istat
working
papers

N. 2
2012

Metodologie di analisi e gestione del rischio nelle istituzioni pubbliche con particolare riferimento ai processi informatici: il caso dell'Istat

Cecilia Colasanti

Istat
Istituto Nazionale
di Statistica

istat
working
papers

N. 2
2012

Metodologie di analisi e gestione del rischio nelle istituzioni pubbliche con particolare riferimento ai processi informatici: il caso dell'Istat

Cecilia Colasanti

Istat

Istat Working Papers

Metodologie di analisi e gestione del rischio nelle istituzioni pubbliche con particolare riferimento ai processi informatici: il caso dell'Istat

N. 2/2012

ISBN 88-458-1706-7

Istituto nazionale di statistica
Servizio Editoria
Via Cesare Balbo, 16 – Roma

Metodologie di analisi e gestione del rischio nelle istituzioni pubbliche con particolare riferimento ai processi informatici: il caso dell'Istat

Cecilia Colasanti[1]

Sommario

Obiettivo di questo lavoro è fornire un approccio metodologico generale teso a porre l'analisi del rischio e l'accettazione o meno di esso come punto cardine rispetto alle scelte strategiche di un'organizzazione. Il documento illustra il significato e l'impatto della gestione del rischio per un'organizzazione pubblica, l'importanza di adottare discipline formali nel processo di risk management, i principali framework di riferimento (CObIT, RiskIT,CoSO), il loro legame con il "risk appetite". Vengono evidenziati, in questo contesto generale, i rischi legati alla funzione informatica ed i metodi preventivi e correttivi per affrontarli. Infine, viene considerato il caso dell'Istat che si è distinta tra le prime pubbliche amministrazioni italiane nell'avvio del processo di risk management al proprio interno nell'ambito delle azioni intraprese per il miglioramento della sicurezza delle proprie attività.

Parole chiave: risk management, risk appetite, early warning, sicurezza.

Abstract

The aim of this paper is to provide a methodological approach to put the risk analysis and its acceptance or rejection as a cornerstone of the strategic choices of an organisation. This document examines the meaning and the impacts of risk management for a public administration, the importance of adopting formal methods for evaluating and monitoring the risk, the main framework available (CObIT, RiskIT,CoSO) and their link with the "risk appetite"., In this general context, IT risks, and prevention and detection methods to face them, are highlighted. Finally, it is taken into consideration the Istat case that has distinguished itself, among the italian government administrations, in the opening a similar internal process as part of the actions taken to improve the security of its activities.

Keywords: risk management, risk appetite, early warning, security.

[1] Tecnologo ISTAT, *Lead auditor* certificata ISO27001:2005 e membro della Commissione per il *risk management* dell'Istat.

1. Introduzione

Con la rapida evoluzione delle tecnologie dell'informazione e della comunicazione, i sistemi informatici hanno assunto importanza centrale nell'assetto organizzativo e funzionale delle imprese e delle istituzioni. Inoltre, la diffusione delle tecnologie fondate sul paradigma Internet ha favorito il ridisegno dei confini organizzativi dell'impresa, sempre più aperta e connessa con altri soggetti e sistemi informatici.

In questo contesto, in cui i dati e la tecnologia che li supporta sono il bene più prezioso da proteggere, ovvero quello esposto a maggiori rischi, è necessario per il *top management* una profonda consapevolezza dei rischi, una chiara visione della propensione al rischio dell'organizzazione, la coscienza dei requisiti di conformità, la trasparenza sia rispetto ai rischi aziendali più significativi sia verso l'attribuzione di responsabilità di *risk management* all'interno dell'impresa.

Obiettivo del documento è fornire un approccio metodologico generale teso a porre l'analisi del rischio e l'accettazione o meno di esso come punto cardine rispetto alle scelte strategiche di un'organizzazione.

2. La gestione del rischio in una organizzazione pubblica

La gestione del rischio[2] non è un tema tradizionalmente legato alle pubbliche amministrazioni in cui spesso i rischi vengono percepiti in modo informale e non strutturato. Questa tematica è stata spesso trattata come problema marginale anziché come disciplina formale da integrare in qualsiasi procedura operativa e decisionale.

In tempi recenti, gli effetti negativi di questo approccio sono divenuti evidenti. La crescente presa di coscienza della necessità di discipline formali per la gestione dei rischi è stata stimolata da diversi fattori, fra cui:

- complessità e interdipendenza dei rischi aziendali;

oggi il mondo del lavoro è molto più complesso rispetto al passato. La disponibilità di dati e applicazioni on-line, l'allargamento dei rapporti a partner e fornitori e la velocità dei mutamenti economici comportano la necessità, anche per le imprese pubbliche, di prendere in considerazione un numero molto maggiore di rischi. Inoltre tali rischi sono raramente indipendenti fra loro; spesso si intersecano gli uni agli altri secondo modalità complesse e di difficile gestione;

- aumento delle normative di legge;

la *compliance* normativa è diventata un argomento sempre più sentito negli ultimi anni. Da un lato le PA devono far fronte ad una serie di richieste, spesso complesse, contenute in normative di legge e di settore, dall'altro la responsabilità è diventata personale: i dirigenti rispondono in prima persona dell'aderenza alla normativa nel proprio settore di competenza;

- crescente "globalizzazione";

anche se questo principio non sembra coinvolgere una PA, in realtà molte organizzazioni governative italiane devono tener conto della corrispondente amministrazione europea (si pensi ad esempio all'Istat ed Eurostat, al Ministero degli Affari Esteri, etc.). La complessità dei regolamenti e delle scadenze da rispettare implica la necessità di una gestione dei rischi su base planetaria;

- maggiore visibilità;

la naturale facilità di diffusione delle informazioni rendono le PA spesso vulnerabili a danni di immagine e di perdita di reputazione. Cresce dunque la necessità di adottare tecniche e misure di controllo nuove e più severe per gestire i rischi aziendali.

I fattori sopra elencati sono alcune delle principali ragioni che rendono più evidente la necessità di iniziative formali per la gestione dei rischi.

[2] Il Gartner Group definisce il rischio come "una possibilità di perdita o di esposizione a una perdita".

2.1 Cosa e come cambia un'organizzazione quando decide di considerare, affrontare e gestire il rischio

Considerare, affrontare e gestire i rischi è profondamente legato al tema della maturità di un'organizzazione. Infatti per avviare un processo strutturato di *risk management* occorre una visione integrata dei principali processi aziendali e la consapevolezza dell'impatto che il malfunzionamento o la perdita di uno dei processi comporta. Richiede la consapevolezza del rischio da parte dei membri della direzione aziendale, una chiara comprensione del proprio livello di *risk appetite*, dei requisiti di adeguamento a leggi e normative, trasparenza riguardo i rischi significativi, e l'inclusione delle responsabilità per il *risk management* nell'organizzazione.

Quello che invece generalmente accade è che ciascun Dipartimento/Direzione tende a valutare le conseguenza di eventi negativi solo per le proprie attività, secondo esigenze in gran parte stabilite a livello locale, per lo più senza alcun coordinamento tra le varie funzioni aziendali.

I principali attributi di un efficace programma di *risk management* sono:

- la scelta di una piattaforma di *Enterprise Risk Management* (ERM) estesa all'intera organizzazione;
- la gestione dei rischi deve essere attuata in modo uniforme, sulla base di priorità e *policy* valide per tutta l'organizzazione. Il metodo più efficace è rappresentato dall'adozione di una piattaforma comune affinché i rischi possano non solo essere comunicati attraverso un modello unico, ma anche gestiti con tecniche omogenee. Nei capitoli 4 e 6 saranno descritti i principali *framework* di riferimento.
- gestione e misurazione costanti;
- il successo (o insuccesso) di un programma ERM deve essere costantemente monitorato, con misurazioni specifiche del livello di funzionamento. Tali informazioni devono quindi essere consolidate a livello centrale per consentire un adeguamento dei parametri che controllano l'attività di *risk management*.
- coinvolgimento di tutti i dipendenti;
- la comunicazione delle strategie e degli obiettivi di gestione dei rischi deve avvenire capillarmente all'interno dell'Ente. Per avere successo, un programma ERM deve coinvolgere la totalità dei dipendenti.
- controllo e visibilità del programma ERM a livello centrale.

Le unità operative hanno la responsabilità di implementare una gestione dei rischi adeguata e conforme alle direttive centrali. Per garantirne l'attuazione è necessario un qualche tipo di "autorità" centrale che supervisioni complessivamente le iniziative di *risk management* dell' azienda.

3. Enterprise Risk Management (ERM)

Scopo del *risk management* è proteggere l'azienda e la sua capacità di portare avanti la propria missione strategica. L'*enterprise risk management* è lo strumento che consente la gestione sistematica e formale dei rischi e che mira non solo a ridurre le perdite, ma anche a sfruttare le opportunità. Obiettivo dell'ERM non è dunque la costituzione di una "burocrazia centralizzata" per la gestione dei rischi, ma piuttosto la creazione di una metodologia efficace e sostenibile in grado di gestire qualsiasi forma di rischio in ogni parte dell'azienda. In termini di *corporate governance* un buon programma di gestione dei rischi può comportare vantaggi notevoli a patto che lo stesso sia un processo che permei tutti i processi decisionali aziendali.

Sebbene il valore di programmi di questo tipo sia ampiamente riconosciuto, la loro adozione rimane alquanto limitata. Secondo un sondaggio[3] svolto fra dirigenti d'azienda, il 91% delle imprese "è ben disposto" verso il valore dell'ERM, ma solo l'11% ha attuato un programma ERM a tutto

[3] http://www.complianceweek.com/.

tondo. Il successo limitato dell'ERM non sorprende se si considerano le problematiche connesse alla sua implementazione: la gestione di rischi complessi, ad esempio, in una organizzazione in cui il livello di maturità è basso, presenta seri problemi organizzativi. Inoltre, la scarsa conoscenza delle *best practice* di settore e la mancanza di esperienza nella loro applicazione lasciano le organizzazioni prive di direttive da seguire. Perciò, pur comprendendo la necessità di un programma ERM formalizzato, molti Enti hanno difficoltà a procedere o ad adottare metodi e tecnologie a supporto di tale processo.

3.1 La classificazione dei rischi

L'ERM gestisce tutti quei rischi in grado di influire in modo non trascurabile sull'azienda e che possono essere classificati come segue:

- rischi naturali (incendi, inondazioni, furti, ecc.);
- rischi finanziari (prezzi, credito, inflazione, ecc.);
- rischi strategici (concorrenza, innovazione tecnologica, modifiche alle norme di legge, danni all'immagine e di reputazione, ecc.);
- rischi operativi (funzionamento dell'IT, minacce alla sicurezza, ecc.).

Il monitoraggio e la gestione di questi tipi di rischi sono cruciali; in casi estremi ciascuno di essi potrebbe infatti avere conseguenze catastrofiche. La tipologia spesso più facile da prevedere e controllare è quella dei rischi operativi che riguardano la normale attività dell'azienda e sui quali è più semplice intervenire attraverso un miglioramento e un rafforzamento dei controlli interni.

I rischi operativi possono essere interni o esterni.

Fra i rischi operativi interni si annoverano quelli legati a:

- persone (ad esempio: perdita di personale dovuto a dimissioni, carenza di know-how, clima interpersonale teso, ecc.);
- processi (ad esempio: controlli di processo inadeguati, fusioni tra enti diversi ecc.);
- tecnologia (ad esempio: sicurezza e affidabilità inadeguate dei sistemi, obsolescenza, ecc.).

