banking non è così ampio come

ci si poteva aspettare. Inoltre, si nota una certa difficoltà nella caratterizzazione delle diverse Risk Analysis.

Le variabili di configurazione dell'ICT Risk Analysis

Gli input types

Per quanto riguarda la tipologia di input su cui sono basate le analisi, si conferma la difficoltà a ricorrere a Serie storiche, sebbene risultino un po' più diffuse nel mondo Utility e Automotive (Figura 2.26). La motivazione potrebbe essere duplice e identificabile sia in una maggiore propensione "culturale" alla tracciatura degli eventi sia in una minore complessità del contesto. Inoltre si può notare come vi sia un utilizzo di Analisi di scenari futuri più diffuso rispetto al settore bancario.

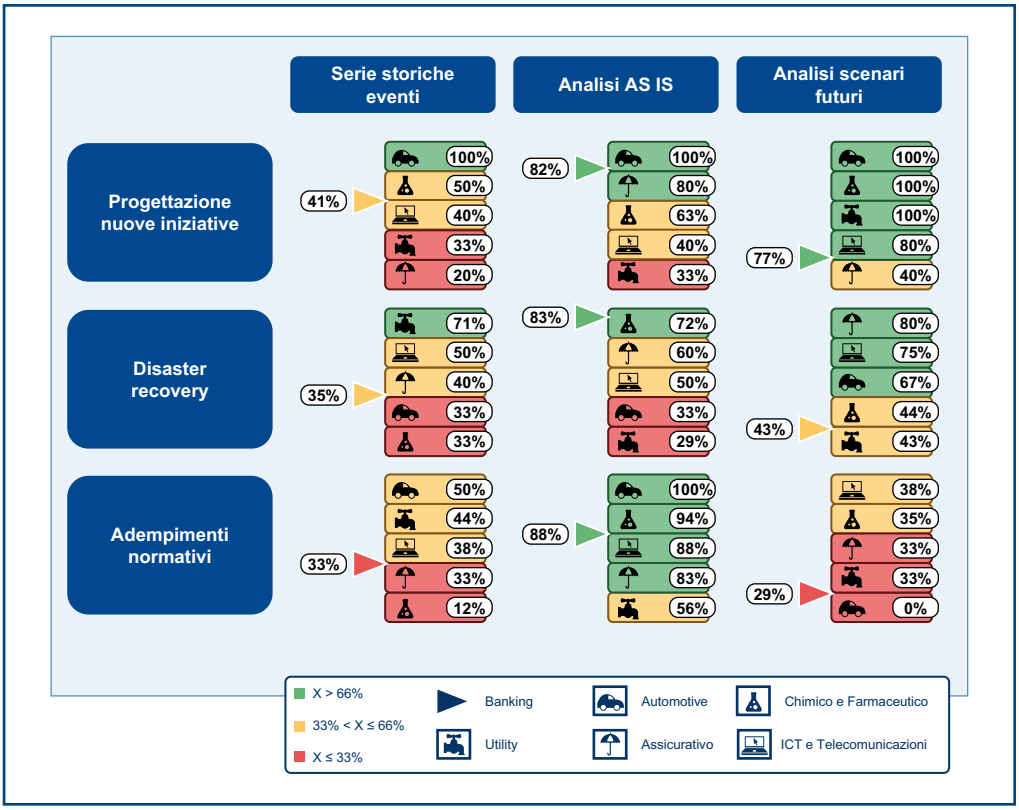
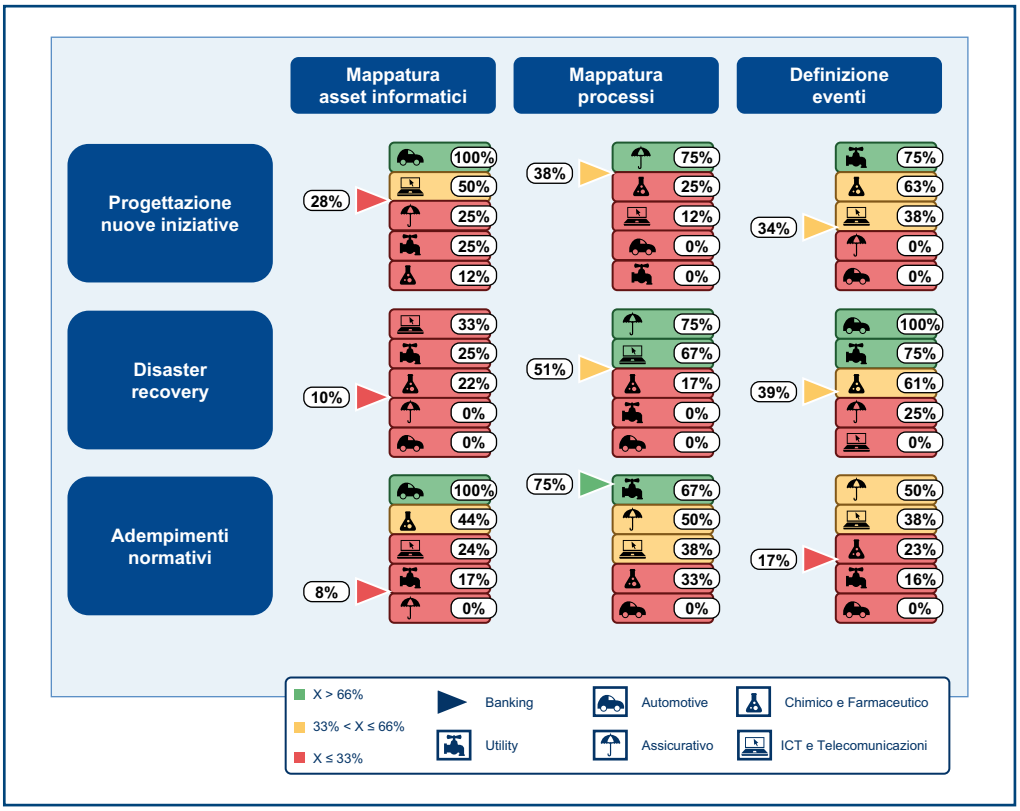


Figura 2.26
La tipologia di input su cui sono basate le ICT Risk Analysis

Il flusso logico

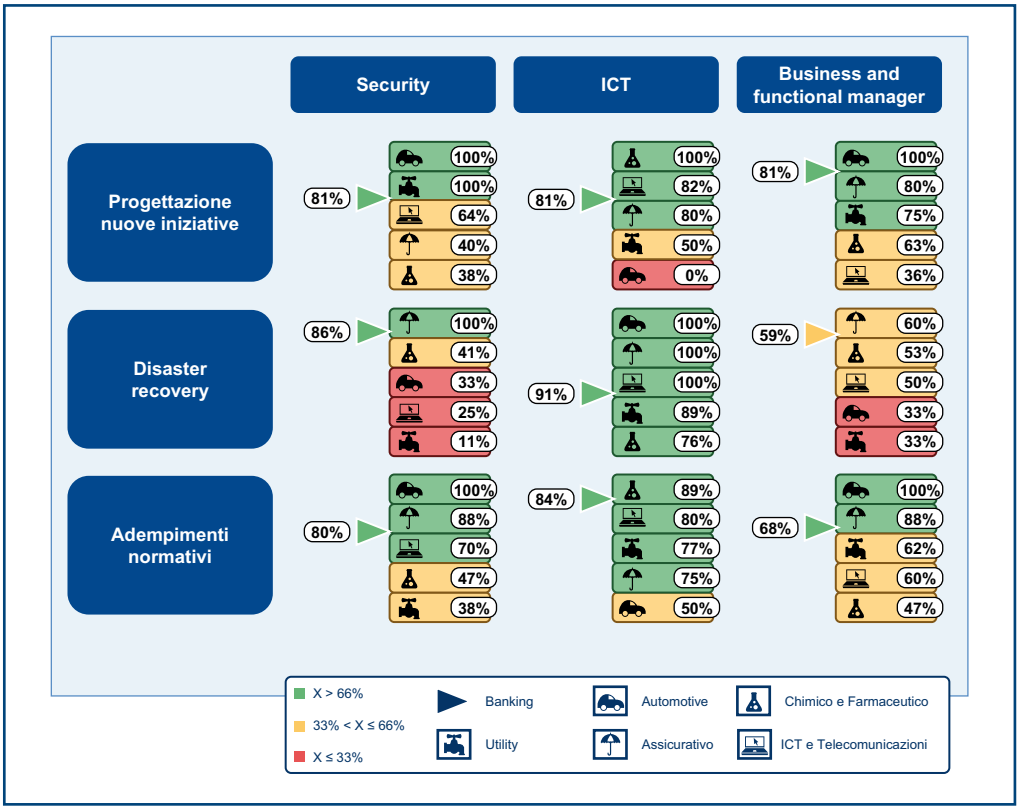
In Figura 2.27 si può notare come la Mappatura dei processi, così diffusa nel settore bancario, sia sostituita spesso dalla Mappatura degli asset e dalla Definizione di eventi. In particolare si può rilevare che nel mondo ICT e Telecomunicazioni è presente una maggiore distribuzione tra gli approcci. Infatti per la "Progettazione nuove iniziative" prevale la Mappatura degli asset informatici, mentre per il "Disaster recovery" la Mappatura processi e la Definizione degli eventi.

Figura 2.27
Il flusso logico che caratterizza le ICT Risk Analysis



Gli attori

Figura 2.28
Gli attori coinvolti nel processo di ICT Risk Analysis



Dalle risposte dei CIO, emerge come nei settori non Banking vi sia una maggiore difficoltà nel coinvolgere interlocutori non ICT, anche se si registrano delle significative differenze tra le diverse macro categorie di analisi, nonché, a parità di tipologia di Risk Analysis, da settore a settore (Figura 2.28). Ad esempio, nel settore Utility per l'analisi

finalizzata alla "Progettazione Nuove iniziative"si coinvolgono significativamente sia gli interlocutori di Security sia i Business and functional manager, mentre tale coinvolgimento è praticamente nullo per la macro categoria "Disaster recovery".

Gli input sources

Come per il Banking, si conferma, anche per gli altri settori, un elevato ricorso a Checklist e schede (Figura 2.29). Si può notare, invece, uno scostamento significativo nel maggiore utilizzo di strumenti di Vulnerability assessment e penetration test.

