Obiettivi di controllo IT per Basilea II

L'importanza della *Governance* e del *Risk Management* per la *Compliance*

Edizione in lingua inglese: dicembre 2007

Edizione in lingua italiana: settembre 2009 a cura di ISACA Roma

Prefazione all'edizione italiana

http://www.isacaroma.it/index.htm

La presente traduzione è stata realizzata da:

- Agatino Grillo, CISA, CISSP, CISM

con il patrocinio di ISACA Roma.

Questo documento viene diffuso via web in formato **pdf** al fine di garantirne la massima diffusione.
Per gli interessati sono disponibili anche le versioni in formato Microsoft **Word 97-2003** e **Open Office 3.1** che possono essere richieste facendone richiesta via email ad Agatino Grillo al quale vanno inviati anche eventuali note, suggerimenti e correzioni alla "traduzione" del testo.

Contatti

- agatino.grillo@gmail.com
- a.grillo@isacaroma.it

Ulteriori informazioni su Agatino Grillo:

- http://www.linkedin.com/in/agatinogrillo
- http://www.compliancenet.it/users/agatino-grillo
- http://www.agatinogrillo.it/

IT Governance Institute®

L'*IT Governance Institute* (ITGI) (http://www.itgi.org/) è stato fondato nel 1998 per incoraggiare la ricerca e la definizione di standard nell'ambito del controllo dei sistemi informativi aziendali. Una *IT Governance* efficace favorisce infatti il supporto dell'IT agli obiettivi di business, ottimizza gli investimenti IT e permette di gestire, in modo appropriato, i rischi e le opportunità offerte dalle nuove tecnologie. ITGI offre risorse in formato elettronico, ricerche originali e casi di studio per assistere il top management ed il Consiglio di Amministrazione nelle attività di *IT Governance*.

Limitazioni di responsabilità

Disclaimer
ITGI e gli autori di "Obiettivi di controllo IT per Basilea II: l'importanza della *Governance* e del *Risk Management* per la *Compliance*" hanno realizzato questa pubblicazione principalmente come risorsa di tipo "educativo"per gli *information risk manager*, i professionisti IT e coloro che lavorano in banca e presso le istituzioni finanziarie. ITGI, gli autori di questa pubblicazione ed il traduttore della versione in italiano non forniscono nessuna assicurazione che l'uso di queste linee guida e degli strumenti indicati in questa pubblicazione possano garantire di per sé la conformità alle norme.
Non si deve infatti presupporre che questa "guida" comprenda tutti i possibili controlli IT, le procedure ed i test che possono essere ragionevolmente adottati in ogni circostanza. Nella determinazione della proprietà di ogni specifico controllo, procedura o test coloro che si occupano di test e controlli devono applicare il proprio giudizio sulle specifiche circostanze di controllo presenti nell'ambiente di *Information Technology* (IT) sotto analisi.

Diritti

Copyright © 2007 IT Governance Institute. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere usata, copiata, riprodotta, modificata, distribuita, visualizzata, memorizzata in un sistema elettronico o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, per mezzo di fotocopie, registrato in maniera elettronica o in altro modo) senza l'autorizzazione scritta preliminare dell'*IT Governance Institute*.
La riproduzione di parte selezionate del documento per uso interno, non commerciale o accademico è permesso ma deve contenere l'attribuzione completa della fonte del materiale. Nessun altro diritto, o permesso, è concesso rispetto a quest'opera.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.606.5700
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: http://www.itgi.org/
ISBN 978-1-893209-38-1
IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance
Printed in the United States of America

Ringranziamenti

*L'*IT Governance Institute *desidera ringraziare:*

Coloro che hanno contribuito in maniera significativa:

- Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

Focus Group

- Urs Fischer, CISA, CIA, CPA, Swiss Life, Switzerland
- Christopher Fox, ACA, eDelta, USA
- Jimmy Heschl, CISA, CISM, KPMG, Austria
- Markus Gaulke, CISA, CISM, KPMG Germany, Germany
- Marcelo Gonzalez, CISA, Banco Central Republica Argentina, Argentina
- Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
- Masaki Nakamura, CIA, Sumitomo Mitsui Banking Corporation, Japan
- Robert Stroud, CA Inc., USA
- Robert White, CISA, ACA, ING Bank, UK

ITGI Board of Trustees

- Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President
- Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
- Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
- Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
- Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
- Robert E. Stroud, CA Inc., USA, Vice President
- Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
- Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
- Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
- Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President
- Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
- Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee

- Tony Hayes, FCPA, Queensland Government, Australia, Chair
- Max Blecher, Virtual Alliance, South Africa
- Sushil Chatterji, Edutech, Singapore
- Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
- John W. Lainhart IV, CISA, CISM, IBM, USA
- Lucio Molina Focazzio, CISA, Colombia
- Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

- Michael Schirmbrand, Ph. D., CISA, CISM, CPA, KPMG LLP, Austria
- Robert E. Stroud, CA Inc., USA
- John Thorp, The Thorp Network Inc., Canada
- Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance Research Institute (ITAG), Belgium

Security Management Committee

- Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJLPD, USA, Chair
- Manuel Aceves, CISA, CISM, CISSP, Cerberian, Mexico
- Kent Anderson, CISM, Network Risk Management LLC, USA
- Yonosuke Harada, CISA, CISM, CAIS, ITGI-Japan, Japan
- Yves Le Roux, CISM, CA Inc., France
- Mark Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA
- Vernon Poole, CISM, Sapphire Technologies Ltd., UK
- Jo Stewart-Rattray, CISA, CISM, Vectra Corp., Australia
- Rolf von Roessing, CISA, CISM, CISSP, FBCI, KPMG Germany, Germany

ITGI Affiliates and Sponsors

- ISACA chapters
- American Institute of Certified Public Accountants
- ASIS International
- The Center for Internet Security
- Commonwealth Association of Corporate Governance Inc.
- FIDA Inform
- Information Security Forum
- Information Systems Security Association
- Institut de la Gouvernance des Systèmes d'Information
- Institute of Management Accountants
- ISACA
- ITGI Japan
- Solvay Business School
- University of Antwerp Management School
- Aldion Consulting Pte. Ltd.
- Analytix Holdings Pty. Ltd.
- BWise B.V.
- CA Inc.
- Hewlett-Packard
- IBM
- ITpreneurs Nederlands B.V.
- LogLogic Inc.
- Phoenix Business and Systems Process Inc.
- Project Rx Inc.
- Symantec Corporation
- Wolcott Group LLC
- World Pass IT Solutions

Indice

PREFAZIONE ALL'EDIZIONE ITALIANA ..... A

RINGRANZIAMENTI II

INDICE IV

PREFAZIONE 1

1. EXECUTIVE SUMMARY 2

OBIETTIVI 2
COME LEGGERE QUESTO DOCUMENTO 2

2. GOVERNANCE, RISK MANAGEMENT E COMPLIANCE: LE PRINCIPALI PRIORITÀ DI BUSINESS 4

3. L'EVOLUZIONE DEL CONTESTO REGOLATORIO 7

4. L'APPROCCIO DI BASILEA II ALLA GESTIONE DEI RISCHI 9

5. LA NECESSITÀ DI GESTIRE I RISCHI OPERATIVI 12

GLI APPROCCI DI RISK MANAGEMENT 12
FRAMEWORK PER IL RISK MANAGEMENT OPERATIVO 14
Risk Strategy 14
Struttura organizzativa 14
Reporting 15
Definizioni, collegamenti e strutture 15
Dati sulle perdite 15
Risk Assessment 15
Key Risk Indicator 16
Mitigazione 16
Capital Modeling 16
Information Technology 16
LE COMPONENTI DI COSO 17
I PRINCIPI DEL RISCHIO OPERATIVO E DELLA IT RELEVANCE 24

6. GESTIRE I RISCHI INFORMATICI 29

PRINCIPI GUIDA PER L'IT 29
CAUSE DI PERDITA E IT RISK 39
ANALISI DI SCENARIO PER GLI IT RISK 41

7. PROCESSI DI BUSINESS PER GLI IT RISK ED I CONTROLLI IT: APPLICARE IL COBIT FRAMEWORK 45

USO DELLA DOCUMENTAZIONE ESISTENTE 45
L'APPROCCIO "BUSINESS LINE" IN BASILEA II 45
DEFINIRE I RISCHI IT 46

DEFINIRE I CONTROLLI IT 50
8. USO DEI "KEY IT RISK INDICATOR" 53
APPENDICE I – SINTESI DI BASILEA II 54
APPENDICE II – COMPARAZIONE DI ALTO LIVELLO TRA COSO ERM E BASILEA II 62
APPENDICE III – COMPARAZIONE DI ALTO LIVELLO TRA IL PRINCIPIO 1 DI BASILEA II: IL SECONDO PILASTRO - SUPERVISORY REVIEW PROCESS (GIUGNO 2006) E COSO ERM - INTEGRATED FRAMEWORK (SETTEMBRE 2004) 64
APPENDICE IV- LA DIPENDENZA DEL COSO ERM FRAMEWORK DALLA "DATA QUALITY" 67
APPENDICE V – BASILEA II E COBIT 69
APPENDICE VI – I PROCESSI COBIT 76
APPENDICE VII- ABC BANK: UN ESEMPIO CONCRETO 84
APPENDICE VIII – REFERENZE 90

Prefazione

Gli intermediari finanziari[1] devono adeguarsi ai requisiti, ed alle sfide, posti da "Basilea II" il nuovo accordo sul capitale del comitato di Basilea sulla supervisione delle banche. Basilea II propone, infatti, un modello per la gestione dei rischi nelle banche e negli intermediari finanziari che, a differenza del primo accordo sul capitale del 1988, attribuisce un valore decisivo anche ai rischi informatici ed in generale all'*Information Technology*.
Gli intermediari finanziari devono di conseguenza adottare significativi cambiamenti in termini di infrastrutture IT, applicazioni e controlli interni in ambito informatico.
Lo scopo di questa pubblicazione è di evidenziare la sempre maggior convergenza tra *governance* ed *information risk management*: gli intermediari finanziari e l'intero sistema finanziario sono ormai considerati strutture altamente critiche per l'economia globale e dunque la gestione dei rischi informatici ed i controlli IT sono parte imprescindibile della *corporate governance*. Al più alto livello strategico, l'alta direzione deve dunque garantire la *governance* dei sistemi finanziari anche tenendo allineati, in termini di obiettivi, il mondo del business con quello della tecnologia.
Dopo la pubblicazione di "*Obiettivi di controllo per la Sarbanes-Oxley*"[♦], giunta alla seconda edizione, l'*IT Governance Institute* continua a proporre una gestione proattiva del rischio con la prima edizione degli "*Obiettivi di controllo IT per Basilea II*".
Questa nuova pubblicazione intende fornire una linea guida, chiara e coerente, per gli *information risk manager*, i professionisti IT e gli esperti bancari, con responsabilità ed incarichi in ambito IT, rispetto ai requisiti e agli obblighi previsti da Basilea II.
Basilea II richiede infatti di adottare un *framework* formale e standardizzato di controlli IT. Esistono ovviamente molti standard, modelli e soluzioni proprietarie tuttavia il *framework* COBIT[2], un insieme consolidato di processi e controlli IT, è l'unico progettato esplicitamente per la *governance* dell'IT anche dal punto di vista dell'*information risk management*. COBIT è internazionalmente riconosciuto come una *global best practice* anche grazie alla sua versatilità e semplicità unite alla iniziative di miglioramento continuo che lo caratterizza; tutto ciò favorisce COBIT rispetto ad altri *framework*.
"*Obiettivi di controllo IT per Basilea II*" è stato scritto da un comitato di esperti in ambito bancario provenienti da un gran numero di società specializzate, adottando un approccio basato sulla condivisione delle esperienze, delle idee e delle iniziative ed utilizzando la formula della "pubblica consultazione".
Questa prima edizione analizza in particolare gli aspetti dell'*information risk management* e dei controlli IT dal punto di vista delle banche, degli intermediari finanziari e degli esperti finanziari.
ITGI e ISACA ringraziamo in anticipo tutti coloro che vorranno inviare commenti e suggerimenti che saranno utili per il processo di miglioramento continuo di questa pubblicazione[♦].

Everett Johnson, CPA
International President
IT Governance Institute

---

[1] Dato che esiste un certo numero di aziende ed organizzazioni che pur non essendo banche sono soggette a Basilea II, la presente pubblicazione usa, ove possibile, il termine "intermediari finanziari" (*financial services organization*) piuttosto che "banche".
[♦] L'edizione originale in lingua inglese è stata pubblicata nel 2006. La traduzione in italiano, a cura di ISACA Roma, è stata pubblicata nel settembre 2008 ed è disponibile in http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=45766 (*nota presente solo nella traduzione italiana di questo documento*)
[2] ITGI, COBIT, USA, 1996-2007, disponibile in http://www.isaca.org/cobit. AIEA, capitolo di Milano di ISACA, ha tradotto in italiano parte di COBIT 4.1, traduzione disponibile in: http://www.aiea.it/html/area_download.html
[♦] Note e suggerimenti relativi alla traduzione in italiano vanno inviati ad **Agatino Grillo** alle email indicate nella "Prefazione all'edizione italiana" di questo documento

1. Executive Summary

Obiettivi

La presente pubblicazione "*Obiettivi di controllo IT per Basilea II*" fornisce un *framework* completo e coerente per la gestione dei rischi informativi (*information risk)* nel contesto di Basilea II.
Il documento è indirizzato a due diversi target:

1. i professionisti IT;
2. gli esperti di servizi finanziari.

Adottando il *framework* presentato in questa pubblicazione, gli intermediari finanziari possono utilizzare con successo i processi e controlli noti e condivisi nella comunità dell'*Information Technology*: gli obiettivi di controllo IT ed i processi di management presi in considerazione riguardano infatti il ruolo dell'IT nella gestione dei rischi operativi e le relative attività che devono intraprendere i professionisti IT, gli internal auditor IT, gli IT *risk manager* e gli *information security officer*.
Il presente capitolo presenta una sintesi del concetto di rischio così come è inteso in Basilea II e illustra le relazioni fra i rischi operativi ed i rischi informativi nonché l'approccio per la gestione dell'*information risk*.

Come leggere questo documento

La *Corporate governance*, il *Risk management* e la *regulatory Compliance* (GRC) sono ormai tra le principali priorità per il business in quanto esso è sempre più influenzato dalle richieste degli *stakeholder*, dalle valutazioni dei mercati, dalle aspettative di performance. La necessità di una migliore *corporate governance* è sempre più diffusa. Quando si parla di *governance* ci si riferisce alla gestione di criticità quali flussi informativi incompleti, comunicazioni non efficienti e incomplete, mancata comprensione dei rischi così come indicato chiaramente nei principi definiti dall'ITGI.
Il **capitolo 2** introduce i concetti fondamentali: *Corporate governance*, *Risk management*, *Compliance*.
La crescente quantità di attività specifiche in ambito regolatorio in aggiunta al livello sempre maggiore di informazioni richieste sono una chiara evidenza del fatto che la *governance*, il *risk management* e la *compliance* sono ormai aree primarie di attenzione per quel che riguarda i *regulator* dei servizi finanziari e bancari.
Negli ultimi anni c'è stato infatti un rapido aumento dei requisiti in ambito GRC. Norme e regolamenti relativi a tali aree si sono evoluti in *framework* dettagliati che riguardano molti aspetti sia dell'ambito bancario sia dell'ambito tecnologico. Negli ultimi anni, norme e leggi nazionali ed internazionali si sono indirizzate, in modo crescente, su temi quali *l'Information Management*, l'*Information Technology* e le varie discipline specialistiche che esse comprendono.
Il **capitolo 3** illustra le componenti rilevanti, in ambito normativo, per i servizi finanziari e l'IT. Nel 2004, il comitato di Basilea per la vigilanza bancaria ha reso pubblico il secondo *framework* relativo alla adeguatezza patrimoniale che introduce un nuovo approccio al rischio nelle istituzioni finanziarie. L'obiettivo di Basilea II è di rafforzare le *practice* di gestione del rischio di credito e del rischio operativo e di fissare un legame tra la valutazione del rischio ed i coefficienti patrimoniali. Le nuove norme forniscono un incentivo alle istituzioni finanziarie in quanto il miglioramento della qualità della gestione del rischio e dei relativi sistemi di controllo permettono di ridurre il capitale da accantonare per la copertura di tali rischi.

In ultima istanza gli intermediari finanziari possono acquisire un vantaggio competitivo se dimostrano di avere un forte *framework* GRC; per ogni azienda infatti l'esposizione al rischio complessivo determina il coefficiente patrimoniale richiesto e dunque le iniziative GRC diventano un fattore importante per ridurre tale coefficiente.
Il **capitolo 4** descrive il nuovo approccio al *risk management* così come è definito nel *framework* di Basilea II. I rischi operativi sono considerati come un'autonoma ed importante categoria di rischio, come è testimoniato, negli ultimi dieci anni, da un gran numero di incidenti e crisi imputabili ad essi. Il rischio operativo si riferisce alle operazioni bancarie ed alla conduzione ordinaria del business, area spesso più ampia ed articolata di quelle a cui si riferiscono altre categorie di rischio come quello relativo al tasso di interesse. Per tale motivo identificare e misurare i rischi operativi si è dimostrato un compito assai impegnativo per le banche e le istituzioni finanziarie.
In generale l'*Information Technology* e l'*Information Management* sono elementi chiave per una strategia completa di gestione del GRC e per l'ottimizzazione dei coefficienti patrimoniali. Le componenti correlate all'IT come le applicazioni software, gli elementi infrastrutturali ed i controlli fanno tutti parte dei rischi operativi.
Il **capitolo 5** fornisce una *overview* dei rischi operativi e della rilevanza che assume, a riguardo, l'*information risk*. Il capitolo inoltre mappa i principi di Basilea per i rischi operativi rispetti ai rischi classici dell'*Information Technology*.
Al fine di indirizzare in maniera adeguata i rischi relativi alle informazioni occorre adottare un approccio *business-driven*. I processi di business devono guidare la definizione dei controlli e delle metriche mentre il set dei controlli relativi all'IT sono completati da un insieme di indicatori per misurare la *compliance* e la maturità. Quando un rischio di tipo informativo ha un impatto sul processo di business, i passi necessari per ridurre e mitigare il rischio devono essere parte integrante del *framework* GRC dell'organizzazione.
Il **capitolo 6** fornisce un ponte tra Basilea II e rischi di tipo informativo definendo un insieme di dieci principi guida per l'*information risk management*. Questi principi guida corrispondono ai principi del *risk management* "operativo" come tracciati nei documenti di Basilea.
Gestire gli *information risk* nel contesto di Basilea richiede l'adeguamento dei noti processi IT, dei controlli e delle relative attività. Queste regole di base per la gestione dei rischi IT sono descritte nel **capitolo 7**.
Il *corporate GRC framework* di solito consiste di diverse componenti ciascuna delle quali gestisce differenti parti ed obiettivi dell'organizzazione. Per i rischi legati alle informazioni, il *framework* COBIT rappresenta un insieme già ottimizzato di processi e *tool* che supportano l'intero *framework* GRC; inoltre COBIT già prevede i collegamenti e la mappatura fra i suoi contenuti ed i più importanti *framework* per la *compliance* e la *governance*.
Basilea II richiede un approccio *business-driven* al *risk management*.
Per utilizzare COBIT come modello di supporto per il GRC, l'insieme dei controlli IT deve essere messo in relazione ai rischi IT; i rischi IT sono un sottoinsieme dei rischi *business-driven* che sono individuabili nei processi di business.
Il **capitolo 8** illustra la sequenza logica dalla vista dei processi di business agli *information risk* ed ai controlli IT. Il capitolo spiega, passo per passo, come i professionisti IT ed i *risk manager* devono utilizzare COBIT per gestire i rischi di Basilea.
La gestione del rischio comprende l'uso di indicatori per denotare gli obiettivi, le performance ed il livello del rischio.
Il **capitolo 9** introduce il concetto dei COBIT *Key Risk Indicator* (KRI) ed il loro uso per Basilea II. Ogni KRI supporta il processo continuo del *risk assessment* e *risk management* al fine di ottenere i miglioramenti nell'insieme dei rischi operativi. Il capitolo descrive i tipi di indicatori, la loro importanza all'interno del processo complessivo di *risk management* e la definizione dei KRI adatti per un *framework* completo e coerente di *information risk management*.

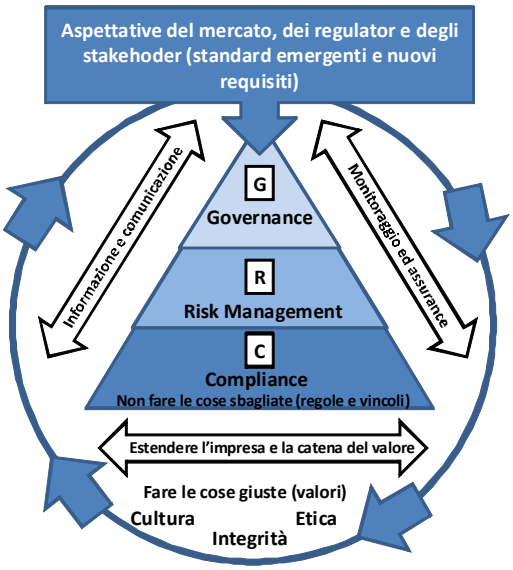
2. Governance, Risk Management e Compliance: *le principali priorità di business*

La *corporate governance*, il *risk management* e la *regulatory compliance* (GRC) sono ormai una priorità per il top business. Il trend verso una migliore *corporate governance* è facilmente individuabile in molte iniziative tra cui:

- la protezione della reputazione aziendale e del valore del marchio (*brand value*);
- la necessità di soddisfare la domande e le aspettative degli investitori, legislatori, regolatori, clienti, impiegati, analisti, consumatori ed altri *stakeholder* chiave;
- la creazione di valore e la gestione delle aspettative di performance in relazione alla *governance*, ai comportamenti etici, al *risk management* ed alla *compliance*;
- la gestione delle crisi e dei processi di correzione e miglioramento delle criticità "difendendo" l'azienda, i suoi dirigenti ed il Consiglio di Amministrazione contro le possibilità, in forte aumento, di azioni legali, multe, sanzioni e relative conseguenze legali e di immagine;
- l'esercizio di una buona amministrazione ed il rafforzamento della fiducia nei mercati attraverso maggiore trasparenza.

Le aziende devono gestire in modo proattivo tutte queste problematiche che, spesso, sono già tenute sotto controllo ma solo in modo episodico; è, viceversa, necessario agire in ambito GRC in modo integrato e continuo. Le analisi e le ricerche delle varie *industry* rivelano invece che molte aziende ritengono di non essere posizionate in modo efficace per garantire la domanda, crescente, dei propri *stakeholder* di piani sostenibili.
La **figura 1** illustra la "responsabilità olistica" per la *corporate governance* che riguarda tutti i livelli aziendali. Anche se la GRC è *in primis* responsabilità del Consiglio di Amministrazione tutte le unità organizzative aziendali devono adottare ed applicare i principi di GRC definiti dal management.

Figura 1 - *Integrity-driven performance*: gestire i rischi dalla "sala di consiglio" fino "all'ufficio postale"



È fondamentale adottare un approccio integrato rispetto al *Corporate governance*, *Risk management* e *regulatory Compliance* (GRC). Le aziende che viceversa gestiscono ciascuna area GRC in modo diverso, senza un framework comune ma solo sulla base delle proprie esperienze pregresse, spesso rilevano un significativo aumento dei costi e duplicazione degli sforzi. Avere un approccio non omogeneo al GRC può avere un effetto negativo sulla efficienza e rende l'implementazione di un processo proattivo e *process-driven* difficile se non impossibile.
Una *governance* integrata e coerente richiede di definire la strategia, gestire i rischi, creare valore e misurare le performance. Un forte *framework* GRC assicura che gli interessi degli *stakeholder* siano adottati ed implementati dal management e dallo staff in tutta l'azienda. Dato che il framework è alla base della fondazione dell'integrità manageriale, occorre fare il miglior uso degli asset aziendali e del capitale intellettuale e avere una chiara comprensione dei rischi e della loro gestione: tutte le componenti del *GRC framework* sono importanti per la buona *corporate governance*.
Le aziende devono inoltre gestire i rischi, che sono in aumento, correlati alla instabilità geopolitica, alla globalizzazione, alla crescita "aggressiva" degli obiettivi commerciali, all'aumento della concorrenza, all'esplosione incontrollata delle informazioni.
Il *risk management* è sempre stato una competenza centrale per le istituzioni finanziarie: oggi le prassi di *risk management*, integrate e globali per tutte le aziende, sono anche un imperativo regolatorio. Le attività imprenditoriali ed i rischi non sono mutualmente esclusivi. Il *risk management* integrato è uno strumento che facilita le decisioni manageriali informate e l'accettazione cosciente del livello di rischio tollerabile ed accettabile. Quindi il *risk management* come parte della *corporate governance* fa aumentare la fiducia degli *stakeholder* e facilita l'indicazione della direzione strategica necessaria per le attività imprenditoriali.
Si noti, inoltre, che la *compliance* si è evoluta passando da un approccio passivo basato su "*check-list*" (il cosiddetto *tick-box approach*) ad una disciplina proattiva che sia di effettiva guida e supporto alla *governance*.
Oggi con il termine "*compliance*" si intende ben più che il semplice compilare una lista di requisiti "prendere-o-lasciare", sebbene la *compliance* prescrittiva, basata su regole, sia ancora un sottoinsieme importante della *compliance* globale. In molti casi i requisiti di *compliance* "fissati" nelle norme e regolamenti o negli standard sono "*maturity-driven*" e progettati per il miglioramento continuo nel tempo.
Le prassi di mercato, i *benchmark* ed i nuovi sviluppi nel business devono essere analizzati costantemente attraverso la lente della *compliance* e ciò a causa dei cambiamenti costanti e delle sfide del business globale.
Adottare un GRC, quando si entra in (o si operi già) in un business, non è un "ripensamento" ma significa prendere atto della necessità di proteggere l'azienda e mantenerne l'integrità – nei confronti degli *stakeholder* esterni, dei *business partner*, degli impiegati, dei collaboratori e dei partner.
Le numerose norme con un *focus* sul GRC che sono continuamente emanate indicano chiaramente l'importanza di questo tema anche presso il grande pubblico: leggi e statuti riflettono il *social agreement* sulla necessità di una buona *governance*; le norme ed i regolamenti GRC trasformano questo *agreemen*t generale nelle "regole" specifiche di settore ed *industry*. Le associazioni industriali e gli organismi di standardizzazione validano il *corpus* normativo mediante la redazione di guide applicative rispetto ai principi del GRC.
Basilea II e le sue disposizioni sul *risk management* riflettono infine il focus crescente sulle strutture di *governance* e su i *framework* nell'*industry* dei servizi finanziari. Il nuovo "accordo sul capitale" va ben oltre le prime iniziative ed i relativi requisiti GRC. Le componenti ed i blocchi che compongono Basilea II coprono un ampio spettro di aspetti manageriali e tecnologici, comprese le problematiche dell'*information technology*, della *security* e della *business continuity* e forniscono così indicazioni chiare e coerenti alle discipline specialistiche che devono gestirne i requisiti nelle aziende bancarie e finanziarie.

Le informazioni, le tecnologie e le sfide dell'*information management* crescono ogni giorno di importanza. Banche e aziende di servizi finanziari ripongono sempre maggiore fiducia nelle proprie infrastrutture tecnologiche in termini sia di gestione del business sia di supporto al controllo. Come parte del GRC, uno degli imperativi maggiori è costruire un ponte tra processi di *core business* e le tecnologie critiche. Un *framework* che garantisca una *governance* integrata e coerente dell'*Information Management* non deve ridursi semplicemente al controllo ed alla *compliance*: viceversa le priorità del GRC devono riflettersi in un approccio globale all'*information technology* ed al suo potenziale per il supporto globale al business. Oltre che alle perdite operative ed al danno reputazionale, le debolezze nella progettazione o nell'efficacia del modello di *IT governance* nel contesto di Basilea II, sono aspetti che possono contribuire fortemente ad aumentare i coefficienti patrimoniali richiesti per i rischi operativi come è discusso più in dettaglio nel **capitolo 5** "La necessità di gestire i rischi operativi".

3. L'evoluzione del contesto regolatorio

Leggi, regolamenti, standard e "prassi condivise" nelle diverse *industry* hanno tutti il medesimo scopo: nel loro insieme devono supportare gli obiettivi GRC. In termini di applicabilità pratica (e del livello di requisito del dettaglio atteso) le norme nazionali ed internazionali costituiscono le "fondamenta" del GRC, in particolare dove le disposizioni regolatorie sono focalizzate su specifici settori delle *industry* come i servizi bancari e finanziari.
La crescita delle attività regolatorie insieme con il livello sempre maggiore del dettaglio richiesto rendono evidente che il GRC è una importante area di attenzione (e preoccupazione) per le autorità di supervisione degli intermediari finanziari e delle banche.
Negli anni passati c'è stata una rapida successione di disposizione regolatorie relative al GRC tra cui:

- Basilea II;
- regolamenti e leggi nazionali sul *financial reporting* (per esempio il *Sarbanes-Oxley Act* statunitense del 2002);
- standard prudenziali.

Regolamenti di tutti i tipi si sono evoluti in framework dettagliati che coprono molteplici aspetti dei servizi finanziari e della tecnologia. Negli ultimi anni regolazioni nazionali ed internazionali hanno reso obbligatorio gestire i temi dell'*information management*, dell'*information technology* e delle discipline specialistiche all'interno di questi campi. Oggi l'alta direzione e gli specialisti delle varie aree devono trasformare le regolamentazioni esistenti in concetti pratici e gestibili che supportino il GRC a livello aziendale.
I *driver* per i cambiamenti regolatori comprendono:

- la crescente sofisticazione della tecnologia di supporto alla finanza che conduce ad attività più complesse e maggiori "profili di rischio" nelle aziende di servizi finanziari;
- la globalizzazione delle istituzioni finanziarie e la diffusione dell'operatività finanziaria attraverso le frontiere nazionali;
- l'aumento della collaborazione tra i regolatori attraverso più giurisdizioni geografiche guidati dalla necessità di supervisionare i mercati diventati globali;
- l'allargarsi dei requisiti di *compliance* in altri settori come ad esempio l'antiriciclaggio;
- la sempre maggior aspettativa verso la *corporate accountability*, che sottolinea l'importanza di una *governance* avanzata, dell'etica, dell'indipendenza, della trasparenza e di rigorose comunicazioni al mercato;
- l'aspettativa in aumento per standard rigorosi che il top management deve rispettare nell'espletare i propri incarichi, il che aumenta considerevolmente il loro ambito di responsabilità e le potenziali esposizioni legali del Consiglio di Amministrazione e dei comitati interni;
- il crescere del pubblico interesse e la pressione dei gruppi di interessi non governativi, degli azionisti e dei *media* sui temi della *governance* e del *risk management*, combinati con una sempre più forte influenza di questi gruppi nel dibattito regolatorio;
- il reporting interno ed esterno da varie applicazioni e database;
- la divergenza negli standard di *compliance* dei regolatori nazionali ed internazionali;
- la necessità di garantire fiducia nelle infrastrutture tecnologiche per fornire servizi efficaci ed efficienti ed aumentare la fiducia nelle terze parti come risultato dello sviluppo degli accordi in ambito finanziario adottati anche in diversi paesi e continenti.

