CONSULTING

IT Risk Assessment.

Il contesto di riferimento.

Uno degli aspetti che in questi anni sta caratterizzando il processo di evoluzione delle moderne istituzioni economico/finanziarie è la crescente attenzione verso la misurazione/gestione del Rischio (di natura quali-quantitativa), rivolto in particolare a quello operativo, oltre al rafforzamento della capacità di garantire la Continuità delle Operazioni essenziali in occorrenza di eventi gravi ed imprevedibili.

In questo contesto generale, si inserisce l'IT Risk Assessment che si prefigge di definire un framework organizzativo e metodologico personalizzato attraverso la realizzazione di un catalogo dei rischi per tutti i rischi inerenti l'uso dell'Information Technology e il conseguente adeguamento delle strategie in tema di sicurezza al fine di ridurre l'esposizione aziendale in relazione ai criteri di:

- Disponibilità
- Riservatezza
- Affidabilità.

Per l'implementazione delle attività si prevede l'adozione dei passi metodologici definiti all'interno dei domini del RiskIT, in sinergia con il framework COBIT 4.1 (ed altri standard metodologici: ISO27001/2, etc.), in linea con quanto suggerito dalle good practice che governano la materia.

I benefici derivanti dall'applicazione di tale approccio sono:

- Riduzione del rischio attraverso l'automazione e regolazione dei processi di business.
- Maggiore visibilità su soglie e profili di rischio ed iniziative di gestione del rischio.
- Diffusione di cultura aziendale più etica e consapevole di rischi e opportunità.

La mappatura dei rischi che BLU Consulting propone è la seguente: i rischi di 1° e 2° Livello saranno conformi a quanto definito dalle principali normative di riferimento (dell'IVASS nel Regolamento 20 del 26 Maggio 2008 e Solvency II / Basilea II), mentre i dettagli relativi alle tipologie di rischi (3° Livello) ed agli eventi di rischio (4° Livello) saranno modellati e personalizzati in base al contesto operativo.

Regolamento IVASS 20/2008
Livello 1
macrocategoria rischi

Solvency II
Basilea II
Livello 2
tipologia rischi

Personalizzazione in base al contesto operativo
Livello 3
dettaglio dei rischi per tipologia

Livello 4
micro rischi

f

Blu Consulting Srl
Sede legale 00189 Roma, Via Flaminia, 964
Sede operativa 00154 Roma, Via Girolamo Benzoni, 31
Tel. e Fax +39.06 45654174
info@blu-consulting.it · www.blu-consulting.it

La proposta di valore di **BLU Consulting.**

BLU Consulting propone un'offerta di servizi di consulenza direzionale volta ad individuare ed implementare un modello strategico, che consenta una più efficiente individuazione e valutazione dei rischi IT facilitando, al contempo, l'individuazione e la definizione delle responsabilità sui diversi livelli aziendali.

Per l'implementazione dell'IT Risk Assessment BLU Consulting da tempo applica una propria metodologia la quale è articolata nelle seguenti fasi:

1 Mappatura dei rischi (Catalogo Rischi) e redazione di uno specifico framework metodologico di gestione dei rischi per la Direzione IT.

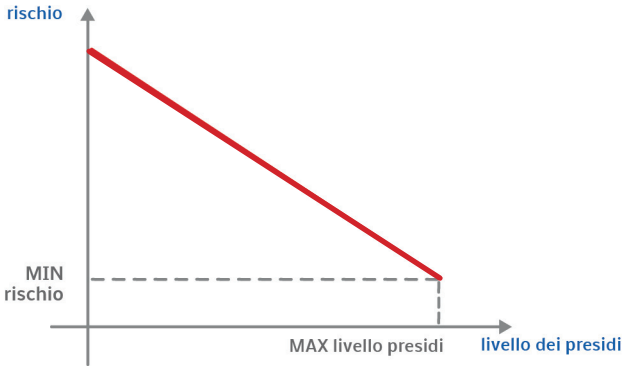
2 Valutazione del Rischio Lordo, avvalendosi del supporto di specifici Case Study (Assumption) per la determinazione di un modello atto a stimare la frequenza e la classe di impatto economico di ogni categoria di rischio (livello 3).