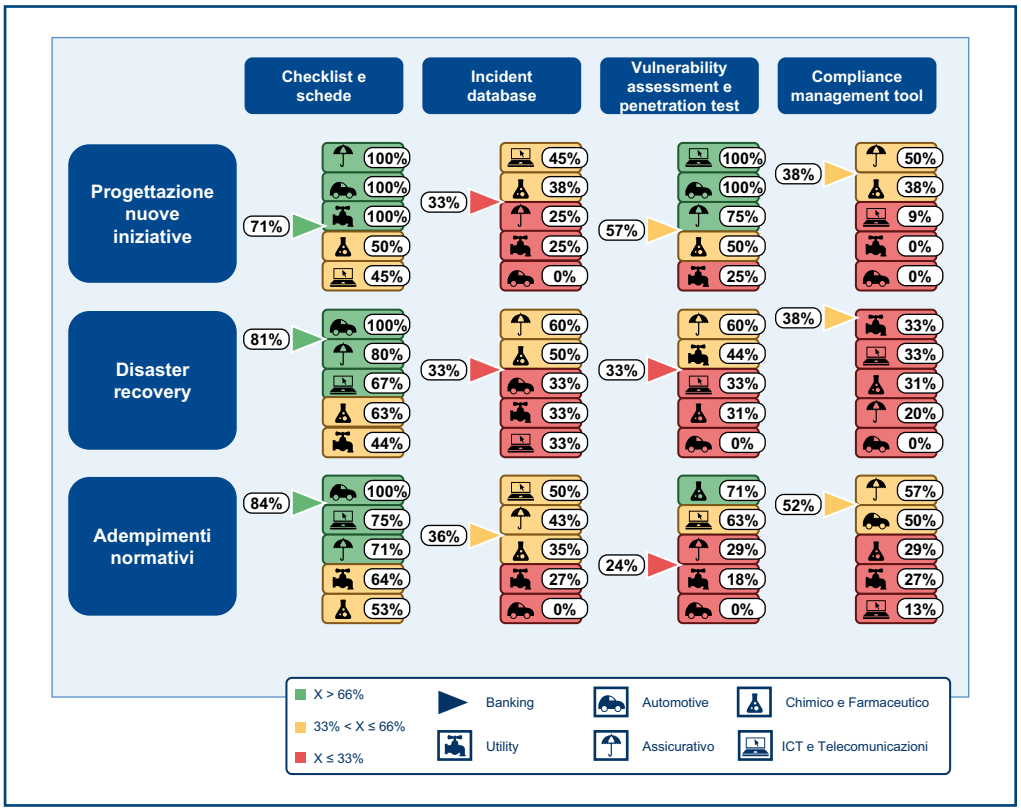


Figura 2.29

Le fonti di input utilizzate per le ICT Risk Analysis

Gli strumenti

Infine, per l'ultima variabile di configurazione rilevata, che riguarda l'utilizzo delle soluzioni informatiche (Figura 2.30), si conferma un'ampia adozione di strumenti Ad hoc/office, anche in misura maggiore rispetto al settore del Banking. L'utilizzo di strumenti Commerciali appare invece anche in questo caso molto limitato.

Figura 2.30

Le tipologie di strumenti informatici utilizzati per le ICT Risk Analysis

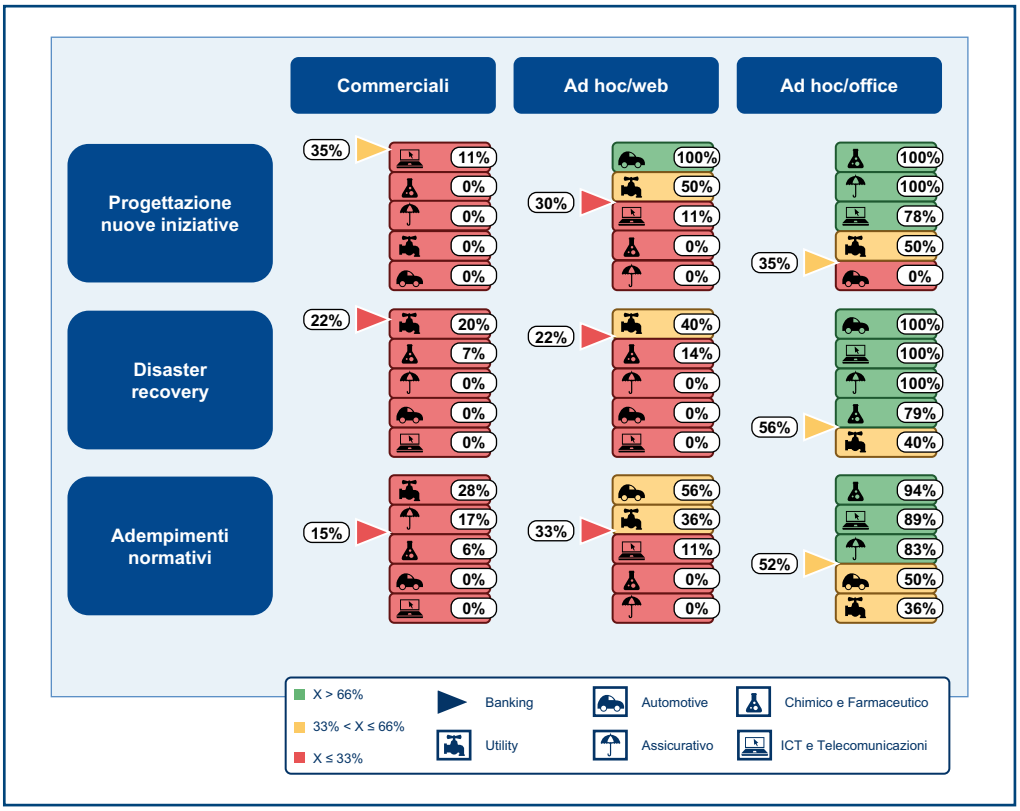
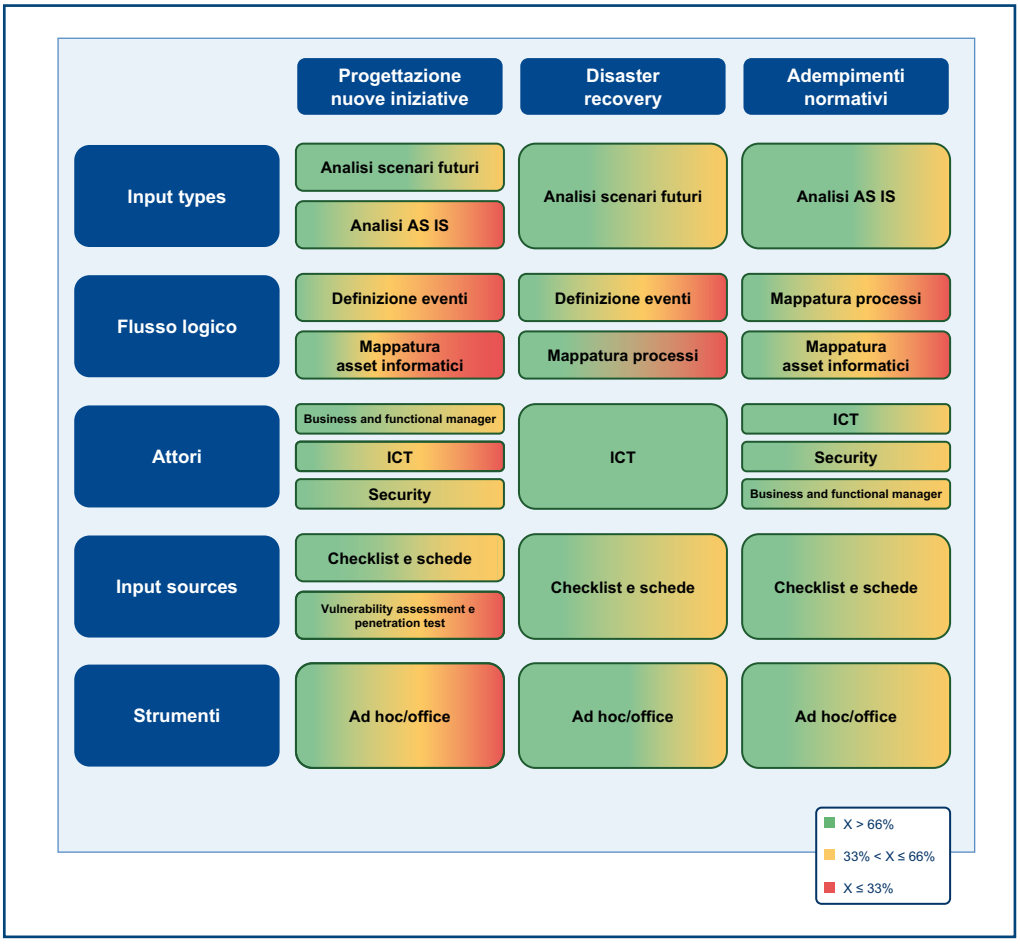


Figura 2.31

Il quadro sinottico delle variabili di configurazione dell'ICT Risk Analysis



Dall'analisi comparata col settore bancario, riassunta nel quadro sinottico in Figura 2.31, emergono molte similitudini, ma anche alcune significative differenze a livello me-

todologico. In particolare, tali differenze riguardano il flusso logico (trasversalmente sulle tre macro categorie di Risk Analysis), nonché nel caso delle analisi finalizzate alla "Progettazione nuove iniziative" in diversi aspetti. In ogni caso, complessivamente si conferma ancora un'elevata frammentazione di approcci.

Proseguendo con l'analisi si può notare come, rispetto al settore Banking, gli altri settori siano caratterizzati da una maggiore frequenza di cambiamento delle metodologie usate per le Risk Analysis (Figura 2.32). Tale risultato può essere letto come una conferma del fatto che nel Banking queste analisi vengono utilizzate da maggiore tempo, e quindi si è raggiunto un livello di maturità più elevato.

