

Convegno

LA CRISI FINANZIARIA E LA GESTIONE DEI RISCHI NEGLI INTERMEDIARI FINANZIARI

*Il ruolo della Funzione Controllo Rischi
nel percorso di Basilea 3*
Centro Studi - I CAPPUCCINI

San Miniato, 13 maggio 2011



Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparency



Importance of Internal Governance & purpose of the Guidebook

Il contesto

La fiducia nel sistema bancario è determinante per il suo corretto funzionamento e costituisce un prerequisito al suo effettivo contributo nell'ambito del sistema economico.

Negli ultimi dieci anni, le questioni inerenti le politiche di un corretto governo societario delle banche hanno interessato sempre di più i vari organismi internazionali in quanto, se è vero che le politiche errate non sono state la causa della recente crisi finanziaria, è anche vero che esse sono state identificate tra gli elementi chiave che hanno contribuito al suo sviluppo.

Il Comitato di Basilea (BCBS) ha pubblicato delle Guideline* iniziali in materia nel 1999, poi riviste nel 2006. I principi stabiliti nel 2006 hanno interessato soprattutto i seguenti aspetti.

- ✓ l'efficace coinvolgimento del Consiglio di Amministrazione nel processo di approvazione delle strategie della banca;
- ✓ la definizione ed il rafforzamento di linee di responsabilità chiare nell'ambito del sistema organizzativo;
- ✓ la definizione di politiche di remunerazione legate ad obiettivi di rendimento di lungo termine;
- ✓ il principio secondo il quale i rischi sottesi (e spesso poco trasparenti) nell'operatività quotidiana debbano essere adeguatamente gestiti.

Nonostante le linee guida del 2006, durante la crisi finanziaria del 2007, tali modelli di governance si sono rivelati non adeguati.

* Rif: "Enhancing Corporate Governance for Banking Organisations, Basel Committee on Banking Supervision, September 1999 and February 2006"

Importance of Internal Governance & purpose of the Guidebook

A fine 2009, il CEBS ha promosso una indagine sullo stato di applicazione da parte delle autorità di Vigilanza e degli istituti bancari delle Linee Guida sul governo societario del 2006 ed è emerso che, nonostante la regolamentazione emanata dalle Autorità di Vigilanza, inerenti la politica di governo societario, fosse esaustiva, la sua effettiva applicazione era frammentata ed evidenziava molteplici gaps. In particolare emerse:

- ✓ una eccessiva complessità organizzativa e rischiosità dei prodotti non bilanciate da idonee politiche di governance interna (strutture poco trasparenti, prodotti e mercati troppo rischiosi, gruppi cross-border, ecc)
- ✓ una carenza del management nell'attività di supervisore e organo di controllo (non in grado quindi di contrastare l'assunzione eccessiva dei rischi)
- ✓ sistemi di risk management e dei controlli interni non integrati con le altre unità di business aziendali e/o di gruppo.

A ottobre 2010 il BCBS emana i nuovi principi di corporate governance (*Principles for enhancing corporate governance* – documento in consultazione già al marzo dello stesso anno).

Il 13 ottobre 2010 il CEBS ha consolidato tutte queste Guidelines nel *Guidebook on Internal Governance* , che rivede e unisce i documenti sulle politiche retributive (*High Level Principles on Remuneration*, aprile 2009, e *High Level Principles on Risk Management*, febbraio 2010).

Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparency



Concepts used in the Guidebook

- **Governo societario** - è un vasto concetto che può essere descritto come l'insieme di relazioni tra un istituto, il suo management, i suoi azionisti e gli altri stakeholders. La governance interna è una componente limitata ma cruciale della corporate governance, che si focalizza sulle strutture interne e sull'organizzazione di un istituto.
- **Internal governance** - nella comunità europea è disciplinata all'art. 22 della Direttiva 2006/48/EC, che richiede che "ogni istituto di credito deve avere delle robuste e trasparenti disposizioni di governance, delle linee di responsabilità coerenti, dei processi efficaci di identificazione, gestione, monitoraggio e report dei rischi a cui è o potrebbe essere esposto e degli adeguati meccanismi di controllo interno, ivi compreso delle procedure di amministrazione e contabilità". Negli Stati Membri esistono sia sistemi societari monistici che dualistici, il documento parla quindi di "management body" che - nei sistemi monistici coincide con il consiglio di amministrazione, in quelle dualistiche si distingue tra organo di governo e organo di supervisione. Il Guidebook non indica la struttura di governo migliore né a quale degli organi di governo o di supervisione debbano andare determinate responsabilità ma stabilisce il principio per cui tali responsabilità debbano essere complessivamente attribuite, ovvero:
 - identificazione, valutazione, misurazione, monitoraggio, mitigazione e report dei rischi attuali e potenziali
 - sistema di controlli interni e di controllo dei rischi
 - prudente condotta degli affari
 - robusto sistema informativo e disclosure
 - conformità alla normativa esterna e interna

Il "management body" deve avvalersi delle funzioni di controllo che sono il Risk Management, la Compliance e l'Internal Audit (indipendenti dalla unità che controllano).

