ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Basel II & IT Risk Management

Integrazione della Gestione del Rischio IT nell'ambito della Misurazione e del Controllo del Rischio Operativo

Metodologia di IT Risk Management in ottica Basel II AMA

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

Policy & Strategy – Security Consulting Services

paolo_ottolino (at) symantec.com

symantec

Agenda

- Basilea 2: Il nuovo accordo sul Capitale
  - Introduzione al Rischio Operativo (Calcolo degli Accantonamenti)
  - Opportunità: Rischi IT – Risk Analysis - SGSI
- Strategia di Intervento
  - Cooperazione fra Controllo Rischi e Sicurezza IT
    - Divisione degli ambiti di Competenza
    - Business vs. IT Organization
    - Capital Charge e Countermeasures Selection
- Processo di Gestione del Rischio
  - Asset Modeling & Selecton
    - Business Lines e Applications
    - Ri-utilizzo del BCP
  - Integrazione nel Calcolo del Rischio Operativo
    - LET (Minacce) e RF (Vulnerabilità)
    - Worst Case Analysis
    - Threats & Vulns Analysis
  - Rischio e Contromisure IT
    - Gap Analysis
    - Remediation Plan: Countermeasures Effectiveness
- Possibili Evoluzioni
  - Calcolo del Rischio di Default

1. Basel II: Nuovo Accordo sul Capitale (1)

Il nuovo accordo sul capitale é mirato a garantire maggiore solidità delle banche, mediante la capacità di far fronte ad eventi imprevisti:

Minacce
Vulnerabilità

Rischi

Accantonamenti

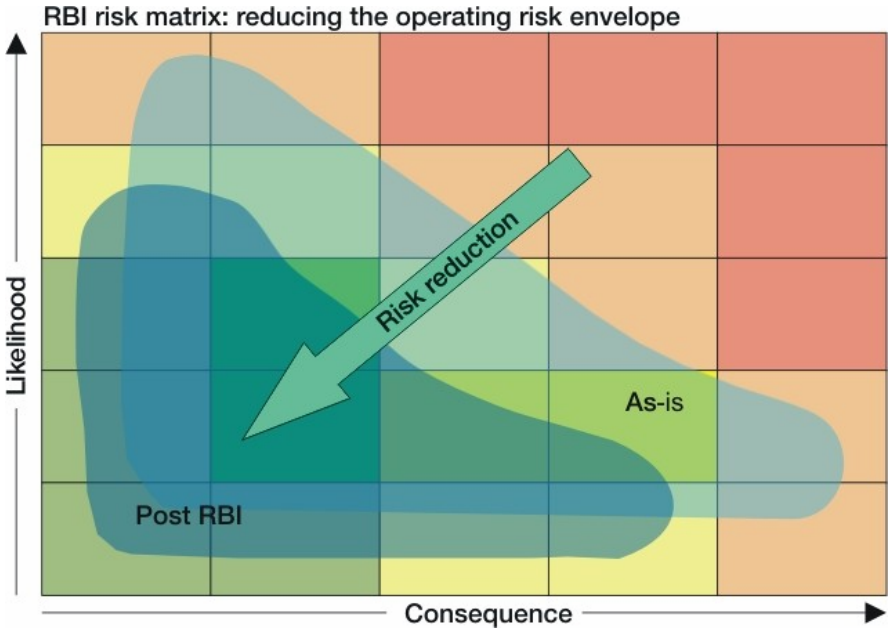
1. Basel II: Nuovo Accordo sul Capitale (2)

Maggiori i rischi, maggiori gli accantonamenti effettuati dalla banca:

→ minore la quantità di soldi liquidi disponibili per il business

Viceversa, minori i rischi (mediante una opportuna strategia di riduzione del rischio ed una corretta politica di gestione della sicurezza), minori gli accantonamenti:

→ maggiore la quantità di denaro liquido, disponibile per il business



1. Basel II: Nuovo Accordo sul Capitale (3)

Il nuovo accordo sul capitale prevede il trattamento dei seguenti due tipi di rischi:

- Rischio di Credito: valutazione del rischio inerente l'erogazione di un credito (mancato ritorno del denaro prestato, per insolvibilità del cliente):
  - Valutazione Quantitativa → Analisi dei documenti di Bilancio della società richiedente il credito
  - Valutazione Qualitativa → Analisi di eventuali informazioni "ufficiose" relative alla società richiedente il credito (es. Valutazione del Rischio di Default)
- Rischio Operativo: valutazione del rischio intrinseco all'esercizio stesso, alla erogazione dei servizi offerti, ad esempio, a causa dei seguenti fattori:
  - Frodi, Falsificazioni
  - Rapine
  - Rischio Informatico

1. Basel II: Nuovo Accordo sul Capitale (4)

3 livelli di calcolo di valutazione, per entrambi i rischi (da attivare secondo scaglioni temporali).

31-12-2007: Livello Massimo per entrambi, consistente nella realizzazione di meccanismi di calcolo appositamente sviluppati:

- ***Rischio di Credito*** → *Internal Rating Based* (IRB): modelli interni di valutazione della solvibilità dei clienti
- ***Rischio Operativo*** → *Advanced Measurement Approach* (AMA): modelli (finanziari) di calcolo del rischio. Importante l'inclusione/integrazione del Rischio IT nel modello di calcolo (necessaria la conoscenza approfondita delle problematiche di IT Security)

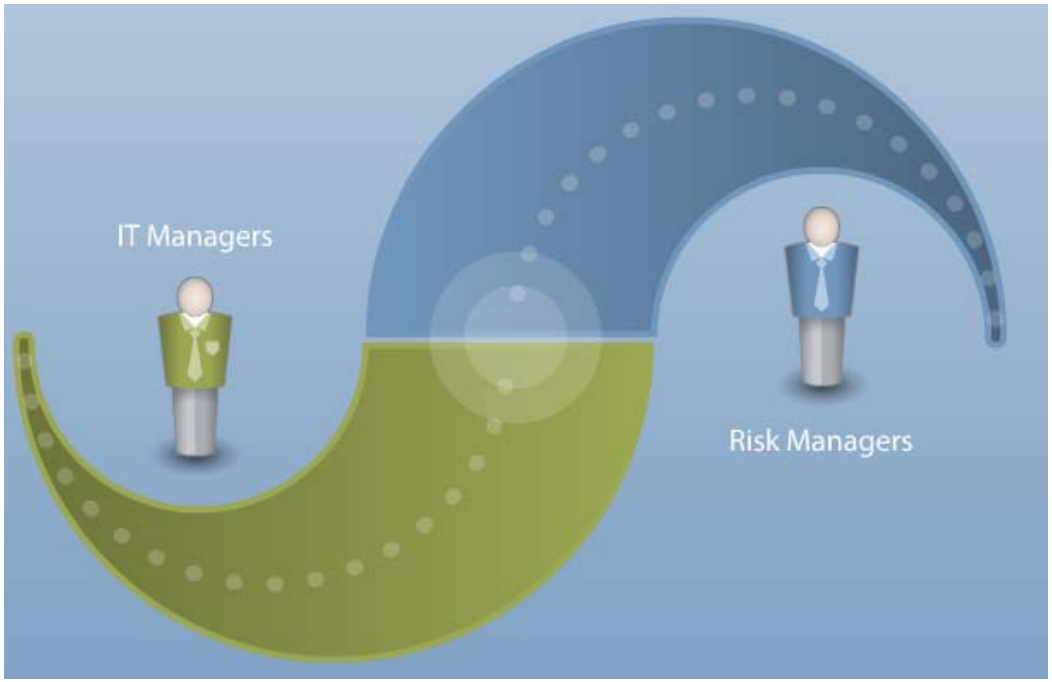
Security Advisor

- **IT Risk Management**
  - **IT Risk Analysis**
  - **IT Risk Treatment**
- **Information Security Management System**

Scenario analogo a quello della SOX

Risk Management & Basel II: new challenge

- Migliorare l'integrazione tra il "Rischio IT" ed il "Rischio Operativo"
- Aumentare l'efficacia della misura del "Rischio Operativo"
- Pianificare gli investimenti, considerando i rischi "complessivi"
- Ottimizzare gli interventi riducendo i costi complessivi ed aumentando i livelli di servizio



2. Strategia d'Intervento (1)

Definizione di Rischio Operativo

"…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."