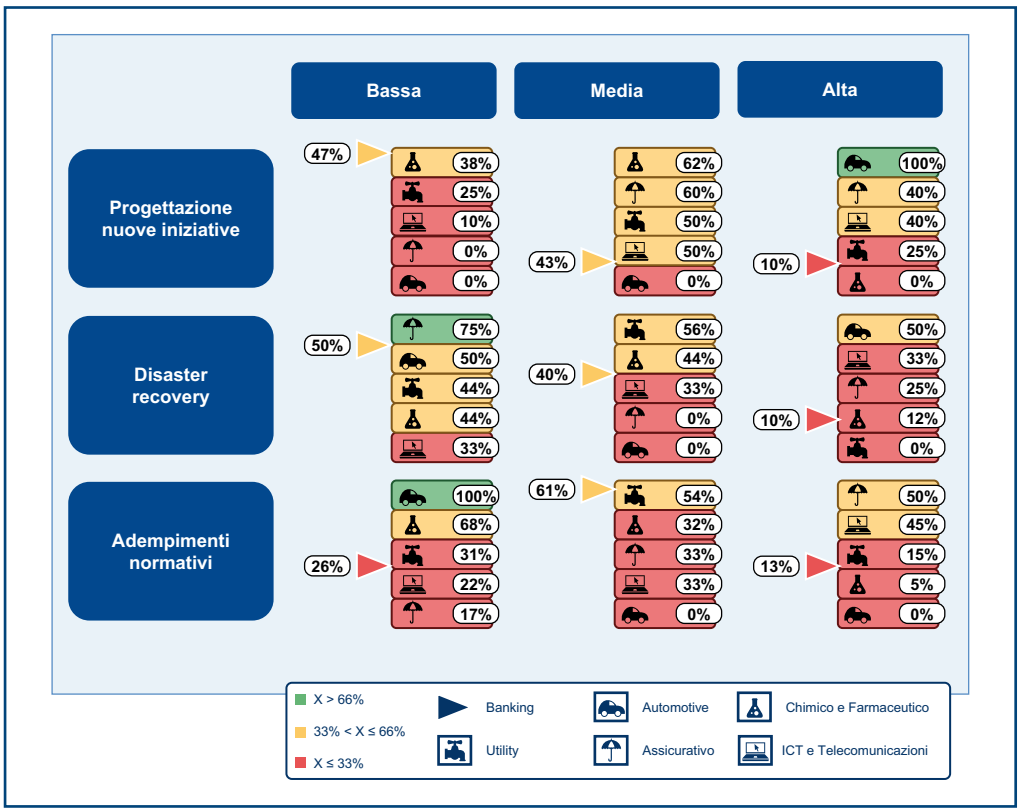


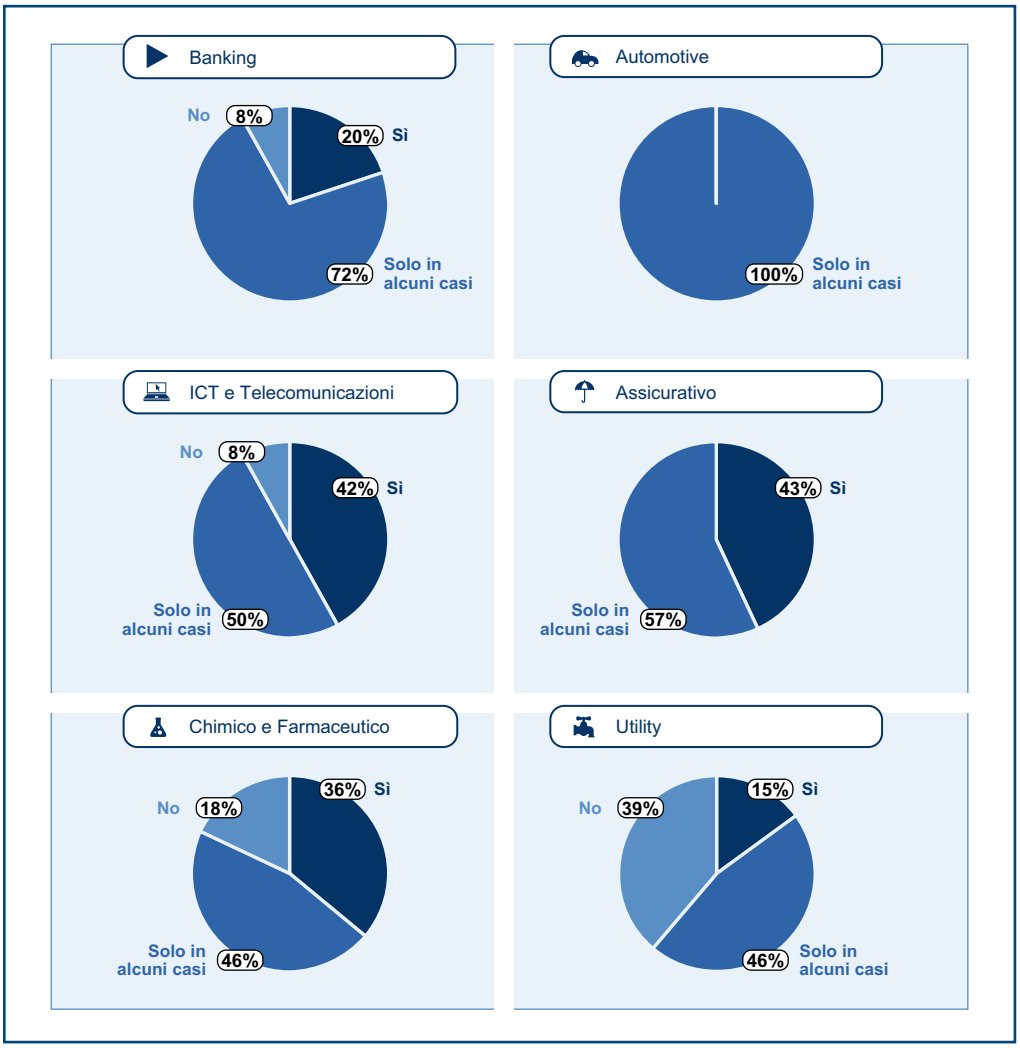
Figura 2.32

La frequenza di cambiamento della metodologia utilizzata per le ICT Risk Analysis

Infine, per ciò che concerne il riuso dell'output delle analisi, si conferma come l'utilizzo di semilavorati comuni sia il caso più diffuso, anche se vi sono delle significative differenze tra settore e settore: ICT e Telecomunicazioni e Assicurativo sembrano i settori che maggiormente lavorano in questa direzione, mentre per Chimico e farmaceutico e Utility tale sinergia si realizza più raramente. Questo potrebbe dipendere dalle peculiarità delle Risk Analysis in tali settori, oppure da una minore esperienza e, quindi, da una minor evoluzione delle soluzioni organizzative in ambito ICT Security.

Figura 2.33

L'utilizzo di semilavorati comuni per le diverse metodologie di ICT Risk Analysis



3. L'ICT Security e l'Enterprise Risk Management nel Banking: un rapporto in continua trasformazione

Il nuovo approccio al Risk Management

Storicamente le imprese adottavano un approccio al Risk Management "a silos" , in cui la responsabilità della gestione dei rischi era assegnata alle unità di business o alle funzioni maggiormente esposte: i rischi di business venivano quindi gestiti dalle unità operative, i rischi assicurabili o trasferibili dall'unità Risk Management a livello corporate, i rischi finanziari (legati al mercato, al tasso d'interesse, ecc.) dalla tesoreria e, in più in generale, dal Corporate Finance, i rischi di compliance dal Legal. Le organizzazioni inoltre si focalizzavano primariamente sui rischi facilmente misurabili. I rischi ambigui o di difficile definizione, come quelli operativi e strategici, spesso non venivano gestiti o venivano semplicemente ignorati. La strategia di gestione dei rischi era solitamente vincolata ai processi esistenti, senza un approccio uniforme o la ricerca di un linguaggio comune.

I danni conseguenti ad alcuni gravi incidenti, che hanno in alcuni casi portato anche a una consistente perdita di fiducia da parte dei consumatori, hanno evidenziato le lacune dell'approccio tradizionale alla gestione dei rischi. Di conseguenza, le imprese hanno cercato di mettere a punto soluzioni innovative per meglio prepararsi alle nuove sfide e alle incertezze emergenti dell'ambiente in evoluzione.

L'Enterprise Risk Management è un approccio olistico e integrato che supporta l'allineamento di strategie, processi, persone e tecnologie, e permette alle organizzazioni di identificare e gestire efficacemente le diverse aree e tipologie di rischio. In questo modo, aumentano per le imprese le probabilità di implementare con successo le proprie strategie di business.

L'approccio ERM è anticipatorio e proattivo, e fornisce un supporto attivo alla realizzazione degli obiettivi strategici dell'organizzazione. In particolare, esso non è un ostacolo all'assunzione dei rischi, ma al contrario, può portare anche all'accettazione di un livello di rischio superiore a quello storicamente ritenuto ammissibile. Il tutto però "a ragion veduta", cioè come frutto di un'analisi rigorosa, all'interno di un framework unico e integrato.

Una volta identificati e opportunamente valutati i principali fattori di rischio, infatti, è possibile decidere quali tra essi debbano essere:
- ridotti, attraverso rigorose pratiche di gestione;
- trasferiti, attraverso assicurazioni o programmi di protezione;
- accettati;
- rifiutati, eliminando un processo, un prodotto o una zona geografica.

L'ERM fornisce strumenti e tecniche per bilanciare realisticamente il trade-off rischi/profitti e cogliere velocemente le opportunità di mercato. Un ERM pienamente e correttamente implementato non è soltanto un elemento fondamentale a completamento della governance dell'impresa, ma fornisce anche l'opportunità di sfruttare il rischio come vantaggio competitivo sul mercato, evitando di trattarlo esclusivamente come una minaccia.

Possiamo vedere in Figura 3.1 le principali differenze tra l'approccio tradizionale alla gestione del rischio e l'ERM.

Figura 3.1
Le differenze tra approccio tradizionale ed ERM

	Approccio tradizionale	Enterprise Risk Management
Visione generale	Approccio frammentato, effetto silos	Approccio olistico, integrato
Visione del rischio	Rischio come minaccia	Rischio come minaccia e opportunità
Ottica	Ottica reattiva, avversione al rischio	Ottica proattiva, che comprende l'elusione e lo sfruttamento del rischio
Valutazione del rischio	Risk Analysis sporadico	Continuo Risk Analysis, rivalutazione e gestione
Reporting	Reporting dei rischi inconsistente	Reporting breve e consolidato
Approccio manageriale	Cost-based	Value-based
Collaborazione con le altre unità	Limitata influenza strategica	Efficace supporto ai piani strategici e di business
Approccio organizzativo	Assenza di una chiara definizione di ruoli e responsabilità	Ruoli e responsabilità chiaramente definiti e comunicati
Comunicazione	Comunicazione chiusa	Comunicazione aperta
Ownership	Ownership ambigua per alcune tipologie di rischi	Ownership dei rischi assegnata e piani di valutazione

Un malinteso comune è che l'ERM trasferisca la responsabilità dei rischi dai manager di linea a unità centralizzate e burocratiche. In realtà è vero proprio il contrario: un principio universale dell'ERM è che i rischi debbano essere gestiti dalle unità di business che li contraggono. Per il successo di un approccio ERM è necessario che i manager di linea comprendano che la gestione del rischio è una loro responsabilità, una volta che sono stati dotati di strumenti in grado di gestirlo in modo efficiente. Chiaramente, un ruolo fondamentale in questo senso è esercitato dal sistema di incentivazione, che deve garantire adeguate remunerazioni nel caso in cui l'accettazione consapevole di un livello di rischio superiore dia luogo a performance economico-finanziarie più elevate.

Box 3.1

Le specificità dell'Enterprise Risk Management nel settore bancario: Basilea 2

Nell'aprile 2003 il Comitato di Basilea ha emanato la normativa relativa ai requisiti patrimoniali sul rischio di credito e sui rischi operativi negli istituti bancari. Questo accordo internazionale ha obbligato le banche a dotarsi di una struttura di valutazione dei rischi integrata. Il rischio assunto dalla banca è visto, ora, come somma di tre componenti:

- rischio di mercato, correlato alle eventuali perdite di portafoglio;
- rischio di credito, cioè la probabilità che i finanziamenti erogati si tramutino in perdita a causa dell'insolvenza dei debitori;
- rischio operativo, connesso alle potenziali inefficienze del sistema di controllo della banca.

In particolare, il Comitato di Basilea ha approfondito il trattamento dei rischi operativi, finalizzato alla determinazione dei requisiti patrimoniali minimi. Tale impostazione ha effetti sull'organizzazione interna delle banche, in quanto richiede un'adeguata attenzione a fattori che in Basilea 1 non erano espressamente indicati. La valutazione dei rischi operativi viene riferita alla totalità delle attività svolte dalle banche.

L'impatto di questo accordo è stato notevole: le banche hanno infatti dovuto dotarsi di strutture organizzative e di sofisticati sistemi di misurazione e gestione del rischio. Il livello di esposizione al rischio dipende ovviamente dalle decisioni prese in sede di pianificazione, che si concretizzano nelle diverse fasi dei processi produttivi e si gestiscono tramite l'interazione tra le funzioni produttive, dove nascono, e le funzioni che li rilevano.

Parlando di rischi ci si trova così a riflettere sull'intera organizzazione dell'impresa. Bisogna

rivedere i processi non solo per ridurre i costi, ma anche per ottimizzare la relazione tra ritorni attesi e rischio esistente. È quindi sulla combinazione di questi due fattori che va formulato l'obiettivo complessivo dell'impresa.

Il rischio operativo è definibile come il rischio di subire perdite, dirette o indirette, a causa di fattori sia interni sia esterni all'organizzazione, riconducibili a specifiche tipologie:

- persone: perdite associate a violazioni intenzionali (negligenze, frodi, ecc.) e non intenzionali (inesperienze e ingenuità) di policy interne da parte di impiegati attuali o passati;
- processi: perdite causate da difetti nelle procedure esistenti, o dalla mancanza di una procedura, e che derivano da errori umani o dall'errata esecuzione di una procedura esistente;
- sistemi: perdite causate da guasti o malfunzionamenti nei sistemi tecnologici esistenti. Sono di tipo non intenzionale;
- eventi esterni: perdite conseguenti ad eventi naturali o causati dall'uomo, o che sono risultato diretto di un'azione di un terzo (furti, atti di terrorismo, calamità naturali, ecc.).