Le categorie dei rischi operativi esterni sono simili, e comprendono:

- processi (ad esempio: rischi legali, rischi legati a partner e fornitori, ecc.);
- tecnologia (ad esempio: sicurezza fisica, sicurezza dei siti di archiviazione dei dati, ecc.).

Nel paragrafo successivo viene descritto come gran parte dei rischi operativi di un'azienda possa essere mitigata con soluzioni tecnologiche accuratamente selezionate.

3.2 Gli approcci di gestione del rischio

Il rischio non è un elemento che deve essere evitato ad ogni costo. Al contrario, la crescita avviene solo accettando livelli di rischio cosiddetti "prudenziali". Alcuni rischi possono e devono essere considerati come parte della normale attività operativa.

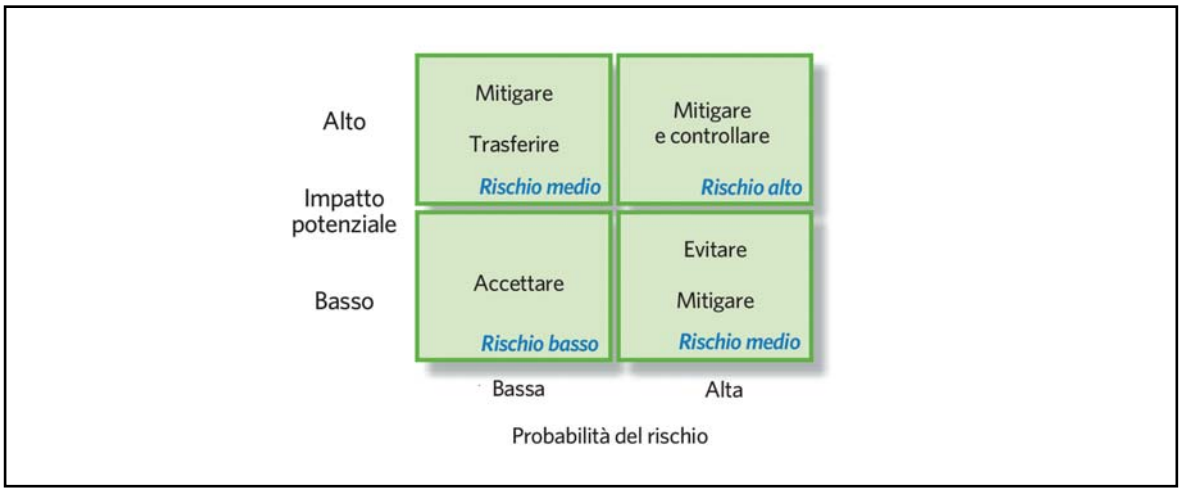
Esistono quattro generici approcci alla gestione di qualsiasi tipologia di rischio:

- evitare, ossia modificare l'attività in modo che un particolare rischio venga eliminato;
- trasferire, cioè passare per intero o in parte il rischio ad altri (compagnie di assicurazione, partner, ecc.);
- mitigare, ovvero creare un numero di controlli e parametri di verifica sufficienti a ridurre il rischio e la gravità della perdita;
- accettare, cioè assumersi il rischio e i costi ad esso associati.

L'approccio più adatto dipende dal tipo di rischio, dalla gravità delle conseguenze e dal grado di propensione al rischio dell'organizzazione.

Pur non rispecchiando per intero la complessità dei molti rischi operativi odierni, il grafico che segue illustra alcuni principi comunemente adottati relativi alla gestione di diverse tipologie di rischi aziendali.

Figura 1 - Possibili approcci al rischio



Evitare i rischi è difficile e a volte limita notevolmente le scelte aziendali. In alcuni casi l'eliminazione di un rischio potrebbe avere ripercussioni ancora più negative sulla crescita dell'azienda del rischio stesso.

Trasferire i rischi può comportare alcuni vantaggi finanziari. Nell'adozione di questo approccio bisogna comunque tener conto del fatto che le attività strettamente legate al *core business* aziendale devono essere interamente controllate dall'organizzazione stessa. Il che significa che possono esserci processi critici i cui rischi non possono essere trasferiti.

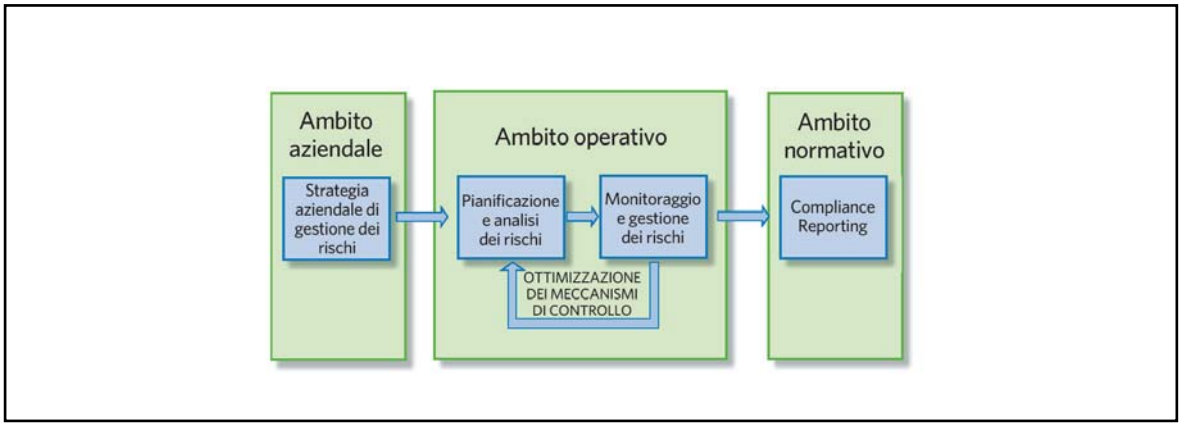
La mitigazione è spesso l'approccio più equilibrato. Esso comporta la creazione di meccanismi di controllo atti a ridurre possibili perdite, nonché capacità di monitoraggio in grado di garantire che l'analisi dei rischi correnti sia corretta. La quantità e il livello dei meccanismi di controllo in uso dipendono largamente dalla gravità del rischio per l'azienda nel suo complesso: alcuni rischi richiedono un monitoraggio e un'analisi costanti e fortemente proattivi, altri un livello di attività inferiore. La mitigazione è anche l'approccio più indicato rispetto ad una soluzione tecnologica che contribuisca alla realizzazione dei meccanismi di controllo.

In alcuni casi accettare il rischio, assumendosi le responsabilità ed i costi ad esso associati è l'unica scelta percorribile oppure un'opportunità da cogliere in situazioni particolarmente favorevoli.

3.3 Gli ambiti di gestione del rischio

Per gestire i rischi in maniera efficiente ed efficace, è importante tener presente i fattori critici in ogni fase dell'attività aziendale, secondo il modello illustrato in figura 2.

Figura 2 - Ambiti di gestione del rischio



3.3.1 Ambito aziendale

Questa fase, di cui è responsabile il *top management*, serve a definire le categorie di rischio complessive, le linee guida sul grado di tolleranza del rischio che l'azienda nel suo insieme è disposta ad accettare, e a tradurle in specifiche politiche aziendali. Dopo questa fase di alto livello, i rischi vengono riconsiderati a livello di Dipartimenti/Direzioni e comunicati in modo capillare nell'ambito delle stesse. A ciascun Dipartimento/Direzione potrebbe essere assegnato un diverso grado di tolleranza al rischio in base agli elementi specifici dell'ambiente in cui opera. E' poi compito di ciascuna struttura rendere operative tali direttive nelle situazioni specifiche che si trova ad affrontare.

3.3.2 Ambito operativo

L'ambito operativo comprende due momenti: *(i)* la pianificazione e l'analisi dei rischi e *(ii)* la gestione e il monitoraggio degli stessi, legati tra loro dall'ottimizzazione dei meccanismi di controllo.

3.3.2.1 Pianificazione e analisi dei rischi

Le direttive emanate a livello strategico vengono calate nella realtà produttiva delle unità organizzative e fungono da linee-guida per la pianificazione e le decisioni legate all'attività quotidiana. Viene sviluppata un'analisi dettagliata dei rischi a cui sono esposte ed una classificazione degli stessi in base al loro potenziale impatto sull'attività specifica del settore. Tale classificazione consente di collocare ciascun rischio in uno dei quattro quadranti della matrice sopra descritta.

Dopo aver analizzato e classificato tutti i rischi, è necessario mettere a punto un piano di risposta che spieghi come verrà gestito ciascuno di essi. In alcuni casi il rischio sarà considerato semplicemente come un "costo dell'attività" e verrà accettato, senza alcun piano per la sua eliminazione. Nella maggior parte degli altri casi dovrà invece essere sviluppato un piano di mitigazione che illustri come creare meccanismi di controllo e capacità di monitoraggio in grado di abbattere notevolmente ciascun rischio e le relative conseguenze.

È opportuno eseguire un'analisi costi/benefici su ciascuno dei rischi mitigati. In alcuni casi, infatti, il costo della mitigazione risulterà superiore alle conseguenze negative del rischio stesso e quindi potrà essere più indicato un approccio alternativo quale il trasferimento o l'accettazione del rischio. Nella maggior parte dei casi, tuttavia, un piano specifico può comportare notevoli vantaggi dal punto di vista della possibilità di controllare i diversi esiti.

3.3.2.2 Gestione e monitoraggio dei rischi

Una volta analizzati i rischi, è necessario mettere in atto meccanismi pratici di controllo e di monitorarne successo ed efficacia. Per "meccanismi di controllo" si intende tutto ciò che può diminuire la probabilità che un rischio si verifichi, o le eventuali ripercussioni: può trattarsi di soluzioni tecnologiche, di migliorie procedurali o, più probabilmente, di entrambe.

Dell'intero processo ERM, questa è l'area su cui la tecnologia può giocare un ruolo chiave. Nel caso della sicurezza informatica, ad esempio, il rischio di determinate minacce o esiti può essere largamente controllato attraverso l'adozione di tecnologie e soluzioni di comprovata efficacia. Questo tipo di approccio può inoltre creare una piattaforma sostenibile in grado di contribuire al contenimento dei rischi in via continuativa che quindi, non solo aumenta la sicurezza, ma spesso riduce anche i costi complessivi legati alla sua gestione.

Ad esempio, la maggioranza delle aziende è soggetta al rischio che persone non autorizzate possano accedere a dati, applicazioni o sistemi protetti. Tale rischio non può essere incluso nella categoria "accettabile" e deve venire ridotto il più possibile tramite l'utilizzo, ad esempio, di una efficace soluzione di *access management*.

Allo stesso modo, uno dei rischi fondamentali per molte imprese riguarda il cosiddetto "eccesso di autorità" che consente a determinate persone di avere più diritti di quelli che sarebbero necessari allo svolgimento degli incarichi loro affidati. Un esempio assai comune è la concessione a molti dipendenti dell'accesso a interi sistemi in qualità di super-utenti, anche se per le loro mansioni baste-

rebbe in realtà una qualifica inferiore. La situazione peggiora quando un dipendente ha facoltà non solo di avviare, ma anche di approvare determinate transazioni commerciali. In casi come questo la probabilità che si verifichi una frode è significativa, e va ridotta a tutti i costi.

Questi meccanismi di controllo interni sono identici a quelli richiesti per la conformità normativa. Qualunque sia infatti la norma in oggetto, una serie di efficaci controlli di sicurezza interni costituisce l'essenza dei suoi requisiti. Creare tali controlli non solo contribuisce alla gestione e alla riduzione dei rischi, ma allo stesso tempo semplifica notevolmente l'ottemperanza alle normative di legge e di settore.