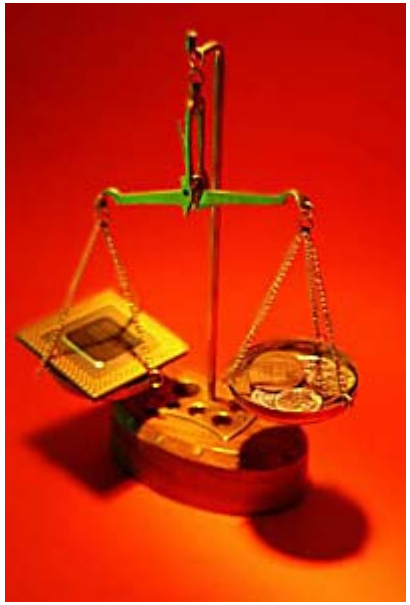
Strutture / Loss Effect Type	Vendita Middle Office	Back Office Governance
Responsabilità Legale	Basel II	
Azione Autorità di Regolamentazione		
Perdita o Danno alle Attività		
Restituzione/Rimborsi		
Perdite per Errore non Recuperate		
Write Down		
Danno Reputazionale		
Mancato Introito		

2. Strategia d'Intervento (2)

Funzioni Bancarie Interessate

Il calcolo del Rischio Operativo, da un punto di vista IT, vede coinvolte, essenzialmente, due funzioni della Banca

- *Misurazione e Controllo dei Rischi* → responsabile, tra l'altro, dell'analisi, della valutazione e della gestione del rischio complessivo aziendale (ivi compreso il Rischio Operativo)
- *Sicurezza IT* → responsabile della definizione della strategia di sicurezza IT, realizzazione e sviluppo della sicurezza logica, mediante individuazione dei meccanismi da applicare sui sistemi e definizione dei criteri di sicurezza delle reti di trasmissioni dati

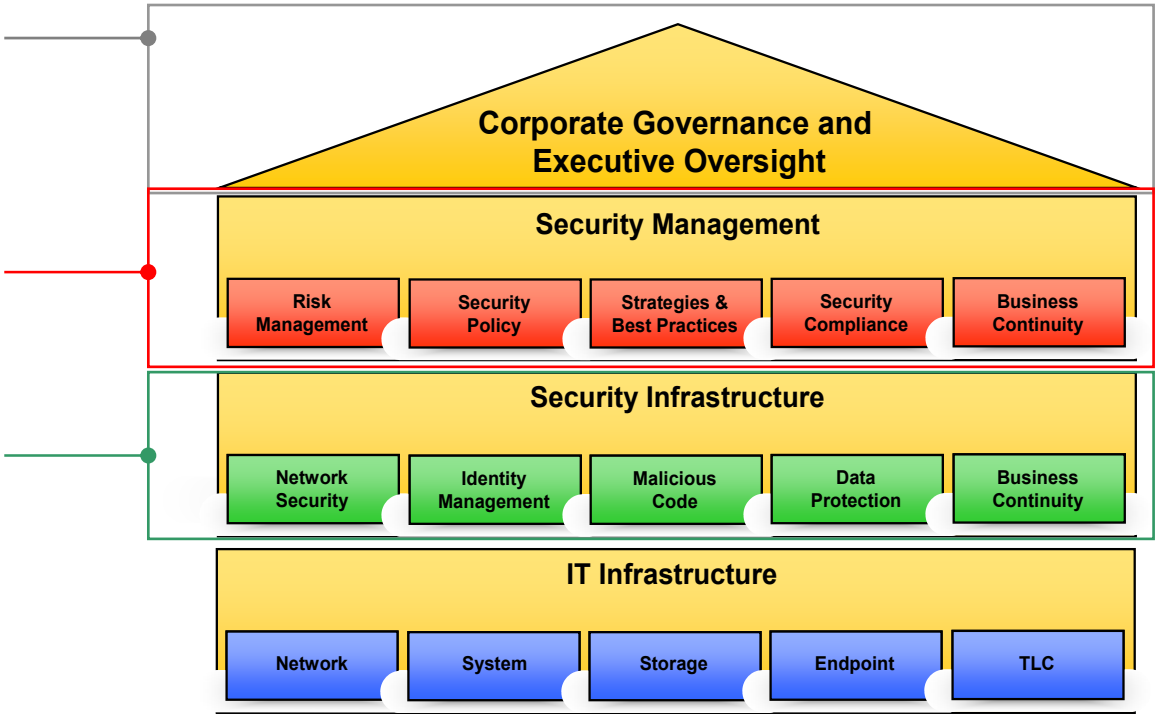


2. Strategia d'Intervento (3)

Livelli d'Intervento

Analogamente agli altri ambiti di compliance IT (e.g. SOX, HIPAA) gli interventi per la gestione del Rischio Operativo secondo Basilea 2 possono avvenire a vari livelli:

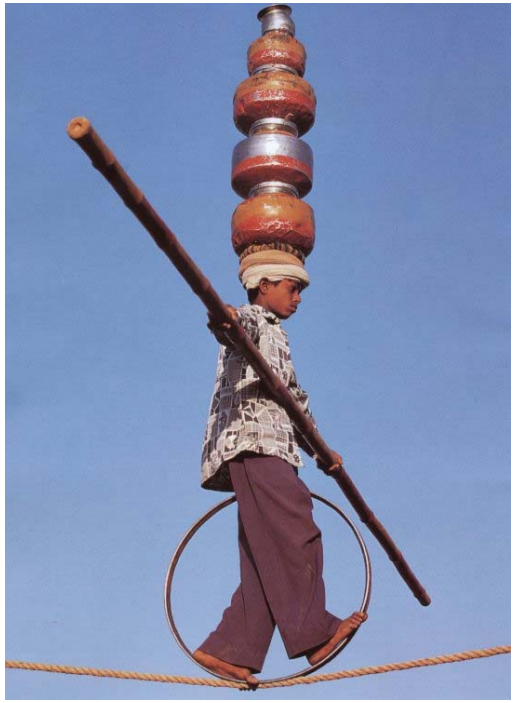
- **ISMS**: definizione del sistema di Governance per la sicurezza delle informazioni, coerentemente con le strategie aziendali
- **Risk Management**: definizione delle metodologie e dei criteri per l'analisi e la gestione della sicurezza IT. Integrazione con le infrastrutture di Operational Risk Management
- **Security Development & Testing**: realizzazione e controllo di soluzioni di sicurezza appositamente sviluppate, allo scopo di soddisfare i requisiti di sicurezza individuati



2. Strategia d'Intervento (4)

Cooperazione fra Controllo Rischi e Sicurezza IT

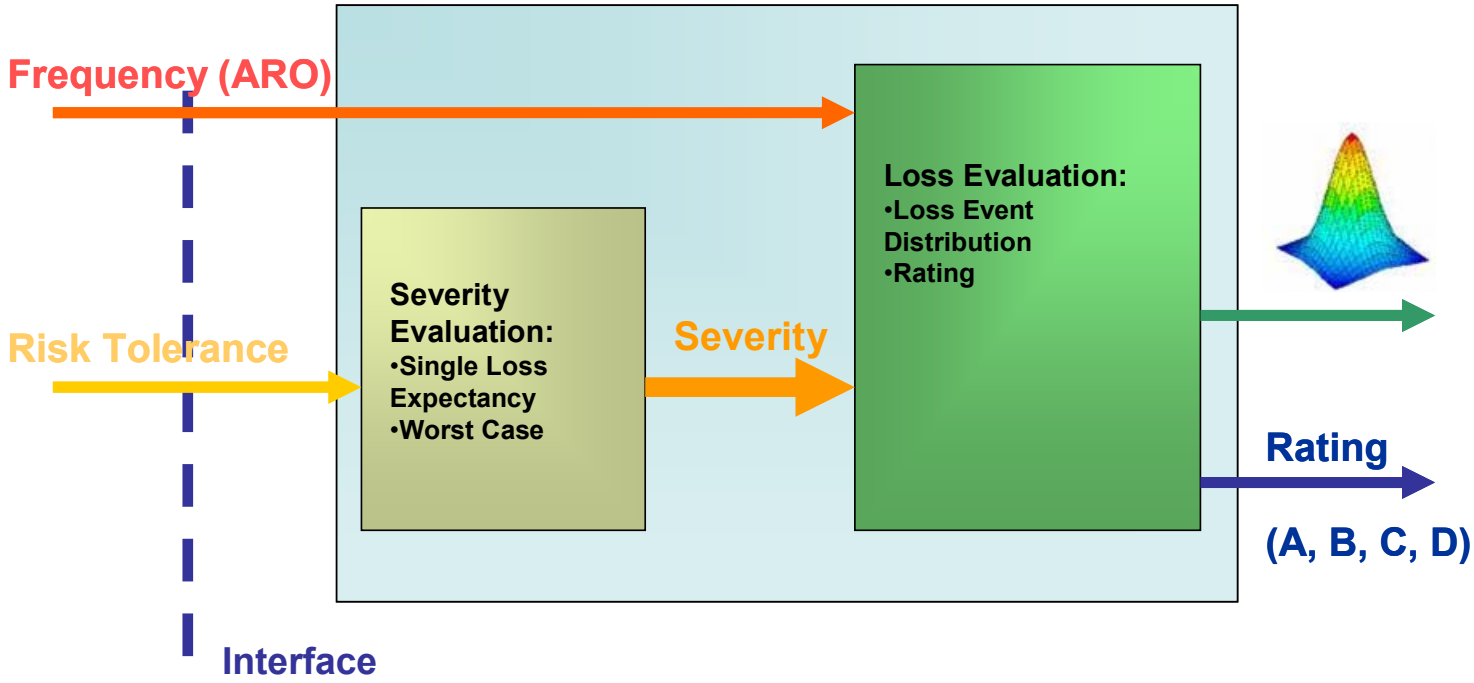
L'integrazione dell'IT Risk Analysis nella Gestione del Rischio Operativo presenta i seguenti punti di attenzione/requisiti:



- **Calcolo del Rischio**: possono essere sfruttati gli stessi strumenti adottati dall'Area di Misurazione e Controllo del Rischio Operativo
- **Divisione per Ambiti di Competenza**: L'entità delle minacce, delle vulnerabilità attuali e dei rischi devono essere stimate attraverso l'ausilio di personale con competenze specifiche
- **Business versus Application**: la misurazione del Rischio Operativo deve essere effettuata a livello di Business Line. Il focus tipico delle analisi e gestione dei Rischi IT é a livello di applicazione/infrastruttura
- **Capital Charge & Countermeasures Selection**: nella scelta delle contromisure da attuare e del piano di rientro, devono essere presi in considerazione gli accantonamenti da effettuare