Data la complessità crescente dell’ambiente globale di business, è molto probabile che nel futuro la normativa diventerà sempre più specifica ed attenta indirizzandosi verso aree che al momento non sono ancora coperte. Sebbene questo cambiamento nello scenario possa essere interpretato come una super regolamentazione, i *regulator* si attendono, come obiettivo finale, che la fiducia nei mercati ne esca rafforzata così come la sicurezza ed affidabilità delle istituzioni finanziarie compresa la protezione degli azionisti, la trasparenza e l’integrità aziendale.
Inoltre si può osservare che c’è un trend verso una regolamentazione basata sui principi anche se le norme e gli standard rimangono (e rimarranno) basati su regole (*rules-based*); in particolare con l’introduzione di Basilea II, la regolamentazione prevede disposizioni basate sui processi (*process-based*) e sui risultati (*outcome-based*).
Per quanto riguarda responsabilità e doveri per la *compliance* regolatoria – sia sotto l’approccio emergente *principle-based* sia per quella classica *rules-based* – essa è ormai un requisito imprescindibile per le aziende di servizi finanziari; il Consiglio di Amministrazione e l’alta direzione devono costantemente dimostrare la “robustezza” dei loro processi GRC e la loro conformità rispetto ad un quadro normativo assai ampio i cui requisiti sono sempre più dettagliati.
C’è quindi la necessità, anche in una prospettiva futura, di introdurre processi affidabili di business per gestire il GRC anche in aree precedentemente non regolamentate come l’*Information Management* e l’*Information Technology* e le discipline connesse, come la sicurezza, la *business continuity* e la privacy.

4. L’approccio di Basilea II alla gestione dei rischi

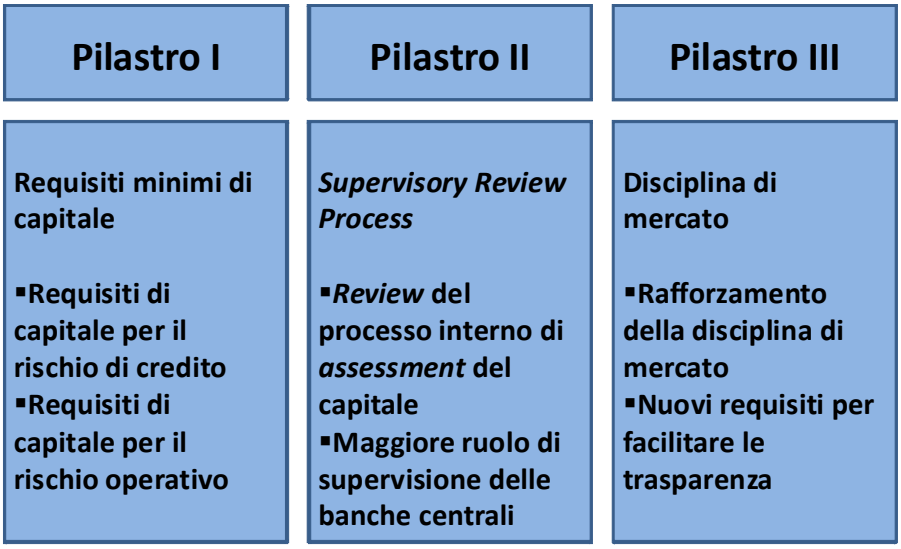
Il rischio, in quanto componente ineliminabile del business, negli ultimi anni è sempre più all’attenzione di una vasta audience a causa di una serie di eventi negativi.
Tra questi ricordiamo frodi, fallimenti di grandi società del credito, attacchi di *hacker* ai sistemi informativi e molto ancora. L’attenzione dei media e del pubblico confermano che il *risk management* è ormai considerato come una delle priorità principali per garantire la fiducia del pubblico nel sistema finanziario internazionale.
All’interno della comunità dei servizi bancari e finanziari il rischio, in generale, richiede una classificazione per creare strutture GRC effettivamente gestibili. Le categorie di rischio sono di solito definite a partire dalle tipiche aree di *core business* che si trovano in una banca o in un’azienda di servizi finanziari.
Tra queste categorie di rischio ci sono:

- rischio di credito;
- rischio di mercato;
- rischio operativo;
- rischio di liquidità;
- rischio di tasso di interesse;
- rischio legale;
- rischio strategico;
- rischio reputazionale.

Il “*Basel Committee on Banking Supervision*” ha pubblicato il secondo framework sulla adeguatezza patrimoniale nel 2004; il nuovo framework ha introdotto un approccio avanzato al rischio per gli intermediari finanziari. L’obiettivo di Basilea II è di favorire l’adozione di prassi più forti di *risk management* per i rischi di credito ed operativi e di rafforzare il link tra rischio e coefficienti patrimoniali. La nuova regolamentazione fornisce, infatti, incentivi alle aziende perché migliorino la qualità dei loro framework di *risk management* riducendo, sotto certe condizioni, i coefficienti patrimoniali richiesti: le aziende di servizi finanziari con un framework GRC affidabile hanno, di fatto, un vantaggio competitivo.
Infatti l’esposizione globale al rischio determina, per ogni azienda , i coefficienti patrimoniali richiesti. Le iniziative GRC possono essere funzionali a ridurre tali coefficienti patrimoniali. Sulla base di questa nuova prospettiva sui requisiti di capitale e sui rischi, molti processi di aziende di servizi finanziari sono state rivisti e rivalutati.
L’approccio di Basilea II al rischio è impostato infatti per tener conto della complessità della tecnologia informatica e dell’*Information Management*. Il framework avanzato, mostrato nella **figura 2**, è costruito su tre pilastri:

1. requisiti minimi di capitale – viene meglio specificato l’approccio di Basilea I al rischio di credito e si introduce un nuovo requisito di capitale per i rischi operativi;
2. vigilanza (*supervisory review process*) – si introducono le *supervisory review* ed il *self-assessment* del processo di adeguamento dei capitali della banca che deve comprendere politiche e procedure affidabili per gestire e controllare il capitale;
3. disciplina di marcato – si introducono nuovi obblighi in relazione all’informativa al pubblico per rafforzare le regole del mercato, per mezzo del *rating* affidato ad agenzie specializzate e la sensibilità degli *shareholder*;

Figura 2 – I tre pilastri del nuovo framework[3]



È fondamentale che i requisiti minimi sul capitale del primo pilastro siano accompagnati da una implementazione effettiva del secondo pilastro. È inoltre essenziale l'informativa al pubblico fornita nell'ambito del terzo pilastro per assicurare che la disciplina di mercato sia di complemento effettivo agli altri due pilastri.
Gli intermediari finanziari possono scegliere fra diversi approcci per misurare e gestire i loro rischi e rispettare i requisiti di mercato: ciò serve per garantire la flessibilità richiesta dai differenti livelli di maturità nel GRC. I coefficienti patrimoniali di capitale inoltre possono essere minori per quelle aziende che scelgono un approccio al *risk management* più avanzato.
Questi approcci variano secondo la categoria di rischio e si può ipotizzare che ci sarà un graduale spostamento verso gli approcci più avanzati. Le aziende possono optare infatti per coefficienti patrimoniali differenziati in base a valutazioni costi-benefici e decisioni strategiche dell'alta direzione ed accettare, di conseguenza, con consapevolezza un livello di rischio più alto. Si noti che le aziende devono dimostrare di aver correttamente adottato l'approccio avanzato per i rischi operativi prima di implementare l'approccio *Internal Ratings-Based* (IRB) per il rischio di credito.
Il pilastro sulla *supervisory review* introduce l'obbligo di una *assurance* qualitativa del GRC adottato dagli intermediari finanziari. Le autorità di vigilanza nazionali degli intermediari finanziari devono monitorare la *compliance* con i requisiti minimi di capitale e prendere azioni in caso di inadeguatezza.
L'appendice I, "Sintesi di Basilea II", descrive in dettaglio i quattro principi della *supervisory review*. I principi e l'ambito del processo di supervisione prevedono inoltre un dialogo continuo tra le aziende di servizi finanziari e le autorità di vigilanza nazionali.
Il pilastro sulla disciplina di mercato introduce l'obbligo dell'informativa delle informazioni sui rischi e il GRC. Questa informativa deve intendersi come volta ad informare tutti gli attori partecipanti al mercato sulla situazione generale di rischio e sulle aree più importanti di rischio potenziale che possono sussistere presso gli intermediari finanziari. L'obiettivo è rafforzare la disciplina di mercato ed evitare la presenza di rischi sproporzionati.

[3] Questa figura mostra solo i cambiamenti nelle componenti di dettaglio del framework di Basilea II. Maggiori dettagli su ogni pilastro si trovano nell'**appendice I**, "Sintesi di Basilea II".

I requisiti sull’informativa in pratica obbligano a calcolare e comunicare le perdite potenziali e reali per ogni tipo di rischio (credito, mercato, operativi, tasso di interesse); ciò permette a tutti i partecipanti al mercato di valutare i dettagli del profilo di rischio dell’azienda.
I dettagli su i vari approcci ai tipi di rischio sono forniti nell’**appendice I**, “Sintesi di Basilea II”.

5. La necessità di gestire i rischi operativi

Il rischio operativo è una componente importante nella determinazione dei requisiti minimi di capitale. Il rischio operativo copre infatti tutte le aree collegate ai potenziali errori nell'operatività generale delle aziende di servizi finanziari ed in particolare per tutto ciò che riguarda le infrastrutture tecnologiche: l'*Information Technology* ha una diretta correlazione con i coefficienti patrimoniali relativi al rischio operativo.
La categoria del rischio operativo è più ampia di quelle del credito, di mercato o di interesse; data la complessità e l'ambito del rischio operativo, i GRC *framework* e le correlate iniziative devono prendere in considerazione tutte le aree di un'azienda che non sono direttamente legate agli altri tipi di rischio.

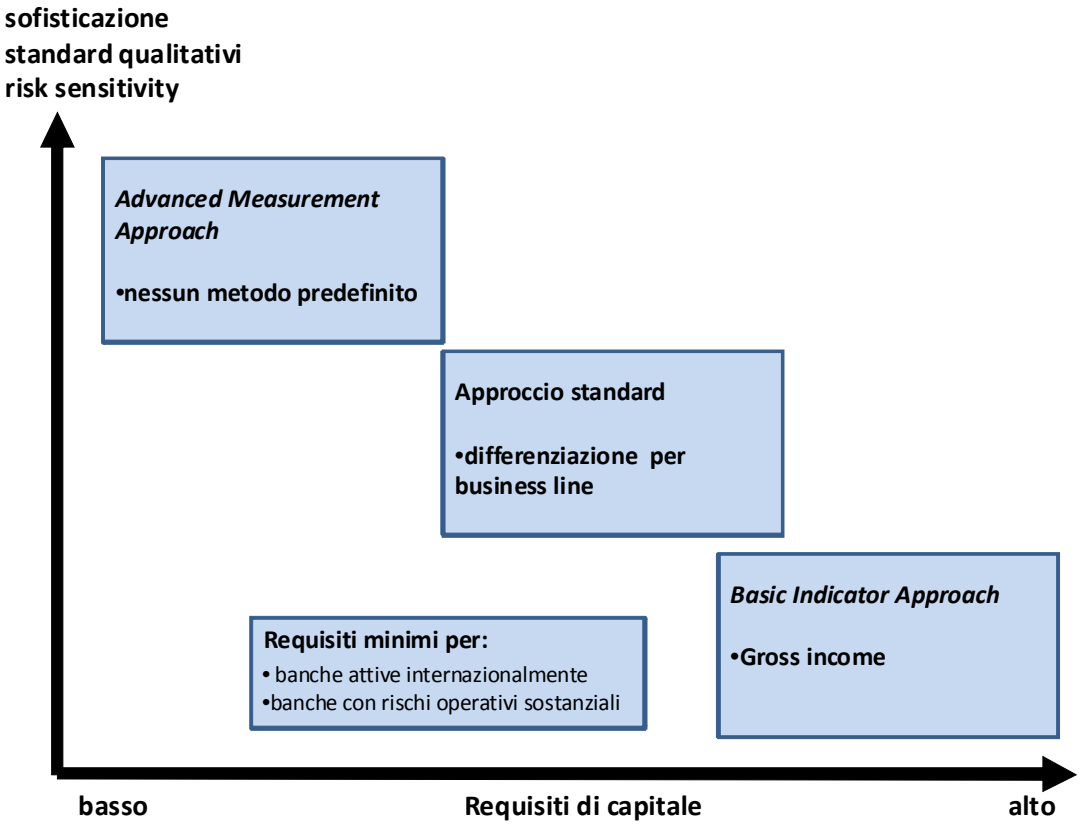
Gli approcci di risk management

Il rischio operativo può essere gestito usando uno dei tre approcci fondamentali:

- il *Basic Indicator Approach* (BIA);
- lo *STandardized Approach* (STA);
- l'*Advanced Measurement Approache* (AMA) che si basa su dati storici relativi alle perdite.

Inoltre per scegliere uno di questi approcci, le aziende di servizi finanziari devono essere conformi con un insieme minimo di requisiti che hanno influenza sul *core business* e sull'IT.
L'**appendice I**, "Sintesi di Basilea II", sottolinea i requisiti di dettaglio degli approcci indicati nel precedente paragrafo.
Si noti che, per la prima volta, Basilea II prende in considerazione, in modo specifico, i rischi operativi nel calcolo dell'adeguatezza patrimoniale.
Le ragioni di questo cambiamento si devono alle notevoli perdite economico-finanziare che si sono verificate in diverse aziende di servizi finanziari negli ultimi anni e che si sarebbero potute evitare se i controlli fossero stati più efficaci e se fossero stati adottati processi di *business* più avanzati.
Inoltre c'è una sempre maggiore dipendenza delle istituzioni di servizi finanziari dall'*Information Technology*, dall'uso esteso di Internet, dalla sempre maggiore complessità dei prodotti finanziari e dall'aumento dei canali di distribuzione: tutto ciò rende necessario identificare e valutare i rischi operativi degli intermediari finanziari.
Il Comitato di Basilea definisce i rischi operativi in Basilea II come segue:
"Il rischio operativo è definito come il rischio di perdite a causa di processi interni, persone, sistemi non adeguati o a causa di eventi esterni."
La definizione include i rischi legali ma esclude i rischi strategici e reputazionali.
Al momento il rischio operativo è valutato, in termini di coefficienti patrimoniali, in misura uguale all'8 per cento dei requisiti di capitale.
Per calcolare il "valore" dei rischi operativi, le banche possono usare diversi approcci metodologici.
Il Comitato di Basilea ha proposto, in particolare, tre approcci - BIA, STA ed AMA – per misurare i coefficienti patrimoniali del rischio operativo nel continuo rispetto alla complessità dei processi di business ed operativi e all'aumento della "*risk sensitivity*", come mostrato in **figura 3**.

Figura 3 – I tre approcci al rischio operativo



In coerenza con la filosofia che sottintende all'intera normativa, in particolare per quel che riguarda l'adeguatezza del capitale in relazione al rischio di credito, i tre approcci sono classificati ed ordinati dal punto di vista della complessità e della *risk sensitivity*.
In sintesi per usare l'approccio avanzato che risulta in minori requisiti di capitale le banche devono soddisfare condizioni più sofisticate.
Gli intermediari finanziari sono incoraggiati a muoversi lungo lo spettro degli approcci disponibili via via che esse sviluppano sistemi e prassi più sofisticate per la misurazione dei rischi operativi: per fornire un incentivo, minore coefficienti patrimoniali sono richiesti se si utilizza un metodo più sofisticato; inoltre è possibile usare l'approccio avanzato anche per una specifica *business line*; infine l'adozione di un approccio individuale richiede agli intermediari di essere conformi anche ad ulteriori requisiti specifici.
Tutte le organizzazioni di servizi finanziari devono essere conformi, infine, con i requisiti minimi che sono definiti nelle note alle linee guida del Comitato "*Operational Risk Sound Practices*".

Questi requisiti includono i seguenti elementi:

- il Consiglio di Amministrazione ed il top management devono giocare un ruolo attivo nella supervisione della gestione dei rischi operativi;
- l'intermediario deve avere un sistema integrato di gestione del rischio;
- quale che sia l'approccio del rischio prescelto, il numero delle risorse umane deve essere sufficiente per essere applicato al rispettivo approccio.

Framework per il risk management *operativo*

Il rischio operativo è considerata una categoria di rischio particolarmente importante.
Il rischio intrinseco alle attività degli intermediari finanziari e la gestione del loro specifico *business* sono spesso più ampi e svariati rispetto alle aree notevolmente più ristrette coperte dalle altre categorie di rischio quali il rischio di tasso di interesse.
Identificare e misurare il rischio operativo è un impegno significativo per gli intermediari finanziari.
All'interno della definizione di rischio operativo così come indicato dai *regulator* e dalle associazioni di categoria, esiste un ampio raggio di specifici fattori di rischio che devono essere presi in considerazione prima di integrare la componente operativa nel più ampio *Enterprise Risk Management framework*.
Ad esempio molti rischi specifici della categoria "operativa" sono connessi alle tematiche della più ampia *compliance* o *corporate governance*; altri richiedono una comprensione profonda della tecnologia e delle infrastrutture che sono di supporto alle attività di *core business*.
Il Comitato di Basilea richiede alle banche di adottare un *framework* per la gestione del rischio operativo; anche se l'ambito e l'estensione del *framework* non è specificato, l'approccio indicato nella **figura 4** suggerisce una possibile strada per gestire i rischi operativi.

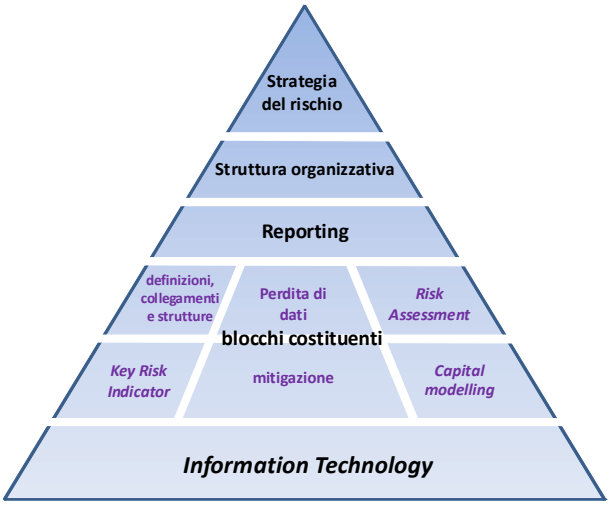
Risk Strategy

Le strategie per il rischio operativo guidano le altre componenti all'interno del framework di gestione del rischio. Una strategia del rischio completa e coerente deve infatti fornire chiare linee guida sulla propensione al rischio, sulla tolleranza al rischio, sulle politiche e sui processi per il *risk management* quotidiano.

Struttura organizzativa

La struttura organizzativa è la base ed il punto di partenza, a livello aziendale, per tutte le attività di gestione del rischio operativo. Entro tale contesto, le organizzazioni di servizi finanziari devono definire ed assegnare i ruoli e responsabilità, sia a livello centrale che in periferia, a tutte le unità organizzative, le funzioni ed, in ultima analisi, ai singoli individui.

Figura 4 - Framework per la gestione del rischio operativo



Reporting

Dato che il rischio operativo ha effetto su tutte le *business unit*, il reporting dell'*operational risk management* ha un ambito molto più vasto rispetto al reporting tradizionale relativo al rischio di mercato o di credito. Tale reporting riguarda infatti due distinti aspetti:

1. il *delivery* delle informazioni rilevanti sui rischi operativi per la gestione ed il controllo del rischio stesso;
2. il reporting delle informazioni aggregate per categorie di rischio al management delle *business line*, al Consiglio di Amministrazione ed al Comitato Rischi.

Definizioni, collegamenti e strutture

Le organizzazioni di servizi finanziari hanno bisogno di un linguaggio comune per descrivere i rischi operativi e gli *event type* delle perdite, delle cause e degli effetti.
Esse hanno anche necessità di "mappare" le regole necessarie per essere conformi con i requisiti normativi.
Lo sviluppo delle definizioni, dei collegamenti e delle strutture rende possibile agli intermediari finanziari di identificare, valutare e produrre il report su tali informazioni relative al rischio operativo in modo efficiente.

Dati sulle perdite

Un framework ben strutturato per il rischio operativo richiede lo sviluppo e l'utilizzo di basi di dati storiche che registrino gli eventi di perdita attribuibili alle varie categorie di rischio operativo.
Prima di dare una formale approvazione per il loro uso nei processi di stima del rischio, i *regulator* richiedono che i database sulle perdite interne siano completi e coerenti e che includano diversi anni di dati storici.
Basilea II, in modo specifico, richiede un minimo di tre anni di dati storici per una implementazione iniziale e cinque anni per l'AMA. La necessità di aver dati storici (compresi i dati esterni) è stato il motivo per cui molte organizzazioni di servizi finanziari hanno portato i loro database in produzione prima possibile.
Oltre ad un linguaggio comune, gli intermediari finanziari hanno bisogno di un processo per collezionare, valutare, monitorare e fare il reporting dei dati sulle perdite operative. Tale processo deve essere progettato per fornire la base per ogni decisione di management, da un reporting ad hoc ad un *risk reporting* regolare e, infine, condurre a supportare i modelli quantitativi così come il *risk assessment*.

Risk Assessment

Il *risk assessment* fornisce un approccio qualitativo per l'identificazione dei rischi potenziali di natura "significativa" ma a condizione che si documentino ed ipotizzino scenari strutturati con l'ausilio dei rappresentanti di tutte le business unit.
Le tecniche di *risk assessment* possono inoltre colmare il *knowledge gap* che spesso risulta dai dati di perdita relativi al passato che spesso sono incompleti. Queste tecniche tentano infatti di identificare in modo proattivo i rischi operativi più importanti.

Key Risk Indicator

Quale parte della misurazione e monitoraggio continui gli intermediari finanziari devono valutare gli aspetti del rischio operativo basati sui *Key Risk Indicator* (KRI) quei fattori cioè che possono fornire segnali di primo allarme e *early warning* sui sistemi, processi, prodotti, persone e l'intero ambiente aziendale. I KRI sono differenti dai *risk assessment* perché essi si basano su dati osservabili non su attività stimate o future.

Mitigazione

Una volta che le organizzazioni di servizi finanziari hanno identificato e quantificato i propri rischi esse possono implementare una strategia per mitigarli con appropriate politiche, procedure, sistemi e controlli.

Capital Modeling

Il *capital modeling* riguarda il calcolo del capitale richiesto sia dal punto di vista delle norme sia da quello economico. Tale calcolo comporta la definizione dei dati di input (dati sulle perdite interne ed esterne, dati sugli scenari possibili, l'ambiente di business ed i fattori di controllo così come le informazioni ausiliarie quali i parametri assicurativi) e consiste nel definire le relazioni matematico/statistiche e le assunzioni per misurare il rischio operativo, l'implementazione del modello e la validazione del modello.

Information Technology

Un *Information Technology* efficace ed efficiente è la base, il punto di partenza ed il "facilitatore" dell'*operational risk management framework*. I sistemi IT hanno necessità di tener conto di un'ampia varietà di informazioni sui rischi operativi e di interfacciarsi con una grande varietà di sistemi interni e di fonti esterne.

Il Comitato di Basilea ha esplicitamente indicato nel suo "*Sound Practices for the Management and Supervision of Operational Risk*"[4] che la crescente complessità dell'*Information Technology* è un fattore che rende le attività degli intermediari finanziari assai più complicate. L'IT gioca un ruolo importante nelle *operation* di un sistema informativo strategico e manageriale.
Di fatto questi sistemi sono oggi inseparabili dalla capacità dell'azienda di rispondere alle richieste del management, dei supervisori degli intermediari finanziari, dei partecipanti al mercato e di altri importanti *stakeholder*. Per l'affidabilità dell'IT e dei sistemi informativi finanziari ed operativi i controlli sono stati riconosciuti, da tempo, come una componente necessaria, in particolare per i sistemi informativi più importanti.
Nel suo "*Framework for Internal Control Systems in Banking Organisations*"[5] il Comitato di Basilea fa affidamento sulle definizioni e sugli elementi di base dei sistemi di controllo interno sviluppati in accordo con le linee guida fornite dal *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) a partire dal suo *Enterprise Risk Management* (ERM) *framework*. Basilea II considera questo standard la base di partenza per gli standard minimi e tenta di rendere, attraverso "buone prassi" di gestione del rischio, i processi regolatori più attenti all'individuazione dei rischi e agli incentivi da fornire alle banche.

---

[4] Basel Committee on Banking Supervision, "*Sound Practices for the Management and Supervision of Operational Risk*", febbraio 2003
[5] Basel Committee on Banking Supervision, "*Framework for Internal Control Systems in Banking Organisations*", settembre 1998

I miglioramenti nella *corporate governance*, nell'*accountability* diretta del Consiglio di Amministrazione e del senior management, nei controlli generali e nei processi di risk management considerati come elementi chiave per una gestione affidabile del capitale.
COSO è una organizzazione privata, formata da volontari, che si dedica al miglioramento della qualità del *financial reporting* attraverso la *business ethics*, il controllo interno efficace e la *corporate governance*. COSO è nato nel 1985 per sponsorizzare il *National Commission on Fraudulent Financial Reporting*, una organizzazione indipendente del settore privato a cui spesso ci si riferisce come la *Treadway Commission*. Le organizzazioni sponsor comprendono l'*American Institute of Certified Public Accountants* (AICPA), l'*American Accounting Association* (AAA), il *Financial Executives International* (FEI), l'*Institute of Internal Auditors* (IIA) e l'*Institute of Management Accountants* (IMA).
Il modello COSO non dà indicazioni specifiche sull'*Information Management* e l'*Information Technology*. Tuttavia l'IT è una parte essenziale in ogni sistema di controllo interno indipendentemente dal tipo di rischio (registrazioni contabili e finanziarie, obblighi di compliance o operativi) e di conseguenza , a livello di impresa, è una componente imprescindibile della gestione del rischio aziendale.
Il framework COBIT offre un insieme coerente, completo e condiviso di processi di controllo IT, obiettivi ed attività tutti progettati per la gestione di rischi IT ed è totalmente allineato con il framework COSO ed i suoi concetti. COBIT, quindi, fa da ponte nel *gap* tra l'*Enterprise Risk Management* di alto livello e i temi specifici IT. La sezione che segue fornisce un quadro d'insieme di COSO e delle sue implicazioni per l'IT.

Le componenti di COSO

Per un'azienda è fondamentale poter dimostrare che i controlli IT supportino il framework COSO ERM. Di conseguenza in azienda ci deve essere competenza sui controlli IT per tutte le componenti COSO.
COSO identifica le seguenti otto componenti essenziali per un controllo interno efficace:

1. ambiente interno (*internal environment*);
2. definizione degli obiettivi (*objective setting*);
3. identificazione degli eventi (*event identification*);
4. valutazione del rischio (*risk assessment*);
5. gestione del rischio (*risk response*);
6. attività di controllo (*control activities*);
7. informazione e comunicazione (*information and communication*);
8. monitoraggio (*monitoring*).

Ciascuna di queste otto componenti è descritta brevemente nelle sezioni che seguono. Successivamente sono fornite considerazioni su come l'IT, ad alto livello, si collega a ciascuna specifica componente. Il testo in corsivo con rientranza è tratto direttamente dal framework COSO ERM.

Ambiente interno

L'ambiente interno definisce le basi per le modalità con cui il rischio è visto, compresa la filosofia di gestione del rischio. Esso è il punto di partenza per il controllo interno efficace, stabilisce il "*tone at the top*" e rappresenta l'apice della struttura di *corporate governance*. Le problematiche che nascono nella componente dell'ambiente interno si applicano infatti all'intera azienda.

L'IT ha spesso caratteristiche tali che è richiesta una particolare attenzione sull'allineamento del business, ruoli e responsabilità, politiche e procedure e competenze tecnologiche. La lista che segue descrive alcune considerazioni in relazione all'ambiente di controllo e all'IT:

- l'IT è spesso erroneamente considerato come una entità separata del business e di conseguenza come un diverso ambiente di controllo;
- l'IT è complesso non solo in relazione alle sue componenti tecnologiche ma anche nel modo in cui tali componenti si integrano nel sistema generali dei controlli dell'azienda;
- l'IT può introdurre nuovi e maggiori rischi che richiedono nuovi e avanzate attività di controllo per gestire e mitigare con successo tali rischi;
- l'IT richiede *skill* specializzati che possono non essere immediatamente disponibili;
- L'IT richiede spesso che sia garantita l'affidabilità anche di terze parti se processi o componenti IT significativi sono dati in *outsourcing;*
- spesso l'*ownership* dei controlli IT non è chiaramente definita ed assegnata.

Le componenti del controllo interno si riferiscono ai principi 1, 3, 6 e 10 di Basilea II.

Definizione degli obiettivi

COSO ERM identifica quattro macro categorie di obiettivi:

1. Obiettivi per le procedure (*operations objectives*) – si riferiscono alle efficacia ed efficienza delle procedure di ciascuna unità organizzativa e comprendono la performance, gli obiettivi di "profittabilità" e la salvaguardia delle risorse contro le possibili perdite. Essi variano sulla base delle scelte di management relative alla struttura e alla performance. Un intermediario finanziario deve identificare i rischi operativi inerenti a tutti i propri processi IT che impattano i prodotti materiali, le attività, i processi ed i sistemi. Ad esempio se un processo chiave richiede elaborazione 24 ore al giorno per 7 giorni la settimana ed il 90% di disponibilità deve essere valutato il rischio IT associato al raggiungimento di questo obiettivo.
2. Obiettivi di reporting (*reporting objectives*) – questi obiettivi si riferiscono alla affidabilità del reporting (interno ed esterno) sia per quanto riguarda le informazioni finanziarie sia l'informativa generale al mercato. Gli obiettivi di reporting di Basilea II ed i relativi processi hanno un ambito più ampio rispetto agli obiettivi di reporting di *Sarbanes-Oxley*. In aggiunta ai report finanziari devono essere presi in considerazione i report relativi al *risk management* ed alle comunicazioni al pubblico.
3. Obiettivi di compliance (*compliance objectives*) – Questi obiettivi fanno riferimento alla conformità alle norme e regolamenti più rilevanti. Essi dipendono da fattori esterni e tendono ad essere simili, in alcun casi, tra le varie *industry*. L'organizzazione IT deve identificare i requisiti regolatori rispetto ai quali occorre essere *compliant*. Questi requisiti comprendono sia requisiti formali (ad esempio la definizione dei piani di *contingency*) sia requisiti meno definiti (ad esempio le aspettative degli analisti dei mercati finanziari o dei regolatori in relazione ad ambienti sicuri ed affidabili).
4. Obiettivi strategici (*strategic objectives*) – Essi si riferiscono ad obiettivi di alto livello che sono stabiliti dal management per identificare gli obiettivi aziendali da raggiungere. Questi obiettivi sono collegati alle procedure aziendali e al reporting che devono direttamente legarsi alle iniziative di *compliance* ed al *risk management*.