Elemento essenziale in questa fase è un monitoraggio costante dell'efficacia di ciascun meccanismo di controllo. Ciò comporta non solo sorveglianza e *reporting* sui meccanismi esistenti, ma una continua rivalutazione dei rischi e dei relativi piani di mitigazione in base ai mutamenti dello scenario operativo. La comparsa di nuovi rischi, come pure l'importanza crescente/decrescente di quelli già noti, richiedono modifiche al piano di gestione e ai meccanismi di controllo utilizzati per mitigarli.

Il monitoraggio, nel caso ad esempio della sicurezza informatica, può comportare *reporting* di eventi specifici, filtraggio e correlazione automatizzata degli eventi al fine di identificare possibili problemi, validazione dei privilegi di accesso di tutti gli utenti per verificare che non siano superiori al necessario, ricerca ed eliminazione di eventuali eccessi di autorità, e così via.

Il monitoraggio comunque non può limitarsi all'analisi di eventi specifici (ad esempio tentativi multipli di autenticazione falliti), ma deve estendersi anche agli eventuali *trend*, dato che a volte i problemi di sicurezza possono essere identificati solo osservando l'evoluzione degli eventi nel tempo. Sebbene richieda spesso una qualche forma di intervento umano, questo tipo di monitoraggio può essere in gran parte automatizzato utilizzando un'efficace soluzione di *security event management*.

3.3.2.3 Ottimizzazione dei meccanismi di controllo

I meccanismi di controllo interni e la loro efficacia devono essere analizzati su base continuativa. Sono molti, infatti, gli elementi che possono modificare la strategia di gestione dei rischi in atto: comparsa di nuovi rischi, variazioni di priorità dei rischi esistenti, fallimento delle tecniche di mitigazione, e così via. Inoltre, l'andamento dell'attività operativa può facilmente comportare mutamenti nella tolleranza ai rischi: quando le cose vanno bene, anche un livello di rischio maggiore può diventare accettabile.

L'ottimizzazione dei meccanismi di controllo richiede semplicemente che l'attività di monitoraggio di cui sopra venga utilizzata per modificare in modo dinamico i meccanismi impiegati nella gestione di ciascun rischio. Si tratta di un processo ciclico, in quanto i rischi sono sempre in una certa misura dinamici: non si arriverà mai alla perfezione, si riuscirà solo a migliorare.

3.3.3 Ambito normativo

L'ultima fase riguarda in genere la creazione di report e informazioni da utilizzare per eventuali revisioni della *compliance* normativa. I documenti prodotti non saranno solo quelli specifici da sottoporre ai revisori ufficiali, ma anche quelli ad uso interno che contribuiscano a determinare il livello di conformità raggiunto Si noti che questa fase, pur non facendo parte dell'ERM in senso stretto, rappresenta una conseguenza naturale dello sforzo e dei risultati prodotti nell'ambito complessivo della procedura. Proprio questo rende l'ERM così importante per un'efficace *compliance* normativa: esso sviluppa una piattaforma in grado di affrontare rischi di qualsiasi tipo in ogni parte dell'azienda, e consente la creazione di meccanismi di controllo interni che non solo pongono rimedio a tali rischi, ma producono anche report e informazioni a riprova dell'avvenuto raggiungimento degli obiettivi di *compliance*. alle direttive centrali. Per garantirne l'attuazione è necessario un qualche tipo di autorità centrale che supervisioni le iniziative di *risk management* dell'intera azienda.

4. L'enterprise risk management CoSO

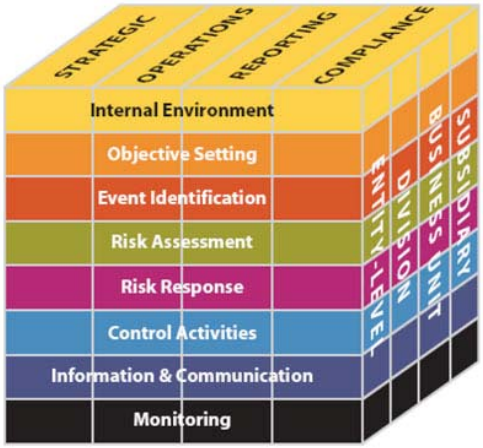
Uno dei più noti Enterprise Risk Management è stato pubblicato nel 2004 dal Committee of Sponsoring Organizations of the Treadway Commission (CoSO).

Il framework descrive i principi, le componenti ed i concetti più importanti della gestione del rischio aziendale e fornisce una roadmap precisa per identificare e gestire i rischi.

L'ERM si basa sull'Internal Control - Integrated Framework, lo standard internazionale più noto e diffuso per il sistema di controlli interni, pubblicato nel 1992 sempre dal CoSO.

Nella figura che segue è evidenziato con chiarezza il legame tra i livelli su cui il framework agisce.

Figura 3 - ERM CoSO



Vengono prese in esame quattro categorie di azione:

- *strategic*: rappresenta gli obiettivi di alto livello, in cui è fondamentale l'allineamento strategico tra l'IT e il business;
- *operations*: rappresenta l'uso efficace ed efficiente delle risorse;
- *reporting*: rappresenta l'affidabilità dei report;
- *compliance*: rappresenta la conformità alla normativa vigente.

Su queste categorie di azioni, si inseriscono le otto componenti del *framework*:

- *internal environment*: mostra qual è lo stile dell'organizzazione, come viene percepito il rischio dal personale a tutti i livelli, qual è la filosofia dell'ente rispetto al *risk management* e al *risk appetite*, fino ad arrivare all'integrità e ai valori etici;
- *objective setting*: gli obiettivi devono essere chiari ben prima dell'identificazione di potenziali eventi che possano minare il loro raggiungimento. L'ERM assicura che il *top management* abbia chiaro un processo di scelta degli obiettivi da perseguire e che tali obiettivi supportino e siano allineati con la missione dell'azienda ed in linea con il proprio *risk appetite*;
- *event identification*: tutti quegli eventi interni ed esterni che minacciano il raggiungimento degli obiettivi di un'azienda devono essere identificati e distinti in rischi e opportunità. Le opportunità vanno colte e usate per potenziare il proprio *business*;
- *risk assessment:* i rischi vengono analizzati, considerando la probabilità di accadimento ed il loro impatto e viene determinato come devono essere gestiti. Sono inoltre classificati i rischi inerenti (ossia quelli strutturali ed inevitabili) e residuali (ossia quelli che restano dopo essere stati trattati e mitigati);

- *risk response:* il management sceglie come rispondere al rischio – evitandolo, accettandolo, riducendolo o trasferendolo – sviluppando una serie di azioni che tengono conto della tolleranza al rischio dell'organizzazione e del *risk appetite*;
- *control activities:* vengono sviluppate politiche e procedure che assicurino che le risposte al rischio siano effettivamente portate avanti;
- *information and communication:* vengono identificate, catturate e comunicate tutte quelle informazioni importanti che possono facilitare il personale ad assumersi le proprie responsabilità;
- *monitoring*: in questa fase l'ERM viene monitorato e/o opportunamente modificato in base alle necessità.

La terza faccia del cubo mostra i diversi livelli dell'organizzazione ed esprime il concetto che le azioni, i controlli e le componenti del *framework* devono essere noti a tutto il Personale.

5. Il *risk appetite* per un'organizzazione

L'elemento più importante di qualsiasi programma di *risk management* è la riduzione dei rischi ad un livello accettabile. Un'infrastruttura del tutto priva di rischi è, all'atto pratico, inattuabile. Persino la riduzione dei rischi a un livello estremamente basso può vincolare eccessivamente la crescita del *business*.

La propensione al rischio (*risk appetite*) è la soglia di tolleranza al rischio o all'impatto di un potenziale evento negativo, che un'organizzazione decide di accettare per salvaguardare i suoi obiettivi strategici. Tale "quantità di rischio" dipende da fattori esterni (quali *stakeholder* coinvolti, tipologia di *business*, scenario competitivo) ed interni (come politiche aziendali e tipi di rischi specifici del proprio ambiente). La misura del *risk appetite* può variare da modelli qualitativi molto semplici, attraverso la definizione di categorie base di rischio, fino allo sviluppo di complessi sistemi quantitativi che danno una misura numerica (generalmente in termini di costi) dei rischi e delle contromisure da adottare.

A seguire sono elencate le caratteristiche per una buona definizione di *risk appetite*. Esso deve:

- riflettere la strategia aziendale, inclusi gli obiettivi organizzativi e le aspettative degli *stakeholder*;
- considerare i principali aspetti chiave del *core business* dell'Ente;
- considerare le risorse e le tecnologie richieste per gestire e monitorare l'esposizione al rischio;
- evidenziare la consapevolezza da parte dell'organizzazione dell'impatto che il malfunzionamento parziale o totale di uno dei processi che concorrono al raggiungimento degli obiettivi aziendali comporta;
- includere una ragionevole quantificazione della tolleranza ai malfunzionamenti di cui sopra;
- essere documentato in un formale documento;
- essere approvato dal *board*.

Misurare il *risk appetite* non è un'operazione semplice. Entrano infatti in gioco misure quantitative, che includono generalmente gli aspetti economici, e qualitative che fanno invece riferimento ad elementi reputazionali, di conformità alla normativa, etc.

Una volta che la soglia di tolleranza viene stabilita, vanno impostati tutti quei controlli sui processi critici per mantenere il livello di esposizione al rischio nell'intervallo accettato.

Questa operazione viene fatta sia a livello sia strategico, sia operativo, considerando:

- in quale settore dovrebbero essere allocate le risorse per minimizzare l'esposizione al rischio;
- quale livello di esposizione al rischio richiede un'azione immediata di risposta o un'azione eventualmente preventiva per mitigare l'impatto potenziale;
- come sono stati gestiti gli eventi negativi accaduti nel passato.

Il *risk appetite* è strettamente connesso all'applicazione del *framework* del *risk management*: il primo definisce infatti la direzione strategica e dà il polso del livello di tolleranza sui controlli da applicare, il secondo evidenzia i rischi legati ai processi critici.

Nella tabella che segue è evidenziato il collegamento tra i due concetti.

Elementi del framework di gestione del rischio	**Collegamento tra risk management e risk appetite**	**Cultura del rischio**
Governance	E' necessario che il *board* sia consapevole del livello di rischio che è disposto ad assumersi per mantenere/accrescere il business dell'azienda ed ha il compito di trasmettere la cultura del rischio a tutti i livelli dell'organizzazione.	
Valutazione	La valutazione del rischio è un processo continuo che va aggiornato in base al cambiamento di contesto ed in relazione al *risk appetite*.	
Quantificazione	Quantificare il rischio su ciascuna attività consente di definire le priorità tra i processi critici e di agire sulla base di tali scelte.	
Monitoraggio	Il monitoraggio delle attività critiche avviene sulla base della loro priorità e sulla tolleranza al rischio che il board è disposto ad accettare.	
Controllo e ottimizzazione	Questa ultima fase consente di calibrare i controlli ed ottimizzare il rapporto costo/beneficio.	

5.1 Lo sviluppo del *risk appetite*

Seguendo un approccio strutturato di definizione del *risk appetite*, un'organizzazione può meglio comprendere i suoi obiettivi strategici, la propria cultura, il mercato, l'aderenza alle leggi a cui è sottoposta e la propria sensibilità finanziaria. Possono essere identificate quattro fasi di definizione del *risk appetite*:

(i) considerare gli obiettivi strategici in funzione del parametro rischio;
(ii) definire il *risk profile;*
(iii) determinare, in termini economici, quanto si è disposti a rischiare;
(iv) formalizzare ed approvare un documento che tenga conto dei passi precedenti.