All'interno del rischio operativo si trova il rischio connesso ai Sistemi Informativi, o rischio ICT, che, a sua volta, è riconducibile a:

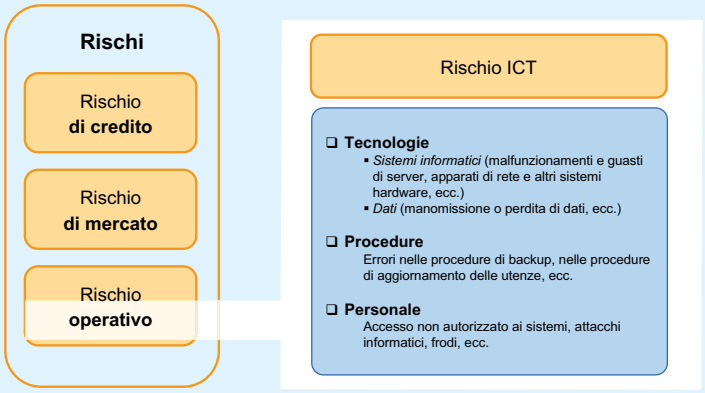
- tecnologie:
  - sistemi informatici (malfunzionamenti e guasti ai server, agli apparati di rete e ad altri sistemi hardware, ecc.);
  - dati (manomissione o perdita dei dati, ecc.);
- procedure:
  - di backup, di aggiornamento delle utenze, ecc.;
- personale:
  - accesso non autorizzato ai sistemi, attacchi informatici, frodi, ecc.

In particolare, Basilea 2 individua tre possibili approcci per valutare l'ammontare di patrimonio da accantonare per il rischio operativo: il Basic Indicator Approach (BIA), lo Standardized Approach (SA) e l'Advanced Measurement Approach (AMA).

Tra questi, il Comitato di Basilea ha ribadito l'importanza dell'applicazione del metodo AMA, flessibile ed esauriente nella misurazione dei rischi operativi e in grado di cogliere le esposizioni più significative. A questo proposito, lo stesso Comitato ha definito rigorosi standard di natura qualitativa, che dovranno essere rispettati. Le banche dovranno rilevare sistematicamente i dati più importanti legati a queste tipologie di rischi, inclusi i dati di perdita, e, da un punto di vista qualitativo, creare incentivi per migliorare la gestione dei rischi operativi all'interno dell'impresa nel suo complesso. Sono poi richiesti alcuni requisiti addizionali, in particolare la programmazione e l'attuazione di metodi di valutazione e di strategie, nonché controlli e azioni correttive. È necessario il rispetto di procedure rigorose, che passino per un sistema capillare di rilevazione dei dati di perdita, su base continuativa e per un periodo di osservazione minimo di 3-5 anni, al fine di giungere a stime empiriche della rischiosità. Possono essere utilizzati anche dati esterni, provenienti da iniziative interbancarie organizzate su base consortile, definendo adeguate procedure di raccordo dei dati.

Figura 3.2

Il rischio ICT all'interno del rischio operativo in base al modello di Basilea 2



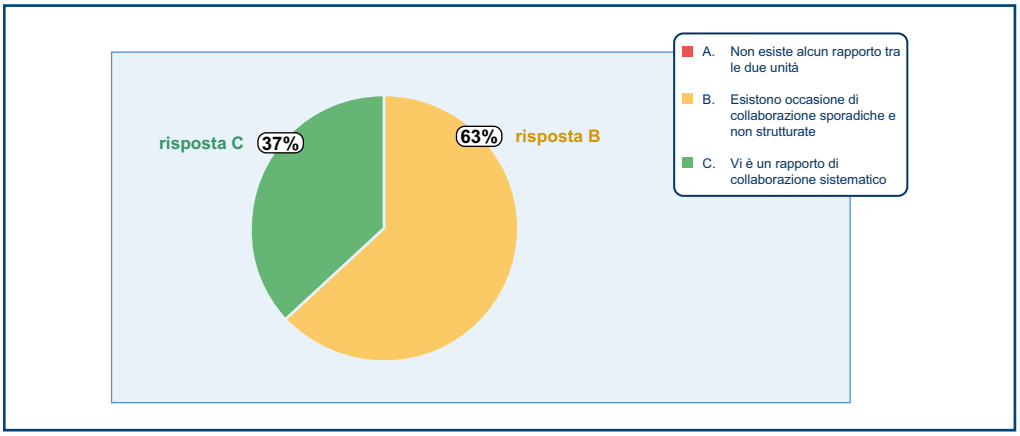
L'integrazione tra ICT Security ed Enterprise Risk Management: i risultati della Ricerca

Sulla base dei presupposti illustrati nel precedente paragrafo, nell'ambito della Ricerca 2009 si è cercato di capire quale sia effettivamente il rapporto tra l'ICT Security e l'Enterprise Risk Management. In questa prima fase l'analisi si è focalizzata sul settore del Banking, viste le peculiarità che caratterizzano tale comparto, come illustrato nel paragrafo precedente. Anche in questo caso il tema è stato trattato con CIO, CISO e Operational Risk Manager, sia nell'ambito di case studies, sia attraverso una Survey estesa.

Il primo dato che emerge dalla Survey (Figura 3.3) appare confortante, in quanto nessuno dei rispondenti ha indicato la mancanza di qualsiasi tipo di rapporto tra ERM e ICT Security. Tuttavia, occorre anche sottolineare che solo poco più di un terzo (37%) delle realtà indagate risulta avere un rapporto di collaborazione sistematico, mentre in tutti gli altri casi si hanno solo relazioni sporadiche e comunque non strutturate, tant'è che il livello di integrazione complessivo viene definito "basso" dai rispondenti.

Figura 3.3

Il livello di interazione tra l'ICT Security e l'Enterprise Risk Management nella definizione del modello di valutazione del rischio ICT



Questa limitata interazione (peraltro confermata anche dalle interviste condotte de visu con CISO e Operational Risk Manager) fa nascere qualche dubbio su come il rischio ICT venga realmente incorporato all'interno del rischio operativo per la valutazione del rischio complessivo.

La Ricerca, quindi, si è focalizzata proprio su questo aspetto, declinandolo secondo alcune dimensioni:

- il livello di coinvolgimento dell'ERM nella definizione delle metodologie di Risk Analysis utilizzate dall'ICT Security per la propria operatività;
- il grado di utilizzo da parte dall'ERM delle elaborazioni effettuate dall'ICT Security;
- la visibilità dell'ICT Security sul processo valutazione dei rischi aziendali complessivi effettuato dall'ERM;
- l'influenza delle valutazioni dei rischi ICT effettuate a livello di Enterprise Risk Management nella scelta delle priorità d'intervento per la mitigazione dei rischi ICT;
- l'importanza attribuita dal Top Management ai rischi ICT all'interno del quadro generale dei rischi aziendali.

Con riferimento al primo punto, il 75% dei CIO e CISO rispondenti ha evidenziato un ruolo limitato dell'ERM, che nel 56% si pone come "consulente" dell'ICT Security, mentre nel 19% non interviene in alcun modo nel processo di definizione della metodologia (Figura 3.4). Solo il 25% dei CIO e CISO del panel della Survey evidenzia una partecipazione attiva dell'ERM nella scelta o definizione della metodologia di ICT Risk Analysis.

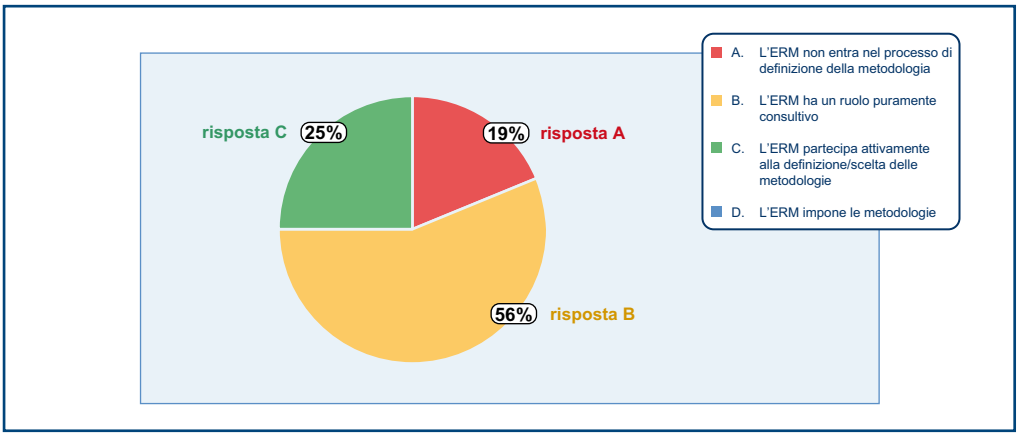


Figura 3.4

Il livello di coinvolgimento dell'ERM nella definizione delle metodologie di Risk Analysis utilizzate dall'ICT Security

Per quanto riguarda invece il grado di utilizzo delle elaborazioni effettuate dall'ICT Security da parte dell'ERM, il panorama appare più variegato (Figura 3.5). Infatti, solo nell'11% dei casi non vi è collaborazione tra le due unità su questo aspetto, in quanto è l'ERM a effettuare autonomamente la valutazione stessa. Nel 50% dei casi l'ICT Security si limita a fornire solo i dati di input e lascia le successive elaborazioni all'ERM. Al contrario, il 39% dei rispondenti dichiara che l'ICT Security effettua una propria analisi. Questo output viene poi utilizzato dall'ERM nel processo di analisi dei rischi complessi dell'impresa.

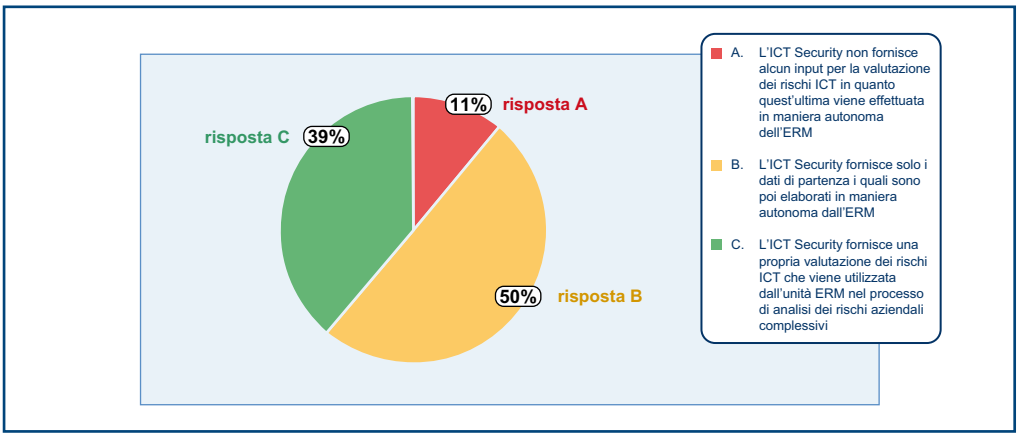


Figura 3.5

La tipologia di informazioni fornite dall'ICT Security all'ERM per la valutazione dei rischi complessivi d'impresa

Un ulteriore aspetto oggetto di indagine è costituito dal grado di visibilità dell'unità ICT Security sul processo di valutazione complessiva dei rischi aziendali effettuata dall'ERM. Questo è un punto chiave per capire il reale grado di integrazione tra le due unità, al di là degli aspetti strettamente legati alla sicurezza ICT.