Obiettivi dipartimentali e procedure di reporting devono essere coerenti con le aspettative del management in relazione ai rischi operativi. L' IT è una componente *core* dell'implementazione e della gestione delle procedure di base dei servizi finanziari. Gli obiettivi dell'IT devono essere allineati con gli obiettivi strategici dell'azienda.

La componente di definizione degli obiettivi si riferisce al principio 4 di Basilea II.

Identificazione dell'evento

Secondo il COSO ERM framework:

> *Il management deve identificare i potenziali eventi che, se occorressero, avrebbero impatti significativi sull'azienda e determinare se tali eventi possano avere un effetto negativo sulla capacità dell'azienda di realizzare la propria strategia e raggiungere i propri obiettivi. I rischi sono eventi con impatti negativi che richiedono una valutazione da parte del management e l'elaborazione delle relative azioni di risposta.*

Le categorie di eventi di tipo tecnologico identificate da COSO ERM sono listate nella **figura 5**.

Figura 5 – Categorie di evento di COSO ERM	
Fattori esterni	***Fattori interni***
Interruzioni	Integrità dei dati
Commercio elettronico	Disponibilità dei dati e dei sistemi
Dati esterni	Selezione dei sistemi
Tecnologie emergenti	Sviluppo
	Deployment
	Manutenzione

Esempi di eventi mappati da processi COBIT sono forniti nell'appendice V "Basilea II e COBIT".
La componente di identificazione degli eventi si riferisce ai principi 4 e 5 di Basilea II.

Risk Assessment

In relazione al risk assessment, COSO ERM recita:

> *Il risk assessment è lo strumento che permette all'azienda di considerare e valutare l'estensione dell'impatto degli eventi potenziali rispetto al raggiungimento degli obiettivi. Il management deve valutare gli eventi da due punti di vista – frequenza ed impatto – e di solito utilizza una combinazione di metodi di valutazione qualitativi e quantitativi.*

Il risk assessment comporta l'identificazione e l'analisi da parte del management dei rischi rilevanti per il raggiungimento di obiettivi predeterminati che a loro volta sono la base per la determinazione delle attività di controllo. È probabile che i rischi di controllo interno possano essere più pervasivi nell'ambito IT rispetto all'altre aree aziendali.
Il risk assessment può essere svolto a livello di entità (cioè a livello di azienda) o a livello di attività (cioè per uno specifico processo o *business unit*).
A livello di entità ci si aspetta i seguenti risultati:

- Le responsabilità del sottocomitato della pianificazione IT include:

- supervision dello sviluppo del piano strategico sui controlli interni IT, la sua esecuzione/implementazione efficace e tempestiva e la sua integrazione con il piano generale di *risk management*.
- assessment dei rischi IT, cioè *IT management*, *data security*, *program change* e *development*.

A livello di attività *activity level* ci si aspetta quanto segue:

- *risk assessment* formali costruiti per mezzo della metodologia di sviluppo dei sistemi;
- *risk assessment* relativo alle operazioni di infrastruttura e al processo di cambiamento;
- *risk assessment* relativo al processo di *program change*.

La componente di *risk assessment* fa riferimento ai principi 4 e 5 di Basilea II.

Risk Response

Secondo il COSO ERM:

Le *risk response* includono la *risk avoidance*, la riduzione, la condivisione e l'accettazione del rischio. Nel considerare le proprie risposte, il management deve valutare l'effetto sulla probabilità ed impatto di rischio così come i costi ed i benefici, selezionando la risposta che riporta il rischio residuo all'interno della tolleranza richiesta. Il management deve identificare tutte le opportunità che sono disponibili ed adottare una visione generale, o per *portfolio*, del rischio determinando se il rischio residuale rientra nei limiti dell'*appetite* indicato dall'entità.

Le *risk response* possono essere classificate nelle seguenti categorie:

- Evitare (*avoidance*) – Abbandonare le attività evitando il rischio. La *risk avoidance* può implicare di muoversi da una infrastruttura IT standardizzata verso, ad esempio, un approccio del tipo "*best of breed*" di componenti architetturali.
- Ridurre – Azioni volte a ridurre la probabilità o l'impatto del rischio o entrambi.

Ciò di solito implica l'adozione di decisioni di business di vario tipo quali, ad esempio, la "centralizzazione" della funzione di *program change*.

- Condividere (*sharing*) – Consiste nel ridurre la probabilità o l'impatto trasferendo o comunque condividendo un parte del rischio. A riguardo tecniche comuni comprendono la stipula di una polizza assicurativa, l'adozione di specifiche procedure di "difesa" o il dare in outsourcing l'attività.
- Accettazione – Non viene adottata nessuna azione per limitare probabilità o impatto del rischio. Ad esempio se la *policy* richiede una password di 8 caratteri e l'applicazione ne permette solo sei allora si può decidere di accettare tale rischio.

La componente di *risk response* fa riferimento ai principi 6 e 7 di Basilea II.

Attività di controllo

Le attività di controllo sono le *policy*, le procedure e le prassi poste in essere per garantire il raggiungimento degli obiettivi e tenere sotto controllo i rischi. Le attività di controllo sono

sviluppate per gestire in modo specifico ciascun obiettivo di controllo che mitiga un certo rischio identificato.
Senza sistemi informativi affidabili ed attività di controllo efficaci le aziende non sono in grado di produrre rapporti finanziari accurati.
COSO riconosce questa relazione ed identifica due ampi raggruppamenti di attività di controllo sui sistemi informativi: controlli generali e controlli applicativi.

I **controlli generali**, che sono disegnati in modo da garantire l'affidabilità dei sistemi informativi che producono le informazioni finanziarie dell'azienda, comprendono le seguenti tipologie:

- controlli sulle procedure operative dei data center (*data center operation controls*) – si tratta di controlli quali *job setup* e *scheduling*, attività degli operatori nonché le procedure di *data backup* e *recovery*;
- controlli sui sistemi software (*system software controls*) – controlli sull'efficacia delle procedure relative all'acquisizione, realizzazione e manutenzione dei sistemi software, il *database management*, il software di telecomunicazioni, il software di sicurezza e le *utility*;
- controlli sulla sicurezza degli accessi (*access security controls*) - controlli che impediscono, in maniera preventiva, l'uso dei sistemi non autorizzato o non appropriato;
- controlli sullo sviluppo e manutenzione (*application system development and maintenance controls*) – i controlli sulla metodologia di sviluppo, compresi gli aspetti di progettazione e realizzazione, che illustrano le fasi specifiche del ciclo di vita del software nonché i requisiti di documentazione, il *change management*, le approvazioni formali ed i *checkpoint* per controllare lo sviluppo e la manutenzione del progetto.

I **controlli applicativi** sono inseriti (*embedded*) all'interno dei programmi software per prevenire o intercettare transazioni non autorizzate. Quando sono combinati con altri controlli, se necessario, i controlli applicativi supportano la completezza, l'accuratezza, l'autorizzazione e la validità delle transazioni processate. Alcuni esempi di controlli applicativi sono:

- bilanciamento delle attività di controllo – intercettazione degli errori di *data entry* per mezzo della riconciliazione dei valori inseriti manualmente o in modo automatico rispetto ad un controllo di "totale"; per esempio una azienda può bilanciare in automatico il numero totale delle transazioni processate e passate dal suo sistema online di *order entry* con il numero di transazioni ricevuta nel suo sistema di fatturazione;
- *check digit* – campo di controllo per validare un dato; una serie di numeri dell'azienda contengono un *check digit* per intercettare e correggere gli ordini non corretti dei propri fornitori; gli *Universal Product Codes* (UPCs) comprendono un *check digit* per verificare il prodotto ed il *vendor*;
- liste predefinite di dati – fornire all'utente una lista predefinita di dati accettabili; per esempio il sito intranet di un'azienda può includere liste già pronte dei prodotti disponibili per l'acquisto;
- test di ragionevolezza sui dati – confrontare i dati inseriti rispetto ad un modello o *pattern* di ragionevolezza basato sui casi passati; per esempio un ordine ad un fornitore da un negozio per un numero inusualmente molto grande di articoli può far scattare un indicatore di *review*;
- test logici – comprendono l'uso di limiti di range o test sul valore o sui caratteri alfanumerici.

Ad esempio i numeri delle carte di credito hanno un format predefinito.

I controlli generali sono necessari per supportare il funzionamento dei controlli applicativi ed entrambi sono necessari per supportare l'accuratezza e l'integrità dei dati processati usati per gestire, governare e fornire report sull'azienda. Dato che i controlli automatizzati stanno sostituendo quelli manuali, i controlli generali stanno diventando sempre più importanti.
Questa componente sulle attività di controllo di riferisce al principio 6 di Basilea II.

Informazione e comunicazione

COSO recita che l'informazione è necessaria a tutti i livelli dell'azienda per permettere il business e garantire il raggiungimento degli obiettivi di controllo dell'organizzazione. Tuttavia l'identificazione, la gestione e la comunicazione delle informazioni rilevanti rappresenta una sfida sempre maggiore per i dipartimenti IT. La determinazione di quali informazioni sono richieste per garantire gli obiettivi di controllo e la relativa comunicazione di tali informazioni in una modalità e con una tempistica che permette alle persone di rispettare le proprie responsabilità è di supporto alle altre sette componenti del COSO *framework*.
L'organizzazione IT gestisce i processi delle informazioni finanziarie più rilevanti.
Tuttavia il suo ambito è, di solito, molto più ampio. Il dipartimento IT può anche essere d'ausilio nell'implementare i meccanismi per identificare e comunicare gli eventi più significativi come il sistema di e-mail o gli *executive decision support systems*.
COSO recita, inoltre, che la qualità delle informazioni comprende di verificare che l'informazione sia:

- appropriata – si tratta dell'informazione giusta?
- tempestiva – essa è disponibile quando richiesto e riportata nel corretto periodo di tempo?
- aggiornata – è l'ultima disponibile?
- accurata – i dati sono corretti?
- accessibile – gli utenti autorizzati possono accedere ad essa quando ne hanno bisogno?

Per l'*entity level* ci si aspetta:

- sviluppo e comunicazione di politiche *corporate*;
- sviluppo e comunicazione dei requisiti sul *reporting* comprese le *deadline*, le riconciliazioni, i formati ed i contenuti per i report di gestione mensili, trimestrali ed annuali e per le comunicazioni al mercato (*public disclosure reporting*);
- consolidamento e comunicazione delle principali informazioni finanziarie.

A livello di *activity level*, ci si aspetta:

- sviluppo e comunicazione di standard per garantire il raggiungimento degli obiettivi delle *corporate policy*;
- identificazione e comunicazione tempestiva delle informazioni per essere di ausilio nel raggiungimento degli obiettivi di business;
- identificazione e reporting tempestivo delle violazioni di sicurezza.

La componente informazione e comunicazione si riferisce ai principi 3, 5, 6 e 10 di Basilea II .

Monitoraggio

Il monitoraggio che copre la supervisione del controllo interno da parte del management per mezzo di processi di assessment continui e puntuali è sempre più importante anche per l'IT management.
Nel 2006 COSO ha suggerito che un monitoraggio efficace:

- sia integrata, quanto più possibile, con le *operation* - il monitoraggio continuo è costruito per mezzo delle attività operative dell'azienda;
- fornisca assessment obiettivi;
- utilizzi personale dotato di opportune conoscenze nello sviluppare le valutazioni – i valutatori devono comprendere le componenti che analizzano e come esse si relazionano alle attività che supportano l'affidabilità delle informazioni;
- prenda in considerazione i *feedback* – il management, i supervisor dei servizi finanziari ed i partecipanti al mercato ricevono *feedback* sull'efficacia del controllo interno sul reporting, il risk management e la compliance;
- moduli ambito e frequenza – il management, i supervisor dei servizi finanziari variano l'ambito e la frequenza delle valutazioni separate in base alla significatività dei rischi che devono essere controllati, l'importanza dei controlli nel mitigare i rischi e l'efficacia del monitoraggio continuo.

L'IT performance e la sua reale efficacia devono essere monitorati in modo continuo per mezzo di strumenti che misurano la performance e che indicano se i controlli previsti operano in modo appropriato.

Si considerino i seguenti esempi:

- identificazione e gestione dei difetti – stabilendo metriche e analizzando i trend dei risultati attuali rispetto alle metriche può fornire una base per comprendere le ragioni sottostanti ai fallimenti nei processi; correggere tali cause può migliorare l'accuratezza dei sistemi, la completezza del *processing* e la disponibilità dei sistemi;
- *security monitoring* – realizzare una infrastruttura IT di sicurezza efficace riduce il rischio di accessi non autorizzati; migliorare la sicurezza riduce il rischio di transazioni non autorizzate e di conseguenza di generare report non affidabili e produce una riduzione della non disponibilità dei sistemi chiave nel caso le componenti infrastrutturali delle applicazioni IT fossero compromesse.

Una organizzazione IT è soggetta anche a molti altri tipi di valutazioni, tra le quali:

- internal audit;
- external audit;
- esami relativi a particolari norme di legge (*regulatory examination*);
- assessment su attacchi informatici e *penetration test*;
- analisi indipendenti sulle performance e sulle capacità elaborative;
- review sull'efficacia dell'IT;
- *control self-assessment*;
- review indipendenti sulla sicurezza;
- review sull'implementazione dei progetti.

Per l'*entity level* ci si aspetta:

- monitoraggio centralizzato e continuo sulle procedure informatiche (*computer operation*);
- monitoraggio centralizzato della sicurezza;
- review IT di internal audit reviews (mentre l'audit può aver luogo a livello di *activity level*, il reporting dei risultati di audit per l'*audit committee* è a livello di *entity level*).

A livello di *activity level*, ci si aspetta:

- identificazione e gestione dei difetti;
- monitoraggio locale delle procedure informatiche o di sicurezza;
- supervisione del personale IT locale.

La componente monitoraggio si riferisce ai principi 2, 8 e 9 di Basilea II.

I principi del rischio operativo e della IT Relevance

L'Information Technology e l'Information Management sono elementi chiave di una strategia coerente e completa per gestire il GRC ed ottimizzare il *capital charge*.
Le componenenti *IT-related* quali applicazioni, infrastrutture e controlli sono tutti definiti quali parti del rischio operativo. La **figura 6** mostra i principi guida di Basilea II sul rischio operativo e le componenti del COSO ERM che ne sono coinvolte così come la loro rilevanza ed i requisiti in termini di Information Technology.
I principi sono forniti per facilitare l'uso e l'implementazione degli "Obiettivi di Controllo IT" per Basilea II nel contesto di un framework GRC integrato.

Figura 6 – Principi di Basilea II, componenti COSO, rilevanza IT e requisiti

Principi di Basilea II **Nota: il testo in corsivo è tratto da Basilea II.**	Componenti COSO	Rilevanza IT e requisiti
Realizzare un ambiente appropriato di *Risk Management*		
Principio : Il Consiglio di amministrazione deve essere consapevole che il rischio operativo a cui è esposta la banca è una categoria autonoma di rischi che deve essere gestita in maniera specifica; il Consiglio deve approvare e periodicamente valutare il framework di gestione del rischio operativo. Tale framework deve fornire la definizione "aziendale" di rischio operativo e stabilire i principi generale per l'identificazione del rischio operativo, la sua valutazione ed il controllo/mitigazione	Ambiente interno	L'IT deve essere integrato nel più ampio processo aziendale generale di gestione del rischio
Principio 2: Il Consiglio di amministrazione deve assicurare che il framework per la gestione del rischio operativo della banca sia sottoposto ad un internal audit efficace e completo da parte di personale indipendente, competente, format in modo appropriato. La funzione di Internal Audit non deve essere direttamente responsabile per la gestione del rischio operativo.	Monitoraggio	Il framework per la gestione del rischio operativo, comprese le componenti IT, deve essere incluso nel piano di internal audit. La funzione di internal IT audit deve essere adeguatamente formata e avere il personale adeguato. Gli skill richiesti devono

		comprendere la conoscenza di Basilea II, dei principi del risk management e dei principali requisiti in ambito regolatorio e per la supervisione per gli intermediari finanziari. La funzione di internal IT audit deve essere valutata dalle funzioni di supervision dell'intermediario finanziario Se necessario possono essere utilizzati specialisti esterni.
Principio 3: L'alta direzione ha la responsabilità di implementare il framework per la gestione del rischio operativo come approvato dal comitato di direzione (*board of directors*). Il framework deve essere implementato in modo coerente in tutta l'organizzazione della banca e tutti i livelli del personale devono aver chiaro ala loro responsabilità rispetto alla gestione del rischio operativo. Il senior management deve anche avere la responsabilità di sviluppare le politiche, i processi e le procedure per la gestione del rischio operativo per quanto riguarda tutti i prodotti materiale della banca, le attività, i processi ed i sistemi.	Ambiente interno Informazione e comunicazione	I membri della direzione IT hanno le stesse responsabilità dell'alta direzione. Il framework adottato dalle banche deve essere adattato per tener conto dei requisiti IT (tuttavia i più diffusi GRC framework non danno indicazioni specifiche su tali aspetti). Deve essere data giusta considerazione per l'implementazione del framework dei controlli IT che può essere "riconciliato" al framework GRC dell'intermediario finanziario. Il framework adottato deve tener conto delle aree che possono riguardare le attività dei supervisori della banca quali l'IT *corporate governance*, la pianificazione ed organizzazione IT, la sicurezza, lo sviluppo dei sistemi e programmi, il *program changes*, le procedure (*operations*)il supporto e le responsabilità sul controllo interno.
Risk Management: identificazione, valutazione, monitoraggio e mitigazione/controllo		
Principio 4: Le banche devono identificare e valutare i rischi operativi inerenti tutti i prodotti	Definizione degli obiettivi	Il Risk Assessment deve essere incorporato in tutte le attività IT che possono avere

materiali, le attività, i processi ed i sistemi . Le banche si devono anche assicurare che i nuovi prodotti, le attività i processi ed i sistemi siano introdotti tenendo sotto controllo i rischi operativi inerenti e nel rispetto delle procedure di assessment previste.	Identificazione degli eventi Risk Assessment	un impatto materiale sulla banca, cioè, nelle modifiche ai programmi ed alle infrastrutture e nel monitoraggio della sicurezza. Il Risk Assessment deve essere integrato nel processo di sviluppo dei sistemi e nel processo di rilascio delle modifiche. Gli stakeholder che potrebbero avere degli impatti devono essere coinvolti nel Risk Assessment. I risultati del Risk Assessment devono essere integrati con i risultati di altri risk assessment ed incorporati nel GRC framework.
Principio 5: Le banche devono implementare un processo per monitorare in modo regolare e continuo i profili di rischio operativo e l'esposizione materiale alle perdite. Deve esistere un reporting "regolare" sulle informazioni importanti per il management ed il Consiglio di Amministrazione che sia di supporto effettivo alla gestione del rischio operativo.	Identificazione degli eventi Risk Assessment Informazione e comunicazione	L'assessment dei rischi operativi deve essere compreso nella pianificazione annuale e nel ciclo di pianificazione strategica. Il rischio operativo deve essere sottoposto a nuovi assessment a seguito di eventi interni o esterni significativi ad esempio se un disastro esterno indica che la strategia del piano di "contingency" deve essere ripensata. Le metriche di *risk performance* devono essere identificate e tenute sotto controllo. Se viene individuato un trend non favorevole deve essere effettuata un'analisi delle cause e devono essere intraprese le opportune azioni correttive.
Principio 6 Le banche devono dotarsi di policy, processi e procedure per tenere sotto controllo e/o	*Risk response* Ambiente	Deve essere adottato un framework di controllo interno dell'IT per mitigare i

mitigare i rischi operativi. Le banche devono rivedere periodicamente la propria analisi dei rischi e le strategie di controllo e modificare il proprio profilo di rischio operativo sulla base di strategie appropriate compatibilmente con il profilo generale di rischio e la predisposizione (*appetite*) al rischio.	interno Informazione e comunicazione Attività di controllo	rischi operativi. Il framework di controllo interno dell'IT deve essere supportato da appropriate policy, processi e procedure. I rischi operativi devono essere rivalutati a seguito di eventi interni o esterni significativi quali ad esempio l'acquisto di una nuova banca che pone problemi di integrazione dei sistemi. Le politiche e procedure IT devono essere riviste e formalmente approvate almeno una volta l'anno.
Principio 7 Le banche devono predisporre e rendere operativi i piani di "*contingency*" e "*business continuity*" così da garantire di poter operare in modo continuo e di essere in grado di limitare le perdite in caso di eventi distruttivi significativi.	*Risk response*	L'IT deve dotarsi di piani di continuità IT e di procedure di gestione che siano correlate alla "*corporate business continuity*" ed alle procedure di gestione degli incidenti.
Ruolo delle autorità di supervisione		
Principio 8: I supervisori delle banche devono richiedere che tutte le banche, indipendentemente dalla loro dimensioni, adottino un framework efficace per identificare, valutare, monitorare e controllare/mitigare i rischi operativi come parte di una gestione generale del rischio.	Monitoraggio	L'IT deve implementare un "*IT risk management framework*" che gestisca e indirizzi i requisiti applicabili agli intermediari finanziari decisi dalle autorità di supervisione.
Principio 9: Le autorità di supervisione devono condurre, direttamente o indirettamente, regolari valutazioni indipendenti sulle politiche, procedure e processi della banca che sono in relazione ai rischi operativi. I supervisori si devono assicurare che esistono appropriati meccanismi organizzativi che permettono la gestione effettiva dei rischi anche in relazione allo sviluppo della banca.	Monitoraggio	L'IT senior management si deve assicurare che i requisiti di "*regulatory compliance*" siano integrati con le politiche generali dell'azienda, che le relative procedure gestiscano in modo effettivo i rischi operativi ed i requisiti delle autorità di supervisione e che le criticità (*deficiencies*) identificate dagli ispettori siano gestite in modo appropriato. La funzione di *IT compliance*

		deve essere integrata con la funzione aziendale di *Compliance* per assicurare che le autorità di supervisione siano costantemente informate sugli sviluppi dell'IT.
Principio 10: Le banche devono effettuare comunicazioni al mercato sufficienti per permettere agli attori economici di valutare l'approccio alla gestione del rischio operativo della banca.	Ambiente interno Informazione e comunicazione	L'IT deve identificare tutti i rischi rilevanti che possono costituire un rischio operativo materiale e comunicarli al Consiglio di Amministrazione ed all'alta direzione per le loro considerazioni.

6. Gestire i rischi informatici

La gestione delle informazioni e dell'IT richiedono un approccio specifico nell'ambito del GRC. La complessità degli ambienti IT, le sue interdipendenze con i processi di business e la necessità di identificare e gestire i rischi anche indiretti sono fattori decisivi nella definizione e nell'attuazione di un *IT risk framework*. La valutazione del rischio, il controllo e la mitigazione devono essere allineati con l'approccio globale al rischio operativo che l'azienda ha impostato in relazione agli adempimenti di Basilea II. I principi del rischi operativi definiti nelle "*Sound Practices for the Management and Supervision of Operational Risk*"[6] portano ad un insieme corrispondente di principi guida per la gestione delle informazioni e dei rischi informatici.

Principi guida per l'IT

Per applicare gli "*IT Control Objectives for Basel II*" sono richiesti principi guida per gli specialisti IT e gli esperti di servizi finanziari i cui compiti e responsabilità includono aspetti anche relativi all'*Information Technology*. I seguenti "principi guida per l'IT" (*IT guiding principles* - ITGP) sono stati sviluppati usando un insieme di fonti tra cui:

- *The International Convergence of Capital Measurement and Capital Standards* (*Basel II Capital Accord or Basel II*) pubblicato dal Comitato di Basilea nel giugno 2006[7];
- i principi definiti nelle "*Sound Practices for the Management and Supervision of Operational Risk*" pubblicati dal Comitato di Basilea nel febbraio 2003[8];
- *The Enterprise Risk Management - Integrated Framework*, pubblicato da COSO nel settembre 2004[9].

ITGP1 (consapevolezza del rischio operativo)
La gestione delle informazioni e dell'IT sono parte integrante della gestione del rischio operativo. Professionisti, internal auditor ed esperti di servizi finanziari devono essere consapevoli dell'importanza del "rischio informativo".

Come l'azienda deve essere consapevole dell'influenza dei rischi operativi sull'esposizione globale al rischio e di conseguenza sui requisiti patrimoniali analogamente devono essere definiti e presi in considerazione con attenzione gli aspetti legati all'IT. La consapevolezza e sensibilizzazione su tali temi non deve essere ristretta al fatto che esista un rischio IT. Tutti gli obiettivi connessi al GRC e le relative prassi devono essere allineate con il framework GRC aziendale.

---

[6] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, February 2003
[7] Maggiori informazioni sulla *International Convergence of Capital Measurement and Capital Standards* sono disponibili in www.bis.org/publ/bcbs107.htm; versione in italiano: "Convergenza internazionale della misurazione del capitale e dei coefficienti patrimoniali" in http://www.bis.org/publ/bcbs128ita.pdf
[8] Maggiori informazioni sulle *Sound Practices for the Management and Supervision of Operational Risk* sono disponibili in http://www.bis.org/publ/bcbs96.htm; versione in italiano: "Prassi corrette per la gestione e il controllo del rischio operativo" in http://www.bis.org/publ/bcbs96ita.pdf
[9] Maggiori informazioni sull'*Enterprise Risk Management - Integrated Framework* sono disponibili in http://www.coso.org/-ERM.htm ; una "introduzione" in lingua italiana dell'ERM frawework è disponibile in http://www.coso.org/documents/COSO_ERM_ExecutiveSummary_Italian.pdf

Secondo Basilea II, il rischio operativo è "il 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"[10].
Il rischio legale include, ma non si limita all'esposizione di multe, penali, sanzioni erogate da enti di vigilanza pubblici o di autoregolamentazione. Il rischio operativo esclude esplicitamente "il rischio strategico e reputazionale". La definizione di rischio operativo indicata precedentemente si deve applicare all'*information technology* ed alla gestione delle informazioni così come ai veri rischi legati alla gestione dei sistemi informativi dato che molti rischi di tipo informatico sono relativi ai sistemi informativi e alle relative problematiche nelle categorie del personale (*people*) o processi interni (*internal process*).

Eventi esterni quail incidenti o disastri che impediscono il funzionamento delle infrastrutture critiche possono avere un impatto significativo sull'*Information Technology*. Attenzione simile deve essere dedicata alla gestione dei rischi operativi così come avviene per la gestione degli altri rischi significativi tipici dei "*financial services*" come il rischio di credito, il rischio di interesse (*interest rate*) ed il rischio di liquidità. Tuttavia i rischi operativi differiscono dagli altri rischi tipici dei "*financial services*" dato che essi non sono assunti direttamente quale "ricompensa" di un possibile vantaggio ma esistono *di per sé* come effetto naturale del normale corso degli eventi di un'azienda e ciò ha influenza nel modo in cui occorre gestire tali rischi[11]. Allo stesso tempo sbagliare nel gestire propriamente tali rischi operativi può causare una grave anomalia nel "profilo di rischio" aziendale ed esporre l'organizzazione a perdite significative.
Per l'*information management* e l'area IT nelle aziende di tipo finanziario ciò significa che i rischi operativi nell'IT devono essere gestiti ad un livello che è meno dettagliato rispetto alle altre componenti GRC quali il rischio di credito di di mercato. In ogni caso la componente GRC dell'IT deve essere gestita in maniera adeguata in termini di budget, risorse ed attenzione e supporto del management.

ITGP2 (Requisiti per l'Internal Audit)
La funzione di *internal IT audit* deve essere efficace e completa. Gli skill, le risorse (anche economiche) devono essere adeguate per assicurare l'efficacia delle attività di audit.

In generale l'importanza dell'internal audit si deve riflettere nel *setup* e nel funzionamento dell'internal audit IT o dell'audit operativo e sui rischi informatici. La dimensione e la complessità degli intermediari finanziari sotto analisi deve indirizzare gli interventi in relazione agli skill, le risorse ed i fondi della funzione di internal audit IT. Essa può avvalersi di terze parte specializzate nel caso le risorse interne non possano fornire un adeguato livello di copertura o di efficacia.
L'internal audit IT deve avere l'*accountability* "finale" in relazione al "Comitato Audit" aziendale e deve riportare, nei modi e nei tempi opportuni, al Consiglio di Amministrazione.

Si noti che l'internal audit IT deve essere imparziale ed indipendente in relazione al management aziendale.

ITGP3 (Gestione delle politiche, dei processi e delle procedure)
L'Informatica ed i sistemi informativi devono essere governati per mezzo di politiche, processi e procedure adeguati anche in relazione alla gestione dei rischi.

[10] "Convergenza internazionale della misurazione del capitale", pag 156 , in http://www.bis.org/publ/bcbs128ita.pdf
[11] Il Comitato di Basilea riconosce che, in certe linee di business con rischio di mercato e di credito minimi (ad esempio, *asset management*, pagamenti), la decisione su come gestire il rischio operativo dipende dalle valutazioni del management relative alla "valorizzazione" del rischio e che ciò è parte integrante del processo della banca di *risk/reward calculus.*

Le linee guida fornite ai professionisti, agli internal auditor ed agli esperti dei servizi finanziari devono essere in linea con quanto previsto dal framework GRC dell'azienda.
La gestione del GRC richiede un insieme di politiche, processi e procedure chiaramente definite e documentate che riflettano la struttura organizzativa complessiva e le politiche generali dell'azienda. Le politiche IT devono essere specifiche ad avere obiettivi ed interlocutori chiari per il loro ambito ed i loro contenuti. Questi principi "guida" riguardano i requisiti relativi al processo di *risk management*, che deve essere distinto dai controlli relativi al rischio (si veda ITGP6).
Le discipline dei rischi operativi si riferiscono solo alla gestione dei rischi operativi distinti dalle funzioni dei rischi che sono responsabili per la gestione degli altri tipi di rischi. Questo significa che il lavoro fatto sul rischio operativo dal management che si occupa di rischio di mercato o di credito non diventa una disciplina del rischio di mercato o credito. In modo simile una criticità nelle funzioni che gestiscono il rischio di mercato o credito non diventa una criticità del rischio di mercato o credito.
Questo principio è particolarmente importante per la funzione IT all'interno degli intermediari finanziari. Le componenti IT sono spesso implementate nella gestione, controllo e report del rischio di credito, di mercato e degli altri tipi di *business risk*. Dunque le applicazioni IT e gli elementi infrastrutturali sono anche all'interno del dominio del rischio operativo indipendentemente dal loro scopo specifico. Ad esempio una criticità nell'applicazione per la misurazione del rischio di credito è una criticità IT e di conseguenza una "*systems failure*" nel senso del rischio operativo.

ITGP4 (Risk Assessment)
Nell'ambito dell'informatica e dei sistemi informativi devono essere effettuati specifici *risk assessment* per mezzo di metodologie approvate, condivise e coerenti con il framework GRC dell'azienda. I *risk assessment* devono analizzare sia gli elementi specifici relativi alla complessità delle tecnologie sia i fattori di rischi indiretti.