5.1.1 Gli obiettivi strategici

Gli obiettivi strategici dell'organizzazione possono includere:

- la quota di "mercato" cioè utenti/cittadini su cui l'Ente ha presa;
- la reputazione;
- la stabilità o la crescita;
- il ritorno degli investimenti;
- la conformità alla normativa vigente.

Un componente chiave nella comprensione dei propri obiettivi strategici è comprendere quali sono i fattori abilitanti (*driver*) degli obiettivi stessi, ovvero gli *stakeholder* e le loro aspettative.

Gli *stakeholder* possono includere *partner*, *board* dei direttori, *management*, impiegati, legislatori. Le aspettative di tali gruppi possono essere molto diverse ma spesso includono la crescita dei profitti, la stabilità aziendale, la conformità alle leggi vigenti, etc.

Gli obiettivi possono essere raggiunti da una combinazione di azioni a breve termine, ad esempio la realizzazione di profitti immediati, e a lungo termine, come ad esempio l'ampliamento di un settore aziendale.

In questa fase, ciò che è davvero importante è la capacità di essere flessibili rispetto ad un cambiamento: al variare dei fattori che hanno impatto sulla strategia dell'organizzazione, anche il *risk appetite* deve essere rimodulato.

5.1.2 Il profilo di rischio

Il passo successivo consiste nella definizione del profilo di rischio, ossia nella stima del rischio che si vuole correre rispetto alle reali possibilità dell'organizzazione.

Elementi che aiutano questo processo sono l'identificazione di due elementi:
(i) dei rischi ai quali l'organizzazione è esposta che potrebbero compromettere il raggiungimento degli obiettivi aziendali;
(ii) della quantità di perdite che l'organizzazione è disposta ad accettare nel caso l'evento indesiderato si verifichi.

5.1.3 Quantificare il rischio

Avendo determinato il capitale disponibile ed il corrente livello di esposizione al rischio, è possibile identificare un intervallo di tolleranza per rischi specifici. La tolleranza è una tipica misura usata per monitorare l'esposizione al rischio ed il *risk appetite* dichiarato. In pratica, il parametro "tolleranza" consente di tradurre rischi definiti a livello strategico, in azioni operative per contrastarli.

5.1.4 Documentare il processo

Infine il processo fin qui descritto deve essere documentato, approvato dal *board* e comunicato a tutta l'organizzazione.

5.2 Il legame tra il *risk appetite* e la funzione di monitoraggio dei risultati

La qualità dei risultati ottenuti nell'esercizio della propria attività è un elemento chiave di successo, che va quindi costantemente monitorato. Un punto di vista che è bene tenere in considerazione è quello della valutazione dei risultati in termini di conformità al proprio *risk appetite*. Se questo non è ben esaminato, si può verificare la situazione di un caso apparentemente di successo ottenuto assumendosi maggiori rischi di quelli tollerati/concordati per raggiungerlo. Se tali episodi non vengono prontamente identificati, il *risk appetite* perde completamente di senso.

La considerazione del *risk appetite* deve governare il processo decisionale a tutti i livelli. Un *framework* di *governance* robusto dovrebbe prevedere, tra le altre cose, anche lo sviluppo di politiche e procedure, matrici di delega di responsabilità e appropriate strategie di mitigazione dei rischi nel caso in cui i limiti di rischio tollerati siano ecceduti.

I vantaggi più significativi derivanti dell'inclusione del *risk appetite* in un modello di *governance* vanno ricercati nella sua positiva influenza sulla cultura ed il comportamento del livello dirigente. Dà infatti ai manager una migliore comprensione del significato di *risk management* e di come esercitare il proprio ruolo nell'ambito aziendale. La profonda comprensione del grado di tolleranza disponibile aiuta ad avere un comportamento coerente e ad assumersi i rischi con maggiore consapevolezza.

6. La gestione dei rischi informatici nell'ambito della IT *governance*

In questo contesto generale in cui la gestione ed il monitoraggio dei rischi è un elemento chiave per conseguire i risultati legati al proprio *business*, di particolare rilevanza è l'analisi dei rischi informatici. In questo paragrafo viene descritto il *framework* Risk IT per la gestione dei rischi informatici che deriva dal più generale modello di *IT governance*, CObIT.

6.1 Control Objectives for Information and related Technology (CObIT)

Il CObIT è un modello per la gestione della funzione informatica creato nel 1992 dall'associazione americana degli *auditor* dei sistemi informativi ISACA,[4] e dall'IT Governance Institute.[5]

Fornisce ai *manager*, agli *auditor* e agli utenti dei sistemi IT una griglia di riferimento costituita da: *(i)* una struttura dei processi della funzione IT, rispetto alla quale si è venuto formando il

[4] http://www.isaca.org.
[5] http://www.itgi.org.

consenso degli esperti del settore, *(ii)* una serie di strumenti teorici e pratici collegati ai processi con l'obiettivo di valutare se è in atto un efficace governo della funzione IT o di fornire una guida per instaurarlo.

CObIT ha raggiunto lo statuto di norma internazionalmente riconosciuta; l'Unione Europea lo ha indicato come uno dei tre standard utilizzabili per garantire la sicurezza dei sistemi informativi.[6] Pubblicato per la prima volta nel 1996, la sua missione è quella di "*ricercare, sviluppare, pubblicizzare e promuovere un insieme internazionale di obiettivi di controllo di accettazione generale per l'utilizzo giornaliero da parte di manager e auditor*". L'attuale versione 4.1 è stata rilasciata nel maggio 2007.

Dal punto di vista di un'azienda, soddisfare i requisiti di qualità, affidabilità e di sicurezza della propria organizzazione IT perseguendo obiettivi di efficacia ed efficienza, significa:

- controllare la funzione IT affinché fornisca le informazioni necessarie all'azienda;
- gestire i rischi che gravano sulle risorse IT;
- assicurarsi che la funzione IT raggiunga i propri obiettivi e che questi siano in sintonia con gli obiettivi aziendali:
- valutare la maturità dei processi misurando le prestazioni della funzione IT.

Il modello CObIT si propone di rispondere a questi bisogni:

- fornendo un collegamento tra gli obiettivi della funzione IT e gli obiettivi aziendali;
- organizzando le attività della funzione IT secondo un modello di processi generalmente accettato;
- definendo gli obiettivi di controllo da utilizzare nella gestione;
- fornendo un modello di maturità rispetto al quale valutare la maturità dei processi IT;
- definendo obiettivi misurabili (*goal*) secondo metriche basate sui principi delle *balanced scorecard*.

CObIT 4.1 divide il controllo della funzione IT in quattro domini:

- Pianificazione e Organizzazione (*Plan and Organise*),
- Acquisizione e Implementazione (*Acquire and Implement*),
- Erogazione ed Assistenza (*Deliver and Support*),
- Monitoraggio e Valutazione (*Monitor and Evaluate*).

Nei quattro domini sono collocati un totale di 34 processi, ai quali fanno capo, nella versione 4.1, un totale di 210 obiettivi di controllo; questi ultimi rivestono un'importanza centrale nel CObIT, al punto di dare il nome al modello stesso.

Per ogni processo sono definiti degli obiettivi di controllo specifici. Inoltre vi sono due insiemi di obiettivi di controllo "generali" applicabili a ciascun processo:

- il primo insieme riguarda i processi medesimi (si tratta controlli identificati con la sigla *PCn - Process control n*);
- il secondo insieme riguarda i dati in ingresso e uscita ai processi (si tratta controlli identificati con la sigla *ACn - Application Control n*).

Secondo il modello, il raggiungimento degli obiettivi di controllo garantisce un ragionevole livello di confidenza riguardo al raggiungimento degli obiettivi aziendali connessi al processo e alla prevenzione dei rischi associati al processo stesso.

Il modello non impone necessariamente il raggiungimento di ogni obiettivo di controllo. Il management aziendale può decidere quali sono i controlli applicabili ad ogni singolo processo all'interno dell'azienda, quali andranno implementati e con quali modalità, o viceversa può accollarsi il rischio di non implementarli.

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:077:0006:0008:IT:PDF.

6.1.1 Plan & Organise

Il dominio copre gli aspetti strategici e tattici e si propone di individuare il modo migliore in cui la funzione IT può contribuire al raggiungimento degli obiettivi aziendali. Lo scopo è di comprendere se gli obiettivi della funzione IT sono noti a tutti all'interno dell'organizzazione, se la funzione IT è in linea con la strategia aziendale, se l'azienda sta utilizzando le proprie risorse in modo ottimale gestendo correttamente i rischi e fornendo la qualità richiesta.

Nella tabella che segue sono esplicitati i dieci processi relativi a quest'area.

PO1	Definire un piano strategico per l'IT
PO2	Definire l'architettura del Sistema Informativo
PO3	Definire gli indirizzi tecnologici
PO4	Definire i processi, l'organizzazione e le relazioni dell'IT
PO5	Gestire gli investimenti IT
PO6	Comunicare gli obiettivi e gli orientamenti della direzione
PO7	Gestire le risorse umane dell'IT
PO8	Gestire la qualità
PO9	Valutare e gestire i rischi informatici
PO10	Gestire i progetti

6.1.2 Acquire & Implement

Le soluzioni al servizio della strategia IT devono essere prima di tutto identificate, poi costruite o acquisite; successivamente devono essere poste in opera e integrate al servizio dei processi aziendali. In aggiunta a ciò, in questo dominio si provvede a controllare la gestione dei cambiamenti e la manutenzione di sistemi, servizi e applicazioni, sempre compatibilmente con gli obiettivi aziendali. Lo scopo è di comprendere se i progetti forniranno soluzioni in linea con le attese e con i tempi e costi stimati, se opereranno correttamente una volta rilasciati e se la modalità di gestione dei cambiamenti è in grado di assicurare che questi vengano posti in essere senza effetti negativi sull'operatività dell'azienda.

A seguire si trovano i sette processi di quest'area:

AI1	Identificare le soluzioni informatiche
AI2	Acquisire e mantenere il software applicativo
AI3	Acquisire e mantenere l'infrastruttura tecnologica
AI4	Consentire il funzionamento e l'uso dei sistemi IT
AI5	Approvvigionamento delle risorse IT
AI6	Gestire le modifiche
AI7	Installare e certificare le soluzioni e le modifiche

6.1.3 Deliver & Support

Questi processi si occupano dell'erogazione effettiva dei servizi, il che comprende anche il controllo della disponibilità, del rispetto dei livelli di servizio e della sicurezza del servizio stesso, così come il supporto agli utenti e la gestione dei dati e dell'ambiente fisico.

I processi del dominio si assicurano che i servizi IT vengano erogati in linea con le priorità aziendali, che venga effettuata una gestione ottimale dei costi, che il personale sia in grado di utilizzare i sistemi con cognizione di causa e in sicurezza e che le informazioni siano protette negli aspetti di riservatezza, integrità, confidenzialità che sono loro propri.