Le interviste hanno infatti messo in luce come in alcuni casi l'ICT Security si limiti a fornire solamente dei dati di base, che poi l'Enterprise Risk Management elabora al suo interno. In questi casi, l'ICT Security non sa come questi dati verranno elaborati e utilizzati nell'ambito dei processi di valutazione del rischio operativo, e, tantomeno, quale sia l'esito di questa analisi. Questo ridotto livello di interazione presenta degli elementi di criticità. In particolare, in questo modo l'ERM non fa tesoro dei risultati delle analisi svolte dall'ICT Security per la gestione delle proprie attività, né può attingere al bagaglio di esperienza e alla profonda conoscenza delle peculiarità della sicurezza informatica che solo chi gestisce quotidianamente queste attività può possedere.

Inoltre, dal momento che l'ICT Security non è informata sui risultati delle valutazioni effettuate dall'ERM, non vi è alcun feedback sulle attività di pianificazione, per cui si corre il rischio che le iniziative previste dall'ICT Security nell'orizzonte di pianificazione non siano in realtà mirate a eliminare delle criticità emerse nel corso delle analisi effettuate

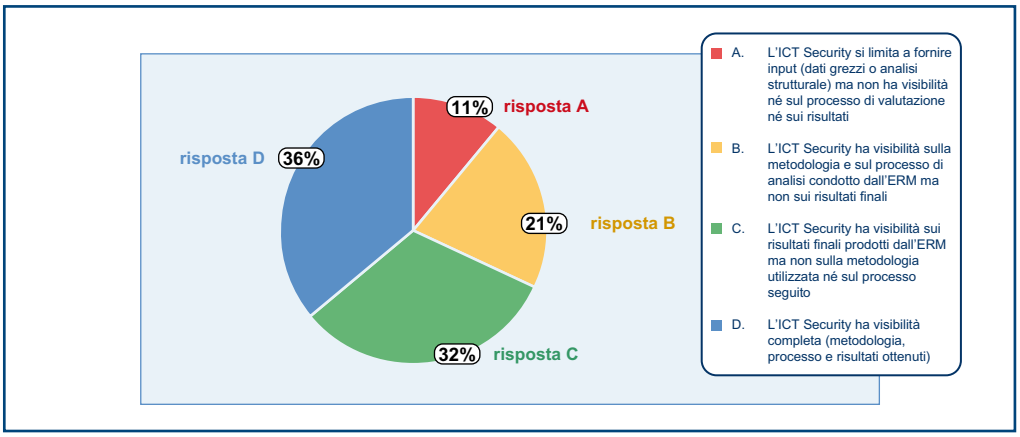
dall'ERM. Questo scollamento è dovuto principalmente al fatto che spesso si ritiene che gli approcci e le metodologie usate per l'ICT Risk Analysis nell'ambito dell'ICT Security non siano replicabili e riutilizzabili anche ai fini dell'Enterprise Risk Management, che ricorre solitamente a metodologie maggiormente orientate ai processi e comunque "di più alto livello", trascurando i dati di dettaglio e quelli più "tecnici"[1].

[1] Per quanto concerne i diversi approcci alla ICT Risk Analysis si rimanda al Capitolo 2.

I risultati della Survey sembrano confermare le evidenze empiriche emerse nel corso delle interviste one to one, anche se il quadro che ne deriva è caratterizzato da una certa eterogeneità (Figura 3.6). La visibilità completa dell'ICT Security sul processo di valutazione dei rischi aziendali si verifica infatti nel 36% delle imprese rispondenti. Negli altri casi l'ICT si limita a fornire i dati grezzi (11%), ha visibilità solo sulla metodologia e sul processo ma non sui risultati finali (21%), oppure ha visibilità solo sui risultati finali, ma non sul processo e sulla metodologia utilizzati per raggiungerli (32%).

Figura 3.6

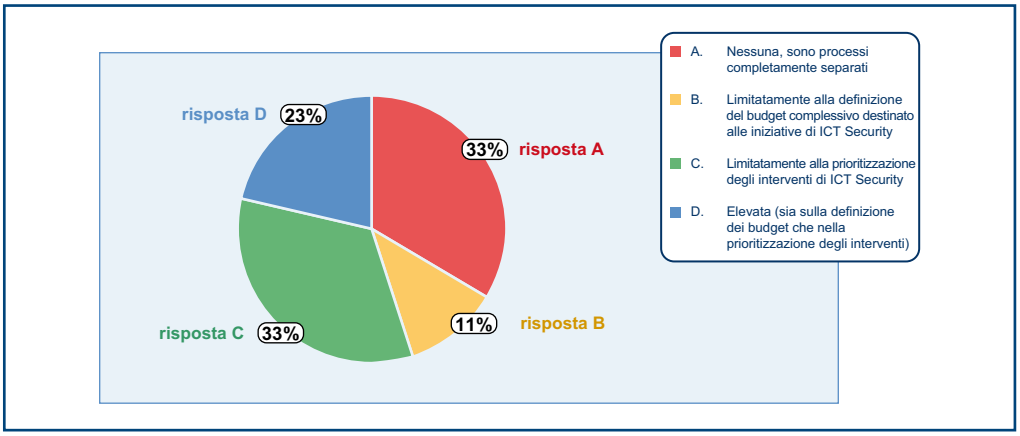
La visibilità dell'ICT Security sul processo di valutazione dei rischi aziendali complessivi effettuato dall'ERM



È stato inoltre chiesto ai CISO quale sia l'impatto dei risultati delle analisi effettuate dall'ERM sui piani di ICT Security (Figura 3.7): si è cercato di capire quanto pesino le analisi dell'ERM nella definizione delle priorità di intervento in ambito ICT Security. I risultati sono anche in questo caso interessanti: un terzo dei rispondenti ritiene che le valutazioni dei rischi ICT effettuate dall'ERM non influiscano affatto sulla scelta delle priorità d'intervento per la mitigazione dei suddetti rischi. Nell'11% dei casi invece si ritiene che l'influenza sia limitata alla definizione del budget complessivo delle iniziative di ICT Security (senza scendere nel merito delle iniziative), mentre un altro terzo dei rispondenti afferma che i risultati delle analisi svolte dall'ERM impattano sulla definizione delle priorità di intervento in ambito ICT Security. Infine, il restante 23% del panel ritiene che il legame sia molto stretto e che vi sia influenza sia sull'identificazione dei programmi da attuare per mitigare i rischi sia sul relativo budget.

Figura 3.7

L'influenza delle valutazioni dei rischi ICT a livello di ERM nella scelta delle priorità di intervento per la mitigazione dei rischi ICT



Le possibili conseguenze e criticità di questo scollamento tra ICT Security ed Enterprise Risk Management consistono nella sottovalutazione del rischio legato all'ICT nell'ambito dei rischi operativi, soprattutto dovuto alla bassa rilevanza strategica attribuita alla sicurezza ICT. Questa non viene resa partecipe, poiché l'Enterprise Risk Management lavora utilizzando il suo approccio senza coinvolgerla nelle analisi e i dati vengono richiesti, ma senza conoscerne il fine all'interno del quadro complessivo.
Proprio questo inasprimento delle barriere fa si che il budget allocato all'attività di ICT Security rimanga pressoché stabile. La maggiore criticità è il rischio di perdere l'opportunità per far comprendere la rilevanza strategica dell'ICT Security e quindi la possibilità, per questa, di acquisire una maggior influenza all'interno dell'azienda.

Alla luce dei dati fin qui presentati, appare piuttosto sorprendente il risultato del quesito, in cui si chiede ai CISO di esprimere un giudizio sul livello di rilevanza attribuita ai rischi ICT, in rapporto alle altre tipologie di rischi aziendali. Come si può notare dalla Figura 3.8, in più dei due terzi dei casi si afferma che i rischi ICT rivestono un'importanza media all'interno dei rischi aziendali (69%), mentre nel 26% dei casi rappresentano la principale categoria di rischio. Solo per il 5% dei CISO l'importanza attribuita dall'ERM ai rischi ICT è da considerarsi bassa.
Si tratta di un risultato apparentemente confortante, ma è necessario fare due importanti considerazioni in merito:

- il giudizio può essere in qualche modo "viziato" dalla relativamente ridotta visibilità dei CISO sulle metodologie adottate dall'ERM per la valutazione dell'esposizione complessiva al rischio;
- è possibile che vi sia un "bias" legato al ruolo del rispondente. In altri termini, è possibile che alcuni CISO sovrastimino l'importanza attribuita dall'ERM ai rischi ICT, in quanto tendono ad applicare i propri schemi mentali e i propri metri di giudizio, in base ai quali il rischio informatico è sicuramente molto rilevante.

La contro intuitività dei risultati ottenuti sembra essere confermata anche dalle interviste condotte con CISO e Operational Risk Manager, da cui sembra emergere che il rischio operativo sia in realtà ancora di gran lunga sottovalutato rispetto a rischio di credito e finanziario, e che, al suo interno, venga ancora data più rilevanza alla sicurezza fisica e/o organizzativa, rispetto a quella legata alle tecnologie informatiche.

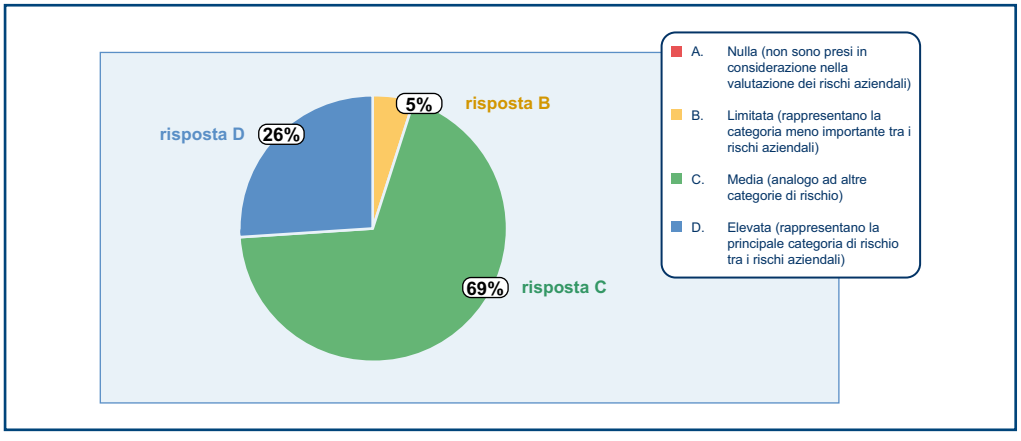


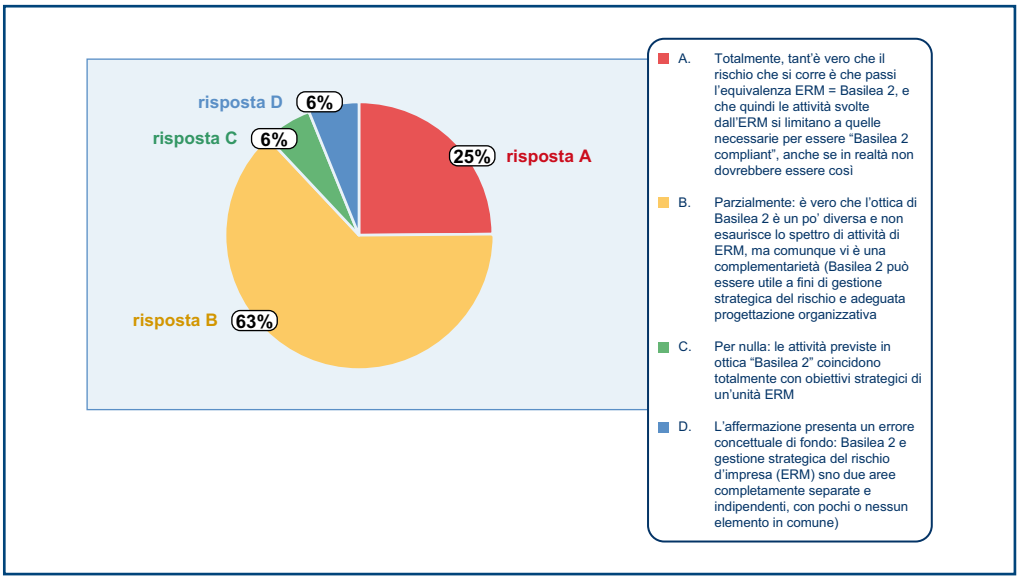
Figura 3.8

La percezione dei CISO sull'importanza che viene attribuita dal Top Management ai rischi ICT all'interno del quadro generale dei rischi aziendali

Un ultimo punto toccato dalla Ricerca ha approfondito il ruolo esercitato da Basilea 2 nel processo di crescita dell'ERM. Se da un lato è chiaro che Basilea 2 ha rappresentato e rappresenta tuttora un elemento di "trigger" importante per l'accelerazione del processo di sviluppo di una cultura integrata del rischio all'interno delle organizzazioni, è altresì vero che l'impostazione data da Basilea 2 potrebbe costituire un limite e portare a modelli organizzativi "distorti" o comunque poco virtuosi.