Per comprendere i rischi IT ed i relativi fattori di rischio, i metodi di risk assessment selezionati devono forire una comprensione approfondita sia dei rischi diretti sia di quelli indiretti. Qualsiasi risk assessment condotto deve coprire sia il rischio intrinseco all'IT sia i rischi indotti dall'uso dell'IT.
Il profilo di rischio dell'azienda che copre i suoi maggiori rischi è un prerequisito per un risk management efficiente ed efficace. Il "*risk profile*" deve fornire un inventario dei maggior rischi dell'azienda ed essere articolato su come le linee di business, il risk management, gli esperti di sicurezza, i piani di continuità e l'internal audit dimostrano la propria *accountability* nella gestione dei rischi che ricadono nelle loro aree di responsabilità e *accountability*. La struttura dell'organizzazione IT deve includere una appropriata segregazione delle funzioni.

ITGP5 (Monitoraggio dei rischi e delle perdite)
Le perdite relative all'informatica ed ai sistemi informativi devono essere misurate e documentate. Gli specifici profili di rischio devono essere monitorati.

Le perdite relative alla tecnologia devono essere monitorate in linea con il più ampio sistema di monitoraggio implementato dall'azienda. I profili di rischio deve riflettere in maniera adeguata la complessità della tecnologia ed il suo uso all'interno delle aziende si servizi finanziari.
L'azienda deve avere una chiara comprensione del proprio *risk appetite*, o di quanto rischio l'azienda intende farsi carico. I rischi o gli eventi che cadono fuori dal *risk appetite* concordato devono essere identificati per l'immediata azione di *remediation*. Le responsabilità sugli incidenti devono essere assegnate in linea con quanto previsto dalla procedura di "gestione incidenti" e le politiche di *escalation*. Queste politiche devono anche definire un processo per la notificazione così

che il *chief executive officer* (CEO), il *chief risk officer*, il *chief information security officer* (CISO), l'internal audit ed i comitati rischi e audit siano consapevoli dei rischi esistenti.
La *compliance* nel sistema regolatorio attuale si sta sempre più orientando anche verso gli aspetti di reporting accurato. Mentre per Basilea II la *data quality* è un mezzo piuttosto che un fine, il *deployment* del capitale basato sui rischi richiede dati di alta qualità ed alta frequenza. Informazioni affidabili sono il cuore di un risk management efficace. Una qualità non adeguata dei dati introduce molto probabilmente errori nelle attività di *decision making* in un ambiente nel quale i *corporate executive* devono attestare l'accuratezza dei propri *financial statement* e la qualità dei controlli interni. Il rapporto "*Observed Range of Practice in Key Elements of Advanced Measurement Approaches* (AMA)"[12] ha identificato i seguenti punti qualificanti nella qualità del dato:

> *La natura e la qualità dei dati relativi al rischio operativo collezionati da AMA bank hanno effetto non solo nei risultati (outcome) del processo di quantificazione della banca ma anche nelle decisioni relative alla gestione dei suoi rischi operativi. Come risultato Basilea II prescrive certi standard che i dati relativi al rischio operativo devono soddisfare prima che la banca sia qualificata per un AMA. Questi standard si riferiscono principalmente alle caratteristiche dei dati, a come essi sono raccolti e a come sono usati. Lo scopo degli standard è fornire delle opinion sulle aspettative minime dei supervisori riguardo alla data integrity ed alla completezza: aspetti entrambi critici per una implementazione efficacia di un AMA.*
> *Il dato per il rischio operativo AMA ha numerose applicazioni comprese la quantificazione del rischio, il risk management ed accounting ed altre forme di reporting. Alcuni dati sono disponibili per più di un applicazione mentre altri dati sono finalizzati ad un solo scopo.*

La *data quality* richiede di instaurare processi, procedure e istruzioni per la gestione delle informazioni e per assicurare la sua integrità, accuratezza, completezza e tempestività. Gli attributi fondamentali che garantiscono la *data quality* sono:

- accuratezza;
- integrità;
- coerenza;
- completezza;
- validità;
- tempestività;
- accessibilità;
- usabilità;
- auditabilità.

La *data quality* fornita dalle diverse applicazioni dipende dalla qualità ed integrità dei dati sui quali le informazioni sono costruite. Entità che trattano dati come un asset aziendale sono in una posizione migliore per gestire i dati in modo proattivo. Entità viceversa che trattano i dati come fossero un problema sono costantemente alla presa con scenari del tipo "ottieni immondizia, fornisci immondizia (*garbage in, garbage out)*".
Il *commitment* alla *data quality* deve essere fornito dal top management, con una chiara linea di *accountability* che deve attraversare tutta l'azienda; il Consiglio di Amministrazione, CEO, CFO,

[12] Pubblicato dall'*Accord Implementation Group's Operational Risk Subgroup* (AIGOR) nell'ottobre 2006, lo studio si focalizza sulle sfide pratiche associate allo sviluppo, implementazione e manutenzione di un framework per il risk management operativo che soddisfi i requisiti di Basilea II in particolare per quanto si riferisce ad AMA.

chief risk officer e CISO devono essere *accountable* per la *data integrity* ed il rispetto dei relativi requisiti di *compliance*.

ITGP6 (Politiche, processi e procedure di controllo e mitigazione)
I sistemi informativi e l'informatica devono essere governati da un insieme di politiche, procedure e processi orientati al controllo ed alla mitigazione del rischio. Le linee guida date ai professionisti, agli internal auditor ed agli esperti di servizi finanziari devono essere in linea con il framework GRC.

Ai fini della mitigazione e del controllo del rischio, devono essere implementati processi, politiche e procedure di complemento e supporto alle politiche di management. Ciò può includere specifici processi per il controllo e la misurazione, la mitigazione delle procedure per specifici rischi ed altre linee guida per fornire una copertura completa dei rischi dei sistemi informativi e dell'informatica. Il *risk control and mitigation* deve essere visto come qualcosa di distinto dal processo generale di risk management (vedi ITGP3).

In un contesto di mercato in cui una persona da sola può minare la reputazione di un'intera istituzione finanziaria tutte le parti dell'azienda devono essere responsabilizzate e assumersi l'impegno e la responsabilità per il rispetto dei requisiti di *compliance* anche in relazione ai rischi. Dato che una azienda è affidabile, conforme alle norme ed "etica", nella misura in cui lo è il suo impiegato più disonesto se l'ambiente di controllo è debole il rischi aumentano in maniera significativa per l'azienda. Il Consiglio di Amministrazione e l'alta direzione devono definire il *tone at the top* dell'azienda per favorire una cultura aziendale che garantisca e favorisca un ambiente di controllo effettivo e ogni persona all'interno dell'azienda deve agire in coerenza con il sistema di controllo interno. Le regole sono inutile senza una cultura della *compliance*.

ITGP7 (*Business Continuity Management*)
I sistemi informativi e l'informatica devono essere protetti per mezzo di un processo di gestione della continuità dei servizi. Il processo di *IT continuity management* deve essere in linea con il framework più ampio di *business continuity management* dell'azienda.

La continuità IT, la gestione degli incidenti e le procedure di *recovery* sono tutte componenti fondamentali per un processo completo di gestione della continuità IT. È essenziale che la gestione dell'IT continuity sia allineata con la *business continuity* aziendale per garantire la continuità dell'IT e dei processi di *core business* in caso di circostanza avverse.
I principi di alto livello della *business continuity* per gli intermediari finanziari sono stati documentati dal Comitato di Basilea[13]. I principi pongono come condizione che una azienda debba progettare e realizzare un processo di *business continuity management* (BCM) affidato alla responsabilità dell'alta direzione sia per realizzazione sia per il monitoraggio. I principi di alto livello includono elementi per un ciclo di vita continuo del BCM, come già indicato in altri standard e pubblicazioni[14]. Per i sistemi informativi e l'informatica così come per i rischi relativi all'IT, l'IT continuity planning, indipendentemente dal metodo e dal framework applicato, deve essere allineato con il più ampio BCM aziendale. Per l'IT continuity, la progettazione, l'implementazione ed il monitoraggio devono essere adeguati ed appropriati, come sottolineato da vari fonti [15]. L'IT è solo una componente delle più ampie capacità di BCM dell'azienda. Si noti che l'IT continuity di livello

[13] Joint Forum, "*High-level Principles for Business Continuity*", 2006
[14] cf. British Standard 25999-1 e the Business Continuity Institute, "*Good Practice Guidelines for Business Continuity Management*", terza edizione, 2007
[15] cf. ITIL (*IT Continuity Management*), ISO 27001 and BS PAS 77

“maturo” richiede un forte supporto da parte del business e l’interazione con gli *owner* dei processi di business dato che l’IT non può esistere da solo o limitarsi ad un continuity plan isolato.

ITGP8 (Framework per il controllo e la mitigazione del rischio)
I sistemi informativi e l’informatica devono essere parte integrante del più ampio framework GRC dell’azienda. Il controllo e la mitigazione dei rischi connessi alle informazioni ed ai sistemi informativi devono essere definiti e riconosciuti nel framework GRC.

I piani e le attività di controllo e mitigazione dei rischi connessi all’IT devono essere progettati, realizzati e monitorati in accordo con il framework GRC. Qualsiasi misura relative alla tecnologia deve essere riconosciuta come un separato e distinto tipo di rischio nel framework GRC. Ciò può includere la gestione organizzativa, i controlli individuali e le linee guida sulla *compliance*. Il controllo e la mitigazione del rischio IT sono spesso definiti come parte del framework ERM, che è, a sua volta, una componente del GRC aziendale. ERM è infatti un tipo di problematica che può avere differenti significati secondo il tipo di interlocutore.

COSO recita che ERM:

- è un processo – è un mezzo per raggiungere uno scopo non un fine esso stesso;
- riguarda e deve essere adottato dalle persone – non si tratta semplicemente di politiche, indagini e questionari; deve coinvolgere le persone ad ogni livello dell’azienda;
- è tenuto in considerazione nel definire la strategia aziendale;
- è applicato in maniera trasversale in tutta l’azienda, in ogni livello ed unità organizzativa, e richiede di adottare una “visione” del portfolio dei rischi a livello di entità organizzativa;
- è progettato per identificare gli eventi che potenzialmente possono avere impatto l’entità aziendale e per gestire il rischio a partire dal suo *risk appetite*;
- fornisce una ragionevole, ma non assoluta, *assurance* al management e Consiglio di Amministrazione;
- è strutturato per permettere il raggiungimento degli obiettivi di una o più entità organizzative sia separate siasovrapposte.

L’assunzione sottointesa di ERM è che ogni entità organizzativa esista per generare valore ai propri *stakeholder*. Tutte le entità hanno a che fare con l’incertezza e la sfida per il management è proprio determinare quanta incertezza accettare così da permettere la crescita del valore degli *stakeholder*. L’incertezza presenta rischi ma offre anche opportunità in quanto potenzialmente può ridurre o incrementare il valore. ERM assiste il management nel gestire in modo efficace l’incertezza ed i relativi rischi ed opportunità e permette di migliorare la capacità di creare valore in azienda.
Il valore è massimizzato quando il management definisce strategie ed obiettivi per ottenere un bilanciamento ottimale tra la crescita, i risultati economici ed i relativi rischi riuscendo contemporaneamente a fare il *deployment* efficace ed efficiente delle risorse seguendo gli obiettivi aziendali.

ERM comprende:

- allineamento del *risk appetite* e della strategia – il management deve considerare la propensione al rischio dell’azienda quando esamina le alternative strategiche, definisce i relativi obiettivi, e sviluppa meccanismi per gestire i relativi rischi;
- miglioramento delle decisioni di risposta al rischio - ERM fornisce una chiara direzione per identificare e selezionare tra differenti risposte ai rischi – evitare il rischio, ridurre il rischio, condividere il rischio, accettare il rischio;

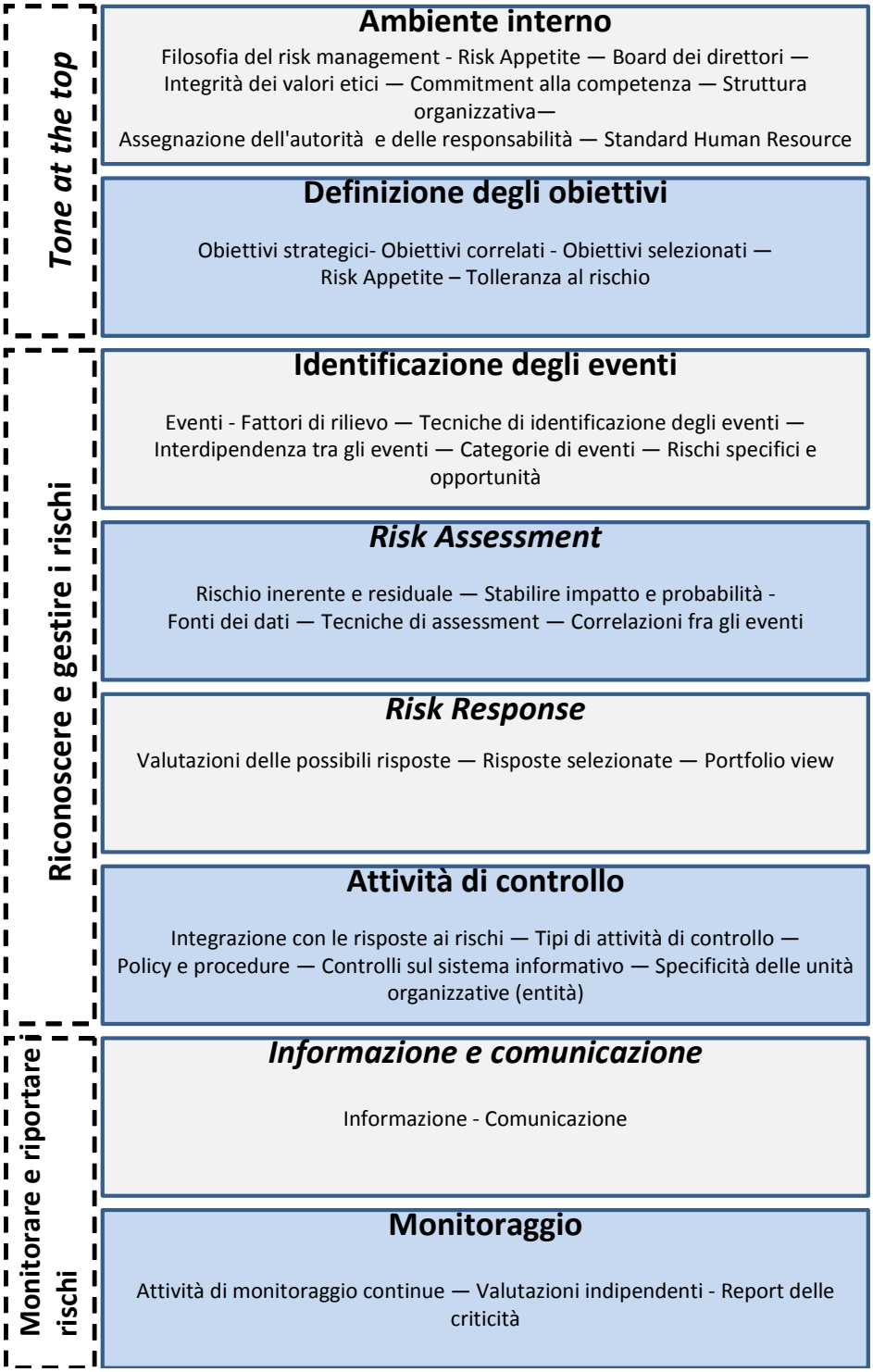
- riduzione delle perdite operative – le aziende devono migliorare la loro capacità di identificare eventi potenzialmente dannosi e la capacità di formulare e mettere in pratica risposte che riducano le "sorprese" ed i relativi costi o perdite;
- identificazione e gestione dei rischi "multipli" trasversali all'intera azienda – ogni azienda deve fronteggiare una grande varietà di rischi che riguardano parti diverse dell'organizzazione; ERM è di aiuto nel predisporre risposte efficaci per gestire gli impatti interconnessi ai rischi "multipli";
- individuazione delle opportunità – considerando il *range* complete degli eventi potenziali, il management è posizionato per identificare e realizzare in modo proattivo le opportunità;
- miglioramento dell'allocazione di capitale – ottenendo delle informazioni sui "rischi informativi" permette al management di valutare in modo efficace il capitale complessivo necessario a migliorare l'allocazione del capitale.

Il COSO ERM framework, illustrato nella **figura 7**, consiste di otto componenti interconnesse, che vanno dall'ambiente interno (*internal environment*) al monitoraggio (*monitoring*) all'interno di tre domini distinti che sono:

- *tone at the top*,
- riconoscere e gestire il rischio,
- monitorare e produrre il reporting del rischio[16].

[16] Ciascuna di queste componenti è descritta in dettaglio nella documentazione di COSO che è disponibile per il download (a pagamento) in www.coso.org/publications.htm.

Figura 7 COSO ERM Framework



ERM propone un approccio olistico alla gestione dei rischi in un'ottica aziendale. È importante notare che il contesto di ERM non si reduce a cercare di ridurre o evitare il rischio ma piuttosto cerca di affrontare il rischio con un approccio informato e bilanciato. Tutti gli otto componenti di controllo devono essere presenti e funzionanti all'interno dell'azienda. Ciò implica l'identificazione dei rischi chiave che hanno un impatto sugli obiettivi aziendali. Questi rischi sono inizialmente valutati in modo "inerente" il che significa valutare i rischi a prescindere dai controlli che esistono già. Il livello residuale dei rischi è successivamente valutato prendendo in considerazione i controlli

che sono in essere per gestire tali rischi. Quando il rischio "residuo" è superiore al *risk appetite*, devono essere implementati controlli aggiuntivi per riportare il rischio all'interno dei valori previsti dal livello di *risk appetite*.
Il raggiungimento degli obiettivi aziendali è considerate come un "risultato" dell'*integrated ERM framework*; gli obiettivi sono categorizzati come:

- strategici – obiettivi di alto livello allineati con la *mission* aziendale e da questa supportata;
- operativi – riguardano l'uso efficace ed efficiente delle risorse;
- reporting – relativi all'affidabilità;
- compliance – relativi a leggi e regolamenti.

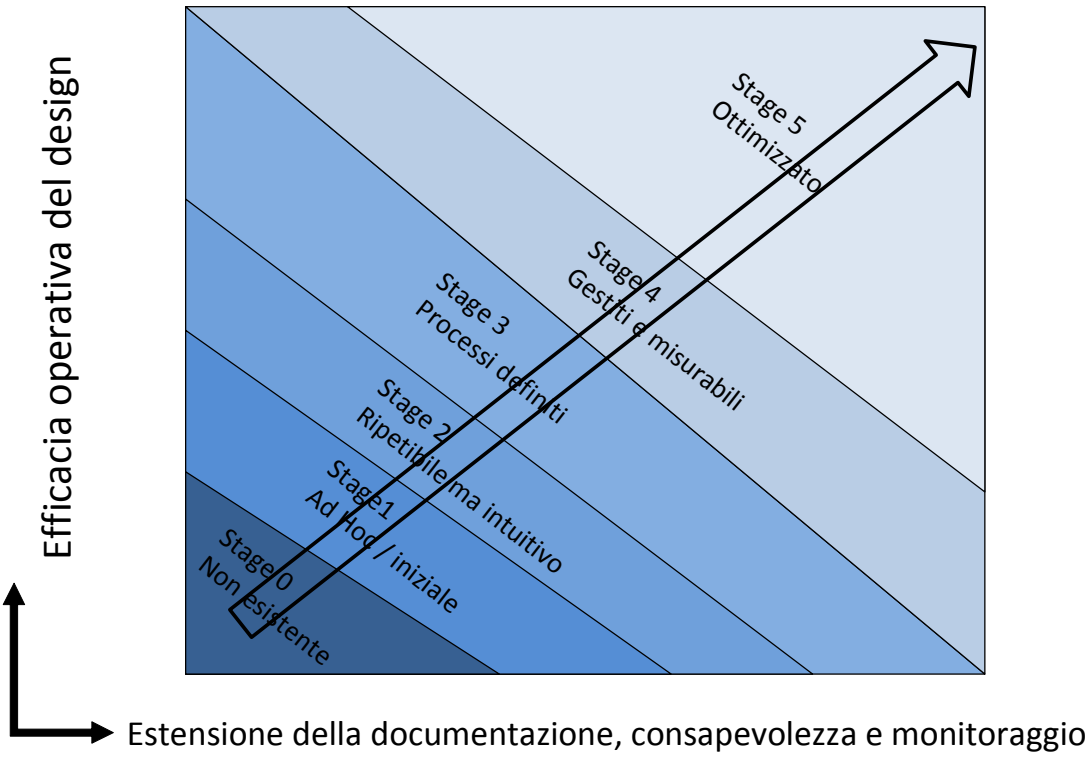
Nei sistemi informativi e nell'informatica le iniziative di *risk management* ed i relativi programmi devono essere integrati con un unico approccio di tipo GRC. Nell'applicare questi principi guida i professionisti possono utilizzare le altre risorse e pubblicazioni di ISACA/ITGI per comprendere ed approfondire i legami tra ERM (coerente con COSO) e l'IT – usando COBIT.

ITGP9 (Valutazione indipendente)
I rischi relativi ai sistemi informativi e all'informatica devono essere adeguatamente documentati per essere di supporto al processo di review delle autorità di supervisione. Una funzione di audit indipendente deve effettuare la review del processo di risk management operativo relative all'IT in linea con quanto previsto dal "profilo di rischio" operativo e dell'IT.

I rischi relativi alle informazioni richiedono documentazione in linea con i requisiti del processo di review dei supervisori per rendere possibile e facilitare tale processo. La documentazione deve essere soggetta ad una review indipendente ed imparziale che comprenda review esterne ad intervalli regolari. Gli audit e le review indipendente della documentazione dei rischi IT devono essere allineati con il profilo di rischio definito dall'azienda. Le aziende devono adottare una valutazione sulla capacità olistica dei loro ERM, dove con "capacità (*capability*)" si intende quanto bene una disciplina o processo lavora e con "maturità" si intende la misura di dove si è giunti con la capacità sviluppata. I processi esaminati entro il contest del *maturity model* devono essere almeno di livello 4, il che richiede loro di essere sia "gestiti" sia "misurabili".

Ciascuna componente del framework ERM è valutata sulla base di sei livelli (*stage*) di affidabilità del controllo come mostrato nella **figura 8**:

Figura 8 – Livelli dell'affidabilità del controllo



0. **Non-esistente -** assenza di qualsiasi processo di risk management. L'azienda non reputa che tale problematica debba essere gestita.
1. **Iniziale/ad hoc** – è evidente che l'azienda ha riconosciuto la necessità di gestire tale problematica. Tuttavia non ci sono processi standardizzati ma un approccio *ad hoc* che di solito è applicato su iniziativa individuale o caso per caso. L'intero approccio alla gestione è disorganizzato.
2. **Ripetibile ma intuitivo** – Sono stati sviluppati dei processi ad un livello dove procedure simili sono eseguite da persone differenti a cui sono affidati gli stessi incarichi. Non esiste un *training* formale o una comunicazione puntuale delle procedure standard e le responsabilità sono lasciate ai singoli individui. Non c'è un elevato livello di fiducia nelle conoscenze degli individui e quindi gli errori sono comuni.
3. **Definito** – Le procedure sono state standardizzate e documentate e comunicate attraverso il *training*. Tuttavia viene lasciato ai singoli individui l'opportunità o meno di seguire tali procedure e non è facile né comune tenere sotto controllo le deviazioni alle regole. Le procedure stesse non sono sofisticate ma sono semplici formalizzazioni delle prassi esistenti.
4. **Gestito e misurabile** – è possibile monitorare e misurare la *compliance* con le procedure ed adottare azioni di risposta quando i processi si rivelano inefficaci. I processi sono sotto costante miglioramento e forniscono una buona prassi. L'automazione e strumenti IT sono usati in modo limitato e a macchia di leopardo.

5. **Ottimizzato** – I processi sono stati raffinati fino al livello di "buona prassi" previsto dagli standard, sulla base dei risultati di un miglioramento continuo e del confronto con i modelli di maturità adottati in altre aziende ed organizzazioni. L'IT è utilizzato in modo integrato per automatizzare il *workflow*, fornire tool per migliorare la qualità e l'efficacia, rendere l'azienda veloce nei cambiamenti. Il *capability maturity framework* dell'ERM aziendale viene valutato e gestito con un approccio sia *bottom-up* sia *top-down*. ERM è un framework integrato; quindi la valutazione sulla *capability maturity* determina i punti di debolezza, quali la *data quality* nel monitoraggio, nella definizione dei ruoli, nei tool e negli skill delle persone, che potrebbero potenzialmente indebolire l'intero ERM framework. Si veda l'appendice IV, "La dipendenza del COSO ERM Framework dalla Data Quality".

ITGP10 [Informativa]
I professionisti, gli internal auditor e gli esperti di servizi finanziari devono identificare tutte le informazioni relative ai rischi che possono essere soggette ad informativa al mercato. Tali informazioni e tali rischi devono essere comunicati agli *stakeholder* come previsto dal framework GRC aziendale. Se necessario devono essere adottate azioni correttive.

Rischi, debolezze e altre criticità identificate in azienda devono essere valutate e misurate dal punto di vista della loro significatività e severità. Quando un rischio individuale o più rischi combinati tra loro possono provocare perdite operative che richiedono una specifica informativa, queste informazioni devono essere comunicate agli appropriati *stakeholder*. Questa *escalation* deve essere chiaramente definita nel GRC framework generale dell'azienda.

Cause di perdita e IT Risk

Il rischio operativo è facilmente individuabile ma tuttavia difficile da definire in modo completo e comprensivo. I fattori di rischio possono essere trovati dovunque nelle "procedure" di una azienda di servizi finanziari. Le perdite potenziali possono nascere da criticità in una o più aree dell'azienda che di solito non sono considerate come centri di profitto o aree che contribuiscono alla creazione di valore.
Il Comitato di Basilea ha definite il rischio operativo come "il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni" [17]. Tale definizione include il rischio legale" ma esclude "il rischio strategico e reputazionale". La definizione sottolinea come tali rischi possano esser interdipendenti.
Come risultato di tutto ciò deve essere preso in considerazione un rischio "sistemico" che interviene in modo trasversale per le aree dell'azienda. Uno dei fattori che contribuiscono al "rischio sistemico" è il fatto gli intermediari finanziari di solito dipendono in modo significativo dall'*information technology* e dai sistemi informativi e che sono richieste infrastrutture tecnologiche complesse per supportare i processi di *core business*.
L'IT è una componente significativa del rischio operativo e di conseguenza è parte fondamentale per il calcolo dei coefficienti patrimoniali relativi a tale rischio.
La definizione di rischio operativo è piuttosto ampia dato che essa deve comprendere un meccanismo efficace per classificare gli eventi.
Le cause comprendono:

[17] Basel Committee on Banking Supervision, "*Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*" giugno 2006, in http://www.bis.org/publ/bcbs128ita.pdf

- processi – eventi di perdita causati dall'esecuzioni di procedure;
- persone – eventi di perdita causati da errori o malfunzionamenti attribuibili al personale;
- sistemi – eventi di perdita o errori nelle procedure informatiche;
- eventi esterni – eventi di perdita causati da eventi che possono minacciare la capacità dell'azienda di continuare ad eseguire le proprie procedure.

L'orientamento strettamente "causale" della definizione è importante nel contesto di Basilea II dato che due delle principali categorie – rischio di credito e di mercato - hanno chiare e distinguibili cause: il rischio di credito essendo "garantito" e la posizione di mercato in relazione ai *competitor* esistenti. Sebbene le banche possano adottare la propria definizione di rischi operativi, la definizione deve considerare il "*range* pieno" dei rischi operativi che la banca deve fronteggiare e deve prendere in considerazione le cause più significative di perdite operative potenzialmente significative.
Tipi di classificazione delle cause possono essere usati come punto di partenza per la gestione del rischio operativo, specialmente per quel che riguarda la mitigazione, il trasferimento o evitare il rischio. Per fornire maggiore chiarezza e differenziazione che è utile nella gestione del rischio IT, i quattro maggior tipi di causa devono essere scomposti in tre livelli di categorie di causa. Questo è particolarmente importante dato che, in pratica, i rischi sono spesso attribuiti a più di una causa e contemporaneamente devono essere allocati ad un solo tipo di classificazione.

Di seguito sono forniti alcuni brevi esempi per aiutare a chiarire i concetti.

Esempio 1
Un *insider* che sfrutta un errore nei programmi informatici in una applicazione web deve essere classificato nella categoria "sistemi" mentre un *intruder* che ottiene un accesso non autorizzato ai computer della banca usando strumenti di *hacking*, *phishing* o *malware* deve essere classificato come "evento esterno".

Esempio 2
Un incendio scoppia nel *data center* e distrugge i sistemi IT con la conseguenza che l'IT non è più capace di garantire le attività di business. Prendendo in considerazione le categorie di Basilea II sulle cause e gli eventi di perdita ciò potrebbe essere classificato come "evento esterno" e la categoria potrebbe essere "danno ad asset fisico/disastro".

Analizzando la catena delle cause gli elementi principali di questo rischio potrebbero essere:
- evento esterno (fuoco);
- disastro (fuoco nel *data center*);
- danno ad asset fisici (sistemi IT distrutti);
- distruzione del business (processo di business non disponibile).

Appare chiaro che questo rischio, di per sé relativamente semplice, si collega a due "tipi di eventi di perdita" (*loss event type*) di Basilea II: danno ad asset fisici, distruzione del business e indisponibilità dei sistemi informativi.

La distruzione del business, di per sé, è attribuibile alla causa "sistemi", se questo *loss event type* della catena di cause è gestito. Se l'incendio è stato causato da un elettricista che ha inavvertitamente cortocircuitato due cavi dell'alta tensione, deve essere aggiunta una terza causa: "persone".
Se qualche componente dello staff IT rilascia in produzione una nuova *release* senza aver effettuato prima i test necessari e senza fare il *back-up* dei dati e delle routine incluse nella nuova *release*,

deve essere aggiunta una quarta categoria: "processi per il rilascio in produzione del nuovo software" o, più in generale "*change management*". Questo esempio mette in evidenza le difficoltà che si possono incontrare nell'identificare e pesare gli *event type* ai quali attribuire la "catena dei rischi" e le perdite che ne possono derivare. Appare chiaro dall'esempio che la definizione "*cause-oriented*" del rischio operativo deve essere applicata anche ai rischi correlati all'IT e alle informazioni. Gli intermediari finanziari che implementano questa identificazione del rischio e metodo di categorizzazione devono identificare un ulteriore livello II di categorie di rischio usando le risorse ed i processi COBIT e devono, di conseguenza, identificare e indicare le priorità del livello III dei rischi che ne risultano da loro risk assessment individuale qualitativo e quantitativo.

Il Comitato di Basilea ha identificato gli *event type* del rischio operativo che possono tradursi potenzialmente in perdite sostanziali:

- frode interna;
- frode esterna;
- prassi degli impiegati e sicurezza sul posto di lavoro (*employment practices and workplace safety*);
- clienti, prodotti e prassi di business (*clients, products and business practices*);
- danni ad asset fisici (*damage to physical assets*);
- distruzione del business e malfunzionamenti dei sistemi informativi (*business disruption and system failures*);
- esecuzione, erogazione e gestione dei processi (*execution, delivery and process management*).

Il Comitato ha fornito una definizione per ciascun *loss event type* con subcategorie ed esempi di attività.