3 Valutazione del Livello dei Presidi esistenti che interessano le categorie di rischio (livello 3) oggetto di analisi. Tale valutazione sarà il risultato delle evidenze emerse nel corso delle interviste con i Risk Owner supportate da specifiche checklist.

Le checklist saranno composte da un set di domande specifiche articolate ponendo particolare focus sui seguenti attributi/presidi (tipici delle Best Practice di settore):

-consapevolezza e comunicazione
-policy e procedure
-strumenti / automatismi
-attitudini / esperienze
-responsabilità
-obiettivi e misurazione

4 Valutazione del Rischio Netto, sulla base delle evidenze emerse nelle fasi precedenti, inteso come Rischio lordo ponderato sulla base di una % di abbattimento del rischio lordo. Tale percentuale è un fattore strettamente correlato al livello dei presidi: maggiore è il livello di presidio, minore sarà l'esposizione al rischio (come illustrato nella figura seguente).



5Definizione di un numero sostenibile di KRI (Key Risk Indicator) e del relativo modello di applicabilità propedeutico al loro successivo utilizzo. L'individuazione di tali parametri garantisce il Continuous Improvement (nel rispetto del Ciclo di Deming - PDCA) dei processi aziendali che impattano sulle categorie di rischio che sono state oggetto dell'assessment.

I nostri progetti.

IT Risk Assessment.

Attività di verifica del rischio legato all'utilizzo del Servizio di Outsourcing Informatico di un primario Gruppo Assicurativo nazionale, definendo i punti di forza e debolezza del servizio erogato, identificando le maggiori aree di miglioramento con l'obiettivo di perseguire una tangibile mitigazione del rischio intrinseco.

1 Definizione degli obiettivi di controllo
Definizione di un sottoinsieme di processi IT e dei relativi obiettivi di controllo (raggruppati in una mappa concettuale), in funzione del piano di intervento stabilito.

2 Acquisizione informazioni
Conduzione dell'attività attraverso: la somministrazione di interviste, l'utilizzo di apposite checklist e la raccolta della documentazione necessaria per una miglior evidenza dei processi IT analizzati.

3 Elaborazione informazioni
Definizione del livello di maturità del processo attraverso lo studio della documentazione ricevuta e delle ulteriori evidenze emerse.

4 Valutazione e Reporting
Redazione di documenti di dettaglio e di sintesi (Executive Summary) dei principali punti meritevoli di attenzione.

Esperienze.

Risk Framework for IT.

Esecuzione di specifiche attività per l'implementazione di un framework organizzativo e metodologico dei rischi tipici della Direzione Tecnologie dell'Informazione di un primario Gruppo Assicurativo nazionale, che ha posto particolare focus sugli ambiti di Information Security e IT Architecture.

L'implementazione delle attività di IT Risk Assessment ha previsto l'utilizzo sinergico del framework Risk IT con il COBIT 4.1 (e ulteriori standard: ISO/IEC 27001/2, etc.), in linea con quanto suggerito dalle good practice che gestiscono la materia, al fine di pervenire ad un modello di governo dei rischi personalizzato per la Compagnia.
Di seguito le attività svolte:

- Mappatura dei rischi e redazione di uno specifico framework metodologico di gestione dei rischi per la Direzione IT.
- Valutazione del Rischio Lordo, avvalendosi del supporto di specifici Case Study.
- Valutazione del Livello dei Presidi esistenti tramite interviste con i Risk Owner.
- Valutazione del Rischio Netto, sulla base delle evidenze emerse nelle fasi precedenti.
- Definizione di un numero sostenibile di KRI (Key Risk Indicator).

Blu Consulting Srl
Sede legale 00189 Roma, Via Flaminia, 964
Sede operativa 00154 Roma, Via Girolamo Benzoni, 31
Tel. e Fax +39.06 45654174
info@blu-consulting.it · www.blu-consulting.it