In relazione a questo aspetto, le opinioni degli intervistati si dividono nuovamente (Figura 3.9), anche se va detto che la maggioranza dei CISO rispondenti (63%) concorda sul fatto che Basilea 2, pur presentando dei limiti, costituisce comunque una buona base sulla quale costruire un sistema di gestione integrata del rischio. È altresì interessante notare che un quarto dei rispondenti vede invece in Basilea 2 una potenziale problematica, in quanto comporta un'ottica eccessivamente "compliance oriented", quindi reattiva e non proattiva, nella gestione del rischio.

Figura 3.9
Il punto di vista sul livello di "overlapping" tra ERM e Basilea 2



In sintesi, è possibile concludere che l'integrazione tra Enterprise Risk Management e ICT Security nel Banking in molte realtà ha, appena mosso i primi passi. Come in tutti i processi di innovazione organizzativa così "importanti", vi sono alcuni casi di eccellenza (costituiti in particolare da alcune banche estere), che nel corso delle interviste svolte nell'ambito dei case studies hanno messo in luce un livello di strutturazione dei processi e di definizione delle procedure piuttosto avanzato, tanto che è possibile affermare che in queste realtà tutte le decisioni (ivi comprese quelle relative all'area ICT Security) sono prese considerando esplicitamente gli impatti sul profilo di rischio complessivo dell'organizzazione. Nel contempo, però, la stragrande maggioranza delle realtà esaminate si trova in uno stadio d'avanzamento molto più arretrato, anche se esistono chiari segnali di un certo "dinamismo", che rende necessario monitorare l'evoluzione del fenomeno.

È inutile sottolineare che l'introduzione di un sistema di gestione integrata del rischio è un'innovazione che presenta dei forti risvolti culturali e di potere. Nell'ottica di tale integrazione è infatti emersa da alcune interviste l'ipotesi che, trattando l'ICT Security di rischi legati all'azienda, nel medio-lungo termine le sue responsabilità saranno inglobate all'interno dell'ERM.

Secondo alcuni esperti di ICT Security, questo scenario presenta però diversi rischi, tra cui una perdita di profondità dell'analisi tecnica, una distanza eccessiva tra chi si occupa di governance e chi deve poi individuare le soluzioni tecnologiche e organizzative, un impoverimento delle competenze. Un'ulteriore criticità è rappresentata da una focalizzazione, da parte dell'ERM, sulle aree di rischio più "vicine" culturalmente, con una conseguente perdita di rilevanza dei rischi informatici, che sicuramente non rientrano tra queste.

A questo si aggiunge Basilea 2, che, come si è visto precedentemente, rischia di portare a un approccio eccessivamente "burocratico", più attento alla compliance delle direttive che a una vera gestione strategica del rischio aziendale.

Inoltre, il quadro è ulteriormente complicato dalla nascita di nuove unità organizzative (quale ad esempio quella che si occupa di "compliance"), caratterizzate da aree di potenziale overlapping sia con l'Enterprise Risk Management che con l'ICT security.
In ogni caso, ammesso che tali rischi siano reali, sicuramente la risposta non consiste nell'isolamento nella torre d'avorio e nella "sindrome dell'incompreso" che a volte contraddistingue gli specialisti di ICT Security. È invece necessario cercare un dialogo continuo e costruttivo con le altre unità organizzative, utilizzando un linguaggio il più possibile comprensibile ai "non addetti ai lavori", che aiuti a far percepire la rilevanza strategica dell'ICT Security e a garantirle il corretto "peso" all'interno dell'organizzazione.

UniCredit Group Box 3.2

UniCredit Group è uno dei maggiori gruppi bancari europei, risultato della fusione di nove fra le principali banche italiane e dalle successive aggregazioni con il Gruppo tedesco HVB e l'italiano Capitalia. In Italia UniCredit presidia i diversi segmenti di mercato tramite le proprie banche Retail, Corporate e Private.

UniCredit Group possiede da sempre al proprio interno un'azienda specializzata nella fornitura di servizi informativi a 360° all'intero Gruppo, UGIS (UniCredit Global Information Services). UGIS dopo il merger con le società informatiche del Gruppo HVB, è oggi un'azienda di oltre 4.500 dipendenti, distribuiti in 19 sedi in otto Paesi europei.

In UGIS sono previste alcune tipologie di Risk Analysis: una è legata alla nascita dei progetti applicativi e una, periodica ed effettuata per ambiti ristretti, legata al DPS e al disaster recovery. Dal 2006 viene utilizzato, nell'ambito della gestione del rischio operativo, un sistema interno per il monitoraggio riguardante la perdita delle informazioni. I rischi, se conosciuti, vengono calcolati sulla base di serie storiche, altrimenti si procede con la creazione delle analisi di scenario. Questa attività è realizzata con l'aiuto di esperti di processo, oppure grazie a database che raccolgono eventi accaduti anche ad aziende bancarie esterne al gruppo. Una volta effettuata l'analisi di scenario, i risultati vengono condivisi con gli utenti interni di UGIS.

La classificazione prevede la combinazione di impatto e probabilità di accadimento. La metodologia, proveniente dalle linee guida definite da Basilea 2, prevede che annualmente vengano eseguite almeno sette analisi, oltre alla revisione di quelle eseguite precedentemente, una per ciascuna delle diverse categorie di rischio. Un'ulteriore attività, che viene condotta all'interno di UGIS, è costituita dalla verifica dei controlli interni per la mitigazione del rischio, attività prevista dalla Legge 262.

La funzione rischi operativi, comprendente i rischi ICT, è stata formalizzata in UGIS dal 2006 in seguito alle norme previste da Basilea 2. Grazie a una serie di indicatori storici (rilevati sin dal 2002), è stato ad esempio possibile evidenziare la stabilità nel numero e nell'impatto degli incidenti accaduti ai sistemi (il cosiddetto downtime), stabilità ovviamente caratterizzata da fluttuazioni casuali, per quanto contenute, e interrotta solo in occasione di eventi particolarmente rari ed eccezionali (2 casi nei 7 anni di osservazione). In generale, nel mondo bancario italiano, l'attenzione riservata ai rischi ICT è piuttosto limitata: questi rappresentano, infatti, solo una piccola parte dei rischi operativi, che, tra l'altro, in momenti di crisi finanziaria come quelli attuali, hanno un peso relativamente basso all'interno del sistema di Enterprise Risk Management.

Per quanto riguarda la collaborazione tra Sicurezza ICT e Operational Risk Management (che include la funzione di Compliance e Legal), non esiste una formalizzazione a livello organizzativo, ma le interazioni sono comunque molto frequenti, soprattutto in punto di valutazione integrata del rischio operativo. È stato recentemente creato un comitato, il Risk Integration Team, che si occupa di monitoraggio degli eventi, di elaborazione delle policy e di risk integration, e fa riferimento al comitato esecutivo di Risk Management, che decide le linee strategiche per il

management e approva le proposte di risk mitigation più rilevanti. Il collante tra questi due comitati è proprio rappresentato dalle figure dell'Operational Risk Management e del responsabile dell'ICT Security.

Nota metodologica

Gli obiettivi generali dell'Osservatorio Information Security Management sono:
- analizzare e comprendere criticamente lo "stato dell'arte" dell'information security, in relazione ai trend e alle best practice emergenti (con particolare riferimento agli aspetti organizzativo-gestionali) e ai fabbisogni (espressi ed inespressi) delle imprese;
- creare e diffondere la conoscenza su questo tema in Italia, contribuendo ad una maggiore sensibilizzazione e consapevolezza della rilevanza strategica dell'information security (e di una sua corretta gestione);
- costituire il punto di riferimento per la community di attori (studiosi, consulenti, imprese) interessati a promuovere lo sviluppo strategico dell'information security nelle imprese.

In particolare, gli obiettivi del secondo anno di Ricerca sono stati:
- analizzare i trend emergenti del mondo ICT Security, in termini di configurazione organizzativa, risorse umane e budget dedicato;
- definire le possibili tipologie di Risk Analysis esistenti, confrontando il settore Banking, storicamente più sensibile a questi temi, con altri settori quali: Assicurativo, Automotive, Chimico e Farmaceutico, ICT e Telecomunicazioni, Utility;
- analizzare gli aspetti metodologici e i diversi strumenti utilizzati per questa fondamentale fase dell'information security management system;
- valutare il grado di maturità e formalizzazione degli approcci utilizzati per l'ICT Risk Analysis, evidenziando trend e modelli ricorrenti, e approfondendone, anche alla luce di normative di riferimento, il rapporto tra ICT Security ed Enterprise Risk Management nel settore Banking.

Per rispondere a questi obiettivi si è scelto di affiancare tre modalità di indagine:
- l'analisi di casi di oltre 15 realtà bancarie italiane e internazionali attraverso interviste a Chief Information Security Officer, Risk Manager e Operational Risk Manager;
- una Survey che ha coinvolto più di 70 Chief Information Security Officer appartenenti al settore Banking;
- una Survey che ha coinvolto più di 400 Chief Information Officer di imprese di medio-grandi dimensioni appartenenti ai settori Assicurativo, Automotive, Banking, Chimico e Farmaceutico, ICT e Telecomunicazioni, Utility.

I risultati delle tre analisi sono stati confrontati e "triangolati" in modo da ottenere una migliore interpretazione dei fenomeni. Di seguito si descrivono brevemente il panel e la metodologia utilizzata nelle analisi.

Il panel della Ricerca

Nel secondo ciclo di studio sono stati intervistati i Chief Information Officer, i Chief Information Security Officer, i Risk Manager e gli Operational Risk Manager di realtà bancarie italiane e internazionali, tra cui: BNP Paribas, Banca Popolare di Sondrio, Cariparma, Credem, Credit Suisse, Deutsche Bank, Intesa Sanpaolo, UBI Banca, UniCredit Group.

In ciascuna intervista sono stati analizzati approfonditamente sia il contesto e la configurazione organizzativa attuale dell'azienda sia il tema dell'ICT Risk Analysis. Infine è stata analizzata la relazione tra Information Security ed Enterprise Risk Management, evidenziandone i rischi e le opportunità, e l'evoluzione delle politiche di budgeting.

I casi sono stati realizzati attraverso analisi documentali seguite da interviste dirette. L'intervista è stata condotta attraverso un protocollo che comprende l'uso di un questionario semi-strutturato, utilizzato come guida per la raccolta delle informazioni.