Considerando le cause e i *loss event type*, ne consegue che molti rischi operativi sono connessi all'IT sia come problematiche dirette di tipo informatico (ad esempio un incendio che distrugge il *data center*) sia come problematiche IT indirette (ad esempio controlli sui processi di business , il cosiddetto principio dei "quattro occhi" [18]) che non funzionano correttamente a causa di errori di programmazione nelle applicazioni informatiche delle aziende di servizi finanziari. Per l'IT risk management, le cause e gli *event type* di perdita di Basilea II devono essere ulteriormente dettagliati. Per il risk management operativo, nel senso dell'identificazione, misurazione e monitoraggio/controllo del rischio operativo, le cause e gli *event type* di perdita di Basilea II potrebbero non essere sufficientemente esaustivi e completi. Le cause multiple e gli eventi che ne risultano formano un network di interdipendenze che potrebbero non essere completamente descritti. Come risultato, gli scenari di rischio possono essere usati per fornire esempi delle catene causali e dei relativi effetti. Questi scenari sono strumenti utili per illustrare i tipi più comuni di IT risk e le loro conseguenze per l'azienda.

Analisi di scenario per gli IT Risk

Basilea II richiede alle aziende di servizi finanziari che utilizzano l'approccio AMA di usare l'analisi di scenario e l'opinione di esperti insieme a dati esterni per valutare la propria esposizione ad eventi di alta criticità e di bassa frequenza. L'approccio all'analisi di scenario deve essere

[18] Il principio dei "quattro occhi" (*the four-eye principle*) significa che tutte le decisioni di business e le transazioni devono essere approvate sia dal CEO sia dal CFO.

effettuata congiuntamente dai business manager e dagli esperti di risk management per valutare le perdite significative plausibili.

In sintesi per un approccio operativo e di information risk management, gli esperti IT, gli specialisti di information security, i business manager, gli esperti di risk management e gli specialisti IT delle funzioni di internal audit e IT compliance devono valutare insieme gli scenari IT ove vi sia la probabilità ragionevole del verificarsi di perdite inattese significative.

Gli scenari IT illustrati nella **figura 9** sono dei semplici esempi classificati in A e B in termini di importanza. Queste categorie mostrano l'importanza relativa di certi scenari IT nell'*industry* dei servizi finanziari.
Nello sviluppare le analisi di scenario devono essere considerate, la frequenza e la "significatività" dei fattori di rischio (*risk driver*); l'obiettivo di questa analisi è di ottenere un assessment ragionevole sulla base delle valutazioni degli esperti per procedere poi a distribuzioni statistiche sulle perdite. Negli *assessment* degli esperti, le stime e le previsioni basate su esperienze passate e sui benchmark di mercato possono essere sostituite se i dati sulle perdite operative non sono disponibili.

Figura 9 – Scenari IT

Esempio di scenario IT	***Definizione dello scenario***	***Categoria***
Svolgimento di attività non autorizzate da parte di utenti autorizzati	Gli utilizzatori hanno accesso e usano in modo non corretto funzioni quali l'aggiornamento dei dati, del software e delle caratteristiche dei sistemi o la modifica di dati, dei privilegi degli utenti o dei dati di input	A
Distruzione del servizio	C'è un "problema significativo" relativo all'hardware o al software o ai servii critici o ai sistemi di controllo ambientale o una perdita di dati o un "denial of service" o un errore significativo nel dimensionamento dei sistemi	A
Processing incompleto della transazione	Gli errori o le transazioni non complete non sono individuati e producono risultati errati	A
Uso non autorizzato di asset critici	Coloro che hanno credenziali di accesso "potenti" abusano dei loro privilegi	A
Fallimento di progetto	I risultati dei progetti non sono distribuiti nei tempi previsti in rispetto dei budget e con la qualità richiesta	A
Fallimento di prodotto	Ci son problemi nell'identificazione ei requisiti di sicurezza o nel progettare la sicurezza nei prodotti e nei servizi erogati	B
Rischi legati alle terze parti	I rischi relativi alla affidabilità dei servizi delle terze parti non sono ben definiti o non sono gestiti in modo corretto	B
Furto di asset critici	Ci sono stati furti di componenti hardware e software, di device, di output dei sistemi, di dati degli archivi, di computer portatili	B
Attività pericolose	Ci sono stati episodi di hacking, phishing, social engineering od "estorsione" cibernetica	B
Fallimento nel processo	Non c'è integrità e sicurezza nei processi critici o sensibili	B

La **figura 10** illustra i *risk driver* per gli scenari IT categorizzati come A.
L'analisi di scenario richiede che sia presa in esame una correlazione di scenari multipli; questo è essenziale per identificare e valutare le perdite potenziali che potrebbero nascere da eventi di perdite operative multiple e simultanee causati da uno o più rischi. Gli scenari devono considerare i dati delle perdite interne per la valutazione della significatività relativa dei rischi connessi all'informatica ed ai sistemi informativi ed ai dati sulle perdite esterne (se disponibili) e verificati in modo ragionevole mediante il confronto sul mercato e con altri dati storici. Le analisi di scenario ed il risk assessment che si basano sull'opinione di esperti devono essere validati frequentemente e soggetti a nuovi assessment comparandoli con i dati di perdita disponibili al momento. Ciò è un aiuto essenziale per assicurare la "ragionevolezza" dei metodi qualitativi applicati al risk management.

Figura 10 – Esempi di *risk driver* per gli scenari IT di categoria A

Scenario IT	Risk Driver per la frequenza	Risk Driver per la criticità
Svolgimento di attività non autorizzate da parte di utenti autorizzati	• Utenti con accesso a funzioni applicative critiche • Perdita di controllo dei supervisori • definizione non corretta dei permessi di accesso • Uso eccessivo degli accessi e dell'uso delle prerogative di supervisione • accesso non corretto al software e ai sistemi	• monitoraggio inadeguato delle eccezioni dei sistemi • mancanza di gestione di controllo • mancanza di audit review • politiche di sicurezza non appropriate • mancanza di appropriata formazione sulla sicurezza • mancata accountability • gestione degli accessi non adeguata
Distruzione del servizio	• numero di incidenti significativi che possono portare alla distruzione del servizio • suscettibilità dell'hardware e software ai danni • incapacità nell'identificare le interdipendenze tra sistemi ed applicazioni	• incapacità di identificare in modo corretto le condizioni che possono portare alla distruzione del servizio • incapacità di monitorare gli eventi che possono produrre distruzione del servizio • incapacità di sviluppare un piano per intercettare gli incidenti e attivar e le relative procedure di gestione
Processing della transazione incompleto	• errori di processo che potenzialmente non vengono intercettati	• danni potenziali che possono risultare da transazioni incomplete
Uso non corretto di asset critici	• numero di credenziali	• mancanza di tool di

	condivise • numero di utilizzatori che accedono ad informazioni critiche o sensibili • poca comprensione delle politiche, procedure e standard di sicurezza • problemi nel creare consapevolezza alla sicurezza • mancato monitoraggio da parte dei supervisori • problemi nel considerare la sicurezza quando si definiscono le procedure di business ed i relativi processi	monitoraggio o uso non corretto di tali tool • mancanza di capacità di gestire gli incidenti di sicurezza
Fallimento di progetti	• numero di progetti • qualità dei programma definiti e approccio al project management	• valore del budget dei progetti • numero dei progetti critici

7. Processi di business per gli IT Risk ed i controlli IT: applicare il CobiT framework

Il Comitato di Basilea raccomanda un approccio a livello di *business line* alla misurazione e gestione dei rischi operativi. Nell'approccio standardizzato il reddito lordo di una *business line* è considerato un buon indicatore per valutare l'importanza delle procedure di business e, quindi, come parametro dell'esposizione al rischio operativo di ciascuna *business line*.

Uso della documentazione esistente

In molte aziende di servizi finanziari esiste già una documentazione che descrive i processi di business. Questa documentazione può comprendere, ad esempio:

- politiche e procedure (specialmente quando richiesto dai *regulator* e gestito, anche nell'aggiornamento, dalla funzione di *compliance*);
- la documentazione relative al *Business Process Reengineering*;
- la documentazione relativa alla *compliance* sul "*financial reporting*" (ad esempio in relazione al *Sarbanes-Oxley Act*).

Questa documentazione può spesso essere usata come base per cominciare un'analisi sui rischi operativi. Per esempio può essere già disponibile la documentazione relativa alla compliance sul *Sarbanes-Oxley* o in generale sul *financial reporting* anche se in questo caso il focus è sull'identificazione dei controlli chiave sugli obblighi del *financial reporting*. In un processo di *trading* il controllo chiave è di solito il processo di accoppiamento (*matching*) e riconciliazione nel *back office*; è poco probabile che si faccia affidamento sui controlli nei sistemi di *front-end*.
Per il rischio operativo i sistemi di *front-end* sono invece molto importanti. I fidi ai clienti, le strategie di *trading* (in modo particolare nell'*assessment* della predisposizione al rischio, *risk appetite*, nel determinare una strategia di *trading*), la sicurezza ed i controlli sul *program change* diventano tutti fattori importanti quando si fa l'assessment dei rischi operativi.

L'approccio "business line" in Basilea II

Un intermediario finanziario deve essere capace di gestire i rischi oltre che in una prospettiva "*business line*" anche in modo centralizzato per le attività che di estendono tra più linee di business ad esempio per quanto riguarda le attività del dipartimento IT. A tale fine il Comitato di Basilea richiede che tutte le attività della banca siano ricondotte ad una delle seguenti otto *business line*:

1. Corporate finance
2. Trading and sales
3. Retail banking
4. Commercial banking
5. Payment and settlement
6. Agency services
7. Asset management
8. Retail brokerage

Molte *business line* non sono in grado di operare senza il supporto dell'IT. Il livello di supporto richiesto, naturalmente, dipende dalla natura del business. Il "*retail brokerage*" come funzione di *electronic banking* per il *retail* dei client ovviamente richiede sistemi IT complessi che devono essere sempre disponibili. Dall'altro lato il "*corporate finance*" ha requisiti molto differenti come ad esempio la capacità di sviluppare rapidamente modelli e scenari basati sul software per produrre innovazione e transazioni individuali. L'esposizione al rischio operativo deve essere stabilita identificando e valutando il rischio operativo inerente in tutti i prodotti materiali, le attività, i processi ed i sistemi. Inoltre per identificare i rischi potenzialmente più critici le banche devono valutare la loro vulnerabilità rispetto a tali rischi. La base di questo *assessment* può essere un'analisi dettagliata e sistematica dei processi all'interno di ciascuna linea di business. Di solito i processi produttivi sono un buon punto di partenza dato che tali processi, dove un prodotto o un servizio è offerto ai clienti esterni, sono fonte di entrate e guadagni. Nel "*retail brokerage*" una azienda di servizi finanziari offre servizi (ad esempio acquisiti, comproprietà, scambio) ai clienti *retail*. Per usare questi servizi i clienti devono inserire i loro ordini in un'applicazione Internet. Dopo l'autenticazione dell'ordine, quest'ultimo viene processato dalla banca e depositato per mezzo dello "scambio" (*exchange*), il deposito è inviato ai cliente, aggiungendo le *share* al loro *portfolio* e addebitando il costo nei loro conti. Prima di effettuare il processo dell'ordine, l'identità dei clienti è verificata mediante autenticazione ed i loro profili sono verificati per assicurare che essi abbiano le autorizzazioni per iniziare quel tipo specifico di transazione. Il processo completo può essere fornito attraverso sistemi IT multipli, sia interni che esterni all'azienda di servizi finanziari, fornendo non solo le componenti per l'applicazione *core*, ma anche l'alimentazione dei prezzi (*pricing feeds*) ed il deposito del cambio (*exchange settlement*).
Un modo per valutare l'esposizione inerente dei rischi in tali processi è di applicare loro degli scenari. Certi scenari, come il furto d'identità nel *retail brokerage*, possono essere valutati molto accuratamente, conoscendo i dettagli del processo sottostante. Altri scenari che sono più specifici dell'ambito dei servizi finanziari sono più difficili da valutare con un ragionevole grado di plausibilità.
Con l'uso di un numero significativo di scenari di rischi operativi i controlli dei processi di business impediscono ai tipici *risk driver* di diventare troppo frequenti o troppo critici. Quando si valutano i possibili impatti di scenario, questi controlli devono essere considerati come ulteriori fattori da valutare insieme ai dati relativi alle perdite interne ed esterne,.

Definire i rischi IT

Quando si progettano e descrivono gli scenari per la valutazione del rischio l'uso di COBIT può essere d'aiuto nel definire un ambiente di controllo standardizzato per lo scenario sotto analisi utilizzando i controlli previsti. La **figura 11** mostra gi obiettivi di controllo corrispondenti alla categoria A degli scenari IT.

Figura 11 – Mappatura di esempio degli scenari IT in relazione ai processi COBIT	
Svolgimento di attività non autorizzate da parte di utenti autorizzati	DS5 Assicurare la sicurezza dei sistemi.
Distruzione del servizio	DS4 Assicurare la continuità del servizio.
Processing della transazione incompleto	AC4 Integrità e validità del processing.
Uso non corretto di asset critici	DS5 Assicurare la sicurezza dei sistemi.
Fallimento di progetti	PO10 Gestione dei progetti.

Ad alto livello, il *risk assessment* deve considerare se l'azienda ha implementato un ambiente di controllo adeguato che consiste di controlli a livello di entità e e processi. I controlli a livello di entità di solito comprendono i seguenti elementi COSO:

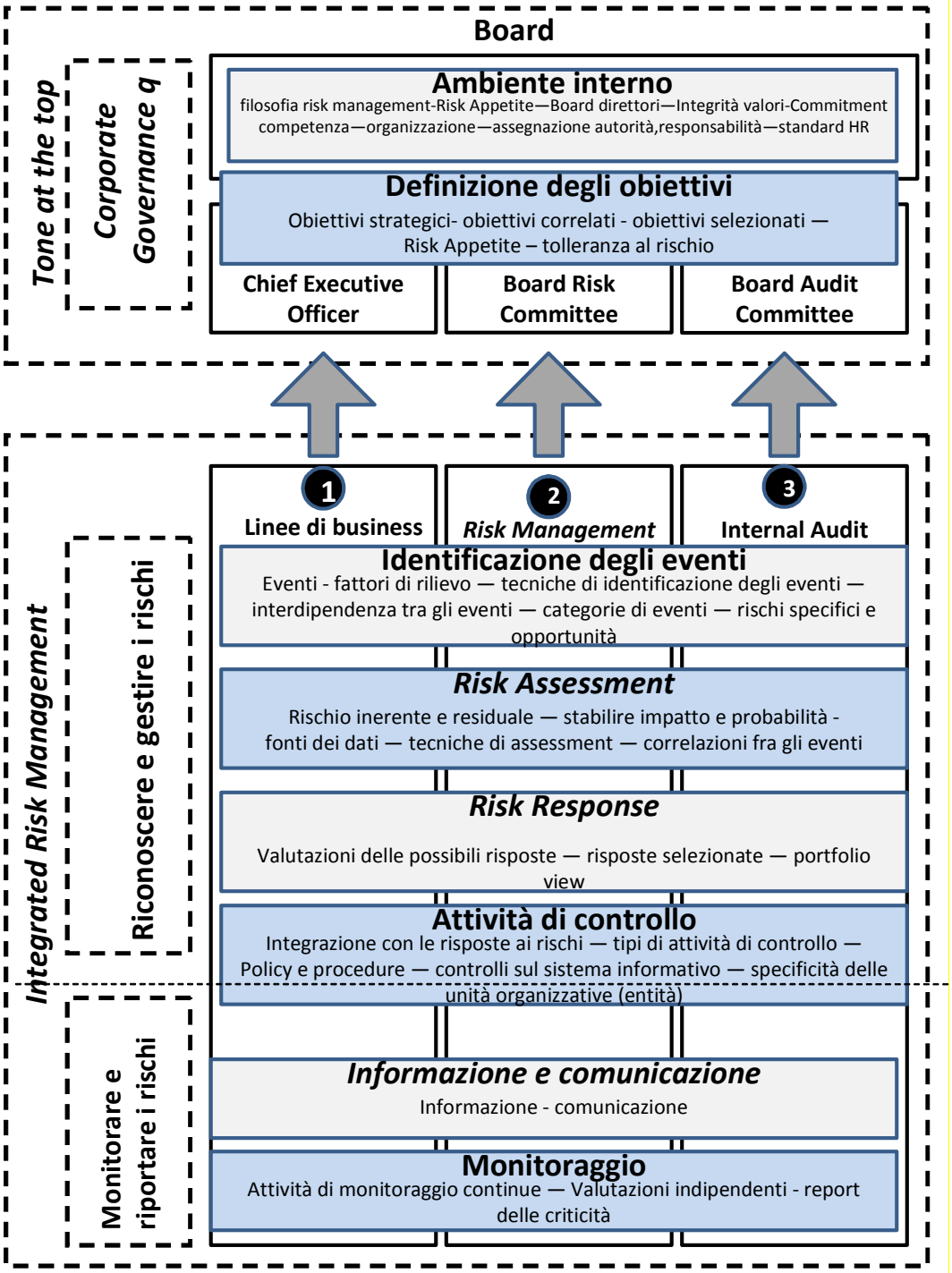
- ambiente di controllo (*control environment*)
- *risk assessment*
- informazione e comunicazione (*information and communication*)
- monitoraggio (*monitoring*), in parte.

Parte dei controlli a livello di entità possono includere il concetto della "difesa a strati" (*multiple layers of defense*) e delle relative responsabilità. Un certo numero di aziende ha nominato i risk manager, ma esiste una considerevole differenziazione nel livello di esperienza, *seniority* e status di queste persone. In alcune organizzazioni, il risk manager ha uno status di *senior* e la possibilità di prendere decisioni e garantire un assessment approfondito (cioè ad esempio verificare le condizioni dei contratti). In altri casi il ruolo è limitato all'effettuazione di un *risk assessment* di base senza la possibilità di prendere decisioni effettive , cosa che è – viceversa un requisito essenziale della funzione di gestione del rischio.
Per organizzare i rispettivi ruoli di *compliance*, internal audit e risk management, alcune aziende si sono strutturate con un modello di difesa[19] a tre strati (vedi **figura 12**) dove il *risk management* garantisce una seconda linea indipendente mentre l'audit fornisce l'*assurance* che le prime due linee operano come previsto.

In conclusione nel contesto di una supervisione regolatoria che si indirizza verso un approccio *risk-based* e guidato dai principi, la *regulatory compliance* è diventato l'interlocutore privilegiato dell'*integrated* ERM framework aziendale. Una governance efficace trasversale a tutte le discipline del *management* (incluso il rischio di credito, il rischio di *interest rate*, il rischio di liquidità ed il rischio operativo) dipende fortemente dalla "maturità" (*capability maturity*) delle tre linee previste dal modello di difesa illustrato nella **figura 12**, modello che si basa sul COSO ERM framework.

[19] Le tre linee del "modello di difesa" sono state adottate da un gran numero di intermediari finanziari [ci s riferisce al modello indicato nel 2006 *Annual Financial Report of the National Australia Bank* (*Risk Management: Introduction* – pagina 15)].

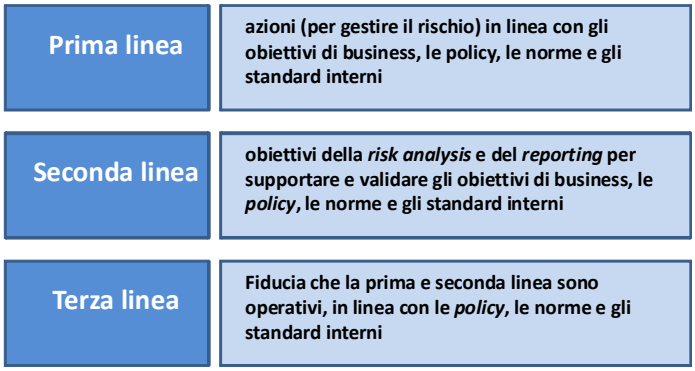
Figura 12 - Linee di difesa: ERM Framework



Il controllo deve essere esercitato attraverso linee di difesa chiare, definite ed indipendenti – la linea di business, il risk management e l'internal audit – linee che giocano tutte una funzione importante nell'*integrated* ERM, come mostrato nella **figura 13**. Il modello basato su tre linee di difesa distingue tra funzioni che sono sia *owner* sia gestore dei rischi, funzioni che supervisionano i rischi e funzioni che forniscono una *assurance* indipendente.

- Il Consiglio di Amministrazione definisce il *risk appetite*, approva la strategia per la gestione del rischio ed è il responsabile ultimo per il sistema di controllo interno dell'azienda[20]. Il CEO, supportato dal senior management, ha la responsabilità generale per la gestione dei rischi che riguardano l'intera azienda.
- Il management e lo staff di ogni linea di business hanno la responsabilità "primaria" di gestire il rischio. A loro è richiesto di assumersi le responsabilità per l'identificazione, l'assessment, la gestione, il monitoraggio ed il *reporting* dei rischi aziendali che nascono all'interno dei rispettivi business.
- Il *chief risk officer*, supportato dalle funzioni che gestiscono il rischio all'interno dell'azienda, ha la responsabilità generale per la seconda linea di difesa. Il *chief risk officer* è *accountable* rispetto al comitato aziendale rischi ed, in ultima istanza, rispetto al Consiglio di Amministrazione. La gestione quotidiana dei rischi non è l'*accountability* del *chief risk officer*; ma resta compito della prima linea di difesa. Di solito la funzione che gestisce il rischio:
    - raccomanda le politiche sul rischio al Cda per la sua approvazione, fornisce gli obiettivi di "supervision" e coordina le attività di ERM con l'ausilio di altri specialisti e delle relative funzioni connesse al rischio
    - fornisce un supporto generale e specialistico e fornisce consulenza e consigli ai componenti della gestione operativa nell'identificazione, assessment, gestione, monitoraggio e reporting dei rischi.
- La terza linea di difesa - internal audit – fornisce una *assurance* indipendente sull'efficacia della gestione dei rischi aziendali attraverso tutta l'azienda. La funzione di internal audit è *accountable* nei confronti del comitato di audit committee ed, uin ultim analisi, nei confronti del Cda.

Figura 13 – Il concetto delle tre linee

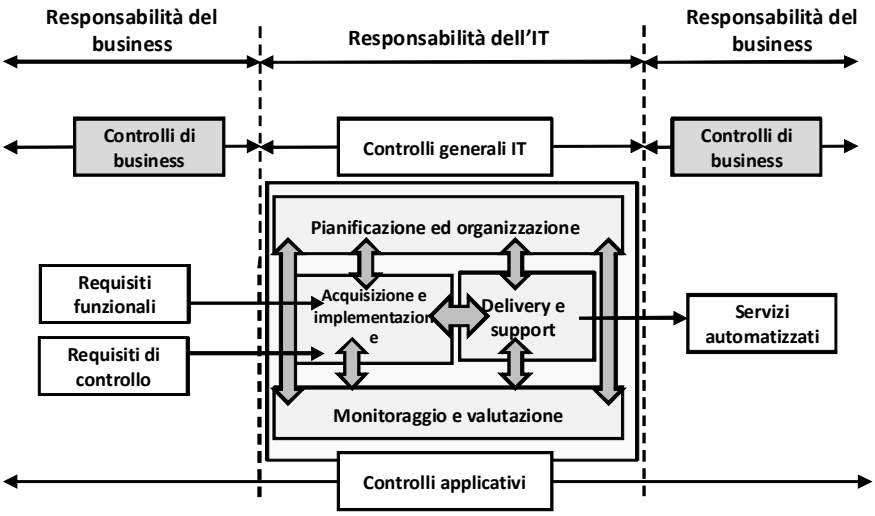


[20] "Il Consiglio di Amministrazione deve avere la responsabilità dell'approvazione e della *review* periodica delle strategie di business e delle politiche più significative della banca; la comprensione dei rischi maggiori che riguardano la banca, la definizione dei livelli accettabili di tali rischi e di assicurarsi che l'alta direzione effettui i passi necessari per identificare, misurare, monitorare e controllare questi rischi; di approvare la struttura organizzativa della banca e di assicurare che l'alta direzione tenga sotto controllo l'efficacia del sistema di controllo interno. Il Consiglio di Amministrazione è il responsabile ultimo della garanzia che sia stato stabilito mantenuto un adeguato ed efficace sistema di controlli interni" Fonte: *Basel Committee on Banking Supervision, Principle 1, Framework for Internal Control Systems in Banking Organisations*.

Definire i controlli IT

Dato che i rischi hanno bisogno di essere definiti e valutati dal punto di vista dell'azienda attraverso considerazioni a livello di processi più dettagliati, l'implementazione dei controlli deve essere effettuata da una prospettiva più generale (a livello di unità organizzativa o entità) verso controlli di processo più specifici e dettagliati. La **figura 14** presenta questa relazione nel contesto di un processo di business condiviso tra business ed IT.

Figura 14 – Confini (limiti) tra controlli di business, generali ed applicativi



Controlli a livello di entità

L'uso di COBIT fornisce alle istituzioni finanziarie un *set* completo di obiettivi di controllo con un focus strategico per i controlli a livello di entità. Questi devono essere visti nel proprio contesto dato che l'ambiente dell'azienda e le sue priorità di business determinano la visione strategica sul GRC. Il *senior management* può optare fra vari modelli per assicurare una buona *corporate governance* ed il COBIT framework deve essere applicato in base a ciò. Mentre le domande di esempio possono essere utili per comunicare una comprensione generale di alto livello dei controlli a livello di entità è tuttavia responsabilità dei manager e dei specialisti dei rischi operativi ed informativi di determinare lo *scope* e l'estensione degli obiettivi di controllo che sono richiesti per ottenere una ragionevole *assurance* sui controlli a livello di entità.

Controlli generali IT

Gli obiettivi di controllo specifici per gli *event type* di rischio specifici di Basilea II sono presentati nell'**appendice V**, "Basilea II e COBIT". I controlli generali IT di solito gestiscono obiettivi di controllo di sintesi che sono "abilitatori" per i controlli a livello di processo ed applicazione. Per i controlli generali IT COBIT ha definite un *set* di oltre 200 obiettivi di controllo che sono o specifici per le applicazioni o applicabili trasversalmente attraverso l'intera azienda. Un controllo generale IT (per esempio l'*access control framework* per le applicazioni) definisce la scena per controlli più

dettagliati nel *business workflow*. I controlli chiave nel *workflow* devono aderire ai set di principi e legami per mezzo del governo dei controlli generali IT. Le restrizioni agli accessi individuali nelle transazioni applicative creando o modificando i dati devono, quindi, seguire la direzione data in un *access control framework*.
I controlli chiave implementati come risultato di un controllo generale supporterà l'efficacia del controllo generale. In uno scenario di *access control* il fatto che un controllo chiave sia stato inserito nel *workflow* conferma che l'*access control framework* (il controllo generale) è stato coerentemente applicato. Viceversa, se un *access control framework* non è stato completamente implementato, esisteranno dei *gap* nel controllo accesso visibili a livello di *workflow*.

Controlli a livello di processo

I controlli a livello di processo sono spesso equivalenti ai controlli applicativi. I processi di business nelle banche sono spesso così strettamente integrati con le applicazioni IT che i controlli del processo di business sono forniti all'interno delle applicazioni IT che supportano quel processo. Per esempio all'interno del *retail brokerage* il rischio di fare vendite errate può essere ridotto dai controlli delle applicazioni IT che forniscono controlli di plausibilità rispetto ai dati inseriti nell'applicazione IT.
Le applicazioni IT stesse sono governate dagli *IT general control*, che assicurano che le applicazioni IT sono sviluppate ed operano in accordo alle specifiche di business e che gli utilizzatori hanno permessi di accesso definiti dalle regole di business.
In aggiunta se gli intermediari finanziari sono interessati, gli obiettivi di controllo di COBIT possono esser eusati per definire i controlli generali richiesti, i controlli applicativi e valutare la maturità dei controlli implementati. Per i controlli applicativi, COBIT ha definito un set di sei obiettivi di controllo raccomandati per le applicazioni. Essi sono identificati per mezzo dell'*application control number* (AC):

- AC1 Preparazione ed autorizzazione delle fonti dei dati (*Source Data Preparation and Authorization*) – Assicura che i documenti fonti siano preparati dal personale autorizzato e qualificato seguendo le procedure previste, garantendo nei conti *account* un'adeguata separazione dei compiti in relazione all'origine e all'approvazione dei documenti. Errori ed omissioni possono essere minimizzati attraverso una buona progettazione dei form di input. Intercetta errori ed irregolarità così che questi possano essere raccolti e corretti.
- AC2 Raccolta e inserimento dei dati sorgenti (*Source Data Collection and Entry*) – Stabiisce che i dati di input sono sviluppati in modo tempestivo dal personale autorizzato e qualificato. La correzione ed il reinserimento dei dati che erano stati erroneamente inseriti deve essere effettuata senza compromettere i livelli autorizzativi della transazione originaria. Quando è appropriato per la ricostruzione, i documenti di origine sono conservati per l'appropriata quantità di tempo.
- AC3 Controlli di accuratezza, completezza ed autenticità (*Accuracy, Completeness and Authenticity Checks*) – Assicura che le transazioni siano accurate, complete e valide. La validazione dei dati che sono stati inseriti ed editati o rimandati indietro per la correzione è quanto più vicina possibile al punto di origine.
- AC4 Processo di integrità e validazione (*Processing Integrity and Validity*) – Mantiene l'integrità e la validità dei dati attraverso il ciclo di *processing*. L'intercettazione di transazioni errate non interrompe il processo delle transazioni valide.
- AC5 Rivisitazione dell'output, riconciliazione e gestione degli errori (*Output Review, Reconciliation and Error Handling*) – Stabilisce procedure e le responsabilità associate per assicurare che l'output è gestito in un modo autorizzato, rilasciato al corretto destinatario, e

protetto durante la trasmissione; tale verifica, intercettazione e correzione dell'accuratezza dell'output è effettiva; e che l'informazione fornita in output è effettivamente usata.

- AC6 Autenticità ed integrità della transazione (*Transaction Authentication and Integrity*) Prima di passare I dati della transazione tra le applicazioni interne e le funzioni operative e di business (dentro o fuori dell'azienda), controlla i dati per indirizzare in modo appropriato l'autenticità dell'origine e l'integrità del contenuto. Mantiene l'autenticità e l'integrità durante la trasmissione ed il trasporto.