Nella tabella che segue sono evidenziati i tredici processi relativi a quest'area:

DS1	Definire e gestire i livelli di servizio
DS2	Gestire i servizi di terze parti
DS3	Gestire le prestazioni e la capacità produttiva
DS4	Assicurare la continuità di servizio
DS5	Garantire la sicurezza dei sistemi
DS6	Identificare e attribuire i costi
DS7	Formare e addestrare gli utenti
DS8	Gestione del service desk e degli incidenti
DS9	Gestire la configurazione
DS10	Gestire i problemi
DS11	Gestire i dati
DS12	Gestire l'ambiente fisico
DS13	Gestire le operazioni

6.1.4 Monitor & Evaluate

È necessaria una valutazione regolare e periodica della qualità dei processi IT. I processi in questo dominio si occupano di verificare se le prestazioni della funzione IT sono in linea con le aspettative del vertice aziendale, se il sistema di controlli interni è ben congegnato, se sono saldi i legami tra le prestazioni della funzione IT e gli obiettivi aziendali e se è garantita la conformità a leggi e regolamenti.

Sono elencati nel seguito i quattro processi di quest'area:

ME1	Monitorare e valutare le prestazioni dell'IT
ME2	Monitorare e valutare i controlli interni
ME3	Garantire la conformità ai regolamenti
ME4	Istituzione dell'IT governance

6.2 Risk IT

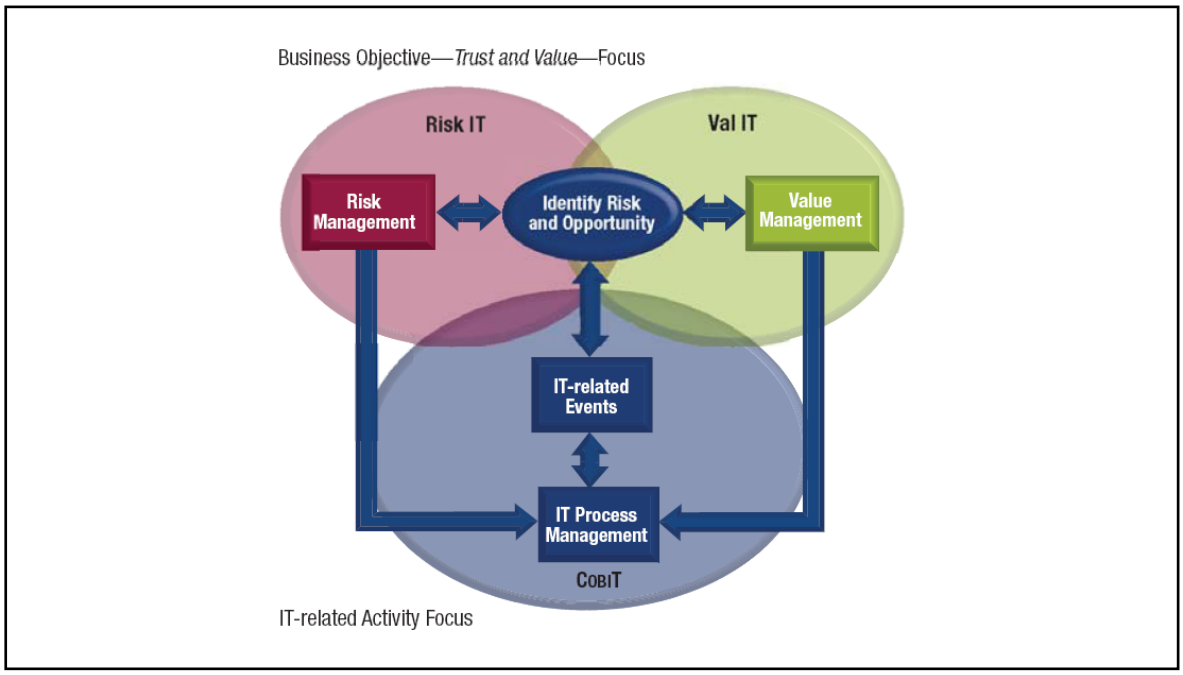
Risk IT è un *framework* focalizzato sulla gestione del rischio della funzione informatica sia dal punto di vista strategico, sia operativo. Mentre CObIT fornisce una serie di controlli per mitigare il rischio IT, Risk IT fornisce un quadro per le imprese per identificare, governare e gestire complessivamente il rischio derivante da eventuali interruzioni della funzione IT o da introduzione di nuove tecnologie, etc. In pratica, il metodo che Risk IT propone è quello di identificare, nell'ambito del proprio Ente, gli eventuali scenari di rischio di alto livello e scegliere, nell'ambito dei controlli CObIT sopra citati, quelli più adeguati al proprio scenario.

La tabella che segue mostra un semplice esempio:

Legame tra Risk IT e CObIT					
Scenario di rischi di alto livello		**Plan & Organise**	**Acquire & Implement**	**Delivery & Support**	**Monitor & Evaluate**
1	Introduzione di nuove tecnologie	PO1, PO2, PO3	AI1, AI3	-	ME1
2	Conformità alla normativa vigente	PO1, PO4, PO6, PO7, PO9	AI1	DS4, DS5	ME3
3	Professionalità del personale IT	PO7	AI5	DS2	ME1, ME4
...	...	...	...	...	...

Per completezza, è utile sottolineare che l'identificazione del rischio porta con sé l'identificazione di opportunità. Da CObIT derivano infatti due framework, uno per la gestione dei rischi (Risk IT) e l'altro per la gestione del valore (ValIT) che si ottiene appunto sfruttando le opportunità, ossia i "rischi positivi". La figura 4 evidenzia il legame tra i diversi aspetti.

Figura 4 - Legame tra COblT, Risk IT e Val IT



7. *Focus* sulla gestione dei rischi legati alla sicurezza informatica

Qualsiasi programma completo di *risk management* dovrà necessariamente comprendere e gestire una vasta gamma di rischi aziendali, ma la sicurezza informatica rappresenta una delle sue aree più critiche. Rischi quali attacchi di *hacker*, *malware* e accessi non autorizzati a risorse e sistemi protetti richiedono efficaci piani di mitigazione per poter essere mantenuti a livelli accettabili.

Oggi la funzione informatica rappresenta un supporto necessario o, in alcuni casi, addirittura un driver rispetto a qualsiasi iniziativa aziendale. Dunque i rischi legati all'IT devono essere affrontati con un approccio olistico al fine di garantire la protezione degli *asset* critici dell'azienda e la disponibilità ininterrotta dei servizi di business. Inoltre, una buona gestione dei rischi informatici può costituire la base di un programma di *compliance* normativa efficiente ed efficace.

Quando si prendono in esame i rischi alla sicurezza informatica che un'azienda deve fronteggiare, tre sono le aree principali da considerare:

- protezione degli *asset*.

E' importante stabilire come garantire che le preziose risorse aziendali siano sicure e protette, accessibili solo a persone debitamente autorizzate ed esclusivamente per gli scopi consentiti:

- continuità del servizio.

E' necessario stilare un piano che illustri come garantire che i servizi forniti a dipendenti, partner e clienti siano sempre disponibili secondo necessità, senza alcuna perdita di qualità o deterioramento del livello di servizio:

- *compliance*.

E' importante poter dimostrare agli auditor informatici interni o esterni che tutte le norme sono state effettivamente rispettate.

E' ovvio che queste aree sono strettamente correlate fra loro. La mancanza di un'efficace strategia per combattere i rischi che minaccia gli *asset* critici potrebbe comportare, ad esempio, il rischio di una compromissione della continuità del servizio. E l'assenza di un programma in grado di gestire i rischi in queste due aree ridurrà la capacità dell'azienda di garantire la *compliance* normativa.

7.1 La protezione degli *asset*

Una delle principali responsabilità dello *staff* informatico è la protezione delle risorse digitali confidenziali e riservate dell'azienda. Qualsiasi rischio di accesso o utilizzo non autorizzato di dati sensibili è per definizione inaccettabile. Di conseguenza, è essenziale un'efficace infrastruttura che controlli l'accesso a tutte le risorse aziendali.

Accesso alle applicazioni

E' una delle aree più critiche, e richiede un'efficace infrastruttura di gestione. Il progressivo espandersi delle catene produttive e distributive delle imprese provoca una crescita costante del numero di clienti e partner che accedono alle applicazioni on-line, e di conseguenza la necessità di robuste misure di *access management*.

Internamente, le informazioni riservate e sensibili devono essere protette tramite una rigida regolamentazione degli accessi. Il personale informatico deve essere in grado di creare *policy* centralizzate che stabiliscano esattamente quali utenti possono accedere a ciascuna applicazione, le condizioni che consentono loro l'accesso e le operazioni che sono autorizzati ad eseguire.

Durante la valutazione delle soluzioni di *access management*, si dovranno tener presenti i seguenti requisiti per poter garantire il soddisfacimento delle esigenze presenti e future:

- supporto di efficaci metodi di autenticazione;
- politiche di gestione degli accessi basate su ruoli e su regole;
- supporto di *policy* di accesso dinamiche, basate sui contenuti di informazioni esterne (eventualmente anche in tempo reale);
- possibilità di federazione delle identità in varie organizzazioni esterne;
- integrazione delle funzioni di autenticazione e autorizzazione con applicazioni *enterprise*;
- supporto dell'integrazione diretta con applicazioni personalizzate;
- *policy* di *access management* uniformi su piattaforme e organizzazioni diverse;
- contenimento e delega dei diritti di super-utente di sistema;
- protezione delle funzioni di *auditing* e dell'integrità dei log;
- *reporting* e *auditing* robusti di tutti gli eventi di accesso.

File critici di sistema e database

Ogni struttura informatica tiene sotto controllo non solo le applicazioni aziendali sensibili, ma anche i sistemi e i file critici che risiedono al loro interno. Fra gli esempi di risorse da proteggere si annoverano *repository* windows, file di sistema UNIX/Linux, elenchi di password e database aziendali di ogni genere. Per garantire che solo il personale debitamente autorizzato possa accedere a queste risorse è necessaria un'efficace infrastruttura di *access management* che dovrà consentire la creazione di *policy* centralizzate con cui vengano definiti gli utenti autorizzati ad accedere a ciascuna risorsa critica in base all'identità, al ruolo, alla divisione di appartenenza, e così via. Per garantire l'efficacia di questa operazione, è indispensabile che il modello di *policy* sia flessibile.

Controllo dei servizi critici di sistema

Sebbene questa possa non essere considerata una "risorsa", la capacità di sospendere determinati servizi critici di sistema deve essere tenuta rigorosamente sotto controllo. In particolare, l'interruzione accidentale o non autorizzata di tali processi (ad esempio la creazione dell'*audit log*) deve essere inclusa in qualsiasi programma completo per la gestione dei rischi informatici. Un'efficace piattaforma di *risk management* provvede ad assegnare in modo granulare i diritti di interruzione dei servizi di questo tipo.

Diritti di accesso in modalità di super-utente

In ogni ambiente IT, a un certo numero di amministratori vengono assegnati diritti di accesso illimitati in modalità super-utente (definita *root* in UNIX e Amministratore in Windows). È raro, tuttavia, che ogni super-utente abbia realmente necessità di tutti i diritti di accesso che tale qualifica concede. Ciò si traduce in un problema di responsabilità e in un'esposizione dei sistemi, cioè nel rischio che vengano eseguite operazioni dalle conseguenze nefaste che non possono essere fatte risalire all'esecutore né annullate con facilità.

Un modo per ridurre tale rischio è costituito dall'adozione di una soluzione che provveda ad assegnare in modo granulare i diritti di super-utente in modo tale ciascun amministratore possa eseguire solo determinate operazioni su determinati sistemi. È altresì necessaria una identificazione individuale degli utenti per evitare le difficoltà che si creano quando tutti gli amministratori utilizzano lo stesso nome.