2. Strategia d'Intervento (5)

Calcolo del Rischio



La valutazione dell'entità del rischio (anche per il contesto IT) può essere svolta mediante l'ausilio degli strumenti già acquisiti dalla banca, utilizzati per il calcolo del Rischio Operativo. Fondamentale determinare l'interfaccia di integrazione con il calcolo)

2. Strategia d'Intervento (6)

Divisione degli Ambiti di Competenza

Event / Context	Fraud	Theft	Disaster	Errors	Fault	Inefficiency
Physical	✓	✓	✓			
Processes	✓		✓	✓	✓	✓
IT-Related	✓		✓	✓	✓	✓

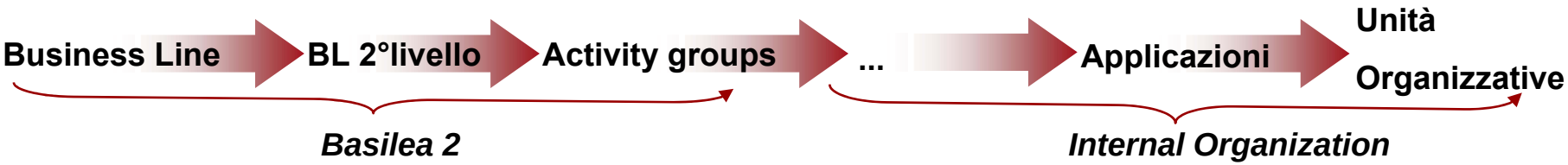
La valutazione dell'entità del rischio deve essere effettuata, per ogni ambito, da personale competente. La tabella illustra la correlazione tra classi di minaccia (Event) e ambito di competenza (Context).

In particolare le problematiche di sicurezza IT devono esaminate da professionisti dell'IT Security.

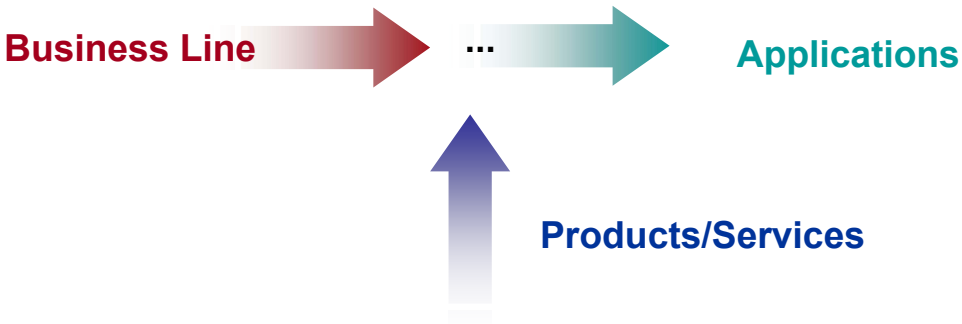
2. Strategia d'Intervento (7)

Business vs. Application

Basilea 2 fissa la suddivisione dell'attività bancaria (e quindi delle attività di analisi) secondo una mappa di macroprocessi standard, per ogni attività di un istituto bancario. Inoltre illustra una tassonomia di alto livello. I valori di Rischio devono essere forniti a livello di Business Line



E' importante determinare il livello da cui partire per l'analisi del Rischio, che non può essere la Business Line (in quanto troppo astratta rispetto alla struttura IT) né l'Applicazione, troppo di dettaglio rispetto alla struttura aziendale.



2. Strategia d'Intervento (8)

Capital Charge & Countermeasure Selection

L'ammontare degli accantonamenti condiziona pesantemente il processi di scelta delle contromisure. Difatti solitamente si ha:

$$Cost(Countermeasure) = f(SLE * ARO)$$

Invece, nel caso di Basilea 2, gli accantonamenti corrispondono ad un costo maggiore, corrispondente a circa un decimo del valore del Capital Charge (dovuto a mancato guadagno), secondo la formula:

$$Cost(Countermeasure) = f(CapitalCh\arg e * 10\%)$$

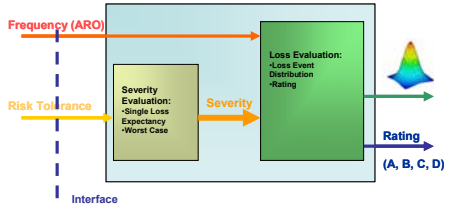
Ovviamente questo implica l'utilizzo di una metodologia di analisi dei rischi quantitativa.

2. Strategia d'Intervento (9)

Cooperazione fra Controllo Rischi e Sicurezza IT

Riassumendo:

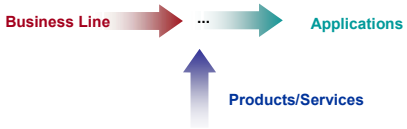
- **Calcolo del Rischio** → Definizione di una Apposita Interfaccia (Valutazione dei LET, RF)



- **Divisione per Ambiti di Competenza** → Partizionamento dell'Analisi per Aree (IT related LET, RF)

Event Context	Fraud	Theft	Disaster	Errors	Fault	Inefficiency
Physical	✓	✓	✓			
Processes	✓		✓	✓	✓	✓
IT-Related	✓		✓	✓	✓	✓

- **Business vs. Application** → Partizionamento e Prioritizzazione dell'Analisi (Prodotti e Servizi)



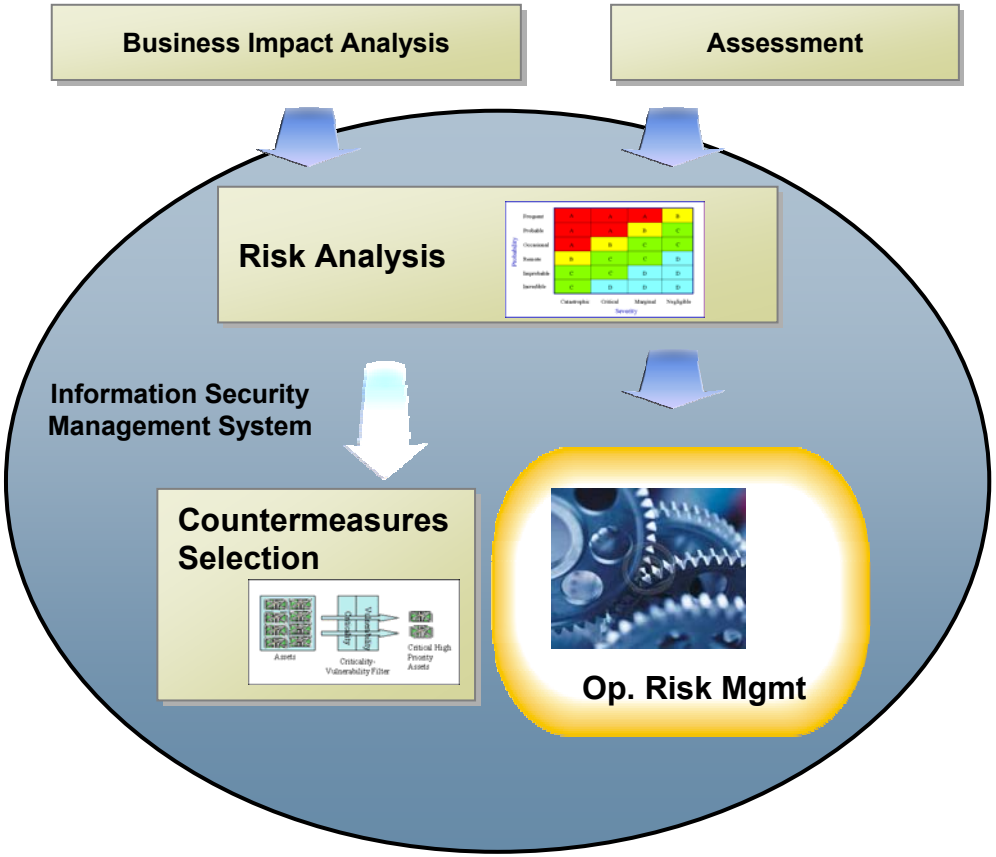
- **Capital Charge & Countermeasures** → Analisi Quantitativa con Valutazione degli Accantonamenti

2. Strategia d'Intervento (10)

Integrazione con le Strutture Esistenti

Nella realtà italiana, le banche si sono già attrezzate allo scopo di effettuare:

- ***Operational Risk Management*** → gestione integrata dei rischi operativi, mediante ***Operational Risk Tools***. Determinazione della misura efficiente del Capitale di Rischio.
- ***Business Continuity Management*** → gestione della continuità del business, secondo i dettami della Banca d'Italia. Redazione della ***Business Impact Analysis***