8. Uso dei "Key IT Risk Indicator"

Gli indicatori di rischio (*risk indicators*) sono parametri che tengono traccia dell'esposizione al rischio operativo e dei cambiamenti nel "profilo di rischio" operativo. Quindi i *risk indicator* sono una sorta di sistema di primo allarme (*early warning*) per il "profilo di rischio" operativo. Essi permettono al management di documentare ed analizzare i trend, fornendo una prospettiva che "guarda in avanti" e segnalando le azioni richieste prima che il rischio diventi effettivamente una perdita. Inoltre i *risk indicator* aiutano a definire il "*risk appetite*" per mezzo della definizione di soglie. In ogni caso i *key risk indicator* (KRI) devono essere parte del processo di misurazione e di monitoraggio e non solo un segnale su dove è richiesto l'intervento del management.
I KRI si riferiscono ad indicatori che tracciano i rischi in modo particolarmente efficace o che tracciano rischi molto importanti. I KRI sono usati per gestire i rischi operativi e giocano un ruolo importante nel reporting del risk management operativo.
L'uso dei KRI può consistere nell'identificazione delle perdite operative potenziali causate da debolezze (*weaknesses*) e criticità (*deficiencies*) relative all'IT. Alcune di queste possono essere di una gravità che può causare un cambiamento nei coefficienti patrimoniali o, peggio, impedire all'azienda di passare ad un approccio più avanzato.
Nel settore bancario, una *library* di KRI è stata sviluppata dalla *Risk Management Association* (RMA)[21]. Essa può essere utile nel processo di definizione dei *risk indicator*.
Un'altra fonte per l'identificazione dei *risk indicator* è la metrica fornita da COBIT. Sebbene le misure di COBIT si focalizzino sui driver di performance, sulla misura dei risultati e sui mezzi di misurazione generalmente accettati, un "tipico" processo COBIT può servire come base per identificare i *risk indicator*.
Un esempio di KRI derivati dal processo COBIT DS 4 "*Ensure continuous service*" è fornito nella **figura 15**. Il processo è misurato su tre livelli: contribuzione agli obiettivi IT, processi IT e attività. Queste misure possono servire come *risk indicator* ed è buona prassi utilizzare la struttura di misurazione raccomandata da COBIT. In aggiunta la maturità dei processi IT più significativi può servire come *risk indicator* dato che il livello di maturità si correla con il livello di riduzione del rischio.

Figura 15 – Metriche DS4

Misurazione di …	Metrica
Obiettivi IT (*IT goal*)	Numero di ore perse per utente per mese a causa di interruzioni di corrente non pianificate
Processo IT DS4	Percentuale di disponibilità soddisfatta dai *Service Level Agreement* (SLA) Numero di processi di business critici che si basano sull'IT che non sono "coperti" dall'*IT continuity plan* Percentuale di test che raggiungono gli obiettivi di *recovery* Frequenza delle interruzioni di servizio nei sistemi critici
Attività	*Elapsed time* tra i test di ogni singolo elemento dell'*IT continuity plan* Numero di ore di training sull'*IT continuity* per anno per ogni impiegato IT "rilevante" Percentuale delle componenti delle infrastrutture critiche con monitoraggio automatizzato della disponibilità. Frequenza di review dell'*IT continuity plan*

[21] http://www.kriex.org/

Appendice I – Sintesi di Basilea II

Fondata intorno agli anni '30, la Banca per gli investimenti internazionali (*Bank for International Settlements* - BIS) ha, attraverso il suo Comitato per la supervisione bancaria, definito gli standard internazionali prudenziali per la gestione degli istituti bancari. Gli standard sono realizzati per mezzo delle legislazioni di ciascun paese[22] e delle istruzioni normative locali.

Le nuove regolamentazioni sull'adeguatezza patrimoniale di Basilea II (il cosiddetto framework rivisto) rappresenta uno dei cambiamenti regolatori più significativi nel settore finanziario nelle ultime decadi. La discussione è iniziata nel 1998 con il primo *consultation paper* ed ha portato al framework che il Comitato di Basilea ha completato nel giugno 2004. Le nuove *regulation* rappresentano un passo significativo verso la supervisione degli intermediari finanziari e hanno prodotto cambiamenti significativi a livello internazionale nell'organizzazione delle banche. I *regulator* bancari nazionali in tutto il mondo hanno pianificato di implementare i requisiti di Basilea II con un approccio per fasi successive che è iniziato nel 2006 e che continuerà, in alcuni paesi, fino al 2015 prima di essere del tutto completato. I *regulator* europei stanno completando l'implementazione che molti si aspettano di completare entro il 2008.
Basilea II sostituisce il framework sull'adeguatezza dei capitali del 1988, che non era allineato rispetto ai moderni approcci al *risk management* e che non prendeva in considerazione il rischio operativo.
L'obiettivo di Basilea II è di promuovere l'adozione di prassi più forti di risk management per il rischio di credito ed il rischio operativo e di rafforzare il legame tra i rischi finanziari delle banche ed i loro requisiti di capitale. Le nuove regole forniscono un incentivo alle banche per muoversi in tale direzione attraverso una maggiore flessibilità dei requisiti di capitale nel caso il sistema di controllo dei rischi sia di alta qualità.
Di conseguenza una gestione dei rischi prudente e di qualità fornisce un vantaggio competitivo agli intermediari finanziari.
I requisiti di adeguatezza patrimoniale devono inoltre tener conto degli sviluppi di mercato e degli avanzamenti nelle prassi di risk management.

Secondo il Comitato, l'accordo di Basilea II ha come finalità:

- il rafforzamento della correttezza e stabilità del sistema bancario internazionale ed il mantenimento dell'attuale livello di capitalizzazione;
- la gestione di tutti i rischi;
- assicurare che il capitale delle banche sia adeguato a coprire il livello del rischio che risulta dalle posizioni assunte e dal tipo di business effettuato;
- l'applicabilità a tutte le banche quale che sia il grado di complessità e di predisposizione al rischio.

I cambiamenti più rilevanti rispetto alla formulazione del 1988 sono:

- le regole si applicano ai gruppi bancari e non più ai singoli istituti;
- il calcolo dell'adeguatezza del capitale si può basare anche su metodi di *internal rating* della singola banca;

[22] In Europa, gli standard sono stati inizialmente adottati a livello di Unione Europea (EU) nella forma di direttiva europea.

- un potenziale migliorato per ridurre l'esposizione al credito grazie alle "garanzie collaterali";
- il riconoscimento del rischio operativo nella determinazione dell'adeguatezza del capitale.

In aggiunta sono stati aggiunti o meglio specificati standard per la *supervisory review* dei sistemi di *risk assessment* delle banche, standard che richiedono rapporti continuativi tra banche ed autorità di vigilanza.

Requisiti estesi per la comunicazione finanziaria volti a rafforzare la disciplina di mercato.

Il focus è sui requisiti minimi di capitale, requisiti che hanno impatto più rilevante sulle banche commerciali. Le nuove regole rappresentano un maggior livello di complessità rispetto alle regole prima vigenti e ciò è in linea con lo sviluppo di varie aree di business ed il miglioramento gestione del rischio di credito delle istituzioni di servizi finanziari.

Agli intermediari finanziari è permesso scegliere l'approccio più appropriato in relazione alle proprie procedure ed alla propria operatività così da tenere sotto controllo i requisiti di capitale in relazione ai rischi di credito, di mercato ed operativo.
Questa opzione deve tener conto delle diverse circostanze del *risk control* e del *risk management* degli intermediari finanziari. Generalmente l'*assessment* dei rischi ed i requisiti di capitale che ne risultano diventa più *risk-sensitive* con l'aumentare della complessità.
Allo stesso tempo devono essere garantiti, quale precondizione, requisiti qualitativi e quantitativi più stringenti. L'approccio più avanzato garantisce, agli intermediari finanziari, una maggiore flessibilità dei requisiti di capitale.
Il framework "rivisto" mantiene alcuni elementi chiave dello schema di adeguatezza patrimoniale del 1988, tra i quali il requisito generale del mantenimento di un ammontare di patrimonio pari ad almeno l'8% delle attività ponderate per il rischio, la struttura di base dell'Emendamento del 1996 volto a incorporare nell'Accordo i rischi di mercato, nonché la definizione di patrimonio idoneo.

I tre pilastri del nuovo framework[23]

Un patrimonio pari ad almeno l'8% delle attività ponderate per il rischio da solo non è sufficiente per stabilizzare i mercati finanziari in caso di crisi: gli intermediari finanziari devono anche essere in grado su base continua di identificare, controllare ed assorbire le potenziali perdite prodotte da tali rischi.
Ciò richiede di attivare e gestire sistemi avanzati di *risk management*. Gli intermediari finanziari che adottano sistemi di controllo "avanzati" per il controllo dei rischi devono rispettare requisiti di capitale ridotti a condizione che l'autorità di supervisione approvi la validità e correttezza dei sistemi adottati. Nell'applicare questa filosofia i *supervisor* si stanno muovendo da metodi quantitativi verso un modello qualitativo della supervisione degli intermediari finanziari.
La *supervisory review* è considerata il secondo pilastro del framework.

I requisiti "estesi" di informativa sono essenziali per assicurare la "regolamentazione" del mercato ed è un complemento efficace agli altri due pilastri.

Il primo pilastro: requisiti minimi di capitale

[23] Il testo che segue si basa sul documento "*Basel II Framework*" pubblicato dal Comitato di Basilea nel giugno 2004.

I requisiti patrimoniali minimi sono definiti in Basilea II: essi sono determinati mediante un calcolo che si basa sulla definizione di patrimonio di vigilanza e di attività ponderate per il rischio. Il coefficiente patrimoniale totale non deve essere inferiore all'8%.
Le attività totali ponderate per il rischio si ricavano moltiplicando i requisiti patrimoniali a fronte dei rischi di mercato e operativo per 12,5 (ossia, il reciproco del coefficiente patrimoniale minimo dell'8%) e aggiungendo i prodotti alla somma delle attività ponderate per il rischio di credito.

Rischio di credito

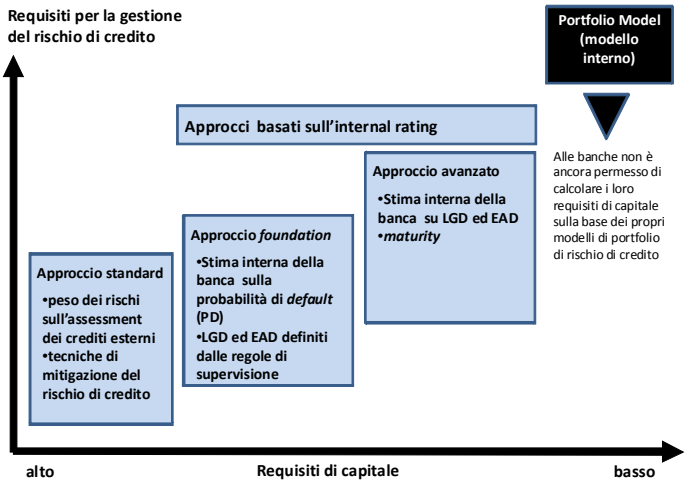
Il comitato di Basilea consente alle banche la scelta tra due metodologie per il calcolo dei requisiti patrimoniali a fronte del rischio di credito come mostrato nella **figura 16**.
La prima consiste nella misurazione di tale tipologia di rischio in modo standardizzato, con l'ausilio di valutazioni esterne del merito creditizio.
La metodologia alternativa, subordinata all'esplicita approvazione dell'autorità di vigilanza, consente alle banche l'impiego dei loro sistemi interni di *rating* per il rischio di credito.
Gli intermediari finanziari possono applicare l'approccio standardizzato (che di solito richiede maggiori requisiti di capitale) o il proprio modello interno (che di solito richiede minori requisiti di capitali).

L'approccio standardizzato[24]

Basilea II continua ad usare, come il precedente accordo, il "peso" per l'esposizione al rischio di credito. Tuttavia i "pesi" di ciascun rischio devono essere corretti sulla base dei *rating* delle istituzioni esterne di valutazione del credito (*External Credit Assessment Institutions* - ECAI), quali Standard & Poor's o Moody's.
I supervisori nazionali selezionano ed approvano le ECAI i cui *rating* sui crediti verso soggetti sovrani, sulle aziende di servizi finanziari, sui clienti *corporate* e sulle perdite su crediti sono usati per determinare il peso del rischio.
Per la prima volta la regolamentazione generale include anche il trattamento delle esposizioni derivanti da cartolarizzazione (ABS). Quando un intermediario finanziari opera nella intermediazione mobiliare (cioè quando la banca agisce come un investitore), essa deve accantonare un certo capitale in accordo al *rating* dell'ECAI esterna. Gli intermediari possono ridurre i requisiti di capitale richiesto, in base al rapporto dell'esposizione al credito diretto o indiretto compresa nella cartolizzazione.
Tecniche per minimizzare i rischi di credito (cioè garanzie reali e personali, *warranties*, derivati su crediti) diventano più importanti quando si devono determinare i livelli di rischio. Il catalogo delle "garanzie" approvate è stato ampliato. Le nuove regolamentazioni richiedono correzioni alle "garanzie" per tener conto delle possibili fluttuazioni future dei prezzi di mercato.

Figura 16 – I tre approcci al rischio di credito

[24] I rischi IT non hanno impatto sui coefficienti patrimoniali quando si usa l'approccio standardizzato.



Approccio basato sull'Internal Ratings (IRB)

Rispetto all'approccio standardizzato, l'approccio IRB fa maggiormente conto sui profili di rischio individuale delle banche e si pone più vicino all'obiettivo di un requisito di capitale pesato sul rischio. Gli intermediari finanziari possono usare i propri modelli e stime delle componenti di rischio nel determinare i requisiti del capitale per una data esposizione a patto di rispettare certi criteri minimi definiti dal supervisore.
Nel sistema IRB le banche devono ripartire i crediti del "*banking book*" in 11 classi con l'indicazione di differenti caratteristiche del rischio. Le classi di attività sono tra le altre: (i) verso imprese; (ii) verso soggetti sovrani; (iii) verso banche; (iv) rispetto ai clienti *retail*; (v) azionarie. Entro queste classi le componenti di rischio sono associate in modo separato con specifici parametri d rischio.
Per ciascuna classe, ci sono differenti regolamentazioni che gestiscono i pesi individuali di rischio. In pratica gli intermediari finanziari possono scegliere tra due approcci:

- l'approccio *foundation* più facile;
- l'approccio avanzato che riconosce una più maggior rilevanza al modello interno dell'azienda e alle stime per le componenti di rischio.

Le seguenti componenti di rischio sono incorporate nell'approccio IRB:

- Probabilità di *default* (PD) – Sulla base dell'*internal rating*, la banca categorizza ciascun debitore in una delle categorie di rischio. Di conseguenza l'azienda di servizi finanziari deve stimare la probabilità di *default* entro un anno per ciascuna categoria.
- Esposizione al *default* – Una linea di credito stabilita non determina necessariamente l'utilizzazione di una linea ad una certa data. L'EAD è una stima del credito in sospeso al tempo del *default*.
- Perdite date per default (*Loss given default*) – Nel caso di *default*, la perdita per l'azienda di servizi finanziari dipende dalla possibilità di *recovery* di ogni *collateral* e ricavi (*revenue*) a partire dalla vendita degli asset del debitore. L'LGD rappresenta la stima e la *total net loss* al tempo del *credit default*.
- *Effective maturity* (M) – L'*effective maturity* è il tempo più lungo possibile che rimane prima che la controparte sia schedulata per soddisfare la sua obbligazione ed è considerata un fattore di rischio nell'approccio IRB. Più il periodo di credito è lungo più viene valutato alto il rischio di fallimento (*failure*).

- Per concedere accesso ai metodi di *internal rating* ad un gran numero di intermediari finanziarie, aziende di servizi finanziari possono scegliere uno dei due approcci IRB:
    - l'approccio base più semplice è basato sulla stima interna delle perdite (PDs) solo per classe di rating; le altre componenti (EAD, LGD e M) sono determinate dai supervisori. *Collateral, warranties, credit derivatives and netting agreements* sono trattate in modo simile all'approccio standardizzato
    - l'approccio avanzato in cui gli intermediari finanziari devono calcolare l'*effective maturity* e fornire le proprie stime per le componenti di rischio; per qualificare per l'approccio avanzato, le aziende di servizi finanziari devono mantenere e gestire una vasta storia di dati storici e soddisfare requisiti minimia avanzati; nessuna restrizione in relazione ai *credit collateral* e *warranties* si applica ad eccezione dell' *off-balance sheet exposure*.

Le stime si basano su funzioni matematiche che concorrono con i modelli di *credit portfolio* e *credit metrics*.
Per ottenere l'approvazione del supervisore per l'approccio IRB le aziende di servizi finanziari devono essere *compliant* con i requisiti minimi (cioè un sistema di *quality rating* e prassi estese sull'informativa come indicato nel terzo pilastro). Questo aiuta ad assicurare l'integrità dei sistemi di *internal risk assessment*.
Le classi di *rating* assegnate ai clienti individuali e l'informazione quantitativa che ne risulta sono parte integrante dei sistemi di *risk assessment*, *risk management*, *pricing* e di previsione del rischio. Naturalmente l'informazione è anche usata per valutare l'adeguatezza del capitale umano. In aggiunta al precedente requisito le aziende di servizi finanziari devono applicare *stress test* sulla base dei loro modelli interni. Tali test devono considerare l'effetto degli scenari di "leggera" recessione.

Rischio di mercato

Il rischio di mercato è il rischio di perdite che sorgono dal mutare della variabili di mercato cioè i ratei degli interessi, *share prices* o valute straniere. Le procedure di misurazione e la considerazione dei rischi di mercato di base rimane la stessa in Basilea II e non sono ulteriormente approfondite nelle nuove regolamentazioni.

Rischi operativi

Come già notato, Il Comitato di Basilea definisce i rischi operativi in Basilea II come segue:
"Il rischio operativo è definito come il rischio di perdite a causa di processi interni, persone, sistemi non adeguati o a causa di eventi esterni." [25]
La definizione include i rischi legali ma esclude i rischi strategici e reputazionali.
Al momento il rischio operativo è valutato pari all'8 percento rispetto ai requisiti patrimoniali. Per valutare il valore dei rischi operativi le aziende di servizi finanziari possono usare diversi approcci alternativi.

Approccio con Basic Indicator

Le banche che usano il BIA devono gestire il capitale per il rischio operativo con una percentuale fissa (*alpha*) della media dei precedenti tre anni di di *gross income* positivo annuale. Il *gross*

[25] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, febbraio 2003

income annuale è usato come indicatore di esposizione *exposure indicato*r (EI), che serve come indicatore per i rischi operativi assunti ed è calcolato a partire dalla somma dell'*interest surplus, commission surplus, trading result, financial asset result and other income*. Questo approccio semplificato può essere usato dalle piccolo aziende di servizi senza un sistema per il controllo dei rischi operativi. Il Comitato di Basilea si aspetta che gli intermediari finanziari che operano internazionalmente usino al minimo l'approccio standardizzato.

Approccio standardizzato

Lo STA segue un concetto simile ma deve essere considerato una diversa significatività del rischio per ciascuna linea di business definita dal Comitato di Basilea. Una scala di esposizione al rischio è definita per ognuna di queste linee di business delle banche *retail*. Il capitale richiesto per ogni *business line* è calcolato a partire dal valore dell'indicatore di rischio di ciascuna *business line* (cioè *positive annual gross income*) moltiplicato per un fattore (beta) assegnato ad ogni *business line*. Fattori di diversificazione non sono presi in considerazione.
Gli intermediari finanziari devono essere *compliant* con ulteriori requisiti quando utilizzano l'approccio standardizzato; essi comprendono l'esistenza di un processo completo e coerente per la riduzione permanente dei rischi ed il rispettivo monitoraggio. Il *board of directors* e l'unità dei controlli indipendenti deve essere coinvolto in modo attivo nel controllo e nel *reporting* mentre la funzione di internal audit deve esaminare la correttezza delle procedure applicate. In aggiunta i dati sui rischi operativi devono essere supportati da dati statistici raccolti dalle transazioni attuali e ci deve essere un appropriato sistema di *reporting* per il management.

Approcci di misurazione avanzati

Una banca che adotta AMA può usare dati specifici tipici dell'intermediario finanziario ed un meccanismo di allocazione allo scopo di determinare i requisiti di capitali richiesti dalla regolamentazione. Come alternativa agli indicatori specifici per *business line* indicati dalla norma, le *regulation* indicano sette ulteriori eventi di perdita standardizzati (*standardized loss events* cioè *legal costs*) che rappresentano tipi di rischi operativi.
Per considerare i differenti metodi che al momento sono stati sviluppati o implementati dalle aziende di servizi finanziari il supervisore ha il diritto di determinare se l'approccio è consono ed appropriato. L'approvazione dipende dalla presenza di vari fattori che i supervisori vogliano verificare come propriamente incorporati nei modelli interni.
È importante che l'approccio degli intermediari finanziari sia basato sui dati sulle perdite interne. Inoltre le aziende di servizi finanziari devono incorporare completamente l'esposizione al rischio attuale nelle loro pianificazione operative e strategiche. Esse devono anche implementare un sistema per la raccolta delle perdite attuali a partire dalle operazione operative che assicuri una raccolta a livello di gruppo e affidabile dei dati sulle perdite storiche perenni. Un metodo appropriato deve essere applicato per supportare, verificare o migliorare i dati interni usando le informazioni da fonti esterne. Le aziende di servizi finanziari devono condurre periodici *stress test* ed analisi di *portfolio* per riesaminare i risultati.
Il comitato di Basilea non indica uno specifico approccio per generare la misura del rischio operativo ai fini del capitale regolatorio. Quale che sia l'approccio utilizzato, un intermediario finanziario deve dimostrare che le misure del suo rischio operativo soddisfano uno standard affidabile comparabile con quello dell'approccio IRB per il rischio di credito (cioè comparabile per il periodo di un anno e con un intervallo di confidenza di 99.9 percentile).
Usando l'AMA alle banche è permesso indicare un'assicurazione quale fattore di mitigazione di impatto nel calcolo del rischio operativo purché certi requisiti siano soddisfatti. L'utilizzo di tali polizze può essere limitato dall'autorità di supervisione.

Il secondo pilastro: il processo di "*Supervisory Review*"

Il primo pilastro si focalizza principalmente sui requisiti quantitativi per gli intermediari finanziari. Il secondo pilastro si concentra sull'aspetto qualitativo delle attività di supervisione. I supervisori nazionali sono responsabili per la *quality assurance* dei sistemi di *risk management* degli intermediari finanziari. I doveri dei supervisori nazionali consistono in :

- monitorare la *compliance* dei requisiti minimi compresi i requisiti sull'informativa;
- promuovere lo sviluppo e l'uso delle tecniche per la gestione avanzata dei rischi;
- emettere un'opinione sulla qualità delle stime interne della banca e dell'adeguatezza del capitale richiesto;
- intraprendere azioni nel caso di inadeguati livelli del capitale.

Tuttavia non si deve pensare che la responsabilità di implementare e valutare i sistemi di gestione adeguati del rischio sia delegata ai supervisori. I supervisori devono solo esaminare le tecniche e le procedure degli intermediari finanziari. Il Comitato di Basilea ha identificato quattro principi chiave per la *supervisory review*:

- le banche devono avere un processo per valutare la loro adeguatezza globale di capitale;
- i supervisori devono riesaminare e valutare l'*assessment* interno delle banche sulla adeguatezza del capitale e le strategie;
- le banche devono operare soprattutto sui *minimum regulatory capital ratio*;
- i supervisori devono cercare di intervenire nelle fasi iniziali.

L'aumentata affidabilità delle metodologie internazionali interne delle banche va intesa a promuovere un dialogo attivo tra le banche ed i supervisori.

Il terzo pilastro: disciplina di mercato

Uno degli obiettivi del Comitato di Basilea è di rafforzare l'affidabilità e stabilità del sistema bancario internazionale. Le informative richieste sotto il "terzo pilastro" sono considerate essenziali per assicurare la regolamentazione del mercato e rappresentano un complemento necessario ed efficace agli altri due pilastri. L'informativa della banca sui propri rischi relativi ai dati interni fornisce agli altri partecipanti al mercato specifiche informazioni sulla situazione di rischio globale dell'istituzione. Il framework richiede una informativa generale principale che è obbligatoria per tutte le banche: le banche devono avere una *policy* formale sull'informativa approvata dal Consiglio di Amministrazione. Come parte di questa *policy*, devono essere specificati la strategia e gli obiettivi della banca, con una prospettiva precisa sull'informativa delle informazioni sulla situazione finanziaria e sulla "profittabilità". In aggiunta le banche devono implementare un processo per valutare l'appropriatezza delle proprie informative.[26]
Questo obiettivo è guidato dall'assunzione che i partecipanti al mercato ben informati terranno in considerazione il livello dei rischi assunti e la qualità della gestione dei rischi nelle loro decisioni relative agli investimenti.

Il Comitato di Basilea fornisce un concetto flessibile della quantità e frequenza delle informazioni richieste per l'informativa. Di base le proposte sono formulate come "raccomandazioni". Tuttavia il

[26] Comitato di Basilea sulla supervisione bancaria, "*Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*," giugno 2006

framework ha regole vincolanti nei casi in cui gli intermediari finanziari scelgano l'opzione di utilizzare i modelli avanzati (cioè gli *internal rating*) per ridurre i requisiti di capitale. In base alla complessità dei processi di business e del rischio di profilo dell'azienda di servizi finanziari la frequenza e la quantità (informazioni *core* ed informazioni supplementari) delle informazioni di informativa possono variare.
I requisiti "informativi" sono composti da quattro aree.

1. Ambito dell'applicazione – il nome dell'entità "top corporate" nel gruppo al quale il framework si applica deve essere citato.
2. Struttura del capitale – una sintesi dell'informazione deve riguardare i termini e le condizioni delle principali caratteristiche di tutti gli elementi del capitale. Ciò include *paid-up shares of capital/common stock, reserves*, ed i tipi e le specifiche degli strumenti innovative del capitale. L'obiettivo è di fornire ai partecipanti al mercato le informazioni richieste per formarsi una opinione sulla capacità della banca di sostenere i rischi finanziari.
3. Rischi attuali e loro struttura – Questa è l'area principale del terzo pilastro. I quattro maggiori rischi sono definiti e sono forniti dati separate per ciascuno di essi: credito, mercato, rischi operativi e di interesse nel *banking book*. Di base le aziende di servizi finanziari devono stimare le loro perdite potenziali per ciascun tipo di rischio e confrontar e le stime con le perdite reali. Il risultato di tale confronto deve essere diffuse al pubblico. Sulla base di questa informazione, i partecipanti al mercato devono esser in grado di valutare l'appropriatezza e l'efficacia del sistema di *risk management*.
4. Adeguatezza del capitale – Deve essere comunicato il rispetto del requisito del capitale equivalente ai rischi assunti ed al *capital ratio* complessivo. In aggiunta deve essere fornita un'analisi dei fattori che riguardano il requisito di capitale e l'allocazione del capitale economico.

Appendice II – Comparazione di alto livello tra COSO ERM e Basilea II

La **figura 17** fornisce una comparazione logica di alto livello tra COSO ERM e Basileal II.

Figura 17 – Comparazione tra COSO ERM e Basilea II

COSO Enterprise Risk Management - Integrated Framework (settembre 2004)	Basilea II: Il secondo pilastro - *Supervisory Review Process* (giugno 2006)
	Supervisione del Consiglio di Amministrazione e del senior management Un processo affidabile di *risk management* è fondamentale per un assessment efficace dell'adeguatezza della posizione di capitale della banca. Il management della banca ha la responsabilità di comprendere la natura ed il livello di rischio assunto dalla banca ed in che modo tale rischio si relazioni ai livelli adeguati del capitale. Il management è anche responsabile di assicurare che la *formality* e la *sophistication* dei processi di *risk management* siano appropriati alla luce del profilo di rischio e del *business plan* (paragrafo 728). **Assessment affidabile del capitale** Gli elementi fondamentali dell'assessment affidabile del capitale comprendono: • politiche e procedure progettate per assicurare che la banca identifichi, misuri e riporti tutti i rischi materiali; • un processo che metta in relazione il capitale al livello del rischio; • un processo che individui e gestisca gli obiettivi di adeguatezza del capitale rispetto al rischio, tenendo conto del focus strategico della banca e del suo *business plan*; • un processo relativo ai controlli interni, review ed audit che assicuri l'integrità del processo generale di management (paragrafo 731).
	Assessment completo dei rischi Tutti i rischi materiali che la banca affronta devono essere gestiti nel processo di *capital assessment*. Il Comitato riconosce che non tutti i

	rischi possono essere misurati in modo preciso, tuttavia è necessario che sia sviluppato un processo per stimare tali rischi. Devono essere comprese le seguenti esposizioni al rischio, che tuttavia non devono essere intesi come una lista completa di tutti i rischi, (paragrafo 732) **Monitoraggio e reporting** La banca deve adottare un adeguato sistema per il monitoraggio ed il reporting dell'esposizione al rischio e valutare in caso di modifica come il profilo di rischio modificato della banca abbia effetto sui requisiti di capitale. L'alta direzione della banca deve, su base regolare, ricevere i rapporti sul profilo di rischio e le necessità di capitale della banca. Questi rapporti devono permettere all'alta direzione di: • valutare il livello ed il trend dei rischi materiali ed il loro effetto sui livelli di capitale; • valutare la sensitività e la "ragionevolezza" delle assunzioni chiavi usati nell'assessment del sistema di misurazione del capitale; • determinare se la banca ha a disposizione capitali sufficienti rispetto ai vari rischi ed è *compliant* rispetto agli obiettivi di adeguatezza del capitale; • determinare i requisiti futuri di capitale sulla base del profilo di rischio riportato della banca e se si rendono necessari aggiustamenti al piano strategico della banca (paragrafo 743). **Review del controllo interno** La struttura organizzativa interna della banca è essenziale nel processo di assessment del capitale. Controlli effettivi del processo di *capital assessment* devono prevedere una review indipendente e, se appropriato, il coinvolgimento degli auditor interni ed esterni. L'alta direzione della banca ha la responsabilità di assicurare che il management attui un sistema per valutare i diversi rischi, sviluppi un sistema per correlare i rischi al livello di capitale della banca e stabilire un metodo per monitorare la *compliance* con le politiche interne. Il *board* deve verificare regolarmente se il suo sistema di controlli interni sia adeguato per assicurare una condotta del business ben ordinata e prudente (paragrafo 744).

Appendice III – Comparazione di alto livello tra il principio 1 di Basilea II: il secondo pilastro - Supervisory Review Process (giugno 2006) e COSO ERM - Integrated Framework (settembre 2004)

La **figura 18** fornisce una comparazione logica di alto livello tra il secondo pilastro di Basilea II ed il *COSO ERM Framework.*

Figura 18 – Comparazione a livello alto tra il secondo pilastro di Basilea II ed il COSO ERM Framework

Secondo pilastro di Basilea II	*COSO ERM Framework*
1. Supervisione del Consiglio di Amministrazione e del senior management Il management della banca ha la responsabilità di comprendere la natura ed il livello di rischio assunto dalla banca ed in che modo tale rischio si relazioni ai livelli adeguati del capitale. Il management è anche responsabile di assicurare che la *formality* e la *sophistication* dei processi di risk management siano appropriati alla luce del profilo di rischio e del *business plan.* Il Consiglio di Amministrazione ha la responsabilità di definire la tolleranza al rischio della banca e di assicurarsi che il management adotti e rendi effettivo un framework di valutazione dei diversi rischi, di sviluppare un sistema che metta in relazione i rischi ai requisiti di capitale della banca e di individuare un metodo per monitorare la *compliance* rispetto alle politiche interne.	1. Ambiente interno – L'ambiente interno riguarda lo stile di un'azienda ed influenza la "consapevolezza" del rischio del suo personale ed è il fondamento per tutte le altre componenti dell'ERM, fornendo regole e struttura organizzativa. Fattori dell'ambiente interno comprendono la filosofia del *risk management* aziendale; la sua predisposizione al rischio la sua cultura del rischio; la supervisione del *board of director*; l'integrità ed i valori etici e la competenza del suo personale; lo stile e la filosofia del management; il modo in cui il management assegna compiti e responsabilità ed organizza e sviluppa le competenze del personale.
2. Assessment affidabile del capitale - gli elementi fondamentali dell'assessment affidabile (*sound*) del capitale comprendono politiche e procedure progettate per assicurare che la banca identifichi, misuri e riporti tutti i rischi materiali, un processo che metta in relazione il capitale al livello del rischio, un processo di controlli interni, review ed audit che assicuri l'integrità del processo generale di management.	2. Definizione degli obiettivi – Ogni azienda fronteggia una gran varietà di rischi che provengono dall'interno e dall'esterno; una precondizione per l'identificazione efficace degli eventi, il *risk assessment* ed il *risk response* consiste nel definire gli obiettivi, collegarli tra i diversi livelli dell'organizzazione e renderli internamente coerenti. Gli obiettivi sono definiti a livello strategico, rappresentano il "fondamento" per le procedure aziendali, il *reporting* ed il rispetto degli obiettivi di *compliance*. Gli obiettivi devono essere allineati con la predisposizione al rischio aziendale, che determina i livelli di tolleranza al rischio per le attività.