Infine, un ulteriore elemento critico da controllare rigorosamente è l'accesso ai log di sistema. Se un singolo amministratore può non solo eseguire un'operazione sospetta, ma anche modificare i relativi file di registro, il rischio che una transazione fraudolenta non venga scoperta diventa reale. Di conseguenza, è importante poter disporre di un metodo centralizzato per la limitazione degli accessi (in modalità di sola lettura o di lettura/scrittura) a tutti i log di sistema. Allo stesso modo, la possibilità di interrompere il *logging* degli eventi deve essere concessa solo agli amministratori più fidati. Dato che la security nativa dei sistemi operativi spesso non offre il livello di granularità richiesto da questo tipo di protezione, si dovrà prendere in considerazione una soluzione di *access control* specializzata.

Account degli utenti

Un'ultima area di rischio riguarda l'utilizzo improprio di *user account* debitamente costituiti. Due sono gli aspetti che destano preoccupazione a questo proposito. Il primo si riferisce all'eventualità che un dipendente lasci l'azienda e che i suoi account e diritti di accesso non vengano tempestivamente disattivati. Quando ciò accade, il rischio di un utilizzo improprio di quegli *account* è elevato, soprattutto se il dipendente è stato sollevato dall'incarico contro la sua volontà.

Una seconda area di rischio riguarda l'esistenza di *user account* che rimangono inutilizzati per parecchio tempo. Ciò può avvenire per diverse ragioni, ma il caso più comune è quello di un utente che cambia ruolo in azienda senza che gli *account* relativi alle sue mansioni precedenti vengano eliminati. Di conseguenza, alcuni dipendenti possono essere proprietari di svariati *account*, alcuni dei quali non più validi. Questi *account* "orfani" creano un rischio di utilizzo improprio che deve essere tenuto sotto controllo. Un'efficace soluzione di *access management* contiene funzioni che analizzano l'intero ambiente alla ricerca di account non utilizzati di recente (dove la definizione di "recente" viene fornita a livello locale) e li chiudono.

Gestione delle identità e degli accessi

Le identità ed i privilegi di accesso degli utenti sono un elemento essenziale della strategia di e-business. Dietro le identità ci sono infatti i dipendenti, i fornitori, i partner, i clienti e tutti coloro che contribuiscono ai diversi aspetti dell'attività operativa. La gestione delle identità è costituita da una serie di processi e procedure che stabiliscono chi possa accedere a determinate applicazioni, database e piattaforme, ed in quali condizioni tale accesso possa essere consentito. Una corretta gestione di questo processo consente di rispondere alle domande seguenti:

- Chi ha accesso a cosa?
- Cosa è stato fatto?
- Quando è stato fatto?
- Come è possibile dimostrarlo?

Con queste informazioni si possono ridurre in modo efficace i rischi legati alla sicurezza informatica, tutelare risorse vitali, semplificare le operazioni di business ed essere conformi alla normativa. Le soluzioni proposte attraverso le piattaforme di *identity management*, consentono di gestire in modo integrato le funzioni descritte in tabella.

Amministrazione delle identità	Consente la creazione e l'amministrazione di identità e di informazioni sul profilo degli utenti.
Provisioning	Permette di assegnare a ciascun utente gli account e i diritti di accesso alle risorse aziendali adeguati al suo ruolo, eliminandoli poi al momento opportuno (ad esempio quando l'utente lascia l'azienda).
Gestione degli accessi	Contribuisce a garantire l'integrità delle informazioni e delle applicazioni aziendali attraverso la prevenzione degli accessi non autorizzati.
Monitoraggio/*Auditing*	Facilita la registrazione ed il *reporting* degli accessi per ridurre il rischio di una mancata identificazione dei problemi di sicurezza, garantisce la *compliance* normativa e, se necessario, consente l'esecuzione di analisi a posteriori per fini legali.

Risorse residenti su *mainframe*

Durante la pianificazione di una strategia di risk management si dimentica spesso l'eventuale esistenza dei mainframe: un errore che può rivelarsi assai dispendioso. È importante che lo stesso livello di controllo degli accessi utilizzato per tutti i sistemi distribuiti sia disponibile anche per i mainframe che operano nel medesimo ambiente. Le soluzioni di questo tipo devono supportare policy basate su ruoli che identifichino gli utenti autorizzati ad accedere a risorse e applicazioni protette residenti su mainframe, nonché le condizioni in cui l'accesso verrà consentito.

7.2 Continuità di servizio

Vista la sempre maggiore diffusione ed il crescente utilizzo dei sistemi *web-based* da parte del cittadino, la disponibilità costante dei servizi *on-line* è un elemento ormai necessario. Lo stesso vale per le applicazioni e i servizi utilizzati dal personale all'interno della propria rete intranet aziendale. Se per qualsiasi motivo un dipendente non riesce a collegarsi, le perdite di produttività e di supporto ai processi di business possono essere pesanti. In breve, la disponibilità ininterrotta dei servizi IT è un imperativo e uno degli aspetti fondamentali della gestione dei rischi informatici.

Uno degli ostacoli principali alla continuità del servizio è rappresentato dalle minacce ai server ed alle postazioni di lavoro in genere. Gli utenti subiscono spesso attacchi da parte di virus e applicazioni fraudolente spesso installate senza autorizzazione e a loro insaputa.

Collettivamente note come *malware*, queste applicazioni possono eseguire una serie di attività che vanno da semplici azioni di disturbo a operazioni potenzialmente devastanti, come ad esempio la riconfigurazione di sistemi operativi, il monitoraggio della posta elettronica, la registrazione e trasmissione di sequenze di tasti (password comprese), e l'accesso a dati riservati. Altri software fraudolenti a carattere non virale, sono, ad esempio, *spyware* e *adware*. Sebbene in genere meno distruttivi di alcuni virus, questi programmi possono ridurre notevolmente la produttività non solo del proprietario della macchina infetta, ma anche degli amministratori della security o del personale dell'Help Desk.

Uno degli elementi chiave di qualsiasi programma per la gestione dei rischi informatici deve quindi essere costituito da meccanismi di controllo efficaci in grado di contrastare virus e tentativi di intrusione di ogni genere.

Un altro elemento critico che minaccia la sicurezza dei server è la gestione delle vulnerabilità di sistema. Normalmente il tempo che intercorre tra l'annuncio di una vulnerabilità ed il rilascio della patch per la sua soluzione viene usato dalla comunità hacker per organizzare un attacco. La tempestiva installazione di *fix* su ciascuna macchina della rete è un'operazione essenziale, ma spesso assai difficile. Queste vulnerabilità rappresentano un rischio assai significativo per la continuità dei servizi IT, e rendono quindi essenziale l'utilizzo di un metodo centralizzato e automatizzato per la registrazione, la gestione e l'installazione delle *patch*.

7.3 Conformità alla normativa

L'ultimo elemento riguarda l'ottemperanza alle normative di legge e di settore. La *compliance* è diventata un imperativo delle strategie aziendali di *risk management*. I suoi requisiti toccano problematiche quali visibilità, sicurezza, disponibilità, *privacy* e trasparenza.

Se un'impresa non affronta adeguatamente questi problemi rischia sanzioni pesanti, accompagnate da un calo di fiducia degli *stakeholder* e da una riduzione del valore della sua credibilità.

In un certo senso, la *compliance* è semplicemente uno dei risultati di un buon programma di *risk management* attuato nelle altre due aree descritte nei paragrfi 7.1 e 7.2. In altre parole, l'esistenza di un programma efficace che mitighi i rischi attraverso la protezione degli *asset* e la garanzia della continuità del servizio crea sostanzialmente le condizioni necessarie per il rispetto delle norme di sicurezza previste dalla maggior parte dei nuovi regolamenti.

La *compliance* normativa sta obbligando gli Enti a rivalutare, ed in molti casi a migliorare notevolmente, *policy* e procedure di sicurezza interne.

Nonostante le norme legali o gli standard in materia di sicurezza (ad esempio la Sarbanes-Oxley, la HIPAA e la GrammLeach-Bliley) possano far riferimento a diversi ambiti, l'unico ele-

mento comune è rappresentato dalla necessità di efficaci controlli interni. Se un'azienda riesce a dimostrare di possederli, può essere pressoché certa di riuscire a ottemperare alle norme di sicurezza di qualsiasi legge.

In pratica, un meccanismo di controllo interno è l'insieme di processi/procedure in grado di garantire il buon esito di una pratica o di una transazione di business. Nel caso della sicurezza, spesso garantisce che solo il personale debitamente autorizzato abbia accesso a informazioni, applicazioni e risorse riservate.

La maggioranza delle aziende dispone di meccanismi di controllo interni di vario tipo che vengono utilizzati nel tentativo di creare un ambiente sicuro.

Sfortunatamente questi controlli sono in genere manuali, costituiti da documenti e iter approvativi, e lasciano spazio a numerose possibilità di errore.

Il "segreto" di una *compliance* sostenibile sta nell'automazione dei controlli di sicurezza interni.

Oltre ad essere l'unico modo per rendere gestibili i costi, consente notevoli aumenti di efficienza nella gestione della sicurezza e dell'*Help Desk*.

L'area in cui l'automazione dei controlli di sicurezza assume la massima importanza è la gestione degli utenti e dei loro accessi alle risorse aziendali protette – ovvero la gestione delle identità degli utenti e dei diritti di accesso loro concessi.

L'automazione dei meccanismi per il controllo dell'identità e dei diritti di accesso presenta tre aspetti importanti:

- politiche centralizzate che controllino automaticamente qualunque accesso a risorse protette di ogni genere all'interno dell'impresa;
- allocazione (e de-allocazione) automatica degli *account* e dell'accesso alle risorse secondo policy definite a livello centrale, generalmente basate sul ruolo o sulla posizione di ciascun utente in seno all'impresa;
- automazione delle attività di raccolta, filtraggio, visualizzazione e analisi di tutti gli eventi ambientali riguardanti la sicurezza.

Quando vengono realizzate capillarmente all'interno dell'azienda, queste funzioni possono migliorare enormemente la *compliance* e renderla sostenibile attraverso l'automazione di tutti i controlli di sicurezza interni.

8. Le soluzioni: metodi preventivi e correttivi

Come abbiamo già visto, parlare di rischi significa anche, soprattutto, parlare di sicurezza. In ambito ICT, l'adozione di efficaci politiche di sicurezza informatica ha rilevanza cruciale, in quanto da essa possono dipendere le stesse sorti dell'impresa/istituzione. Si tratta di un compito non facile, in ragione soprattutto dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale.

D'altra parte l'offerta di servizi sicuri e affidabili ha da sempre costituito un fattore di vantaggio competitivo. Oggi, con la diffusione dei canali distributivi ad elevato contenuto tecnologico, eventuali disservizi conseguenti a una non adeguata politica di sicurezza possono ancor più tradursi in danni alla reputazione e all'immagine dell'azienda.

Quanto agli aspetti qualitativi, le osservazioni condotte mostrano che è in atto un mutamento di concezione della sicurezza, che diventa sempre più attiva e, tramite servizi avanzati di monitoraggio, tende a "prevenire" per evitare che "attacchi" di varia natura possano arrecare danni all'immagine dell'azienda e comprometterne il business.

