Il rischio da punta di vista dell'IS auditor

James Cheyne , CISA, CISM
NCR Italia s.r.l.

Contenuto

- Preambolo
- La percezione del rischio
- Il dilemma
- Le strategie
- Conclusione

Preambolo

- Il rischio di audit = business risk
- L'auditor si tutela attraverso:
  - Una valutazione del rischio che comprende
    - Inherent Risk
    - Control Risk
    - Detection Risk (o Substantive Risk)
  - La definizione di materialità

Preambolo

- Tutto ciò è insito nell'approcio standard alla revisione
- Tuttavia questo non è il punto di vista dell'IS auditor

Preambolo

- Come IS auditor devo:
  - Evidenziare tutti i rischi informatici
  - Valutarne l'impatto e le conseguenze
  - Stabilire dei processi di salvaguardia
  - Implementare tutto quanto serve per ridurre il rischio
  - Monitorare le procedure e processi di sicurezza

Preambolo

- Non avendo certezze e essendo l'IS il fattore chiave di un'azienda ho una diversa percezione del rischio

La percezione del rischio

- La conoscenza delle problematiche IT e dei rischi inerenti porta ad una valutazione del rischio elevato
- L'informatico è portato ad essere catastrofico
- Qualsiasi evento avrà le conseguenze peggiori

Veduta del management

- Dall'altra parte il management
  - Non conosce a fondo le problematiche e quindi non condivide il rischio
  - Pensa che l'auditor esagera
  - Crede che non capiterà "a me"
  - Se dovesse capitare non avrà le conseguenze descritte
  - Quindi non spende inutilmente

Il dilema

- Il problema è dunque di offerta e domanda
- L'offerta c'è ma bisogna stimulare la domanda
- come

Le Strategie

- Come fa L'IS auditor a conciliare le proprie paure di danni dovuti alla conoscenza con lo scettiscismo
- In sostanza bisogna:
  - Educare
  - Spaventare

Le Strategie

- Solo se il management ha “l’imprinting” delle conseguenze sarà disposto ad investire
- Il “topo” e “l’imprinting”
- Casi veri

Le Strategie

- Creare paura che l'evento:
  - Accadrà (certezza e tempistica)
  - Avrà conseguenze disastrose
  - É inevitabile
- É reale (ma limitato) e ad esso sono stati associati degli eventi drammatici ma credibili
- Risultato: grande spese e zero rischio (per l'auditor)

Conclusione

- L'IS auditor ha una veduta catastrofica perchè tratta un argomento non facilmente valutabile e imprevedibile