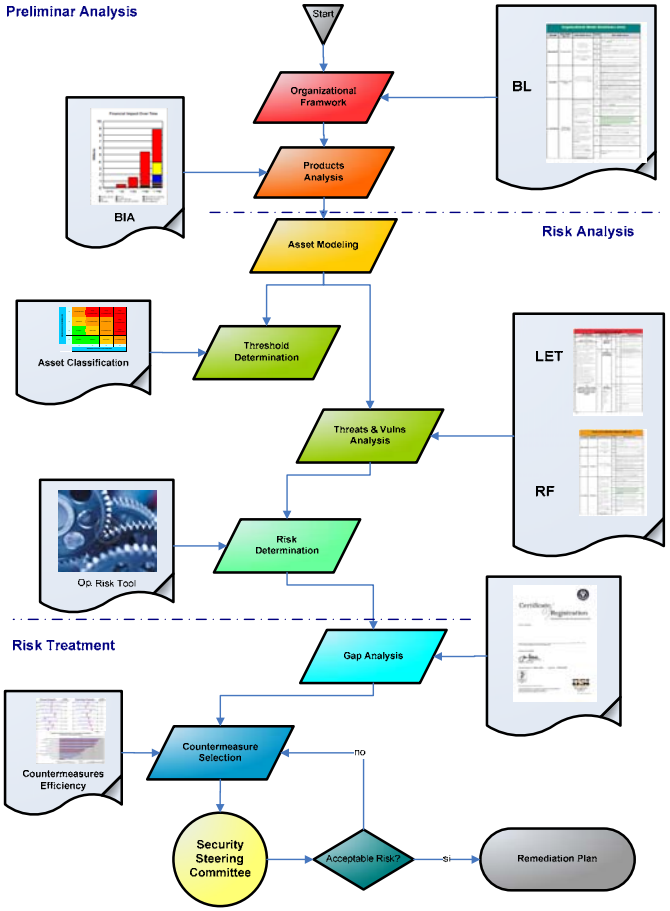


3. Processo di Gestione del Rischio (1)

Process Overview

Il processo di misurazione e gestione del rischio IT integrato, é stato ideato nel seguente modo:

- Preliminar Analysis
  - Organizational Framework
  - Product Analysis
- Risk Analysis
  - Asset Modeling
  - Threshold Determination
  - Threats & Vulns Analysis
  - Risk Determination
- Risk Treatment
  - Gap Analysis
  - Countermeasures Selection (Countermeasures Effectivess)
  - Remediation Plan (Steering Committee)



3. Processo di Gestione del Rischio (2)

Preliminar Analysis (1)

Organizational Framework

Obiettivo: determinare l'ambito e le modalità di analisi, sulla base delle 8 B.L.:

1. **Corporate Finance**
2. **Trading & Sales**
3. **Retail Banking**
4. **Commercial Banking**
5. **Payment & Settlement**
6. **Agency Services**
7. **Asset Management**
8. **Retail Brokerage**

Organizational Model (Business Lines)

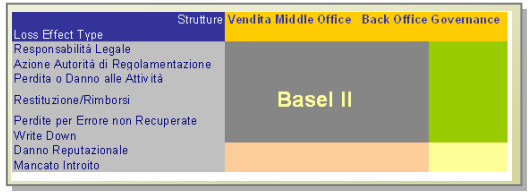
B.L.	B.L. 2° liv.	Activity Group	Code	Products
Corporate Fiance	*Merchant Banking*	Incompetenza / Impreparazione professionale. Inadeguata gestione del "clima aziendale" Inefficiente/inefficace/ inadeguata organizzazione del lavoro	P 1.1.a	**Security Awareness**: Insufficiente cultura aziendale in tema di Security
			P 1.1.b	**People Selection**: Inadeguato sistema selezione (assunzione).
			P 1.1.c	**Roles & Responsibilities**: Mancanza di una chiara assegnazione di ruoli e responsabilità alle risorse.
			P 1.1.d	**Resource Allocation**: Inadeguata allocazione risorse
			P 1.1.e	**Work Loads**: Inadeguata distribuzione carichi di lavoro
Trading & Sales	*Market Making*	Carenze / inadeguatezze nella gestione del rapporto con gli outsourcer/fornitori	P 4.1.a	**Outsourcing Clauses**: Assenza/inadeguatezza di formalizzazione del rapporto con gli outsourcer/fornitori (comunicazione, modalità e livello di erogazione dei servizi,…)
			P 4.1.b	**NDA**: Carenze/inadeguatezze nella fase di definizione degli aspetti di riservatezza all'interno di accordi contrattuali relativi prodotti/servizi.
			P 4.1.c	**SLA**: Carente / Inadeguata definizione sulle modalità e il livello di erogazione del servizio (SLA).
			P 4.1.d	**Provider Selection**: Inadeguato sistema di selezione dei fornitori.
			P 4.1.e	**Source Escrow**: Assenza/Inadeguatezza dei vincoli contrattuali con terze parti fornitrici di SW relativamente al rilascio e conservazione (in caso di fallimento) dei codici sorgente degli applicativi commissionati
Retail Banking	*Bank Services*	Assenza / Inadeguatezza misure a fronte di calamità naturali (business continuity plan, …) Assenza / inadeguatezza misure di prevenzione e sicurezza verso eventi di natura accidentale (per causa umana e/o naturale) - *"safety"* Inadeguatezza/obsolescenza delle infrastrutture Assenza / inadeguatezza misure di prevenzione e di sicurezza verso atti di natura criminosa (rapine, terrorismo, vandalismo,…) - *"security"* Assenza / Inadeguatezza di passaggi autorizzativi per l'esecuzione delle attività operative Assenza / inadeguatezza misure di controllo verso attività non autorizzate e frodi da parte di dipendenti Assenza / inadeguatezza misure preventive verso frodi da parte esterni	P 5.1.a	**Physical Access**: Inefficiente/Inefficace processo di identificazione/registrazione per l'accesso fisico ai locali ed alle aree sensibili
			P 5.1.b	**Personal Badge**: Non è ben definito il processo per la corretta individuazione di personale non autorizzato (esposizione badge, differenziazione badge ecc.).
			P 5.1.c	**Physical Devices**: Non sono presenti o risultano inadeguate misure di sicurezza di tipo fisico (es. telecamere a circuito chiuso, installazione di barriere anti-intrusione dall'esterno: grate, vetri anti-sfondamento).
			P 5.1.d	**Supplier Access**: L'accesso da parte di esterni (consulenti, addetti alla manutenzione ecc.) non avviene previa autorizzazione di personale interno
			P 5.1.e	**Safety Devices**: Assenza / inadeguatezza misure di prevenzione e sicurezza (es.: estintori, dispositivi salvavita, porte tagliafuoco, manutenzione impianti, rilevatori fumo e acqua, materiali ignifughi, ...) - "safety".
			P 5.1.f	**Media Handling**: Inadeguata conservazione dei supporti

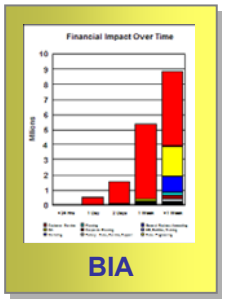
3. Processo di Gestione del Rischio (3)

Preliminar Analysis (2)

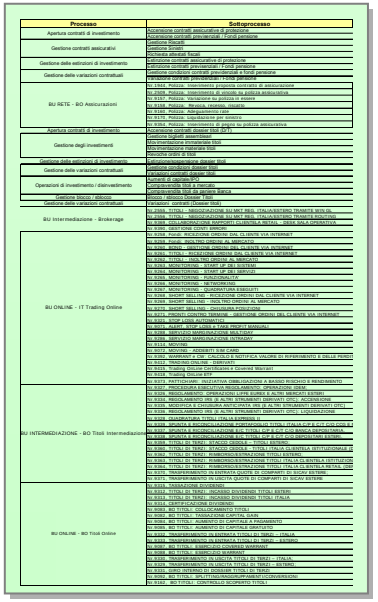
Product Analysis

Obiettivo: determinare le priorità e la schedulazione delle attività di analisi





Processo	Sottoprocesso	Area / Funzione di Staff	Unità / Ufficio	RTO	Altre società del gruppo	Descrizione attività	Input / output al processo
Gestione portafogli	Gestione ordini e tesoreria	Gestione Investimenti	- Unità Bond&FX - Unità Equity - Unità Trading&Execution - Unità Private - Unità Equity Research	4 h			
Gestione portafogli	Gestione ordini e tesoreria	Gestione Investimenti	Unità Total Return&Quant	1 g			
Gestione portafogli	Gestione ordini e tesoreria fondi comuni bilanciati	Gestione Investimenti	Unità Balanced Funds	1 g			
Gestione portafogli	Gestione ordini e tesoreria fondo Fineco IA	Amministrazione e Sviluppo	Amm. Prodotti/Uff. Controlli e Reporting Prodotti Individuali	4 h			
Gestione portafogli	Gestioni ordini e tesoreria per fondi GPF multibrand	Amministrazione e Sviluppo	Amm. Prodotti/Uff. Controlli e Reporting Prodotti Individuali	4 h			
Gestione portafogli	Analisi e valutazioni macro economiche	Gestione Investimenti	Unità Macro Resarch	1 g			
Gestione portafogli	Monitoraggio rischi di gestione	Staff di Direzione	Risk Management	1 s			
Gestione portafogli	Partenza prodotti	- Marketing&Prodotti - Amministrazione e Sviluppo	- Staff Coordinamento Prodotti - Organizzazione e Sistemi/Uff. Business Application - Organizzazione e Sistemi/Uff. System&Knowledge Management	1 s			
Gestione portafogli	Pricing dei portafogli	Staff di Direzione	Risk Mangement	4 h			
Gestione portafogli	Reportistica per CdA e CG	Staff di Direzione	Risk Mangement	1 s			
Gestione portafogli	Rilevazione scostamento limiti di gestione	Staff di Direzione	Risk Mangement	3 gg			
Amministrazione portafogli	Attività di backoffice e valorizzazione portafogli	Amministrazione e Sviluppo	- Amm. Prodotti/Uff. Back Office e Controlli - Amm. Prodotti/Uff. Controlli e Reporting Prodotti Individuali - Amministrazione Clientela	4 h			
Amministrazione clienti	Assistenza clientela, gestione reclami e movimentazioni	Marketing&Prodotti	Unità Marketing&Communication	1 g			
Amministrazione clienti	Assistenza clientela prodotti individuali e reportistica	Amministrazione e Sviluppo	Amm. Prodotti/Uff. Controlli e Reporting Prodotti Individuali	1 s			
Amministrazione clienti	Comunicazione reportistica gestionale	Marketing&Prodotti	Unità Institutionals Advisory	1 s			
Amministrazione portafogli	Segnalazioni di Vigilanza	Amministrazione e Sviluppo	Amm. Prodotti/Uff. Segnalazioni	1 s			
Partenza gestioni	Comunicazione conferimenti e disinvestimenti	Marketing&Prodotti	Unità Institutionals Advisory	1 g			
Partenza gestioni	Comunicazione contratto	Marketing&Prodotti	Unità Institutionals Advisory	3 gg			
Gestione interventi su S.I.	Rilasci in produzione e modifica dati in produzione	Amministrazione e Sviluppo	Organizzazione e Sistemi/Uff. Front Office Gestioni Collettive	1 g			
Gestione interventi su S.I.	Rilasci in produzione e modifica dati in produzione	Amministrazione e Sviluppo	- Organizzazione e Sistemi/Uff. Business Application - Organizzazione e Sistemi/Uff. System&Knowledge Management	1 s			



