Presentazione gruppo di Ricerca ISACA Roma

Basel II and Information Systems

Operational Risk Management

(a cura di **Paolo Ottolino – CCSE OPST CISSP-ISSAP**)

INDICE DELLA PRESENTAZIONE:

1. Introduzione a Basel II
2. Operational Risk Management
3. Operational Risk & ISMS
4. Impatto sulle Aziende
5. Varie – Q&A

The Three Pillars

I tre pilastri di Basilea II e le loro implicazioni:

1. Minimum Capital Requirements (Requisiti Patrimoniali Minimi)
2. Supervisory Review Process (Supervisione delle Autorita' di Vigilanza, nazionali e di Comunita' Europea)
3. Market Discipline (Disciplina di mercato)

Introduzione a Basel II

The Minimum Capital Requirements

1. Risk Management
    - Credit Risk
    - Market Risk (Trading Book)
    - Operational Risk (=> Information System Management) NEW!
2. Differenze fra Basel I e Basel II => Introduzione dell' Operational Risk Management
3. Rating

Introduzione a Basel II

$$\frac{\text{Capitale Totale}}{\text{Credit Risk} + \text{Market Risk} + \text{Operational Risk}} = \text{Capital Ratio (>= 8\%)}$$

Rivisto **Non Rivisto** **Nuovo!**

Operational Risk

Operational Risk Definition

"… rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Tale definizione include il rischio legale ma non quello strategico e di reputazione."

Le cause:

- Processi Interni
- Personale
- Sistemi
- Eventi Esterni

Operational Risk Approaches

Approcci previsti per il calcolo del Rischio Operativo:

- Basic Indicator Approach (dal 1 Gennaio 2006) => $\alpha = 15\%$
- Standardized Approach (entro 31/12/2006) => $\beta =$ 12, 15, 18%, indipendenza dalle Business Lines
- Advanced Measurement Approach (entro 31/12/2007) => Internal Operational Risk Measurement

Operational Risk & ISMS

Gli obiettivi di studio, relativamente all'impatto dell'AMA sulle Banche, potrebbero essere i seguenti:

1. il rischio operativo e l'Information System Security => ISMS
   - rischio tecnologico (malfunzionamenti, manomissioni)
   - rischio procedurale (errori nelle procedure)
   - rischio personale (Access Control, Fraudes, ...)
2. metodologie ottimali (ITIL, BS7799, CObIT,...) per la gestione del rischio operativo
3. strumenti, soluzioni ed architetture standard per la gestione del rischio operativo, compatibili con altre esigenze correlate (e.g. SOX, International Accounting Standard)

Operational Risk & ISMS

Le aree di interesse, rispetto alle quali identificare degli standard, potrebbero essere le seguenti:

1. Incident Management & Incident Handling (e gestione dei relativi Report)
2. Business Continuity
3. Identity Management
4. Hardening dei Sistemi
5. Network & System Security (e.g. OSSTMM)
6. Application Security (e.g. Web Banking => OWASP)
7. Aspetti Procedurali e Personali
8. …

Impatto sulle Aziende

Rating & Rischio di Default

Il Credit Risk Management da parte delle Banche impone l'utilizzo di appropriati strumenti di Rating per stabilire il grado di solvibilità (eventualmente tramite metodi interni IRB).

I Rischio di Default viene calcolato in base a:

- Elementi Quantitativi (desumibili dal Bilancio)
- Elementi Qualitativi (quali la Capacità di Gestione del Rischio)

=> Gestione del Rischio Operativo (trasferimento della esperienza Basel II fuori dal settore Bancario)

Impatto sulle Aziende

Rating & Information Security

Gli obiettivi di studio, relativamente all'impatto dell'adozione del Rating sulle aziende, potrebbero essere i seguenti:

1. IAS
2. SOX Compliance
3. … ed in generale tutto quanto possa concernere l'aumento del rating mediante l'IS

Organizzazione Possibile

- Esplorazione iniziale della problematica al fine di individuare gli argomenti di maggiore interesse
- Attività di approfondimento di ogni argomento, possibilmente condotta in parallelo
- Collezione dei risultati e presentazione a Isaca di un report

Bibliografia

I riferimenti “iniziali”:

1. Bank of International Settlement (http://www.bis.org)
2. International Accounting Standard Board (http://www.iasb.org)
3. Sarbanes Oxley Act
4. CObIT
5. BS 7799
6. …

Varie Q&A

Sono gradite le domande

Grazie dell'attenzione!

Paolo Ottolino
Tel 3481303916
Paolo.Ottolino (at) business-e.it