3. Assessment completo di tutti i rischi - tutti i rischi materiali che la banca affronta devono essere gestiti nel processo di *capital assessment*. Mentre il Comitato riconosce che non tutti i rischi possono essere misurati in modo preciso, tuttavia deve essere sviluppato un processo per stimare i rischi. .	3. Identificazione degli eventi – il management deve identificare i possibili eventi che possano avere impatto sulle capacità dell'azienda di implementare con successo la propria strategia raggiungere gli obiettivi. Eventi con un impatto potenziale negativo rappresentano rischi che richiedono una risposta del management. Eventi con un impatto potenzialmente positivo possono compensare gli impatti negativi o rappresentare opportunità. Il management deve fare rientrare le opportunità nella strategia e nei processi di definizione degli obiettivi. Una gran varietà di fattori interni ed esterni può dar luogo al realizzarsi degli eventi. Quando si identificano gli eventi potenziali il management deve considerare l'ambito completo dell'azienda. Il management deve considerare il contesto entro cui l'azienda opera e la sua tolleranza al rischio.
4. Review del controllo interno – L'alta direzione della banca ha la responsibilità di assicurare che il management attui un sistema per valutare i diversi rischi, sviluppi un sistema per correlare i rischi al livello di capitale della banca e stabilire un metodo per monitorare la *compliance* con le politiche interne. L'alta direzione deve verificare regolarmente se il suo sistema di controlli interni sia adeguato per assicurare una condotta del business ben ordinata e prudente. La banca deve condurre review periodici del proprio processo di IT risk management per assicurar la sua integrità, accuratezza e ragionevolezza .	4. *Risk assessment* – il risk assessment permette all'azienda di considerare l'estensione rispetto a quali i potenziali eventi possano avere un impatto sul raggiungimento degli obiettivi. Il management deve valutare gli eventi da due prospettive – probabilità ed impatto e di solito si usa una combinazione di metodi qualitativi e quantitativi. Gli impatti positivi e negativi degli impatti degli eventi potenziali devono essere analizzati, individualmente o per categorie, attraverso tutta l'azienda. Gli eventi potenzialmente negativi devono essere valutati sia dal punto di vista inerente (potenziale) sia dal punto di vista residuale.
5. Monitoraggio e reporting - La banca deve stabilire un adeguato sistema per il monitoraggio ed il reporting dell'esposizione al rischio e valutare come il profilo di rischio modificato della banca ha effetto sulle necessità del capitale. Il senior management o il *board of director* della banca deve, su base regolare, ricevere i rapporti sul profilo di rischio e le necessità di capitale della banca. Questi rapporti devono permettere al senior management di valutare i requisiti attuali e futuri, la sensitività e la "ragionevolezza" delle assunzioni chiavi usati nell'assessment del sistema di misurazione del capitale, determinare se la banca ha a disposizione capitali sufficienti rispetto ai vari rischi ed è *compliant* rispetto agli obiettivi di	5. *Risk response* – Dopo aver valutato i rischi rilevanti, il management deve decidere come gestirli. Le possibili risposte comprendono: evitare il rischio, ridurre l'esposizione al rischio, condividere il rischio con altri, accettare il rischio. Nel considerare il tipo di risposta da adottare, il management deve considerare i costi ed i benefici e selezionare la "risposta"che riporta i fattori "probabilità" e "l'impatto" entri i limiti desiderati.

adeguatezza del capitale.	
	6. Attività di controllo – le attività di controllo consistono in politiche e procedure che sono di ausilio per rendere effettive le "risposte ai rischi" del management. Le attività di controllo sono trasversali a tutta l'azienda in tutti i livelli e in tutte le funzioni. Esse includono un vasto *range* di attività diverse quali approvazioni, autorizzazioni, verifiche, riconciliazioni, *review* delle performance, sicurezza degli asset e segregazione di incarichi.
	7. Informazione e comunicazione – le informazioni pertinenti devo essere identificate, raccolte e comunicate nella forma e nei tempi utili per permettere alle persone di poter eseguire le azioni che sono di loro responsabilità. I sistemi informativi usano dati generati internamente ed informazioni su eventi esterni, attività e considerazioni, creando nuove informazioni per gestire i rischi delle imprese per rendere possibili decisioni informate in relazione agli obiettivi. Comunicazioni efficaci devono transitare per tutta l'azienda. Tutto il personale deve ricevere un chiaro messaggio da parte del *top management* che le responsabilità dell'ERM devono essere prese in considerazione in modo serio. Il personale deve aver chiaro il proprio ruolo in relazione all'ERM, così come le attività relative al lavoro degli altri. Il personale deve avere i mezzi per comunicare le informazioni significative e deve esistere una comunicazione efficace anche con le terze parti.
	8. *Monitoring* – L'ERM deve essere monitorato – un processo che valuta la presenza ed il funzionamento delle proprie componenti in modo continuo. Ciò è conseguito attraverso il monitoraggio continuo delle attività, la valutazione indipendente ed anche con la combinazione dei due. Il monitoring continuo deve riguardare il corso delle attività di management tenuto conto dell'ambito e della frequenza delle valutazioni indipendenti.

Appendice IV- La dipendenza del COSO ERM Framework dalla “data quality”[27]

Componenti di COSO	Considerazioni sulla *data quality*
Tone at the Top	
Ambiente interno – L’ambiente interno riguarda lo stile (*the tone*) di un’azienda e definisce la base per come viene visto il rischio e gestito dalle persone dell’organizzazione, compresa la filosofia del *risk management* e la propensione al rischio, l’integrità ed i valori etici e l’ambiente in cui essi operano.	• La *data quality* rafforza l’ambiente di controllo generale. • I dati devono essere considerati come un asset dell’azienda. • La *data quality governance* e controllo devono essere chiare priorità aziendali.
Definizione degli obiettivi – Gli obiettivi devono essere identificati prima che il management possa identificare gli eventi potenziali che possono influenzare il loro conseguimento. L’*Enterprise Risk Management* assicura che il management ha messo in essere un processo di definizione degli obiettivi e che gli obiettivi prescelti siano di supporto ed allineati con la *mission* aziendale e coerenti con la predisposizione al rischio.	• Il Consiglio di Amministrazione, CEO, CFO e CRO hanno la responsabilità finale della *data quality*. • Esistono regolamenti e responsabilità per la gestione dei dati e la qualità delle informazioni. • Esistono politiche e procedure di supporto al *data management*.

Riconoscere e gestire i rischi	
Identificazione degli eventi – Gli eventi interni ed esterni che hanno riflesso sul raggiungimento degli obiettivi aziendali devono essere identificati, distinguendo tra rischi ed opportunità. Le opportunità sono resi coerenti con la strategia del management o con il processo volto al raggiungimento degli stessi.	Una scarsa qualità dei dati può: • provocare decisioni non basate su informazioni corrette con un impatto negativo sugli obiettivi aziendali
Risk Assessment – I rischi sono analizzati considerando la probabilità e l’impatto come base per determinare come essi devono essere gestiti. I rischi sono valutati su base inerente (potenziale) e residua (effettiva).	• esporre l’azienda a rischi non identificati (compresi il rischio operativo, rischio di mercato, rischio di credito) che possono potenzialmente portare ad implicazioni di rischio assai vaste (ad esempio rischio reputazionale, rischio finanziario, *compliance* regolatoria/rischio legale e rischio di “contagio”)
Risk Response – Il management deve individuare le risposte al rischio – evitare,	• Se non puoi misurarlo non puoi gestirlo. • I dati rappresentano i mezzi “granulari”

[27] Basato sull’articolo “*Data Quality: The Hidden Assumption behind COSO*” di George Marinos, Partner, PricewaterhouseCoopers.

accettare, ridurre, condividere – sviluppando un insieme di azioni per allineare i rischi sia con la predisposizione al rischio aziendale sia con la sua tolleranza al rischio.	di controllo.
Attività di controllo – Sono state stabilite ed implementate politiche e procedure per facilitare che le risposte ai rischi siano effettivamente compiute	• Esistono regole e responsabilità chiare per il *data management* e la qualità delle informazioni. • Esistono politiche e procedure che supportano in modo rigoroso il *data management*.

.

Appendice V – Basilea II e CobiT

Come già precedentemente notato, Basilea II si basa su 10 principi, COSO ERM suddivide il controllo interno in otto componenti e CobiT ha quattro domini. La **figura 19** mostra come tutte tali necessità possono essere realizzate ed integrate per soddisfare gli obiettivi di rischio operativo di Basilea II. CobiT fornisce linee guida con un dettaglio simile per l'IT. Le otto componenti di COSO ERM – a cominciare dall'identificazione dell'ambiente di controllo fino al monitoraggio dei controlli interni – può essere visualizzato come strati (*layer*) orizzontali di un cubo tridimensionale, con gli obiettivi dei domini CobiT – dalla "Pianificazione ed Organizzazione" (*Plan and Organize*) fino al "Monitoraggio e Valutazione" (*Monitor and Evaluate*) che si applicano a ciascuno in modo individuale o per aggregazione.

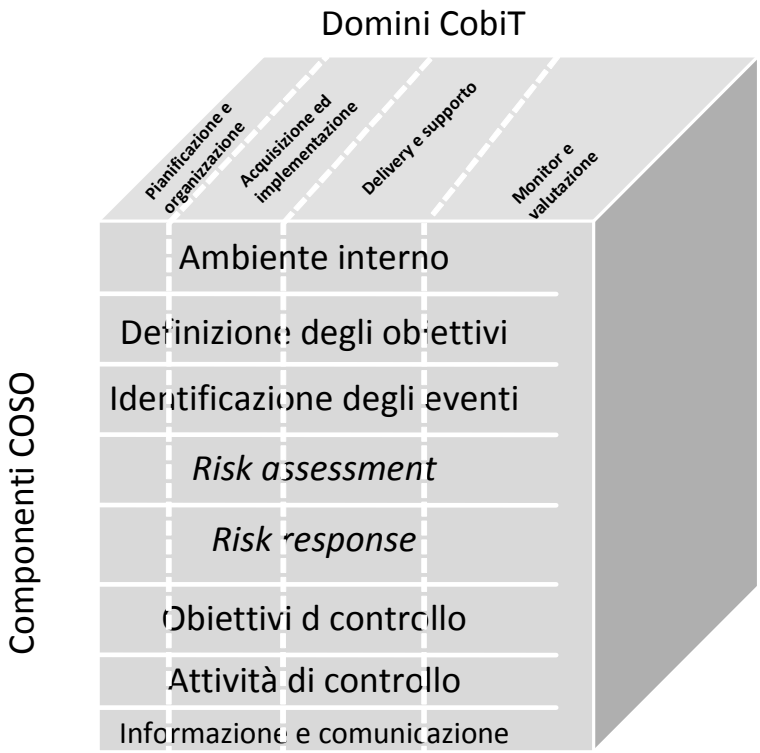
La **figura 19** illustra i prìncipi di Basila II e "mappa"la loro relazione appropriata componente e allo specifico dominio CobiT. È immediatamente evidente che molti processi IT di CobiT hanno relazioni con più di una componente di Basilea II e COSO. Ciò è ovvio data la natura generale dei controlli IT ed il modo in cui essi formano la base per l'affidabilità dei controlli applicativi. Questo attributo di relazione multiple dimostra ancora una volta perché i controlli IT sono la base per tutti gli altri e sono essenziali per un programma di controllo interno affidabile.

I principi di Basilea II:

- consapevolezza ed approvazione del board
- internal audit indipendente
- risk management framework
- identificazione ed assessement
- monitoraggio del rischio operativo
- politiche, processi e procedure
- piani di *contingency* e *business continuity*
- requisiti di supervisione delle banche per un framework efficace
- valutazione continua ed indipendente della supervisione bancaria
- sufficiente informative al pubblico da parte delle banche

Sono necessarie competenze specializzate in tutti gli 8 *layer* del framework COSO per ottenere un *integrated control framework*.

Figura 19 - *Cross-reference* tra COSO ERM e COBIT



COBIT è un framework coerente e completo per la gestione ed il governo dei rischi e dei controlli dell'IT. COBIT è composto da quattro domini, 34 processi IT ed oltre 200 obiettivi di controllo. COBIT include i controlli che gestiscono tutti gli aspetti dell'*IT governance*, ma solo quelli significativi per gli obiettivi di risk management di Basilea II sono stati usati per redigere questo documento. COBIT è un framework liberamente utilizzabile che segue lo "spirito" del requisito di Basilea II che il framework usato sia facilmente accessibile e condiviso dalla comunità internazionale. COBIT fornisce obiettivi sia a livello di azienda (entità) sia a livello di attività con i relativi controlli, ed è diffuso in tutto il mondo nelle aziende come supplemento per gli aspetti IT non previsti in COSO e negli altri framework di *governance*.
Per selezionare i processi e di controlli IT rilevanti, sono possibili due approcci:

- approccio *risk-driven* (guidato dai rischi) – selezionando i *risk driver* rilevanti (ITGI's) *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance*, seconda edizione può essere d'ausilio in questa selezione), classificando questi *risk driver* (critici, importanti, qualche impatto, nessuna rilevanza) ed identificando gli obiettivi di controllo ed i processi correlati
- approccio *goal-driven* (guidato dagli obiettivi)- identificando gli obiettivi IT rilevanti per Basilea II ed usando le linee guida fornite nel "*core content*" di COBIT e la pubblicazione ITGI "*IT Governance Implementation Guide: Using COBIT and Val IT*", seconda edizione.

Approccio *risk-driven*

Nella definizione di rischio operativo, come indicato dai *regulator* e dalle altre associazioni, c'è un ampio *range* di fattori di rischio individuali che possono essere presi in considerazione prima di

integrare la componente operativa nel più ampio ERM framework. In generale, devono essere adottate le seguenti strategie *risk-driven*:

- Identificare i rischi più significativi e gli obiettivi di controllo ed i processi ad essi correlati – è adottata una cultura del *risk management* ed è usato un framework di *IT risk management* nella gestione dei rischi IT. I risultati di questo approccio sono integrati nell'ERM framework. Questo approccio ha il vantaggio che il *risk management* diviene parte della cultura IT e che i rischi emergenti sono gestiti non appena identificati.
- Identificare un largo numero di tipo di eventi di rischio potenziale, valutando o controlli ed i fattori di mitigazione ed effettuando azioni correttive dove applicabile – Questo approccio ha lo svantaggio potenziale di essere ancora focalizzato sui rischi identificati e di non garantire la flessibilità di reazione a fronte di rischi non previsti. Se sono identificati molti *risk driver*, aumenta il rischio che il focus sui rischi più significativi possa ridursi.

La **figura 20** fornisce esempi esemplificativi degli *IT event type* che gestiscono i *risk event type* di Basilea II e dei processi COBIT che gestiscono questi aspetti IT.

Figura 20 - Basel II Risk Event Types and Related IT Risk Aspects and COBIT Processes

Basel II RiskEvent Types	IT Aspects	COBIT Processes

Basel II Risk Event Types	IT Aspects	COBIT Processes
Internal fraud	• Deliberate manipulation of programs • Unauthorized usage of modification functions Deliberate manipulation of system instructions • Deliberate manipulation of hardware • Deliberate unauthorized changing of system and application data • Using/copying unlicensed or unauthorized software • Internal circumvention of access privileges	• PO6 • DS5 • DS9 • DS12
External fraud	• Deliberate changing of system and application data through hacking • Outsiders gaining sight of confidential physical or electronic documents • External circumvention of access privileges • Eavesdropping and interception of communication links • Password compromise • Viruses	• DS5
Employment practices and workplace safety	• Misuse of IT resources	• PO6

	• Lack of security responsiveness	• DS5
Clients, products and business practices	• Disclosure of sensitive information to outsiders by employees • Management of third-party suppliers	• PO6 • DS2
Damage to physical assets	• Deliberate or accidental damage to physical IT infrastructure	• DS12
Business disruption and system failures	• Hardware or software malfunction • Communications failure • Employee sabotage • Loss of key IT staff member(s) • Destruction of software/data files • Theft of software or sensitive information • Computer viruses • Failure to back up • (Distributed) denial-of-service attacks • Configuration control error	• AI7 • DS3 • DS4 • DS5 • DS9 • DS10
Execution,delivery and process management	• Error in handling electronic media • Unattended workstation • Change control error • Incomplete input of transactions • Errors on data input/output • Programming/testing error • Operator error, e.g., in recovery procedural error	• AI3 • AI6 • AI7 • DS5 • DS10

Approccio *goal-driven*

L'approccio *goal-driven* ha il vantaggio di facilitare l'allineamento degli sforzi IT con i *business goal*. La **figura 21** mostra la tabella degli *IT goal* fornita in COBIT. La colonna destra indica se l'*IT goa*l è rilevante o meno per Basilea II. IT goal senza l'indicazione di "rilevanza" sono ritenuti non rilevanti per le finalità di Basilea II.

Figura 21 - COBIT IT Goals

Obiettivo		Rilevanza
1.	Respond to business requirements in alignment with the business strategy	
2.	Respond to governance requirements in line with board direction	●
3.	Ensure satisfaction of end users with service offerings and service levels	

4.	Optimize the use of information	
5.	Create IT agility	
6.	Define how business functional and control requirements are translated into effective and efficient automated solutions	
7.	Acquire and maintain integrated standardized application systems	
8.	Acquire and maintain an integrated and standardized IT infrastructure	●
9.	Acquire and maintain IT skills that respond to the IT strategy	●
10.	Ensure mutual satisfaction of third-party relationships	●
11.	Ensure seamless integration of applications into business processes	
12.	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels	●
13.	Ensure proper use and performance of the applications and technology solutions	●
14.	Account for and protect all IT assets	●
15.	Optimize the IT infrastructure, resources and capabilities	●
16.	Reduce solution and service delivery defects and rework	●
17.	Protect the achievement of IT objectives	●
18.	Establish clarity on the business impact of risks to IT objectives and resources	●
19.	Ensure that critical and confidential information is withheld from those who should not have access to it	●
20.	Ensure that automated business transactions and information exchanges can be trusted	●
21.	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster	●

La selezione dei processi IT nella **figura 22** può rappresentare la base per il programma di implementazione.

Figura 22 - Sample IT Processes for Implementation Program COBIT IT Process Overall

COBIT	IT Process	Overall
PO1	Define a strategic IT plan.	●
PO2	Define the information architecture.	
PO3	Determine technological direction.	
PO4	Define the IT processes, organization and relationships	.
PO5	Manage the IT investment.	
PO6	Communicate management aims and direction.	●
PO7	Manage IT human resources.	
PO8	Manage quality.	
PO9	Assess and manage IT risks.	
PO10	Manage projects.	
AI1	Identify automated solutions.	
AI2	Acquire and maintain application software.	
AI3	Acquire and maintain technology infrastructure.	
AI4	Enable operation and use.	●

AI5	Procure IT resources.	
AI6	Manage changes.	●
AI7	Install and accredit solutions and changes.	●
DS1	Define and manage service levels.	
DS2	Manage third-party services.	
DS3	Manage performance and capacity.	
DS4	Ensure continuous service.	●
DS5	Ensure systems security.	●
DS6	Identify and allocate costs.	
DS7	Educate and train users.	●
DS8	Manage service desk and incidents.	
DS9	Manage the configuration.	●
DS10	Manage problems.	
DS11	Manage data.	●
DS12	Manage the physical environment.	●
DS13	Manage operations.	
ME1	Monitor and evaluate IT performance.	
ME2	Monitor and evaluate internal control.	●
ME3	Ensure regulatory compliance.	
ME4	Provide IT governance.	●

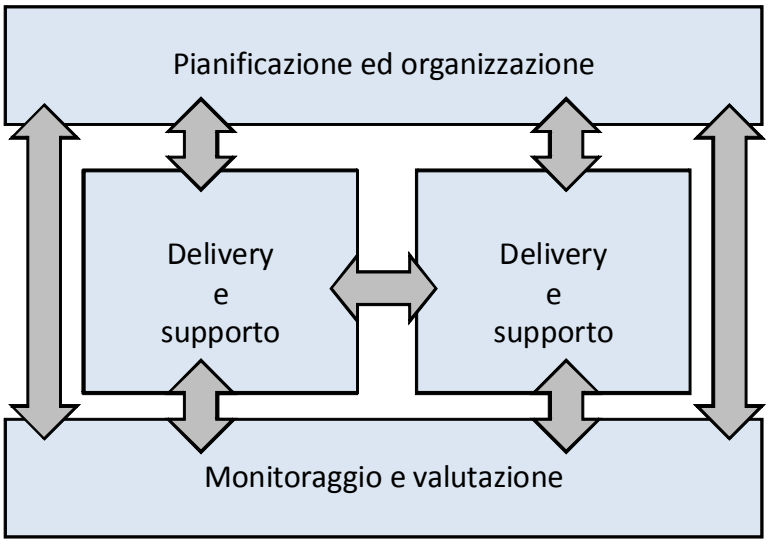
Figura 23 - Basel Principles Mapped to COBIT Processes

	COBIT IT Processes																															
	Plan and Organize										Acquire and Implement							Deliver and Support												Monitor and Evaluate			
Basel II and IT Guiding Principles	PO1 Define a strategic IT plan.	PO2 Define the information architecture.	PO3 Determine technological direction.	PO4 Define the IT processes, organization and relationships	PO5 Manage the IT investment.	PO6 Communicate management aims and direction	PO7 Manage IT human resources.	PO8 Manage quality.	PO9 Assess and manage IT risks.	PO10 Manage projects.	AI1 Identify automated solutions.	AI2 Acquire and maintain application software	AI3 Acquire and maintain technology infrastructure	AI4 Enable operation and use.	AI5 Procure IT resources.	AI6 Manage changes.	AI7 Install and accredit solutions and changes	DS1 Define and manage service levels.	DS2 Manage third-party services.	DS3 Manage performance and capacity.	DS4 Ensure continuous service.	DS5 Ensure systems security.	DS6 Identify and allocate costs.	DS7 Educate and train users.	DS8 Manage service desk and incidents.	DS9 Manage the configuration.	DS10 Manage problems.	DS11 Manage data.	DS12 Manage the physical environment.	DS13 Manage operations.	ME1 Monitor and evaluate IT performance.	ME2 Monitor and evaluate internal control.	ME3 Ensure compliance with external requirements	ME4 Provide IT governance
1			●					●																										●
2																															●	●	
3			●		●		●																							●			
4								●																									●
5								●																						●	●		●
6			●		●		●	●						●																●	●	●	●
7		●																●		●	●									●			
8			●		●		●	●																						●	●	●	●
9																															●	●	
10																																	●

Appendice VI – I processi CobiT

Una parte importante dello scopo di questa pubblicazione è fornire ai professionisti IT una linea guida sui processi specifici che devono essere presi in considerazione per la *compliance* con Basilea II. Come sempre le aziende IT devono considerare la natura e l'estensione delle loro procedure per determinare quali degli obiettivi di controllo, controlli di esempio e test di controllo devono essere compresi nel programma di controllo interno. Basilea II non indicate requisiti obbligatori per tali obiettivi di controllo e per le relative attività di controllo. Tali decisioni sono rimesse alla discrezione ed alla valutazione di ciascuna azienda. In accordo a ciò le aziende devono valutare la natura e l'estensione dei controlli IT necessari a supportare il rischio operativo con un'analisi caso-per-caso[28]. Le interrelazioni dei quattro domini COBIT sono illustrati nella **figura 24**.

Figura 24 I quattro domini COBIT e le loro interrelazioni



I seguenti processi di controllo sono stati "mappati" rispetto agli *IT goal* ed ai processi di Basilea II.

Pianificazione ed Organizzazione (*Plan and Organize*)

PO2 Definire l'architettura informativa

La funzione dei sistemi informativi crea e regolarmente aggiorna un modello di *business information* e definisce i sistemi appropriati per ottimizzare l'uso delle informazioni.

Questo riguarda lo sviluppo di un *corporate data dictionary* con regole sulla sintassi dei dati aziendali, uno schema di classificazione dei dati e la definizione dei livelli di sicurezza. Questo processo migliora la qualità del processo di *decision making* del management rendendo sicuro ed affidabile che siano fornite le informazioni sicure e che siano razionalizzate le risorse dei sistemi informativi in modo congruo con le strategie di business.

[28] La pubblicazione ITGI "*COBIT Control Practices*" fornisce esempi di *value driver*, *risk driver* e prassi di controllo che supportano gli obiettivi di controllo che supportano i processi COBIT.

Questo processo IT è anche necessario per aumentare l'*accountability* per l'integrità e la sicurezza dei dati e per migliorare l'efficacia ed il controllo delle informazioni condivise tra le applicazioni e le funzioni organizzative.

PO4 Definire i processi IT, l'organizzazione e le relazioni

Una organizzazione IT è definita considerando i requisiti per lo staff, gli skill, le funzioni, l'*accountability*, l'autorità, i ruoli e le responsabilità, la supervisione.
Questa organizzazione è *embedded* nell'*IT process framework* che assicura trasparenza e controllo così come il coinvolgimento dei *senior executive* e del business management.
Un comitato sulla strategia assicura che il board supervisioni l'IT, uno o più *steering committee* nei quali il business e l'IT participino congiuntamente per determinare le priorità in relazione alle risorse IT in linea con le necessità di business.
Processi, politiche amministrative e procedure devono esistere per tutte le funzioni, con specifica attenzione ai controlli, alla *quality assurance*, al *risk management*, all'*information security*, alla *ownership* dei dati e dei sistemi ed alla segregazione degli incarichi.
Per assicurare un supporto tempestivo ai requisiti di business, l'IT deve essere coinvolto nei processi relativi alle decisioni rilevanti.

PO6 Comunicare gli obiettivi di management e la direzione

Il management deve sviluppare un *enterprise IT control framework* e definire e comunicare le *policy*.
Deve essere realizzato un programma di comunicazione continua per articolare la *mission*, gli obiettivi di servizio, le politiche e le procedure, eccetera, programma approvato e supportato dal management.
La comunicazione supporta il raggiungimento degli obiettivi IT ed assicura la consapevolezza e la comprensione del business e dei rischi IT, gli obiettivi e la direzione.
Il processo assicura la compliance con le leggi più rilevanti e le regolamentazioni.

PO8 Manage Quality

Deve essere sviluppato e manutenuto un *quality management system* (QMS) che include processi e standard comprovati di sviluppo ed acquisizione. Ciò è reso possibile dalla pianificazione, implementazione e manutenzione del QMS fornendo requisiti, procedure e politiche chiare e di qualità.
I requisiti di qualità sono individuati e comunicati attraverso indicatori quantificabili e raggiungibili.
Il miglioramento continuo è raggiunto sviluppando un monitoraggio ed un'analisi continua, agendo in modo corretto in caso di deviazioni e comunicando i risultati agli *stakeholder*.
La gestione della qualità è essenziale per assicurare che l'IT distribuisca valore al business, miglioramento continuo e trasparenza per gli *stakeholder*.

PO9 Assess and Manage IT Risks

Deve essere creato e manutenuto un *risk management framework*.
Il framework documenta i livelli dei rischi IT in modo comune e condiviso così come le strategie di mitigazione ed i rischi residui.
Ogni impatto potenziale degli obiettivi *goal* dell'azienda causati da eventi non pianificati è identificato, analizzato e valutato.

Sono adottate strategie di *risk mitigation* per minimizzare il rischio "residuale" ad un livello accettabile.
Il risultato dell'*assessment* è reso comprensibile agli *stakeholder* ed espresso in termini economici per rendere possibile agli *stakeholder* di allineare il rischio ad un livello accettabile di tolleranza.

Acquisire ed implementare (*Acquire and Implement*)

AI3 Acquisire e manutenere l'infrastruttura tecnologica
Le aziende hanno processi per l'acquisizione, l'implementazione e l'aggiornamento delle infrastrutture tecnologiche.
Ciò richiede un approccio pianificato all'acquisizione, manutenzione e protezione dell'infrastruttura in linea con le strategie condivise sulla tecnologia e le previsioni sugli ambienti di sviluppo e test.
Ciò assicura che esiste un supporto tecnologico continuo per le applicazioni di business.

AI4 Abilitare l'operatività e l'uso
Deve essere resa disponibile la conoscenza sui nuovi sistemi.
Questo processo richiede la produzione di documentazione e manuali per gli utilizzatori e l'ITe fornisce il training per garantire l'uso appropriato delle applicazioni e infrastrutture.

AI6 Gestione dei cambiamenti
Tutti i cambiamenti, incluso la manutenzione in emergenza e le *patch*, relativi alle infrastrutture ed applicazioni nell'ambiente di produzione sono formalmente gestiti in modo controllato.
I cambiamenti (inclusi quelli delle procedure, dei processi e dei parametri del sistema e dei servizi) sono loggati, valutati ed autorizzati prima di essere implementati e rivisti in relazione ai risultati pianificati a seguito dell'implementazione.
Ciò assicura la mitigazione dei rischi di impattare in modo negative sulla stabilità o integrità dell'ambiente di produzione.

AI7 Installare ed accreditare soluzioni e cambiamenti
I nuovi sistemi devono essere messi in produzione dopo ce lo sviluppo è stato completato.
Ciò richiede un *testing* appropriato in un ambiente dedicato con dati di test significativi, definizione del *rollout* e le istruzioni per la migrazione, la pianificazione delle *release* e la promozione in produzione nonché la *post implementation review*.
Tutto ciò assicura che i sistemi e le procedure siano in linea con le aspettative ed risultati convenuti.

Erogare e dare supporto (*Deliver and Support*)

DS1 Definire e gestire i livelli di servizio
Una comunicazione efficace tra l'IT management ed i clienti di business riguardo ai servizi richiesti è reso possibile dalla definizione documentata e condivisa dei servizi IT e dei livelli di servizio.
Questo processo comprende anche il monitoraggio ed il reporting tempestivo agli *stakeholder* sul conseguimento dei *service level*.
Questo processo permette l'allineamento tra i servizi IT ed i relativi requisiti di business.