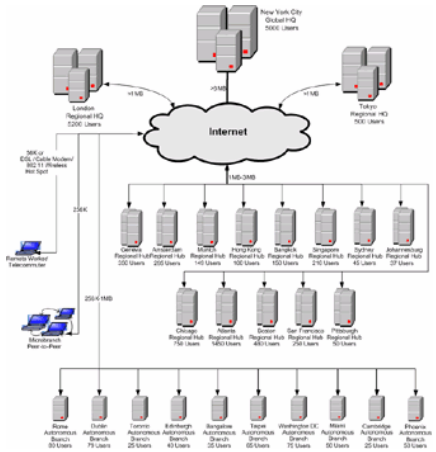
Processo	Sottoprocesso
Apertura contratti di investimento	Acquisizione contratti assicurativi di protezione
	Acquisizione contratti previdenziali / fondi pensione
Gestione contratti assicurativi	Gestione Riscatti
	Gestione Prestiti
	Richieste attestati fiscali
Gestione delle estinzioni di investimento	Estinzione contratti assicurativi di protezione
	Estinzione contratti previdenziali / fondi pensione
Gestione delle variazioni contrattuali	Gestione condizioni contratti previdenziali e fondi pensione
	Variazione nome per previdenziali / fondi pensione
BU RETE - BO Assicurazioni	SI 1842, Polizza: Intermediaria proposta contratto di assicurazione
	SI 2504, Polizza: Inadempienza di consulti da politica assicurativa
	SI 9397, Polizza: Variazione su polizza in essere
	SI 9146, Polizza: Allegato/Variazione quota
	SI 9148, Polizza: Allegato/Variazione rate
	SI 9179, Polizza: Liquidazione per sinistro
	SI 9362, Polizza: Intermediaria di pagto su polizza assicurativa
Apertura contratti di investimento	Acquisizione contratti deposit Bdl (ICT)
Gestione degli investimenti	Gestione sigilli assicurazioni
	Mandate/operazione immateriale titoli
	Mandate/operazione materiale titoli
	Rilevazione ordini di Vita
Gestione delle estinzioni di investimento	Gestione condizioni deposit Bdl
Gestione delle variazioni contrattuali	Gestione condizioni deposit Bdl
	Aggiornamento contratto deposit Bdl
	Richiesta di capitale BOC
Operazioni di investimento / disinvestimento	Compravendita titoli a mercato
	Compravendita titoli da società Banca
Gestione Blocco / Sblocco	Blocco / Sblocco Deposit Titoli
Gestione delle variazioni contrattuali	Aggiornamento contratto Deposit Bdl
BU Intermediazione - Brokerage	SI 2503, TITOLI - NEGOZIAZIONE SU MKT REG. ITALIA/ESTERO TRAMITE BON.IN
	SI 2504, TITOLI - NEGOZIAZIONE SU MKT REG. ITALIA/ESTERO TRAMITE BON.IN
	SI 3383, COLLABORAZIONE REPORTI CLIENTELA RETAIL - SIBM SOLA OPERATIVA
	SI 3384, GESTIONE CONTI ERRORI
	SI 3386, Fondi, RICEVIMENTO ORDINI DAL CLIENTE VIA INTERNET
	SI 3393, Fondi, REALTRO ORDINI AL MERCATO
	SI 3394, BOND - RICEVIMENTO ORDINI DAL CLIENTE VIA INTERNET
	SI 3395, TITOLI - RICEVIMENTO ORDINI DAL CLIENTE VIA INTERNET
	SI 3396, TITOLI - REALTRO ORDINI AL MERCATO
	SI 3398, MONITORING - START UP DEL SISTEMA
	SI 3399, MONITORING - START UP DEL SISTEMA
	SI 3400, MONITORING - SHARP UP DEL SISTEMA
	SI 3401, MONITORING - FUNZIONALITA'
	SI 3402, MONITORING - METODOLOGIA
	SI 3403, MONITORING - QUARANTUNA ESECUTTI
	SI 3406, SHARP SELLING - RICEVIMENTO ORDINI DAL CLIENTE VIA INTERNET
	SI 3408, SHARP SELLING - REALTRO ORDINI AL MERCATO
	SI 3410, SHARP SELLING - TAGLIANDI POSIZIONE
	SI 3411, SHARP SELLING - GESTIONE ORDINI DAL CLIENTE VIA INTERNET
	SI 3420, STOP LOSS AUTOMATICI
	SI 3423, ALERT, STOP LOSS E TAKE PROFIT MANUALI
	SI 3424, SERVIZIO MARGINALIZZAZIONE INIZIATIVA
	SI 3426, SERVIZIO MARGINALIZZAZIONE INTRADAY
	SI 3513, MOVIMS
	SI 3515, MOVIMS - AVVISATI E NM CARD
	SI 3516, MOVIMS - AVVISATI E NM CARD - VERIFICA VALORE DI RIFERIMENTO E DELLE PERDITE
	SI 3522, TRADING ONLINE - ESECUTI
	SI 3523, Trading Online Cancellazione e Governo Mandati
	SI 3524, Trading Online STP
	SI 3573, PATTICHIARI - INIZIATIVA OBBLIGAZIONI A BASSO RISCHIO E RENDIMENTO
BU INTERMEDIAZIONE - BO Titoli Intermediazione	SI 3327, PROCEDURA ESECUTIVA REGOLAMENTO OPERAZIONI OMAP
	SI 3328, REGOLAMENTO OPERAZIONI LUPIR EUREX E ALTRI MERCATI ESTERI
	SI 3329, REGOLAMENTO OPERAZIONI LUPIR EUREX E ALTRI MERCATI ESTERI
	SI 3330, MEMORIZZ.E CIRCOLAR.ANTICIPATA VAS DI ALTRI STRUMENTI DERIVATI OTC
	SI 3330, REGOLAMENTO VAS DI ALTRI STRUMENTI DERIVATI OTC - LIQUIDAZIONE
	SI 3331, DOCUMENTAZIONE TITOLI ITALIA EUROSIM 11
	SI 3334, MONITR & RICONCILIAZIONE PARTAPERTA DI TITOLI ITALIA VAF E VTT CON CDS E P
	SI 3335, MONITR & RICONCILIAZIONE EUROSIM TITOLI DIP & CUI CON BANCA DEPOSITARIA
	SI 3338, MONITR & RICONCILIAZIONE EUROSIM TITOLI DIP & CUI CON BROKER ESTERI
	SI 3339, TITOLI DI TERZI - RITACCO DIVIDENDI TITOLI ITALIA
	SI 3340, TITOLI DI TERZI - RITACCO DIVIDENDI TITOLI ITALIA
	SI 3341, TITOLI DI TERZI - RITACCO CEDOLA - TITOLI ITALIA CLIENTELA ISTITUZIONALE DI
	SI 3342, TITOLI DI TERZI - RITACCO CEDOLA - TITOLI ITALIA CLIENTELA ISTITUZIONALE DI
	SI 3363, TITOLI DI TERZI - RIMBORSI/ESTRAZIONE TITOLI ITALIA CLIENTELA ISTITUZIONA
	SI 3364, TITOLI DI TERZI - RIMBORSI/ESTRAZIONE TITOLI ITALIA CLIENTELA RETAIL DIR
	SI 3370, TRASFERIMENTO IN ENTRATA QUOTE DI COMPARTI DI SICAV ESTERE
	SI 3371, TRASFERIMENTO IN USCITA QUOTE DI COMPARTI DI SICAV ESTERE
BU ONLINE - BO Titoli Online	SI 3324, TASSAZIONE SUCCESSIONI
	SI 3332, TITOLI DI TERZI - INCASSO DIVIDENDI TITOLI ESTERI
	SI 3333, TITOLI DI TERZI - INCASSO DIVIDENDI TITOLI ITALIA
	SI 3354, CARTA CLIENTE DIVIDENDI
	SI 3680, BO TITOLI - COLLOCAMENTO TITOLI
	SI 3682, BO TITOLI - TASSAZIONE CAPITAL GAIN
	SI 3684, BO TITOLI - AUMENTO DI CAPITALE A PAGAMENTO
	SI 3685, BO TITOLI - AUMENTO DI CAPITALE GRATUITO
	SI 3326, TRASFERIMENTO IN ENTRATA TITOLI DI TERZI – ITALIA
	SI 3325, TRASFERIMENTO IN ENTRATA TITOLI DI TERZI – ESTERO
	SI 3681, BO TITOLI - ESERCIZIO CONVERSIONE RAPPORTI
	SI 3683, BO TITOLI - SPLIT/FUSIONE/GRUPPAMENTO/CONVERSIONI
	SI 3329, TRASFERIMENTO IN USCITA TITOLI DI TERZI – ITALIA
	SI 3329, TRASFERIMENTO IN USCITA TITOLI DI TERZI – ESTERO
	SI 3333, ERRORI INTERNI DI DIVIDENDI TITOLI DI TERZI
	SI 3683, BO TITOLI - SPLIT/FUSIONE/GRUPPAMENTO/CONVERSIONI
	SI 3180, BO TITOLI - CONTROLLO SCOPERTO TITOLI

