Associazione Italiana Internal Auditors

"IT Risk-Assessment: il ruolo dell'Auditor nel processo."

Davide SUSA - ACSec

AIIA - Consigliere del Chapter di Roma

Agenda

- ✓ Overview sul Risk-Management
- ✓ Il processo di Risk-Assessment
- ✓ Internal Auditor e Risk-Management
- ✓ Il ruolo dell'Auditor nel processo
- ✓ Spunti operativi

Risk-Management: Overview

Il ***Risk-Management*** è il processo che permette di:

- ✗ identificare i rischi
- ✗ fare assessing dei rischi
- ✗ mettere in atto gli step per ridurli a livelli accettabili sulla base delle policy aziendali.

Aiuta un'organizzazione a meglio gestire i rischi inerenti le attività IT, mettendola in grado di raggiungere i seguenti obiettivi:

- ✓ migliorare la sicurezza dei sistemi IT
- ✓ mettere in grado il management di prendere decisioni ponderate dalla conoscenza dei rischi
- ✓ assistere i manager nel creare una politica di sviluppo dell'IT sulla base dei risultati del processo.

Risk-Management: Overview

Il processo di Risk-Management si fonda sui seguenti processi:

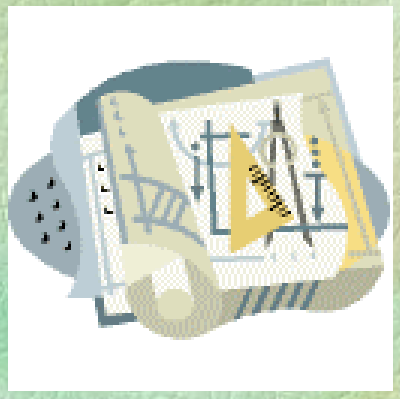
- ✓ ***Risk-Assessment*** - si occupa dell'identificazione e valutazione dei rischi e del loro impatto, nonché delle raccomandazioni per la loro riduzione
- ✓ ***Risk-Mitigation*** - serve a determinare le priorità di intervento, implementazioni e mantenimento delle misure di riduzione del rischio
- ✓ ***Evaluation e Assessment*** - si occupa di determinare i rischi residuali e la loro gestione, nonché della valutazione globale dell'andamento del programma complessivo.

Risk-Assessment

Il ***Risk-Assessment*** è un processo che determina l'estensione delle potenziali minacce e dei rischi associati ai sistemi IT.

Il ***Rischio*** è in funzione della probabilità che una data minaccia crei una potenziale vulnerabilità, e un conseguente impatto negativo nei confronti dell'organizzazione.

Risk-Assessment



Descrizione dei Sistemi

Identificazione delle minacce

Identificazione delle vulnerabilità

Control Analysis

Analisi dell'impatto

Determinazione delle probabilità

Determinazione del rischio

Raccomandazioni di controllo

Documentazione dei risultati

Naturalmente il ciclo è ricorsivo, nel senso che modifiche apportate ai Sistemi, o nuove vulnerabilità, fanno ripartire tutto il processo.

Risk-Assessment 1/2

Gli step del processo di ***Risk-Assessment*** sono i seguenti:

- **Descrizione dei sistemi** - identificare l'area in cui operano i Sistemi IT, con le informazioni inerenti alle risorse che li caratterizzano
- **Identificazione delle minacce** - ossia le fonti potenziali per esercitare (accidentalmente o meno) una specifica vulnerabilità dei sistemi
- **Identificazione delle vulnerabilità** - cioè i buchi o criticità inerenti la sicurezza dei sistemi, sfruttabili (accidentalmente o meno) che si risolvono in violazioni delle policy di sicurezza
- **Control Analysis** - riguarda l'analisi dei controlli implementati, o in fase di realizzazione, che l'organizzazione utilizza per minimizzare la probabilità che una minaccia si trasformi in vulnerabilità

Risk-Assessment 2/2

Gli step del processo di ***Risk-Assessment*** (continua):

- **Determinazione delle probabilità** - serve a realizzare un rating della probabilità che una vulnerabilità possa essere utilizzata per realizzare una minaccia ai sistemi
- **Analisi dell'impatto** - ossia misurare il livello di rischio associato all'impatto risultante dallo sfruttamento della vulnerabilità
- **Determinazione del rischio** - dei vari Sistemi analizzati
- **Raccomandazioni di controllo** - in questo step vengono suggeriti i controlli che debbono eliminare o mitigare i rischi identificati
- **Documentazione dei risultati** - report manageriale che aiuti l'Organizzazione a prendere decisioni su come allocare risorse per ridurre e correggere potenziali perdite, collegate ai rischi

Internal Auditor & IT Auditor

"L'Internal Auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza dell'organizzazione. Assiste l'organizzazione nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, che genera valore aggiunto in quanto finalizzato a valutare e migliorare i processi di controllo, di gestione dei rischi e di corporate governance."

La definizione si può rigirare per l'IT auditor per quello che riguarda le problematiche EDP.

IA e Risk-Management

Gli standard prevedono che l'Internal Auditor:

- assista l'Organizzazione nell'indicazione e nella valutazione delle maggiori esposizioni al rischio
- contribuisca al miglioramento del sistema di risk-management e di controllo
- che si occupi del monitoraggio e valutazione dell'efficacia del sistema di risk-management

Concetti Chiave:

- Il Risk-Management è responsabilità del Management
- Supporto in merito all'adeguatezza ed efficienza del processo
- Consulenza per l'implementazione della metodologia di Risk-Management

Il ruolo dell'Auditor

I ruoli che l'internal auditor può ricoprire nell'ambito del processo sono vari:

- ✗ Sottoporre ad audit il processo di IT Risk-Assessment, in funzione della sua criticità
- ✗ Operare come fornitore di strumenti metodologici per il management
- ✗ Partecipare come membro effettivo a comitati di analisi, supervisione e monitoraggio sul processo
- ✗ Agire come risk & control analyst
- ✗ Diventare centro di competenza per la gestione dei rischi in azienda
- ✗ Svolgere servizi di Enterprise-wide Risk-Management, coordinando e monitorando il processo a livello di intera organizzazione

Spunti operativi

Alcuni possibili interventi di audit da effettuare sul processo di risk-assessment:

- Stato dei controlli rispetto alle vulnerabilità
- Analisi della Risk determination
- Analisi delle policy aziendali rispetto alle minacce (profilo organizzativo)
- Determinazione dell'adeguatezza delle risorse (umane, finanziarie, tecnologiche) rispetto ai rischi

GRAZIE PER L'ATTENZIONE!

Per scaricare la presentazione
http://it.geocities.com/davide_susa/

EDP Auditor: **Davide SUSA - ACSec**
davide_susa@yahoo.it