I temi trattati nell'intervista sono stati:
- il contesto aziendale;
- l'organizzazione e il ruolo della Direzione ICT;
- il modello organizzativo attuale e sua evoluzione a seguito dei cambiamenti apportati;
- l'ICT Risk Analysis in termini di responsabilità, caratteristiche, input, metodologie;
- il rapporto con l'Enterprise Risk Management;
- le politiche di budgeting.

Grazie ai risultati delle Survey è stato possibile validare ed estendere alcuni dei principali risultati emersi dalle interviste.

La Survey ai CISO

La Survey è stata erogata ai Chief Information Security Officer, con oltre 70 questionari inviati. Obiettivo dichiarato dell'iniziativa è stato analizzare i diversi approcci all'ICT Risk Analysis e il loro ruolo nell'ambito dell'Enterprise Risk Management.

Il questionario è stato realizzato in modo da essere uno strumento accessibile via web di facile e univoca compilazione. Allo scopo di facilitarne la comprensione ed evitare possibili ambiguità, tuttavia, è stato previsto un servizio di assistenza telefonica e via mail.

Partendo dal panel selezionato, e a seguito di un unico recall, è stato ottenuto un tasso di risposta complessivo del 35%.

Il questionario si concentra su:
- le tipologie di ICT Risk Analysis effettuate all'interno dell'azienda;
- le motivazioni che spingono all'attivazione di ICT Risk Analysis;
- le caratteristiche delle ICT Risk Analysis;
- la relazione tra ICT Security ed Enterprise Risk Management.

Grazie ai risultati della Survey è stato possibile validare ed estendere alcuni dei principali risultati dell'analisi e identificare priorità e bisogni di approfondimento relativi al tema dell'ICT Security nel settore Banking.

La Survey ai CIO

La Survey è stata erogata ai Chief Information Officer, con oltre 400 questionari inviati. Obiettivo dichiarato dell'iniziativa è stato analizzare lo stato dell'arte della governance dell'ICT Security e i diversi approcci all'ICT Risk Analysis.

Il questionario è stato realizzato in modo da essere uno strumento accessibile via web di facile ed univoca compilazione. Allo scopo di facilitarne la comprensione ed evitare possibili ambiguità, tuttavia, è stato previsto un servizio di assistenza telefonica e via mail.

Partendo dal campione selezionato, e a seguito di un unico recall, è stato ottenuto un tasso di risposta complessivo del 24%.

Il questionario si concentra su:
- la strutturazione dell'unità di ICT Security;
- il processo di pianificazione e controllo e le funzioni coinvolte;
- il budget di ICT Security e il suo trend;
- le principali aree di investimento, attuali e future, nell'ambito della sicurezza ICT;
- i fattori critici di successo e la misura delle prestazioni per i progetti di ICT Security;
- le tipologie di ICT Risk Analysis effettuate all'interno dell'azienda;
- le motivazioni che spingono all'attivazione di ICT Risk Analysis;
- le caratteristiche delle ICT Risk Analysis;
- la relazione tra ICT Risk Management ed Enterprise Risk Management.

Grazie ai risultati della Survey è stato possibile approfondire il tema generale della governance, e validare ed estendere alcuni dei principali risultati dell'analisi relativi al tema dell'ICT Security, identificando priorità e bisogni di approfondimento.

Il Workshop Banking

L'obiettivo dichiarato del Workshop Banking è stato interpretare in modo collaborativo i risultati preliminari emersi dalle interviste e dalla Survey. Gli spunti emersi dal Workshop Banking sono stati preziosi per sviluppare e approfondire i risultati della Ricerca e discuterne le implicazioni.

Le banche che hanno partecipato al Workshop sono state: Banca Mediolanum, Banca Popolare di Milano, Bankadati – Gruppo Credito Bancario Valtellinese, Citigroup, Credit Suisse, Deltas – Gruppo Credito Bancario Valtellinese, Deutsche Bank, ING Direct N.V., International Barclays Bank, Società Gestione Servizi BP, UniCredit Global Information Services, UniCredit Group, We@service – Gruppo Bipiemme.

Il Gruppo di Lavoro

Paolo Maccarrone
Luca Marzegalli

Marco Pozzoni

Silvia Cavenago

Rocco Mazzei
Giulio Narciso

Per qualsiasi commento e richiesta di informazioni:

marco.pozzoni@polimi.it

La School of Management

La School of Management del Politecnico di Milano

La School of Management del Politecnico di Milano è stata costituita nel 2003.
Essa accoglie le molteplici attività di ricerca, formazione e alta consulenza, nel campo del management, dell'economia e dell'industrial engineering, che il Politecnico porta avanti attraverso le sue diverse strutture interne e consortili.

Fanno parte della Scuola: il Dipartimento di Ingegneria Gestionale, le Lauree e il PhD Program di Ingegneria Gestionale e il MIP, la business school del Politecnico di Milano, focalizzata in particolare sulla formazione executive e sui programmi Master.
Essa si avvale attualmente – per le sue molteplici attività di formazione, ricerca e consulenza – di oltre 240 docenti (di ruolo o a contratto, italiani o di provenienza estera) e di circa 80 dottorandi e collaboratori alla ricerca.

La School of Management ha ricevuto l'accreditamento EQUIS, creato nel 1997 come primo standard globale per l'auditing e l'accreditamento di istituti al di fuori dei confini nazionali, tenendo conto e valorizzando le differenze culturali e normative dei vari Paesi.

Le attività della School of Management legate ad ICT & Strategia si articolano in:
- Osservatori *ICT & Management*, che fanno capo per le attività di ricerca al Dipartimento di Ingegneria Gestionale;
- formazione executive e programmi Master, erogati dal MIP.

Gli Osservatori *ICT & Management*

Gli Osservatori *ICT & Management* della School of Management del Politecnico di Milano (www.osservatori.net), che si avvalgono della collaborazione del ICT Institute del Politecnico di Milano, vogliono offrire una fotografia accurata e continuamente aggiornata sugli impatti che le tecnologie dell'informazione e della comunicazione (ICT) hanno in Italia su imprese, pubbliche amministrazioni, filiere, mercati, ecc.
Guardare all'impatto che le nuove tecnologie hanno sulle imprese – sul loro modo di dimensionarsi, organizzarsi, rapportarsi – e di converso al ruolo propulsivo che i bisogni originati dalle trasformazioni nelle imprese hanno sullo sviluppo di nuove tecnologie è un qualcosa di connaturato all'ingegneria gestionale sin dalla sua nascita.
E le ICT rappresentano sicuramente, da questo punto di vista, un terreno estremamente fertile – e apparentemente inesauribile – di studio.

Gli Osservatori affrontano queste tematiche con lo stile tipico della School of Management del Politecnico di Milano: che è quello di coniugare l'analisi "sperimentale" minuta dei singoli casi reali con il tentativo di costruire quadri di sintesi credibili, di guardare a ciò che accade nel nostro Paese avendo come benchmark le esperienze più avanzate su scala mondiale, di razionalizzare la realtà che si osserva per tratteggiare linee guida che possano essere utili alle imprese.

Gli Osservatori sono ormai molteplici e affrontano in particolare tutte le tematiche più innovative nell'ambito delle ICT.

- B2b: eProcurement e eSupply Chain
- Business Intelligence
- Canale ICT
- eCommerce B2c
- eGovernment
- Enterprise 2.0
- eProcurement nella PA
- Fatturazione Elettronica e Dematerializzazione
- Gestione Strategica dell'ICT
- ICT Accessibile e Disabilità
- ICT in Sanità
- ICT nel Real Estate
- ICT Strategic Sourcing
- ICT & CIO nel Fashion-Retail
- ICT & PMI
- Information Security Management
- Intelligent Transportation Systems
- Intranet Banche
- Mobile Content & Internet
- Mobile Finance
- Mobile Marketing & Service
- Mobile & Wireless Business
- Multicanalità
- New Tv & Media
- NFC & Mobile Payment
- RFId
- Social Network

Riportiamo di seguito alcuni Osservatori in parte correlati all'Osservatorio Information Security Management:

- **ICT Strategic Sourcing**
- **Gestione Strategica dell'ICT**
- **ICT & PMI**

Per maggiori informazioni si veda il sito **www.osservatori.net**.

Il MIP

Gli Osservatori *ICT & Management* sono fortemente integrati con le attività formative della Scuola: nel senso che rappresentano una importante sorgente per la produzione di materiale di insegnamento e di discussione per i corsi e traggono anche spesso linfa vitale dalle esperienze di coloro che partecipano ai corsi (in particolare a quelli post-universitari erogati dal MIP) o vi hanno partecipato nel passato.

In sinergia con gli Osservatori, il MIP Politecnico di Milano ha lanciato diverse iniziative nell'ambito ICT & Management:

- **EMBA ICT – Executive Master of Business Administration ICT**
- **Corso Executive in Gestione Strategica dell'ICT**
- **Corsi Brevi ICT&Management**
- **Corso di Alta Formazione in Information Security Management**

Per maggiori informazioni si veda il sito **www.mip.polimi.it**.

L'ICT Institute

POLITECNICO DI MILANO

ict institute

DIPARTIMENTO DI ELETTRONICA E INFORMAZIONE

CEFRIEL FORGING INNOVATION

L'ICT Institute del Politecnico di Milano

In risposta alla diffusione senza precedenti dell'ICT negli ultimi decenni, che ha cambiato profondamente il modo di fare ricerca e innovazione, il Politecnico di Milano ha creato l'ICT Institute (http://ictinstitute.polimi.it/).

Questa istituzione comprende il Dipartimento di Elettronica e Informazione (DEI), La Facoltà di Ingegneria dell'Informazione, la società consortile CEFRIEL e gli Spin-off nel campo dell'ICT. Tutti questi enti partecipano all'iniziativa con ruoli complementari: il DEI si dedica alla ricerca avanzata, la Facoltà alle attività didattiche nel settore dell'Informazione, il CEFRIEL e gli Spin-off alla progettazione e realizzazione di prodotti e servizi innovativi.

I fondamenti della ricerca in ICT svolta dall'ICT Institute

L'ICT Institute promuove anche l'integrazione dei programmi didattici della Facoltà dell'Ingegneria dell'Informazione con l'offerta didattica a livello di Master gestita dal CEFRIEL e con il programma di Dottorato del DEI.

I numeri dell'ICT Institute

L'ICT Institute del Politecnico di Milano è uno dei centri di ricerca in ICT più grandi d'Europa. Al suo interno operano circa 1000 persone, tra professionisti, docenti e ricercatori. Il budget complessivo degli enti partecipanti si aggira intorno ai 25 milioni di Euro all'anno.

I sostenitori della Ricerca

Partner

- IBM
- KPMG
- Symantec

Supporter

- Venticento

IBM
www.ibm.com/it

Azienda globale leader nell'Information Technology, **IBM** Corporation (Armonk, NY) opera in 170 paesi con 398.500 dipendenti con un giro d'affari che, nel 2008, hanno raggiunto i 103,6 miliardi di dollari. IBM costruisce e attua, insieme ai propri clienti, piani e progetti per l'innovazione e la competività basati sulle più avanzate soluzioni di information technology. Il valore unico che tali soluzioni trasferiscono al mercato nasce dall'integrazione di hardware e software, leader per prestazioni e affidabilità, con una gamma di servizi tecnologici e consulenziali specializzati per le diverse aree industriali: da quello manifatturiero a quello finanziario, dalla grande distribuzione alle piccole e medie imprese, dalle telecomunicazioni alla pubblica amministrazione.

IBM e' la prima societa' di informatica in Italia, dove e' presente dal 1927.
Partner di aziende e istituzioni in progetti spesso all'avanguardia e comunque sempre innovativi, ha contribuito ad ammodernare le infrastrutture e i modelli di business, sostenendo la competitività dell'intero sistema paese. Oggi, la IBM Italia è una realtà con un giro d'affari prossimo ai 2 miliardi e mezzo di euro (operazioni nazionali) che opera con filiali e centri di supporto tecnico su tutto il territorio nazionale e si avvale della collaborazione di una rete di oltre 3.500 business partner.