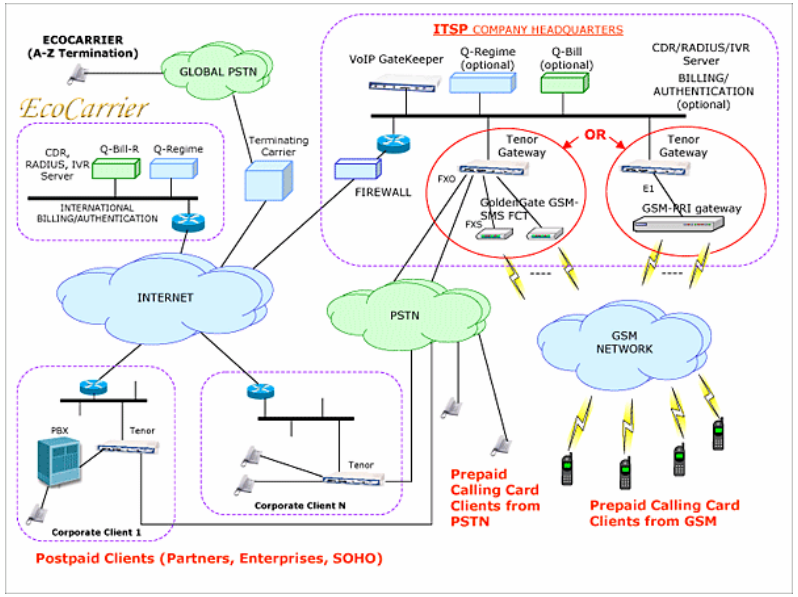
3. Processo di Gestione del Rischio (4)

Risk Analysis (1)

Asset Modeling

Obiettivo: determinare la composizione degli asset di ciascuna applicazione





flusso	Da	A	Protocollo PORTE	Traffico (kb)
1	10.41.73.130	10.41.52.30	snmptrap udp 162	18Kb/s
2	10.41.73.131	10.41.52.30	snmptrap udp 162	18 Kb/s
3	10.41.73.130	10.41.52.93	telnet TCP 23	10 Kb/s
4	10.41.73.131	10.41.52.93	http tcp 80	100 Kb/s
5	10.41.73.130	10.41.52.94	http tcp 8080	200 Kb/s
6	10.41.73.131	10.41.52.94	http tcp 8081	200 Kb/s
7	10.41.52.30	10.41.73.130	ssh tcp 22	10 Kb/s
8	10.41.52.30	10.41.73.131	telnet tcp 23	10 Kb/s
9	10.41.52.93	10.41.73.130	snmp udp 161	5 Kb/s
10	10.41.52.93	10.41.73.131	snmp udp 161	5 Kb/s
11	10.41.52.94	10.41.73.130	ssh tcp 22	1 Kb/s
12	10.41.52.94	10.41.73.131	ftp unidir. tcp 20/21	400 Kb/s
13	10.41.73.130	10.6.85.51	ftp unidir. tcp 20/21	500 Kb/s
14	10.41.73.131	10.6.85.51	http tcp 8081	100 Kb/s

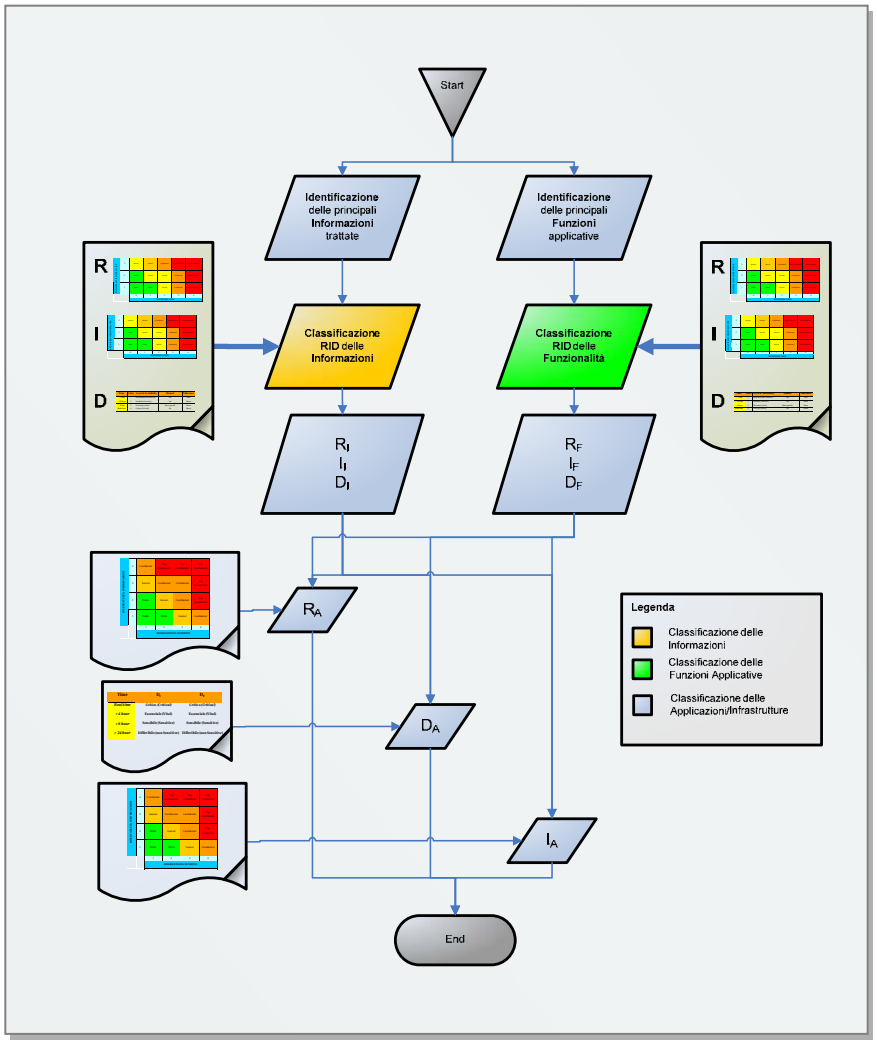
3. Processo di Gestione del Rischio (5)

Risk Analysis (2)

Threshold Determination

Obiettivo: determinare i livelli massimi di rischio ammissibili per ogni applicazione afferente ad un prodotto/servizio

App.	R	I	D	C	%
App1	2	2	1	2	
App2	3	3	2	3	
App3	4	1	2	2	
...	...	...	...	...	
AppN	1	1	1	1	



3. Processo di Gestione del Rischio (6)

Risk Analysis (3)

Threat Analysis

Tassonomia delle Minacce (Basel II Loss Event Type, 1° livello):

1. Frodi Interne
2. Frodi Esterne
3. Relazione con il Personale (Safety)
4. Rapporti con i Clienti
5. Disastri ed altri eventi
6. Malfunzionamento Sistemi Tecnologici
7. Prodotti e Servizi (Financial)