Nella sua accezione più ampia, pertanto, la sicurezza si presenta oggi caratterizzata da una triplice dimensione:

1. una sicurezza che promuove la protezione dei sistemi e delle informazioni dai potenziali attacchi;
   - questa sicurezza deve essere attuata secondo due direttrici: quella organizzativa e quella tecnologica. Con riferimento alla prima, va ricordato che l'elemento umano rappresenta da sempre l'anello più debole della catena della sicurezza; la creazione di una "cultura aziendale" attenta agli aspetti di sicurezza è presupposto necessario per la

protezione del patrimonio informativo aziendale e va perseguita anche mediante un'adeguata sensibilizzazione di tutto il personale. Con riferimento alla direttrice tecnologica, la sicurezza come difesa viene perseguita attraverso gli strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attaccanti (dipendenti, collaboratori esterni, *hacker*, terroristi, ecc.) e di attacchi (*malicious code*, *spamming*, *sniffing*, *spoofing*, *cracking*, *defacement*, ecc.);

2. una sicurezza che mira a garantire – in ogni situazione – la massima continuità di servizio;
   – tale obiettivo rientra in una visione allargata della sicurezza informatica che tiene in considerazione non solo gli strumenti di *disaster recovery* ma anche tutti gli altri presi di tecnici e organizzativi che confluiscono nel *business continuity plan*;
3. una sicurezza che promuove la qualità del servizio, venendo incontro alla domanda di "fiducia" dell'utente. È il caso, ad esempio, dei servizi censuari offerti via rete, il cui successo dipende anche dal livello di sicurezza offerto nello svolgimento dell'operazione.

8.1 Metodi preventivi: gli *early warning*

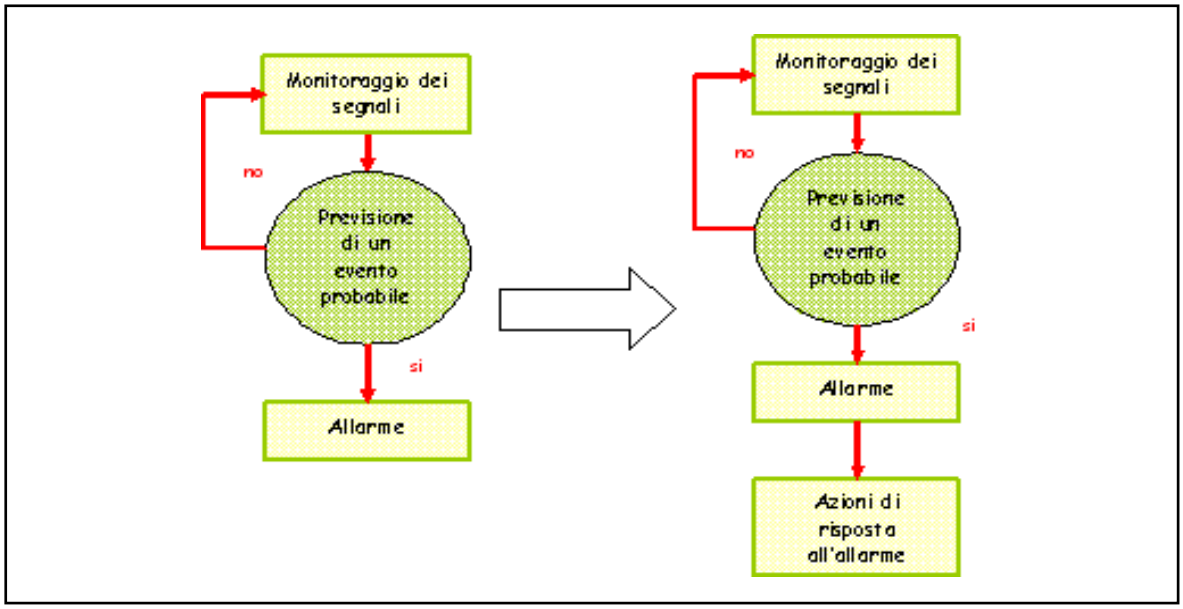
Gli early warning sono tutti quei segnali, anche non apparentemente connessi ad un determinato fenomeno, che ne indicano la possibilità di accadimento.

In letteratura questo concetto si trova espresso in più modi: Ray Bradbury, nel suo celebre racconto A Sound of Thunder parla dell'effetto farfalla, ossia di come un evento apparentemente insignificante possa causare in prospettiva cambiamenti radicali. Il concetto fu ripreso da E. Lorenz che, in un documento del 1963 per la New York Academy of Sciences, scrisse "Un meteorologo fece notare che, se le teorie erano corrette, un battito delle ali di una farfalla sarebbe stato sufficiente ad alterare il corso del clima per sempre."

Nello studio di alcuni fenomeni economici e sociali è stato osservato come il calo di consumo di carne negli Stati Uniti fosse associato al calo di consumo di benzina. Molti venditori di hamburger si trovano infatti nei pressi dei distributori di benzina. Quando gli automobilisti si fermano per il rifornimento, spesso prendono anche un hamburger. In caso di sciopero dei benzinai questa correlazione viene meno e dunque il consumo di carne diminuisce.

Tornando agli aspetti ICT, nell'ottica della prevenzione dei rischi, un approccio innovativo è sicuramente quello di realizzare un early warning system (EWS) rispetto al quale ci si attivi prima che il disastro avvenga. I tradizionali framework sono basati su tre fasi: monitoraggio dei segnali, previsione di un evento probabile, notifica di un allarme. Un elemento migliorativo può essere senz'altro l'aggiunta di una quarta fase che comprenda le attività per la risposta all'emergenza, una volta che l'allarme venga lanciato (Figura 5).

Figura 5 - Il sistema degli EWS



Un EWS efficace richiede comunque, al di là di una buona base tecnica, una profonda consapevolezza del rischio ed un sistema *people-centered.* Quattro sono le caratteristiche di un sistema basato sulle persone: consapevolezza del rischio, sistema di allarme, comunicazione e capacità di risposta.

Consapevolezza del rischio

Il rischio è la combinazione di minacce e vulnerabilità. Conoscere l'andamento di questi fattori è cruciale per una valutazione dei rischi appropriata, per la definizione delle priorità all'interno del sistema di early warning e delle relative azioni di risposta.

Sistema di allarme

Per prevedere eventi potenzialmente disastrosi, considerare correttamente le minacce e generare in tempo allarmi è necessaria una solida base scientifica costruita attraverso il costante monitoraggio dei segnali che precedono un evento. E' proprio da questa osservazione che risulta possibile una appropriata formulazione degli indicatori di rischio (KRI *Key Risk Indicator*). Tali indicatori sono una componente essenziale dell'intero EWS perché aiutano il *business* ad agire attivamente rispetto a situazioni critiche, riducendo così le perdite e prevenendo eventuali disastri. Una volta definiti, tali indicatori vanno messi in relazione con gli allarmi che generano, il valore dei propri beni, il supporto alle decisioni che il top management deve prendere.

Comunicazione

Le persone coinvolte in un processo critico devono comprendere chiaramente ed il prima possibile tutti i segnali d'allarme. Questi devono contenere informazioni utili e lineari che sollecitino una risposta appropriata.

Capacità di risposta

Le reazioni a fronte degli allarmi ricevuti devono essere appropriate e ben indirizzate. L'investimento nell'educazione del proprio personale e la costante comunicazione sui temi del rischio e della sua gestione sono dunque elementi chiave per il successo di ogni operazione preventiva o correttiva.

Le sfide da affrontare per costruire un sistema di questo genere sono molte: l'aggiornamento costante e continuo del EWS a fronte del monitoraggio dei segnali d'allarme, la capacità di considerare quei fenomeni poco visibili, che sembrano insignificanti ma che potrebbero produrre danni, la capacità di fornire pronte risposte, la sensibilizzazione del proprio personale.

8.2 Metodi correttivi: tecniche di *disaster/recovery*

Per disaster recovery (brevemente DR) si intende l'insieme di misure tecnologiche e organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze. Si stima che la maggior parte delle grandi imprese spendano fra il 2% ed il 4% del proprio budget IT nella pianificazione della gestione del disaster recovery, allo scopo di evitare perdite maggiori nel caso che l'attività non possa continuare a seguito della perdita di dati ed infrastrutture IT. Delle imprese che hanno subito disastri con pesanti perdite di dati, circa il 43% non ha più ripreso l'attività, il 51% ha chiuso entro due anni e solo il 6% è riuscita a sopravvivere nel lungo termine. I disastri informatici con ingenti perdite di dati nella maggioranza dei casi provocano quindi il fallimento dell'impresa o dell'organizzazione, ragion per cui investire in opportune strategie di recupero diventa una scelta quasi obbligata. Il Piano di disaster recovery (DRP Disaster Recovery Plan) è il documento che esplicita tali misure. Esso fa parte del più ampio Piano di business continuity (BCP Business Continuity Plan). Affinché una organizzazione possa rispondere in maniera efficiente ad una situazione di emergenza, devono essere analizzati i possibili livelli di disastro e la criticità dei sistemi/applicazioni.

Per una corretta applicazione del piano, i sistemi devono essere classificati secondo le seguenti definizioni: critici, vitali, delicati, non-critici.

Critici	Sono quei sistemi le cui relative funzioni non possono essere eseguite senza essere sostituite da strumenti o mezzi di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto
Vitali	Appartengono a questa categoria quei sistemi le cui relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, conseguentemente il costo di una interruzione è inferiore, anche perché queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).
Delicati	In questo caso le funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.
Non critici	Fanno parte di questa classe i sistemi le cui relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.

Le procedure applicative, il software di sistema ed i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente. Applicazioni, software e file classificati come critici hanno una tolleranza molto bassa alle interruzioni. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.

Un piano d'emergenza deve prevedere il ripristino di tutte le funzioni aziendali e non solo il servizio ICT centrale. Per la definizione del DRP devono essere valutate le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione degli equipaggiamenti e ruoli e responsabilità dei team. La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.

Allo stato attuale, la tecnologia offre la possibilità di realizzare varie soluzioni di continuità e *disaster recovery*, fino alla garanzia di fatto di un'erogazione continua dei servizi IT, necessaria per tutti i sistemi definiti *mission critical*.

In pratica i sistemi e i dati considerati importanti vengono ridondati in un "sito secondario" o "sito di *disaster recovery*" per far sì che, in caso di disastro (terremoto, inondazione, attacco terroristico, ecc...) tale da rendere inutilizzabili i sistemi informativi del sito primario, sia possibile attivare le attività sul sito secondario al più presto e con la minima perdita di dati possibile.

Chiaramente quanto più stringenti saranno i livelli di continuità tanto più alti saranno i costi di implementazione della soluzione.

In particolare, i livelli di servizio sono usualmente definiti dai due parametri *Recovery Time Objective* (RTO) e *Recovery Point Objective* (RPO).

Il primo parametro (RTO) è il tempo necessario per il pieno recupero dell'operatività di un sistema o di un processo organizzativo in un sistema di analisi *Business Critical System*. È in pratica la massima durata, prevista o tollerata, del *downtime* occorso. Aspetto di primaria importanza riveste il fatto che il valore di RTO sia definito, conosciuto e verificato, tenendo presente che se un *downtime* lungo danneggia la possibilità di fruire del servizio più di uno breve, il danno maggiore deriva dall'inconsapevolezza di quanto possa essere il tempo previsto per il ripristino dei servizi danneggiati. Un'utile misura per la riduzione dell'RTO consiste nell'avere dei backup dei dati disponibili integralmente su siti secondari qualora il sito primario risulti danneggiato.

Il secondo (RPO) è uno dei parametri usati nell'ambito delle politiche di *disaster recovery* per descrivere la tolleranza ai guasti di un sistema informatico. Esso rappresenta il massimo tempo che intercorre tra la produzione di un dato e la sua messa in sicurezza (ad esempio attraverso *backup*) e, conseguentemente, fornisce la misura della massima quantità di dati che il sistema può perdere a causa di guasto improvviso.