In Italia la IBM svolge anche attività di sviluppo software e di ricerca applicata che fanno capo al Rome Tivoli Laboratory, con una missione mondiale nel campo del software di rete, e ai centri di sviluppo soluzioni a Napoli, Bari, Catania e Cagliari. All'innovazione per la Pubblica Amministrazione è dedicato l'e-Government Open Solution Center, aperto a Roma nel 2005.

Sicurezza

Per un'azienda la crescita sostenibile dipende da una strategia di sicurezza allineata al business: i clienti di tutto il mondo lavorano con IBM per ridurre le complessità della sicurezza e gestire strategicamente il rischio. Le soluzioni IBM per la security combinano in diversa misura servizi consulenziali con tecnologie hardware e software, a seconda delle varie esigenze delle aziende, sia nel mercato enterprise che in quello delle medie e piccole imprese.
Nel corso degli ultimi anni IBM ha effettuato significativi investimenti nell'area della sicurezza per la creazione di asset e metodologie a supporto della governance e del risk management, nonché per l'acquisizione di aziende leader nel mercato delle soluzioni e dei servizi di sicurezza che hanno ulteriormente arricchito l'offerta IBM, rendendola anora più completa, modulare e basata sugli standard.
In particolare, il team di ricerca X-Force cataloga, analizza e conduce ricerche sulle divulgazioni delle vulnerabilità sin dal 1997. Con oltre 43.000 vulnerabilità della sicurezza catalogate, possiede il più grande database delle vulnerabilità del mondo. Questo database unico aiuta i ricercatori X-Force a comprendere le dinamiche che costituiscono la scoperta e la divulgazione delle vulnerabilità.

IBM collabora con enti governativi, società e istituzioni a livello mondiale e favorisce l'adozione di open standard per rafforzare i protocolli aziendali e implementare un approccio olistico alla sicurezza.

Per maggiori informazioni, www.ibm.com/security oppure www.ibm.com/services/it

KPMG è un network globale di società di servizi professionali, attivo in 145 paesi del mondo con oltre 123 mila persone. L'obiettivo di KPMG è quello di trasformare la conoscenza in valore per i clienti, per la propria comunità e per i mercati finanziari. Le società aderenti a KPMG forniscono alle aziende clienti una vasta gamma di servizi multidisciplinari, secondo standard d'eccellenza omogenei. In Italia, il network KPMG è rappresentato da diverse entità giuridiche attive nella revisione e organizzazione contabile, nel business advisory, e nei servizi fiscali e legali.

La focalizzazione su differenti settori di business ed il costante aggiornamento dei propri professionisti costituiscono un servizio professionale indipendente e di alta qualità, realizzato con competenze tecniche all'avanguardia e con l'applicazione delle metodologie più avanzate.

In particolare, gli *IT Advisory Services* di KPMG in Italia contano su oltre 400 professionisti presenti in 6 uffici e si focalizzano sullo sviluppo, sulla gestione dei sistemi informativi e sul presidio dei relativi rischi, fornendo servizi relativi a:

- *IT strategy and performance* - attraverso la controllata Nolan, Norton Italia;
- *Security, IT Risk & Compliance* - attraverso la struttura Information Risk Management;
- *Solutions* – attraverso la struttura Enterprise Solutions;

La struttura *Information Risk Management* di KPMG assiste le aziende nella valutazione e nello sviluppo di strategie e soluzioni a supporto del business per gestire i rischi associati alla tecnologia:

- fornire valore e soluzioni per l'impresa nell'ambito della sicurezza, della compliance e della gestione dei rischi IT;
- condividere e diffondere esperienze e conoscenze;
- rendere disponibili risorse altamente qualificate e specializzate;
- effettuare valutazioni indipendenti.

In particolare, nell'ambito dei servizi di *Security, IT Risk & Compliance*, KPMG supporta le aziende nella seguenti aree progettuali:

- *Security Strategy*: definizione delle strategie di sicurezza e protezione delle informazioni;
- *Security Policy*: implementazione e verifica di framework di gestione;
- *Organizational security*: definizione di modelli organizzativi per la gestione della sicurezza;
- *Identity Management*: realizzazione di progetti IAM e/o per review di progetti esistenti;
- *Security Risk Assessment & Management*: analisi dei rischi di sicurezza e definizione di processi di gestione dei rischi;
- *Security controls & testing*: verifiche dei controlli di sicurezza su diversi ambiti tecnologici (penetration test, vulnerabilità assessment, ecc.);
- *Sicurezza fisica e protezione degli asset*: audit di sicurezza di aree critiche o particolarmente sensibili (edifici, CED, sale di controllo, ecc.) ;
- *Privacy*: verifica dei requisiti previsti dalla Legge e definizione di processi e modelli per il governo della compliance
- *Business Continuity Management*: supporto completo in tutte le attività necessarie a garantire la continuità dei processi e dei sistemi IT di supporto.

Grazie alla forte integrazione con il network globale e ad un approccio multidisciplinare unico all'interno del panorama nazionale, KPMG è in grado di assistere le aziende nei processi di allineamento dei servizi IT alle strategie aziendali, offrendo un giusto bilanciamento di rischi, innovazione, performance, con attenzione ai costi e alle best practice di settore e nel rispetto della compliance.

KPMG
www.kpmg.it

Symantec
www.symantec.com/it

Symantec è leader globale nel software per l'infrastruttura di rete e permette a imprese e utenti privati di operare in totale sicurezza in un mondo connesso. Symantec aiuta i propri clienti a proteggere l'infrastruttura, le informazioni e le interazioni grazie a soluzioni software e servizi che soddisfano le esigenze di sicurezza, disponibilità, conformità, integrità e prestazioni. Con sede a Cupertino, in California, Symantec è presente in oltre 40 paesi. Ulteriori informazioni sono disponibili all'indirizzo www.symantec.com o www.symantec.it.

Presenza globale

- Symantec è presente in più di 40 Paesi, con laboratori di ricerca e sviluppo in tutto il mondo.
- Symantec gestisce diversi Security Operation Center e Security Response Lab in posizione strategica in diverse aree del mondo, attivi 24x7.
- Lo stabilimento produttivo principale è situato a Dublino, Irlanda.
- Symantec conta oltre 2.000 professionisti dedicati al supporto in 29 centri, in grado di offrire assistenza ai clienti in 10 lingue.
- Symantec ha più di 350 brevetti depositati negli USA per tecnologie di sicurezza, gestione delle infrastrutture e conservazione dei dati per consumatori, piccole aziende e grandi imprese.

Clienti

Symantec collabora con il 99% delle aziende FORTUNE 1.000.

Consumer

Il marchio Norton di Symantec, leader tra le soluzioni di sicurezza destinate al mercato consumer, identifica i prodotti per la protezione dei desktop dei singoli utenti, della clientela home office e delle piccole aziende.

Security 2.0 è il concetto che esprime la volontà di Symantec di proteggere i consumatori che utilizzano Internet ed effettuano transazioni online: oggi infatti le minacce informatiche non sono più associate ad uno specifico dispositivo, ma possono riguardare le informazioni e le transazioni in generale. Con Security 2.0, Symantec sottolinea il proprio impegno nel garantire la sicurezza delle operazioni sensibili effettuate online dagli utenti, come ad esempio transazioni finanziarie e instant messaging, oltre a proteggerli da minacce e crimini informatici sempre più insidiosi.

Sicurezza e gestione delle informazioni

La visione di Symantec per Security 2.0 si estende anche alle aziende. Le nuove tecnologie, gli attuali modelli di business e la concorrenza su scala globale hanno modificato radicalmente il modo in cui le imprese devono proteggere infrastrutture, dati e interazioni. Symantec offre un'ampia gamma di soluzioni per la sicurezza aziendale, la conformità IT e la gestione delle informazioni.

Soluzioni Altiris

Le soluzioni Altiris consentono di automatizzare e migliorare l'amministrazione delle risorse IT, riducendo la complessità e i costi di gestione. La business unit Altiris ha una visione fortemente orientata ai servizi e propone tecnologie per la gestione delle risorse IT che aiutano i clienti ad amministrare sistemi e dati eterogenei e distribuiti, allineando il ciclo di vita dell'IT agli obiettivi di business dell'impresa.

Venticento Srl è una società, nata nel 2005, specializzata nell'erogare servizi di assistenza e consulenza nel settore IT. L'attività è focalizzata su *3 business unit:*

BU IT
vendita di hardware, realizzazione di cablaggi strutturati, realizzazione impianti telefonici, progettazione ed implementazione di sistemi di *business continuity*; assistenza di primo, secondo e terzo livello. Le attività precipue del call center sono:

- fornire supporto help desk di primo livello ai clienti, tutti i giorni lavorativi dell'anno con orario che va dalle 9 alle 18.
- utilizzare software di controllo remoto e di *help desk on demand* via web.
- mettere a disposizione dei clienti delle linee telefoniche, un sito web pubblico per inserire richieste di assistenza e, un innovativo software di *problem solving* tramite internet.
- fornire supporto di help desk di secondo livello tutti i giorni dell'anno dalle 8 alle 22.

Venticento fornisce la propria assistenza direttamente via internet. Utilizzando un software di controllo remoto, raggiungibile tramite browser, il cliente è in grado di ricevere assistenza diretta su qualsiasi postazione connessa alla rete. Questo innovativo sistema di controllo remoto, permette all'utente di essere supportato dall'help desk in tempo reale, non facendosi così carico del costo del tecnico on site, del suo spostamento e senza acquistare ulteriori licenze software. Bastano pochi passaggi per permettere al tecnico di prendere possesso della postazione di lavoro, per ricevere files o per avviare sistemi di videochiamata in modo da interagire senza costi aggiuntivi e con estrema velocità.

BU Sviluppo
rivendita ed installazione del documentale Esa Software; progettazione sistemi di comunicazione integrata per le aziende:

- Intranet;
- Project management;
- Migrazione verso extranet;
- Sviluppiamo inoltre software ad hoc, utilizzando i linguaggi di programmazione più diffusi in commercio.
- Siamo esperti nella realizzazione di siti intranet in tecnologia MOSS 2007 e SPP Team Services.

Progettiamo e realizziamo siti web utilizzando diversi linguaggi: html, xml, java, flash, gestendo internamente sia la parte di programmazione, sia quella grafica.
Realizziamo inoltre siti che interagiscono con le strutture interne delle aziende (intranet e database), con i reparti di vendita (e-commerce) e con le sedi distaccate (extranet, agenti itineranti).
Forniamo consulenti specializzati nei seguenti ambiti:

- IT management (progettazione e gestione di sistemi anche in outsourcing, co-sourcing).
- Help desk (progettazione, realizzazione, outsourcing).
- Data Ware House (in ambiente Oracle, Sql Server 2005 e 2008).

BU Products
commercializzazione, promozione ed installazione di una selezionata gamma di prodotti, quali soluzioni di sicurezza Sophos (endpoint, antispam, web security e NAC – tutti prodotti di cui abbiamo la certificazione tecnica e commerciale); gestionali per aziende e professionisti e gestionale documentale del nostro partner Esa Software; software di archiviazione sostitutiva Comped; organizzazione di una vasta serie di corsi di formazione on site nell'ambito dell'informatica.

Venticento
www.venticento.com

Impostazione grafica e impaginazione: Stefano Erba e Emanuela Micello
Stampa: Grafiche Ponzio

www.osservatori.net