Classificazione a tre livelli

Loss Event Type Model

LET Category (Level 1 – Basilea II)	LET Category (Level 2 - Basilea)		Code	ID	LET Category (Level 3 – Internal Classication)
Rapporti con clienti, prestazioni di servizi/prodotti Perdite dovute all'incapacità di realizzare gli impegni professionali con specifici clienti (compresi i requisiti fiduciari e di adeguata informazione sugli investimenti) Perdite dovute a vizi nella natura e nelle caratteristiche dei prodotti Sono ricomprese tutte le perdite legate a prestazioni di servizi e fornitura di prodotti alla clientela eseguite in modo illecito, improprio o scadente. Sono escluse le perdite legate a errori specifici nella gestione dei conti della clientela nella gestione degli affidamenti, nel regolamento titoli (categoria 7). Gli storni da interessi e gli storni da commissioni effettuati per ragioni di natura commerciale non rientrano fra le perdite operative. *RISCHI LEGALI: L'incapacità di realizzare impegni professionali, esclusa l'intenzionalità, fa pensare, con riferimento alle categorie giuridiche italiane, al concetto di COLPA, ossia alla IMPRUDENZA, IMPERIZIA o NEGLIGENZA dell'operatore, quindi alla inosservanza di norme primarie e secondarie da parte degli operatori che comportano manifestazioni dannose. L'attività colposa può essere rinvenuta anche nella progettazione di un prodotto realizzato in maniera non conforme (per vizi o errori nel modello normativo) ovvero privo di autorizzazione*	4.1	**Sicurezza/ Rapporto fiduciario**	L2_08		***• Violazione privacy del cliente***
				IT4.1.a	*- Violazione della privacy del Cliente (D.Lgs 196/03)*
				IT4.1.b	*- Uso improprio / illecito di informazioni di carattere riservato/confidenziale - Mancato rispetto obblighi di riservatezza*
	4.3	**Difettosità di prodotti e di servizi forniti**	L2_10		***• Prodotti/Servizi/Applicativi non rispettosi delle performance minime: errori di progettazione, errori di modello, vizi originali in genere.***
				IT4.3.a	*- Errori di progettazione*
				IT4.3.b	*- Errorri in fase di collaudo*
				IT4.3.c	*- Messa in produzione non adeguata*
Disastri o altri eventi Perdite derivanti da danni ad asset fisici per cause naturali disastri o altri eventi	5.1	**Disastri o altri eventi** *(Perdite causate da danni ad assets fisici per cause naturali, disastri o altri eventi e/o incidenti (alluvioni, vandalismo, terrorismo, terremoti, incendio)*	L2_13	IT5.1.a	*- Incendio*
				IT5.1.b	*- Allagamento*
				IT5.1.c	*- Terremoto*
				IT5.1.e	*- Atti di terrorismo / guerra / vandalismo)*
				IT5.1.f	*- Malfunzionamento Sistemi HVAC / Sbalzi di Temperatura*
				IT5.1.g	*- Sbalzi d'umidità*
				IT5.1.h	*- Fulmine/Interferenze Eletromagnetiche*

3. Processo di Gestione del Rischio (7)

Risk Analysis (4)

Vulnerabilities Analysis

Tassonomia delle Vulnerabilità (1° livello):

1. People Risk
2. Business Process Risk
3. Product & Service Risk
4. Outsourcing Risk
5. Physical Asset Risk
6. IT Security Risk
7. IT Availability Risk
8. Compliance Risk

Classificazione a tre livelli

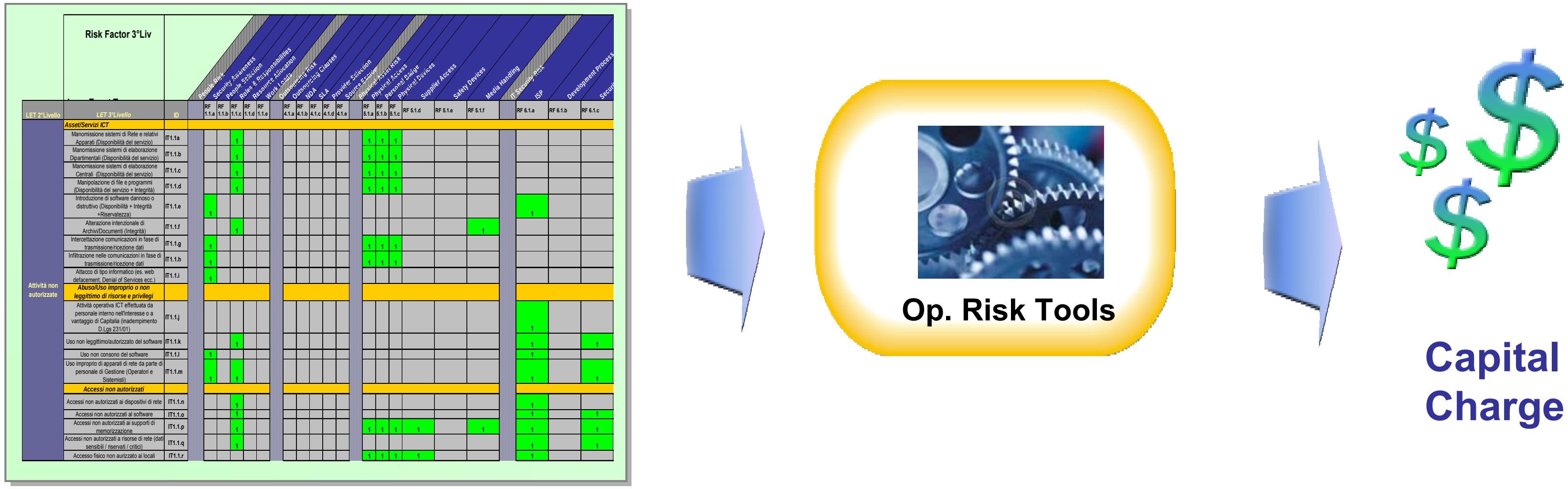
Risk Factor Model (Vulnerabilities)

DRIVER	Risk Factor (lev.1)	Risk Factor (lev.2)	Code	Risk Factor (lev.3)
Dipendenti	*People Risk*	Incompetenza / Impreparazione professionale. Inadeguata gestione del "clima aziendale" Inefficiente/inefficace/ inadeguata organizzazione del lavoro	RF 1.1.a	**Security Awareness**: Insufficiente cultura aziendale in tema di Security
			RF 1.1.b	**People Selection**: Inadeguato sistema selezione (assunzione).
			RF 1.1.c	**Roles & Responsibilities**: Mancanza di una chiara assegnazione di ruoli e responsabilità alle risorse.
			RF 1.1.d	**Resource Allocation**: Inadeguata allocazione risorse
			RF 1.1.e	**Work Loads**: Inadeguata distribuzione carichi di lavoro
Fornitori	*Outsourcing Risk*	Carenze / inadeguatezze nella gestione del rapporto con gli outsourcer/fornitori	RF 4.1.a	**Outsourcing Clauses**: Assenza/inadeguatezza di formalizzazione del rapporto con gli outsourcer/fornitori (comunicazione, modalità e livello di erogazione dei servizi,...)
			RF 4.1.b	**NDA**: Carenze/inadeguatezze nella fase di definizione degli aspetti di riservatezza all'interno di accordi contrattuali relativi prodotti/servizi.
			RF 4.1.c	**SLA**: Carente / Inadeguata definizione sulle modalità e il livello di erogazione del servizio (SLA).
			RF 4.1.d	**Provider Selection**: Inadeguato sistema di selezione dei fornitori.
			RF 4.1.e	**Source Escrow**: Assenza/Inadeguatezza dei vincoli contrattuali con terze parti fornitrici di SW relativamente al rilascio e conservazione (in caso di fallimento) dei codici sorgente degli applicativi commissionati
Asset Fisici	*Physical Asset Risk*	Assenza / Inadeguatezza misure a fronte di calamità naturali (business continuity plan, ...) Assenza / inadeguatezza misure di prevenzione e sicurezza verso eventi di natura accidentale (per causa umana e/o naturale) - *"safety"* Inadeguatezza/obsolescenza delle infrastrutture Assenza / inadeguatezza misure di prevenzione e di sicurezza verso atti di natura criminosa (rapine, terrorismo, vandalismo,...) - *"security"* Assenza / Inadeguatezza di passaggi autorizzativi per l'esecuzione delle attività operative Assenza / inadeguatezza misure di controllo verso attività non autorizzate e frodi da parte di dipendenti Assenza / inadeguatezza misure preventive verso frodi da parte esterni	RF 5.1.a	**Physical Access**: Inefficiente/Inefficace processo di identificazione/registrazione per l'accesso fisico ai locali ed alle aree sensibili
			RF 5.1.b	**Personal Badge**: Non è ben definito il processo per la corretta individuazione di personale non autorizzato (esposizione badge, differenziazione badge ecc.).
			RF 5.1.c	**Physical Devices**: Non sono presenti o risultano inadeguate misure di sicurezza di tipo fisico (es. telecamere a circuito chiuso, installazione di barriere anti-intrusione dall'esterno: grate, vetri anti-sfondamento).
			RF 5.1.d	**Supplier Access**: L'accesso da parte di esterni (consulenti, addetti alla manutenzione ecc.) non avviene previa autorizzazione di personale interno
			RF 5.1.e	**Safety Devices**: Assenza / inadeguatezza misure di prevenzione e sicurezza (es.: estintori, dispositivi salvavita, porte tagliafuoco, manutenzione impianti, rilevatori fumo e acqua, materiali ignifughi, ...) - "safety".
			RF 5.1.f	**Media Handling**: Inadeguata conservazione dei supporti

3. Processo di Gestione del Rischio (8)

Risk Analysis (5)

Correlazione LET (Minacce) –RF (Vulnerabilità)...