DS2 Gestire i servizi delle terze parti
La necessità di assicurare che i servizi forniti dalle terze parti (fornitori, *vendor* e partner) soddisfino i requisiti di business richiede un processo di gestione efficiente delle terze parti.

Questo processo è reso effettivo per mezzo di regole ben definite, responsabilità e aspettative negli accordi con le terze parti così come rivedendo e monitorando tali accordi dal punto di vista dell'efficacia e della *compliance*.
Una gestione efficace dei servizi delle terze parti minimizza i rischi di business associati con fornitori *nonperforming*.

DS3 Gestire la performance e la capacità
La necessità di gestire la *performance* e la capacità delle risorse IT richiede un processo di review periodica delle performance correnti e della capacità delle risorse IT.
Questo processo include la previsione delle necessità future basata sull'*on workload, storage* e dei requisiti di *contingency*.
Questo processo fornisce l'*assurance* che le risorse informative siano di supporto ai requisiti di business e continuamente disponibili.

DS4 Assicurare i servizi nel continuo
La necessità di fornire servizi IT continui richiede di sviluppare, manutenere e testare i piani di IT continuity; utilizzando *backup storage offsite* e fornendo formazione in continuo sui piani di *continuity*.
Un processo efficace di servizi continui minimizza la probabilità e l'impatto dell'interruzione dei principali servizi IT relativi alle funzioni ed ai processi chiavi del business.

DS5 Assicurare la sicurezza dei sistemi
La necessità di garantire l'integrità delle informazioni e di proteggere gli asset IT richiede un processo di gestione della sicurezza.
Questo processo consiste nello stabilire e mantenere regole, responsabilità, politiche, standard e procedure di sicurezza IT.
La gestione della sicurezza comprende anche sviluppare il monitoraggio della sicurezza, condurre test periodici ed implementare azioni correttive per le debolezze o gli incidenti di sicurezza noti.
Una gestione efficace della sicurezza protegge tutti gli asset IT e minimizza l'impatto di business delle vulnerabilità ed incidenti di sicurezza.

DS9 Gestire la configurazione
Assicurare l'integrità delle configurazioni hardware e software richiede di stabilire e mantenere un accurato e completo *configuration repository*.
Questo processo include la raccolta delle informazioni sulla configurazione iniziale, stabilire le *baseline*, verificare e fare l'audit delle informazioni sulla configurazione ed aggiornare il *configuration repository* quando necessario.
Una gestione efficace della configurazione permette una maggiore disponibilità dei sistemi, minimizza le problematiche della produzione e risolve i problemi in modo più veloce.

DS10 Gestire i problemi
Un *problem management* efficace richiede l'identificazione e la classificazione dei problemi , l'analisi delle cause profonde e la risoluzione dei problemi stessi.
Il processo di *problem management* comprende anche la formulazione di raccomandazioni per il miglioramento, la manutenzione delle registrazioni dei problemi e la *review* dello status delle azioni correttive.
Un processo efficace di *problem management* massimizza la disponibilità del sistema, migliora i livelli di servizio, riduce i costi e migliora la *customer convenience* e *satisfaction*.

DS12 Gestire l'ambiente fisico

La protezione delle infrastrutture, dei computer e delle persone richiede *physical facility* ben progettate e ben gestite.
Il processo di gestione dell'ambiente fisico comprende la definizione dei requisiti del sito fisico, la selezione delle appropriate *facility* ed il disegno di processi efficaci per monitorare i fattori ambientali e gestire gli accessi fisici.
La gestione efficace dell'ambiente fisico reduce le interruzioni di business causate da danni all'equipaggiamento dei computer e del personale.

Monitorare e valutare (*Monitor and Evaluate*)

ME1 Monitorare e valutare le performance IT
Una gestione efficace della performance IT richiede un processo di monitoraggio.
Questo processo include di definire indicatori di performance rilevanti, di fare il report della performance in modo sistematico e puntuale e di agire in modo rapido a fronte delle deviazioni.
Il monitoraggio è necessario per essere sicuri che sinao fatte le cose giuste e che siano fatte in modo coerente con le direzioni e le politiche definite.

ME2 Monitorare e valutare i controlli interni
Realizzare un programma efficace di controlli interni per l'IT richiede un processo di monitoraggio ben definito.
Questo processo include il monitoraggio e reporting delle eccezioni al controllo, i risultati dei *self-assessment* e la *review* delle terze parti.
Un beneficio chiave del monitoraggio del controllo interno è fornire l'*assurance* in relazione all'uso efficace ed efficiente delle procedure e la *compliance* con le leggi ed i regolamenti di riferimento.

ME3 Assicurare la *compliance* con i requisiti esterni
Una supervisione efficace della *compliance* richiede lo stabilire un processo di *review* per assicurare la *compliance* con leggi, regolamenti e requisiti contrattuali.
Questo processo comprende l'identificazione dei requisiti di *compliance*, l'ottimizzazione e la valutazione della risposta, ottenere l'*assurance* che i requisiti siano stati rispettati, ed, infine, l'integrazione del reporting di IT *compliance* con il resto del business.

ME4 Assicurare la *IT Governance*
Realizzare un framework di *governance* efficace comporta definire le strutture organizzative, i processi, la *leadership*, i ruoli e le responsabilità per assicurare che gli investimenti IT dell'azienda siano allineati ed erogati in accordo alle strategie ed obiettivi aziendali.
Altri processi di controllo definiti all'interno di COBIT che non sono stati mappati né agli *IT goal* relativi a Basilea II né ai processi di Basilea II devono essere considerati come parte del processo che stabilisce i controlli IT generali.

Pianificazione ed Organizzazione (*Plan and Organize*)

PO1 Definire un piano IT strategico
È necessaria una pianificazione strategica IT per gestire e indirizzare tutte le risorse IT in linea con la strategia di business e le priorità.
La funzione IT ed i *business stakeholder* sono responsabili di assicurare che un valore ottimale sia realizzato a partite dai progetti e dai *portfolio* dei servizi.

La pianificazione strategica migliora la comprensione degli *stakeholder* chiave riguardo le opportunità ed i limiti dell'IT, le valutazioni delle attuali performance, l'identificazione della capacità e dei requisiti legati alle risorse umane e fa chiarezza sul livello di investimenti richiesti.
La strategia di business e le priorità si devono reflettere nei *portfolio* ed esser eseguiti per mezzo di piani IT tattici che specificano gli obiettivi di sintesi, gli *action plan* ed i compiti che devono essere compresi ed accettati sia dal business sia dall'IT.

PO3 Determinare la direzione della tecnologia
La funzione di *information service* determina la direzione della tecnologia per supportare il business.
Ciò richiede la creazione di un piano delle infrastrutture ed un "*architecture board*" che definisca e gestisca chiare e realistiche aspettative di cosa la tecnologia può offrire in termini di prodotti, servizi ed i meccanismi di *delivery*.
Il piano deve essere regolarmente aggiornato e comprendere aspetti quali l'architettura del sistema, la direzione della tecnologia, i piani di acquisizione, gli standard, la strategia di migrazione di *contingency*.
Ciò facilita le risposte tempestive ai cambiamenti nell'ambiente competitivo, le economie di scala per lo *staffing* e gli investimenti dei sistemi informativi ed il miglioramento dell'interoperabilità delle piattaforme e delle applicazioni.

PO5 Gestione degli investimenti IT
Deve essere realizzato e manutenuto un framework per gestire i programmi degli investimenti *IT-enabled* che tiene conto dei costi, benefici, priorità, budget e comprende un processo formale di *budgeting* e di gestione del *budget*.
Gli *stakeholder* sono consultati per identificare e controllare i costi totali ed i benefici nel contesto dei piani IT strategici e tattici e dar inizio alle azioni correttive dove necessario.
Il processo incoraggia la *partnership* tra IT e *business stakeholder*; abilita l'uso efficiente ed efficace delle risorse IT, garantisce trasparenza ed *accountability* riguardo al *total cost of ownership* (TCO), la realizzazione dei benefici di business ed il ritorno degli investimenti (*return on investment* - ROI) degli investimenti *IT-enabled*.

PO7 Gestione delle risorse umane IT
È acquisita e mantenuta un *competent workforce* per la creazione ed il *delivery* dei servizi IT al business.
Ciò è raggiunto rispettando prassi definite e condivise che supportano il *recruiting*, *training*, valutazione delle performance, le promozioni e la fine dei rapporti di lavoro.
Questo processo è critico, dato che le persone sono un asset importante, e la *governance* e l'ambiente di controllo interno sono pesantemente dipendenti dalla motivazione e competenza del personale.

PO10 Gestione dei progetti
È instaurato un *program* e *project management framework* per la gestione di tutti i progetti IT.
Il framework assicura il rispetto delle priorità corrette e la coordinazione di tutti i progetti.
Il framework include un *master plan*, l'assegnazione delle risorse, la definizione dei *deliverable*, approvati dagli utilizzatori, un approccio per fase per il *delivery*, *Quality Assurance*, un piano formale di *testing* e la *postimplementation review* dopo l'installazione per assicurare il *project risk management* ed il *value delivery* al business.
Questo approccio reduce il rischio di costi inattesi e della cancellazione dei progetti, migliora la comunicazione ed il coinvolgimento del business e degli utenti finali, assicura il valore e la qualità dei deliverable dei progetti e massimizza il loro contributo ai programmi di investimento *IT-enabled*

Acquisire ed implementare (*Acquire and Implement*)

AI1 Identificare le soluzioni automatizzate
La necessità di una nuova applicazione o funzione richiede un'analisi prima dell'acquisizione o dello sviluppo per assicurare che i requisiti di business siano soddisfatti con un approccio efficace ed efficiente.
Questo processo copre la definizion e delle necessità, la considerazione delle possibili fonti alternative, la *review* della fattibilità tecnologica ed economica, l'esecuzione della *risk analysis* e dell'analisi costi-benefici e la decisione finale di sviluppare ("*make*") o comprare ("*buy*").
Tutti questi prassi rendono capaci le aziende di minimizzare il costo di acquisizione ed implementazione che assicurano che il business può raggiungere gli obiettivi.

AI2 Acquisire e manutenere il software applicativo
Le applicazioni devono essere rese disponibili in linea con i requisiti di business.
Questo processo copre il *design* delle applicazioni, l'inclusione corretta dei controlli applicative e dei requisiti di sicurezza e lo sviluppo e configurazione secondo gli standard.
Ciò permette alle aziende di supportare in modo corretto le operazioni di business per mezzo di applicazioni automatizzate corrette.

AI5 Procurare le risorse IT
Devono essere disponibili le "giuste" risorse IT, comprese le persone, l'hardware, il software ed i servizi.
Ciò richiede la definizione e l'imposizione delle procedure di *procurement*, la selezione dei *vendor*, la definizione degli accordi contrattuali e l'acquisizione stessa delle risorse.
Fare ciò assicura all'azienda di avere tutte le risorse IT richieste in modo tempestivo e ai giusti costi.

Erogare e dare supporto (*Deliver and Support*)

DS6 Identificare ed allocare i costi
La necessità di una sistema corretto ed equilibrato per allocare i costi IT rispetto al business richiede misurazioni accurate dei costi IT ed un accordo con gli utilizzatori del business sulla corretta allocazione.
Questo processo include la costruzione e la messa in opera di un sistema che raccolga, allochi e produca il report dei costi IT rispetto agli utilizzatori dei servizi.
Un sistema corretto di allocazione abilita il business a prendere decisioni informate che riguardano l'uso degli IT *service*.

DS7 Formare gli utilizzatori
Una formazione efficace di tutti gli utenti dei sistemi IT, inclusi coloro che lavorano nell'IT, richiede l'identificazione delle necessità di training di ciascun gruppo di utilizzatori.
In aggiunta all'identificazione delle necessità, questo processo comprende la definizione e l'esecuzione di una strategia per un training efficace e per la misurazione dei risultati.
Un programma efficace di training aumenta l'uso efficace della tecnologia riducendo gli errori degli utilizzatori, aumentando la produttività ed aumentando la *compliance* con i controlli chiave, ad esempio le misure di sicurezza dell'utente.

DS8 Gestione del "*Service Desk*" e degli incidenti

Per garantire risposte tempestive ed efficaci ai problemi degli utenti IT è necessario aver progettato un buon "*service desk*" ed avere un processo di gestione degli incidenti.
Questo processo comprende la costituzione di una funzione di *service desk* che preveda la registrazione dell'incidente, l'*incident escalation*, analisi dei trend e delle cause "profonde" e la loro risoluzione.
I benefici di business comprendono una maggiore produttività grazie alla rapida risoluzione delle richieste degli utenti.
In aggiunta il business può gestire le cause "profonde" (ad esempio il training non sufficiente degli utenti) per mezzo di un reporting efficace.

DS11 Gestione dei dati
Una gestione efficace dei dati richiede una preliminare identificazione dei requisiti sui dati.
Il processo di gestione dei dati comprende anche lo stabilire una procedura efficace di gestione della *media library*, dei back up e del *recover data* ed una corretta conservazione dei supporti.
Una gestione efficace dei dati facilità la qualità, la disponibilità e la tempestività dei dati necessari al business.

DS13 Gestione delle procedure (*Operation*)
Un *processing* completo ed accurato dei dati richiede una gestione efficiente delle procedure di *data processing* ed un'accurata manutenzione dell'hardware.
Questo processo include la definizione delle policy operative e delle procedure per una gestione efficace del processo di schedulazione, della protezione degli output "sensibili", il monitoraggio delle performance delle infrastrutture, la manutenzione preventiva dell'hardware.
La gestione efficace delle procedure (*operation*) aiuta a mantenere la *data integrity* e riduce i ritardi del business ed i costi delle operazioni IT.

Appendice VII- ABC Bank: un esempio concreto

L'obiettivo di questo esempio è dimostrare il processo che si può adottare quando si valutano e misurano i rischi. L'esempio si limita all'organizzazione IT e ad un singolo rischio. Nella realtà il processo di gestione del *risk assessment* dovrebbe essere a livello generale di azienda e dovrebbe essere integrato con la gestione degli altri rischi e con i programmi già esistenti.

ABC Bank vuole gestire i rischi associati con la "frode interna". Si è determinato che la *risk tolerance* associata con la frode interna è bassa. La probabilità della frode materiale è considerata bassa mentre l'impatto potenziale sulla reputazione della banca e sui costi associati al mancato rispetto della compliance alle regolamentazioni è considerato alto. Questi processi gestiscono anche il rischio associato con le frodi esterne, la distruzione del business, l'indisponibilità dei sistemi informativi: tutti fattori che possono aumentare l'impatto del "fallimento" del controllo.

Gli aspetti IT associati con la frode interna sono mostrati nella **figura 25**.

Figura 25 Aspetti IT associati con la frode interna

Event Types di Basilea II	Aspetti IT	Processi COBIT
Frode interna	• Manipolazione deliberata dei programmi • Uso non autorizzato delle funzioni di modifica • Manipolazione deliberata delle istruzioni di sistema • Manipolazione deliberata dell'hardware • Modifiche deliberate dei sistemi e dei dati applicativi per mezzo di hacking • Uso/copia di software non autorizzato o non licenziato • Elusione delle regole relative ai privilegi di accesso ai sistemi	• PO6 • DS5 • DS9 • DS12

ABC Bank ha utilizzato il materiale e gli strumenti metodologici forniti da COBIT che sono in relazione alla "frode interna" per definire gli obiettivi, considerare le soluzioni possibili e stabilire le metriche di performance come segue.

PO6 Comunicare gli obiettivi di management e la direzione
ABC ha preso in considerazione PO6 che recita:

> *Il management realizza un* enterprise IT control framework *e definisce e comunica le relative policy. Deve essere realizzato un programma continuo di comunicazione per articolare la* mission*, gli obiettivi di servizio, le* policy *e procedure, eccetera, approvate e supportate dal management. La comunicazione è fondamentale per il raggiungimento degli obiettivi IT ed assicura la consapevolezza (*awareness*) e la comprensione del business e dei rischi IT, degli obiettivi e della direzione strategica. Il processo assicura la* compliance *con le leggi e le regolamentazioni più rilevanti.*

Sono date considerazioni anche nell'ITGP6 *Control and Mitigation Policies, Processes, Procedures*, che recita:

> *I sistemi informativi e l'infrastruttura tecnologica devono essere governati da un insieme adeguato di* policy*, processi e procedure per il controllo del rischio e la sua mitigazione. Le linee guida date ai professionisti, internal auditor ed esperti di servizi finanziari devono essere in linea con il framework GRC dell'azienda.*

I COBIT *maturity level* sono stati rivisti per avere ausilio nello stabilire gli obiettivi. Gli aspetti dei *maturity level* considerati come rilevanti sono stati:

- Maturity level 3 – Definito:
  - Deve essere sviluppato un ambiente di controllo completo delle informazioni e di gestione della qualità, documentato e comunicato al management, ambiente che comprende ed include un *framework* per le politiche, i piani e le procedure.
  - Il processo di sviluppo delle policy è strutturato, manutenuto e noto allo staff, e le politiche esistenti, i piani e le procedure sono ragionevolmente affidabili e coprono le principali problematiche.
  - Il management comprende l'importanza della "sensibilizzazione" in tema di sicurezza (*IT security awareness*) e gestisce programmi ed iniziative di *awareness*.
  - Le tecniche per promuovere la *security awareness* sono state standardizzate e formalizzate.
- Maturity level 4 – Gestito e Misurabile:
  - Il management accetta la responsabilità di comunicare le politiche di controllo interno e delega la responsibilità ed alloca sufficienti risorse per mantenere l'ambiente in linea con i cambiamenti più significativi.
  - È stabilito un ambiente di controllo "positivo", proattivo, che prevede il *commitment* alla qualità e alla *IT security awareness*.
  - È realizzato, manutenuto e comunicato un insieme completo di policy, piani e procedure che tiene conto anche delle "buone pratiche" interne.
  - È stabilito un framework per il rilascio delle procedure (*rollout*) che comprende i controlli di *compliance*.
- Maturity level 5 - ottimizzato:
  - L'ambiente di controllo informativo è allineato con il framework strategico del management e la relativa *vision* ed è frequentemente rivisto ed aggiornato e continuamente migliorato.
  - Il monitoraggio, il *self-assessment* ed i controlli di *compliance* sono pervasivi in tutta l'azienda.
  - La tecnologia è usata per mantenere la base di conoscenza relative alle *policy* e all'*awareness* e per ottimizzare la comunicazione, usando strumenti di office automation e strumenti di training *computerbased*.

Le caratteristiche chiavi delle soluzioni di comunicazione sono considerate le seguenti:

- Essa deve tenere in considerazione le "buone pratiche" e quelle desiderate (ma non le *best practices* che non possono essere conseguite).
- Essa deve essere integrata in una soluzione organica e generale di comunicazione.
- Non deve essere eccessivamente costosa o richiedere tempi troppo impegnativi.
- Deve essere letta e compresa così che se ne possa dimostrare la conformità alle regole stabilite.
- La compliance deve essere misurabile.

La soluzione presa in considerazione può comprendere i seguenti elementi:

- una *review* dell'estensione e della rilevanza delle *policy* e procedure esistenti; dove sono individuati *gap*, *policy* e procedure devono essere aggiornate o devono essere redatte nuove *policy* e procedure;
- Una *policy* deve essere sottoposta ad una *review* annuale che prevede una approvazione formale delle *policy* e delle procedure.
- Tutte le policy e procedure devono essere disponibili sulla intranet.
- A tutti i membri dello staff deve essere richiesto di prendere parte ad una sessione di aggiornamento basato su intranet sulle modifiche alle *policy* e procedure. La sessione dovrebbe includere un esame automatizzato di verifica della comprensione degli aggiornamenti e sulle componenti più significative delle *policy* e delle procedure. Il test dovrebbe prevedere un voto minimo per essere superato.

Inoltre devono essere introdotte le seguenti misurazioni:

- numero di *policy* e procedure non riviste e non sottoscritte oltre un mese dopo la *deadline* prevista dalla approvazione annuale;
- numero e percentuale dei membri dello staff che non hanno completato in modo soddisfacente il corso di aggiornamento basato su intranet entro due settimane dalla *deadline* prevista;
- i risultati degli esami distribuiti per percentuale rispetto al numero di domande con risposte non corrette.

DS5 Assicurare la sicurezza dei sistemi informativi

Quanto segue deve essere integrato con il piano di sicurezza generale. L'intento di questo esempio è di mostrare come implementare un piano di sicurezza. Lo scopo è mostrare gli aspetti del processo sottostante.

DS5 recita come segue:

> *La necessità di mantenere l'integrità delle informazioni e proteggere gli asset IT richiede un processo di gestione della sicurezza. Questo processo include lo stabilire e mantenere regole sulla sicurezza IT nonché responsabilità,* policy, *standard e procedure. La gestione della sicurezza include anche effettuare il monitoraggio della sicurezza , effettuare test periodici ed implementare le azioni correttive per le debolezze identificate o per gli incidenti rilevati. Una efficace gestione della sicurezza protegge tutti gli asset IT e minimizza l'impatto sul business delle vulnerabilità ed incidenti di sicurezza.*

I COBIT *maturity level* sono stati rivisti per avere assistenza nello stabilire gli obiettivi. Gli aspetti dei *maturity level* considerati come rilevanti sono stati:

- Maturity level 4 - Gestito e Misurabile:
  - le responsabilità per la sicurezza IT sono chiare, gestite e rese obbligatorie;
  - l'analisi dei rischi IT e dei relativi impatti è sviluppata in modo coerente e completo;
  - le politiche di sicurezza e le procedure sono completate in specifiche "*security baseline*";
  - è obbligatorio adottare metodi che promuovono la consapevolezza verso al sicurezza (*security awareness*);
  - l'identificazione, l'autenticazione e l'autorizzazione degli utenti è standardizzata;
  - i test di sicurezza sono completati usando processi e standard formalizzati che portano ad un miglioramento dei livelli di sicurezza;
  - i processi di sicurezza IT sono coordinate con la funzione di sicurezza generale dell'azienda;

  - il *reporting* della sicurezza IT è collegato agli obiettivi di business;
  - il *training* della sicurezza IT è condotto sia in ambito business sia in ambito IT;
  - il *training* della sicurezza IT è pianificato e gestito in modo che risponda alle necessità di business e ai profili di rischio che sono stati definiti.
- Maturity level 5 – Ottimizzato:
  - la sicurezza IT è una responsabilità condivisa tra il management del business e dell'IT e deve essere integrata con gli obiettivi di sicurezza a livello di *corporate*;
  - i requisiti della sicurezza IT sono chiaramente definiti, ottimizzati e inclusi nel piano di sicurezza;
  - gli utenti ed i clienti sono *accountable* in maniera incrementale per la definizione dei requisiti di sicurezza e le funzioni di sicurezza sono integrate con le applicazioni già nella fase di *design*;
  - gli incidenti di sicurezza sono prontamente gestiti con procedure di gestione degli incidenti formalizzate e supportate da *tool* automatizzati;
  - sono condotti *security assessment* periodici per valutare l'efficacia dell'implementazione dei piani di sicurezza;
  - le minacce alle informazioni e le vulnerabilità sono raccolte ed analizzate in modo sistematico;
  - adeguati controlli per mitigare i rischi sono prontamente comunicati ed implementati;
  - i test di sicurezza, l'analisi delle "cause profonde" degli incidenti di sicurezza e l'identificazione proattiva dei rischi sono usati per il miglioramento continuo dei processi;
  - i processi di sicurezza e le relative tecnologie sono integrate a livello di intera azienda;
  - le metriche per la gestione della sicurezza sono misurate, raccolte e comunicate;
  - il management usa misure condivise per calibrare il piano di sicurezza nel processo di miglioramento continuo.

L'illustrazione dei dettagli della soluzione prescelta va oltre lo scopo di questa pubblicazione; va tuttavia sottolineato quanto segue:

- l'uso dei concetti di ISO 27000, inclusa la certificazione, la valutazione indipendente ed il *self-assessment*;
- lo sviluppo di una strategia di sicurezza; realisticamente non è possibile tenere sotto controllo ogni evento potenziale di tutti gli aspetti della infrastruttura tecnologica e sociale (ad esempio gli eventi di *social engineering*). Le componenti più importanti dell'infrastruttura ed I relative eventi devono però essere monitorati per essere identificati;
- le tipologie di eventi devono essere classificati; gli eventi più importanti devono immediatamente essere segnalati per mezzo di telefono cellulare ed e-mail al servizio centralizzato delle *operation*; gli eventi meno importanti possono essere segnalati semplicemente per e-mail, anche in forma complessiva sintetizzate per giorno e non in modo individuale; tali eventi meno importanti possono non essere registrati o possono essere loggati ma non segnalati o possono essere segnalati in report periodici di sintesi per permettere l'analisi dei trend;
- va fatto il monitoraggio degli eventi esterni che potrebbero essere usati per favorire le frodi interne cioè l'individuazione di debolezze nei *package* di sicurezza.

COBIT fornisce i seguenti esempi di misurazioni che possono essere prese in considerazione; come sempre tuttavia le reali misure da intraprendere dipendono dalle caratteristiche proprie di ogni organizzazione:

- numero dei sistemi in cui I requisiti di sicurezza non sono soddisfatti;
- numero e tipo delle violazioni di accesso sospette e reali;

- numero delle violazioni della segregazione di incarichi incompatibili;
- percentuali di utilizzatori che non sono conformi con gli standard delle password;
- numero e tipo dei codici maligni che sono stati bloccati;
- frequenza e *review* del tipo di eventi di sicurezza che devono essere monitorati;
- numero e tipo degli *account* obsoleti;
- numero degli indirizzi IP non autorizzati, porte e tipo di traffico non permesso;
- percentuali di chiavi di crittografia compromesse e revocate;
- numero di diritti di accesso autorizzati, revocati, resettati o modificati.

Queste misurazioni devono includere gli obiettivi misurabili ed i progressi, se misurabili, verso gli obiettivi.

DS9 Gestire la configurazione

DS9 recita:

> *Assicurare l'integrità della configurazione dell'hardware e del software richiede di stabilire e mantenere un* configuration repository *curato e completo. Questo processo prevede di raccogliere e registrare le informazioni sulla configurazione iniziale, di stabilire* delle baseline*, di verificare e auditare le informazioni di configurazione e di aggiornare, se necessario, il* configuration repository*. La gestione efficace del* configuration management *facilita la disponibilità dei sistemi, minimizza i problemi di produzione e risolve i problemi in maniera più veloce.*

I COBIT *maturity level* sono stati analizzati per avere assistenza nel conseguire tali obiettivi. Gli aspetti del *maturity level* che sono stati considerati rilevanti sono:

- Maturity level 4 – Gestito e Misurabile:
  - La necessità di gestire la configurazione è riconosciuta a tutti i livelli dell'azienda e le relative "buone pratiche" continuano a svilupparsi;
  - procedure e standard sono comunicati ed incorporate nel training e le deviazioni sono monitorate, tracciate e oggetto di reporting;
  - tools automatizzari, quail la *push technology*, sono utilizzati per rinforzare gli standard e migliorare la stabilità;
  - i sistemi di *configuration management* prendono in considerazione la maggior parte degli asset IT e permettono un appropriato *release management* e controllo della distribuzione;
  - l'analisi delle eccezioni, così come le verifiche "fisiche", sono applicate in modo coerente e sono investigate le loro "cause profonde".
- Maturity level 5 - Ottimizzato:
  - i report di *baseline* audit forniscono i dati essenziali sull'hardware e software data per riparare, dare servizio, dare garanzia, aggiornare e fare *assessment* tecnologici di ciascuna singola unità;
  - sono forzate le regole per limitare l'installazione di software non autorizzato;
  - il tracciamento e monitoraggio dei singoli asset IT proteggono dal furto, dall'errato utilizzo e dall'abuso;

La soluzione presa in considerazione può comprendere i seguenti elementi:

- usare/copiare software non licenziato o non autorizzato - server e workstation devono essere periodicamente analizzati per verificare la presenza di software non licenziato o non autorizzato o tipi di file non identificati;

- workstation “invisibili” o utilizzo di *device*s non autorizzati - le workstation devono essere messe a confronto con un inventario centralizzato delle workstation e le discrepanze analizzate; devono essere sviluppati standard e forzate le regole comuni per tutti i *device* collegati al network (ad esempio un *home computer* deve avere un sistema di antivirus aggiornato ed autorizzato).

COBIT fornisce i seguenti esempi di misurazioni che possono essere prese in considerazione; tuttavia ogni azienda deve valutare quali misure sono più adatte alle proprie caratteristiche:

- numero di problematiche di *compliance* emerse a causa di una impropria configurazione degli asset;
- numero di “deviazioni” identificate tra il *configuration repository* e le configurazioni effettive degli asset;
- percentuale di licenze acquistate e non “conteggiate” per il *repository*.

Inoltre si può anche considerare:

- numero dei prodotti licenziati installati;
- numero dei prodotti licenziati installati sulle workstation che devono essere usati solo come server;
- numero di prodotti installati che risultano non standard e potenzialmente non licenziati;
- reporting per area geografia e dipartimento.

Appendice VIII – Referenze

Accord Implementation Group (Operational Risk) (AIGOR), "*Observed Range of Practice in Key Elements of Advanced Measurement Approaches* (AMA)", ottobre 2006
Bank Systems and Equipment, "*Basel II Converges With Business Performance*", ottobre 2004
Basel Committee on Banking Supervision, *Principle 1 - Framework for Internal Control Systems in Banking Organisations*, settembre 1998
Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*, giugno 2004, www.bis.org/publ/bcbs107.htm, e giugno 2006, www.bis.org/publ/bcbs128.htm
Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, febbraio 2003, www.bis.org/publ/bcbs91.htm
BearingPoint, "*Basel II Operational Risks*", giugno 2005
BearingPoint, "*Data Quality: A Stumbling Block to Basel Compliance*", marzo 2006
British Standards Institution (BSI), BS 25999-1 "*Business Continuity Management*", 2006
British Standards Institution (BSI), PAS 77 "*IT Service Continuity Management*", 2006
Business Continuity Institute (BCI), *Good Practice Guidelines for Business Continuity Management*, terza edizione, 2007
COSO, *Enterprise Risk Management - Integrated Framework*, settembre 2004, www.coso.org/publications.htm
International Organization for Standardization (ISO), ISO 27001 "*Information Security Management Systems - Code of Practice*", 2006
IT Governance Institute, *COBIT 4.1*, USA, 2007 (fonte della figura 14.)
IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, seconda edizione, 2006 (fonte della figura 8.)
Joint Forum, "*High-level principles for Business Continuity*", agosto 2006
KPMG Financial Services, "*Basel II - A Closer Look: Managing Operational Risk,*" 2003 (fonte delle figure 4 e 13.)
Office of Government Commerce (OGC), *IT Infrastructure Library*® (ITIL), UK
Paisley Consulting, "*The Case for Operational Risk Management*", febbraio 2006
PricewaterhouseCoopers, "*Basel II: Making It Work for You*", marzo 2004
Symantec, "*Risk Management Challenge and Basel II*", maggio 2006

Leading the It Governance Community

3701 ALGONQUIN ROAD, SUITE
1010
ROLLING MEADOWS, IL 60008 USA
PHONE: +1.847.660.5700
FAX: +1.847.253.1443
E-MAIL: *info@itgi.org*
WEB SITE: *www.itgi.org*