Al diminuire dell'RPO richiesto si rendono necessarie politiche di sicurezza sempre più

stringenti e dispendiose, che possono andare dal salvataggio dei dati su supporti ridondanti tolleranti ai guasti fino alla loro pressoché immediata replicazione su un sistema informatico secondario d'emergenza (soluzione in grado di garantire, in linea teorica, valori di RPO prossimi allo zero).

In base alla definizione e alla correlazione di questi parametri, possono essere scelte diverse strategie di salvataggio dei dati.

Replica sincrona

La replica sincrona garantisce la specularità dei dati presenti sui due siti poiché considera ultimata una transazione solo se i dati sono stati scritti sia sulla postazione locale che su quella remota. In caso di evento disastroso sulla sede principale, le operazioni sul sito di *disaster recovery* possono essere riavviate molto rapidamente (basso RTO e RPO praticamente nullo).

La replica sincrona è limitata dalla incapacità dell'applicazione di gestire l'impatto del ritardo di propagazione (vincolo fisico quindi, e non tecnologico) sulle prestazioni. In funzione della sensibilità dell'applicazione e della tecnologia di comunicazione tra i due siti, l'efficacia della copia sincrona inizia a diminuire a una distanza variabile tra i 35 km e i 100 km.

Replica asincrona

Per far fronte al limite di distanza tra i due siti imposto da tecniche sincrone, si ricorre spesso alla tecnica di copia asincrona. In questo caso il sito che si occuperà della replica può trovarsi anche a distanze notevoli (> 100 km). In questo modo è possibile affrontare anche disastri con ripercussioni su larga scala (come ad esempio forti scosse sismiche) che altrimenti potrebbero coinvolgere entrambi i siti (se questi si trovano nelle vicinanze).

Un ulteriore vantaggio della copia asincrona è la possibilità di essere implementata via software non dovendo necessariamente ricorrere a sofisticate e costose tecnologie di *storage*.

Tecnica mista

Per garantire la disponibilità dei servizi anche in caso di disastro esteso e al tempo stesso ridurre al minimo la perdita di dati vitali si può ricorrere ad una soluzione di tipo misto: effettuare una copia sincrona su un sito intermedio relativamente vicino al primario (distanza< 100 km) e una copia asincrona su un sito a grande distanza.

9. Il caso Istat

In Istat è stata istituita nel maggio 2010 la Commissione[7] per il *risk management* che si occupa specificatamente della:

- definizione della strategia e della determinazione del livello di accettabilità del rischio, compatibilmente con le linee di indirizzo formulate dagli organi di governo e in conformità con le decisioni sulla ritenzione, trasferimento ed eliminazione dei fattori di rischio;
- evoluzione del sistema, dalla fase preliminare, orientata all'applicazione del modello su di un numero limitato e predefinito di processi di produzione e servizio, all'estensione dello schema agli altri processi di produzione e servizio che verranno successivamente individuati;
- definizione e manutenzione del catalogo dei rischi, formato sulla base delle risultanze di analisi, *survey* sulla percezione del rischio e altre modalità di rilevazione dell'evento rischioso condotte di concerto con le strutture coinvolte nel Sistema;
- elaborazione delle tecniche per la quantificazione dei rischi (incluse le analisi delle serie storiche di dati), nell'ambito delle fasi di valutazione (assessment) e quantificazione del livello di gravità e del grado di probabilità di accadimento dell'evento rischioso;
- formulazione delle metodologie per l'implementazione delle azioni di risposta al rischio,

[7] Coordinatore: Fabrizio Rotundi; Membri: Katia Ambrosino, Cecilia Colasanti, Sara Demofonti, Rosa Elia, Concetta Ferruzzi, Alessandra Lucchese, Sonia Meluzzi, Simona Menegon.

con la costruzione di un Sistema di reporting periodico per il monitoraggio delle variazioni del livello di rischiosità e dell'efficacia delle azioni poste in essere dalle strutture per il contenimento degli effetti del rischio;

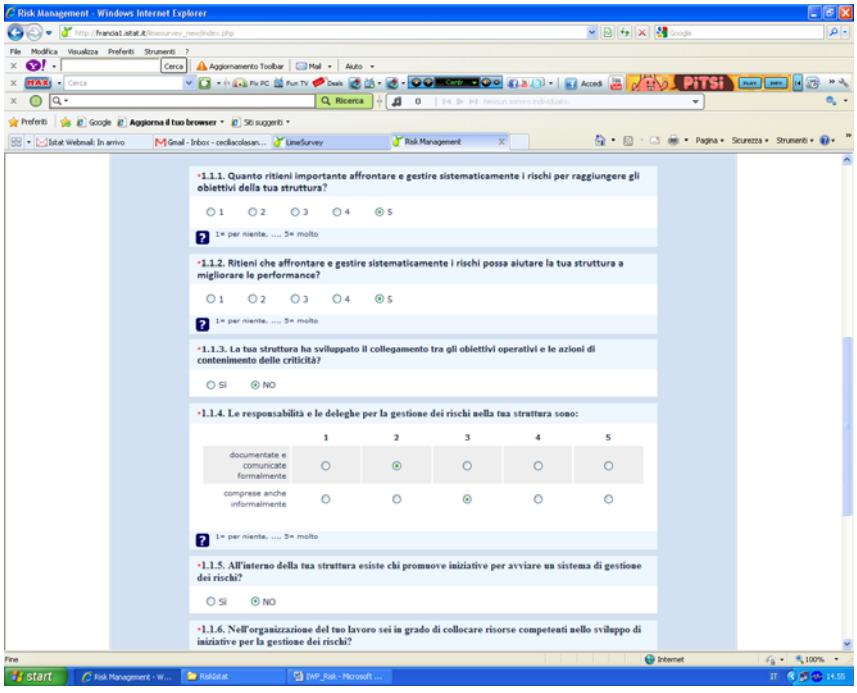
- diffusione della cultura del rischio a tutti i livelli organizzativi, fornendo anche il supporto alle strutture competenti per la formazione e per la comunicazione interna/esterna, allo scopo di contribuire allo sviluppo di una visione dell'organizzazione improntata alla tutela e valorizzazione del patrimonio detenuto.

La Commissione, inoltre, provvede ad elaborare report periodici sull'andamento delle attività realizzate e sui risultati conseguiti, la cui diffusione è prevista nei confronti degli organi di governo e delle strutture decisionali nell'ambito del processo di Risk management

I lavori della Commissione stanno seguendo vari filoni: il primo mira ad acquisire elementi sulla percezione del rischio da parte del *top management* dell'Istituto, il secondo fa riferimento alle classiche fasi del processo di gestione del rischio, il terzo alla diffusione della cultura del rischio internamente ed esternamente all'Istituto.

Inizialmente è stata avviata una indagine interna sulla percezione del rischio da parte del top management che indaga 1) sulla definizione dell'ambiente di controllo dei rischi; 2) sulla determinazione degli obiettivi dell'organizzazione e del processo di *risk management*; 3) sull'identificazione degli eventi e dei fattori di rischio. L'indagine fruibile via web, è stata realizzata attraverso l'applicativo Limesurvey e si presenta all'utente come riportato nella figura 6.

Figura 6 - Questionario on line sulla percezione del rischio



La fase di analisi dei processi ha messo in evidenza le diverse anime dell'Istat: quella della produzione statistica in primo luogo, quella amministrativa (economica e gestionale), e quella tecnica (informatica e comunicazione). Rispetto a ciascuna sono stati analizzati e valutati quei processi ritenuti critici.

Il framework di riferimento scelto dall'Istat è il CoSO Internal Control - Integrated framework, applicato già da altre organizzazioni pubbliche e private, conforme agli standard di riferimento per la certificazione della qualità dei sistemi organizzativi.

Per ciò che concerne gli aspetti legati alla diffusione della cultura del rischio, sono stati avviati momenti seminariali e formativi ed è stato realizzato il sito web (figura 7), raggiungibile al link http://risk.istat.it che raccoglie i lavori, la documentazione, i prodotti realizzati dalla Commissione, i riferimenti normativi, lo stato di avanzamento dei lavori del gruppo e gli eventi legati a questo tema.

Figura 7 - Il sito web

Riferimenti bibliografici

Computer Associates, 2006, *Ridurre i rischi della sicurezza*. http://www.ca.com

Crescenzi, F., 2011, *Dove osano le farfalle*. http://segnalazionit.org/?s=farfalla

Information System Audit and Control Association (ISACA) http://www.isaca.org

International Organization for Standardization (ISO), ISO 27001 Information Security Management Systems - *Code of Practice***,** 2006.

IT Governance Institute, IT Governance *Implementation Guide: Using COBIT® and Val IT TM, 2nd Edition*, United States of America, ITGI.

IT Governance Institute, COBIT Mapping, *Overview of International IT Guidance, 2ndEdition*, United States of America, 2007, ITGI.

IT Governance Institute, COBIT 4.1 *Control Objectives Management Guideines maturity Models*, United States of America, 2007, ITGI.

IT Governance Institute, *IT assurance guide using COBIT*, United States of America, 2007, ITGI.

IT Governance Institute, *The Risk IT framework, Principles Process Details Management Guidelines Maturity Models* United States of America, 2009, ITGI.

KPGM, *Understanding and articulate risk appetite*, 2008.

Losco S., Colasanti C., *Strumenti metodologici per l'audit della funzione informatica nelle organizzazioni complesse: alcune soluzioni adottate dall'Istituto Nazionale di Statistica nell'esperienza del processo di audit ICT*, 2011, http://www.istat.it/it/archivio/istat+working+papers

Rotundi, F., 2011, *Il sistema di risk management applicato ai censimenti generali* http://saperi.forumpa.it/relazione/il-sistema-di-risk-management-applicato-ai-censimenti-generali-0

Rotundi, F., 2011, http://www.istat.it/it/archivio/29057

Sinibaldi, A., 2007, *Risk Management*: Milano: Hoepli Editore.

Informazioni per gli autori

La collana è aperta ad autori dell'Istat e del Sistema statistico nazionale, e ad altri studiosi che abbiano partecipato ad attività promosse dal Sistan (convegni, seminari, gruppi di lavoro, ecc.). Da gennaio 2011 essa sostituirà Documenti Istat e Contributi Istat.

Coloro che desiderano pubblicare sulla nuova collana dovranno sottoporre il proprio contributo alla redazione degli Istat Working Papers inviandolo per posta elettronica all'indirizzo iwp@istat.it. Il saggio deve essere redatto seguendo gli standard editoriali previsti, corredato di un sommario in italiano e in inglese; deve, altresì, essere accompagnato da una dichiarazione di paternità dell'opera. Per la stesura del testo occorre seguire le indicazioni presenti nel foglio di stile, con le citazioni e i riferimenti bibliografici redatti secondo il protocollo internazionale 'Autore-Data' del *Chicago Manual of Style*.

Per gli autori Istat, la sottomissione dei lavori deve essere accompagnata da una mail del proprio dirigente di Servizio/Struttura, che ne assicura la presa visione. Per gli autori degli altri enti del Sistan la trasmissione avviene attraverso il responsabile dell'ufficio di statistica, che ne prende visione. Per tutti gli altri autori, esterni all'Istat e al Sistan, non è necessaria alcuna presa visione. Tutti i lavori saranno sottoposti al Comitato di redazione, che valuterà la significatività del lavoro per il progresso dell'attività statistica istituzionale. La pubblicazione sarà disponibile su formato digitale e sarà consultabile on line.

Gli articoli pubblicati impegnano esclusivamente gli autori, le opinioni espresse non implicano alcuna responsabilità da parte dell'Istat. Si autorizza la riproduzione a fini non commerciali e con citazione della fonte.