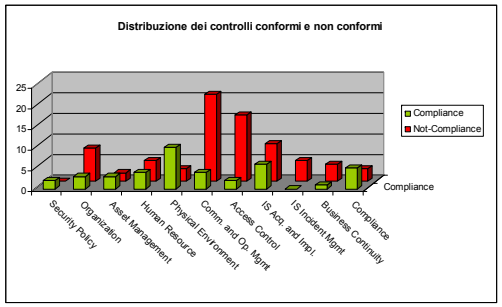
... e calcolo Accantonamenti

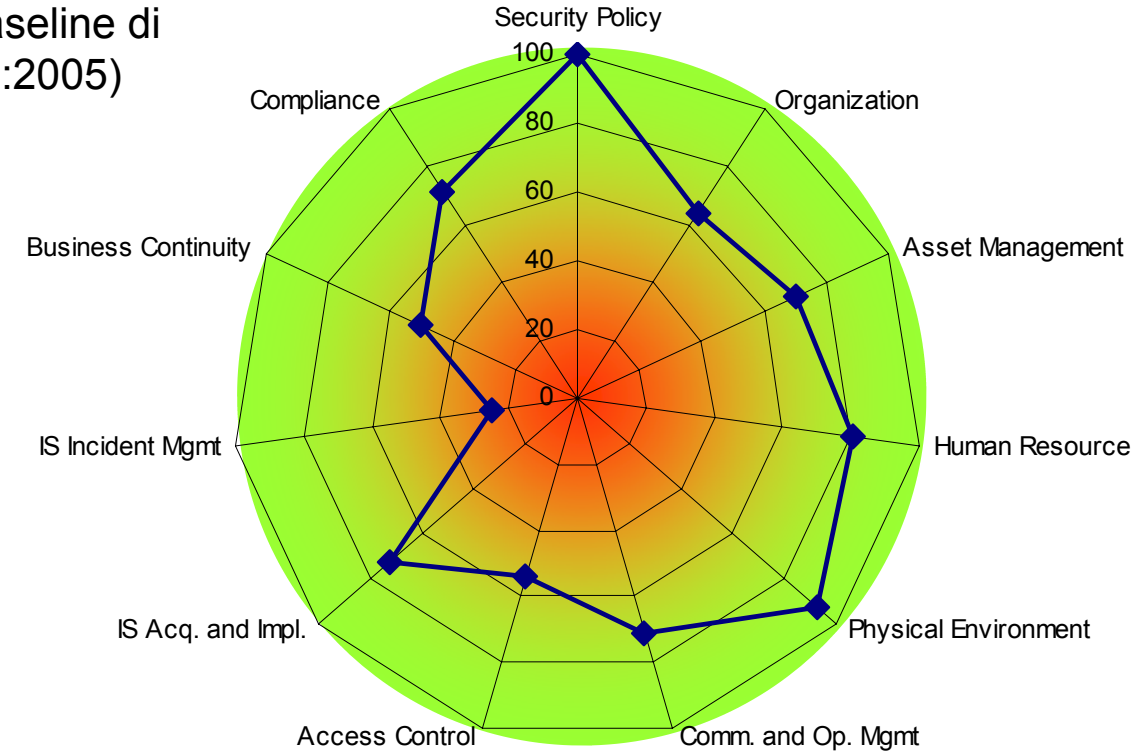
3. Processo di Gestione del Rischio (9)

Risk Treatment (1)

Gap Analysis

Individuazione delle non conformità rispetto ai requisiti di una Baseline di Riferimento (e.g. ISO 17799:2005)





3. Processo di Gestione del Rischio (10)

Risk Treatment (2)

Countermeasures Selection

Definizione della strategia di intervento per il contenimento del rischio

Creazione di una serie di scenari

Ecosystems, LLC - INFORM_Charter_version 5.1.xls

INFORM
INFOrmation assurance Risk Model

ABC Company - Domestic Operations

Risk Exposure	Current SPE	Improved SPE	Reduced Risk	Annual Cost	Net Benefit
$40,464,000	52.0%	55.5%	$1,400,000	$132,000	$1,268,000

<< Back | Reset Default | Help

General | Risk Exposure | Security Controls | >Action Plan Solutions | Dashboard | Reports

Click next to each Solution you wish to include in the Action Plan, and then enter Costs

Select Action Plan Solutions	Degree of Current Successful Implementation	Security Program Effectiveness Improvement (if selected)	Annual Cost	Risk Reduction per Dollar of Solution Cost
☑ Professional, educational, response, and managed security	40%	2.6%	$79,000	$13.37
☑ Asset management solutions	35%	0.8%	$53,000	$6.48
☐ Policy management and compliance solutions	50%	0.7%		
☐ Information Risk management	50%	0.6%		
☐ Physical access controls and security equipment solutions	50%	0.5%		
☐ Remediation management solutions	50%	0.5%		
☐ Incident management solutions	50%	0.4%		
☐ Network security solutions	50%	0.3%		
☐ Identity management	50%	0.3%		
☐ Encryption and public key Infrastructure solutions	50%	0.2%		
☐ Threat and vulnerability management solutions	50%	0.2%		
☐ Configuration and change management	50%	0.2%		
☐ Intrusion detection and prevention solutions	50%	0.1%		
☐ Malicious code and content management solutions	50%	0.1%		
☐ Logging, auditing and monitoring	50%	0.1%		
Action Plan		3.5%	$132,000	$10.61

Graphs: Improved Effectiveness | Risk reduction per $

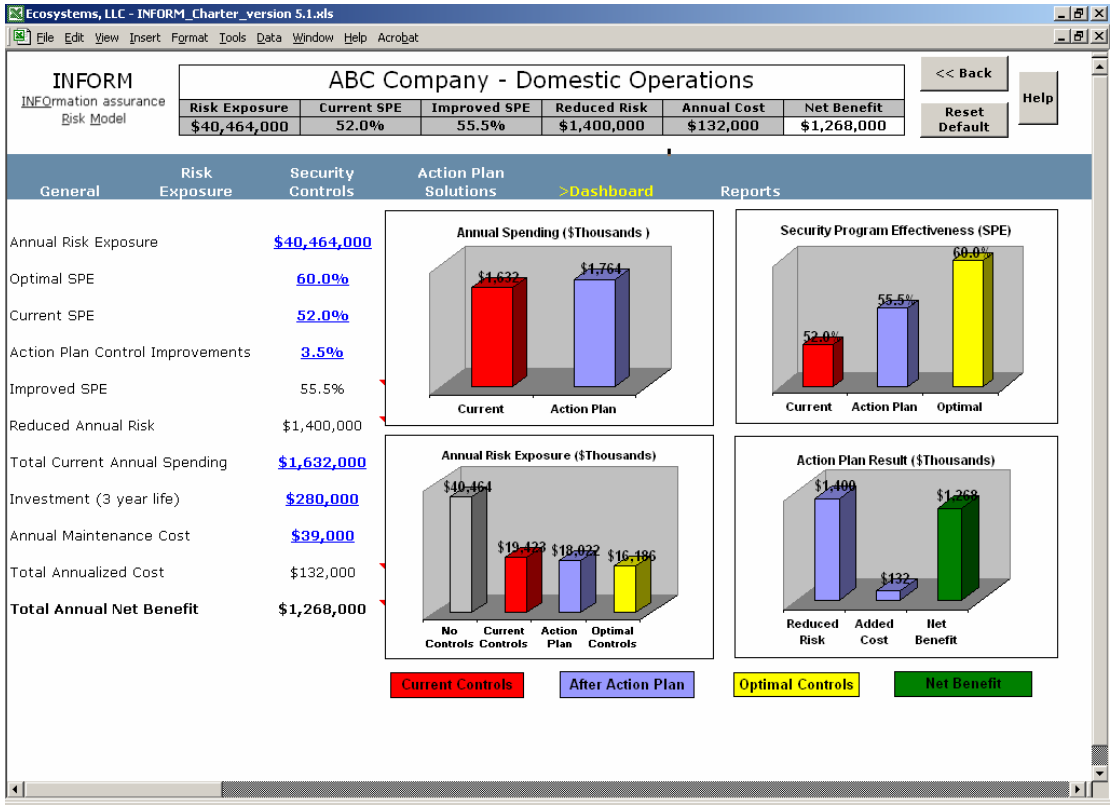
Selected Opportunities

7 Physical and Environmental Security	614	0.2%	0.1%
Total	25,059	8.0%	3.5%
Selected Opportunities =		8.0%	

3. Processo di Gestione del Rischio (11)

Risk Treatment (3)

Remediation Plan



Creazione del piano di rientro annuale, che avrà effetti sulla determinazione del rischio operativa da effettuarsi l'anno successivo

4. Evoluzioni Possibili (1)

Default Risk Management

In una fase successiva, l'esperienza maturata con le banche potrà essere portata anche in altri ambiti.

L'accesso al credito avviene attraverso una attenta valutazione dello stato economico e finanziario dell'azienda cliente (Rischio di Credito). Esame anche di fattori qualitativi, attraverso meccanismi propri di ogni banca (Internal Rating Based). Tra questi:

Rischio di Default → rischio che una determinata azienda non riesca, per eventi avversi esterni od interni, a fornire i servizi fondamentali e quindi, in definitiva per le banche, il rischio che sia impossibile restituire i soldi avuti in prestito e gli interessi

Le società che non daranno abbastanza garanzie di avere un basso rischio di default (ivi compreso il rischio informatico) sostanzialmente non accederanno al credito.

Bibliografia e sitografia :

Riferimenti Essenziali:

- Bank of International Settlement (http://www.bis.org)
- Banca d'Italia – Vigilanza e Tutela (http://www.bancaditalia.it/vigilanza_tutela/vig_ban/pubblicazioni/basilea)
- International Accounting Standard Board (http://www.iasb.org)
- European Central Bank (http://www.ecb.eu)

Basel II & IT Risk Management

Grazie!

(**Paolo Ottolino – OPST CISSP-ISSAP CISA**)

Policy & Strategy – Security Consulting Services

paolo_ottolino (at) symantec.com