Concepts used in the Guidebook

- **Risk tolerance/appetite** - questo termine abbraccia tutte le definizioni rilevanti usate dai diversi istituti e dalle autorità di vigilanza. Mentre alcuni utilizzano il termine risk tolerance per descrivere l'ammontare di rischio che un istituto intende accettare, altri utilizzano il termine risk appetite per fare una distinzione tra i rischi assoluti che l'istituto è disposto ad accettare *a priori* (risk appetite) ed i limiti effettivi di risk appetite che l'istituto persegue (risk tolerance).



Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparency



Implementation of the Guidebook

- **Lo scopo del Guidebook** è di armonizzare le aspettative della Autorità di Vigilanza e di promuovere la regolamentazione della governance interna, specialmente negli istituti più grandi e complessi. I principi contenuti nel Guidebook devono essere considerati sia da parte degli istituti che delle autorità di vigilanza nell'ambito di uno schema di review da parte del supervisore sotto il Pillar 2. Essi devono essere implementati dagli istituti come parte integrante del loro processo interno di valutazione dell'adeguatezza di capitale (ICAAP) e rivisto da parte delle Autorità di Vigilanza nell'ambito del processo di SREP.
- **La proporzionalità** – come emerso dalle CRD – vale per tutte le linee guida contenute in questo Guidebook. Un istituto deve dimostrare come il suo approccio, nell'attuare i principi guida richiesti dal Guidebook, rispetti la natura, la dimensione e la complessità delle sue attività (non esiste un approccio "one size fits all").
- Con l'adozione e la pubblicazione del Guidebook verranno sovrascritte le altre guidelines precedenti riguardanti i medesimi argomenti;
- il CEBS si aspetta che i suoi membri implementino il Guidebook on Internal Governance e lo incorporino nelle loro procedure di supervisione (SREP) entro il **30 settembre 2011**.

Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparenza

Corporate Structure and organisation

- **Il “Management body”** deve garantire una struttura di governo proporzionata/adatta all’azienda e trasparente. La struttura deve promuovere e dimostrare l’esistenza di una **gestione efficace e prudente** a livello individuale e/o di gruppo. Le linee di reporting e l’allocazione delle responsabilità e dell’autorità all’interno di un istituto devono essere chiare, ben definite, coerenti e fatte rispettare.
- **In un gruppo**, il “Management body” della capogruppo ha la piena responsabilità dell’adeguatezza della governance di gruppo e si assicura che la struttura di governo sia appropriata alle dimensioni, al business e ai rischi del gruppo e delle sue componenti.
- **“Conosci la tua struttura”** - il “Management body” deve conoscere/comprendere pienamente la propria struttura organizzativa ed assicurarsi che sia in linea con la strategia di business adottata e con il proprio profilo di rischio.
- **Attività non standard e non trasparenti** - laddove un istituto operi attraverso strutture “special purpose” o attraverso strutture collegate o in giurisdizioni che impediscano la trasparenza o dove non vengono rispettati gli standard internazionali del settore bancario, il “Management body” deve capire il loro scopo/mission e la loro struttura e i rischi associati a tali società. Il management deve accettare tali attività solo quando è sufficientemente convinto che i rischi connessi siano governabili.

Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparency



Management body

- **Responsabilità del "Management body"** - il "Management body" ha la piena responsabilità dell'istituto e stabilisce/determina la strategia e il risk appetite dello stesso. Le responsabilità del management deve essere ben definita ed approvata.
- **Organi di governo (management) e di supervisione** – il "Management body" di un istituto ha due funzioni chiave: il management (organo di governo) e la funzione di supervisione. Queste funzioni devono interagire in modo effettivo/reale.
- **Composizione, incarico e sostituzione** – il "Management body" deve avere un adeguato numero di componenti/membri e una composizione appropriata. Il management body deve avere delle policy di selezione, monitoraggio e pianificazione per la sostituzione dei suoi membri.
- **Commitment, indipendenza e gestione dei conflitti di interesse** – i componenti del "Management body" devono essere coinvolti attivamente negli affari dell'istituto e devono essere in grado di prendere decisioni ed esprimere giudizi oggettivi ed indipendenti.
- **Competenze** - i componenti del "Management body" devono essere (e restare) qualificati – anche attraverso formazione - rispetto alla posizione che ricoprono. Devono comprendere perfettamente l'organizzazione della governance del loro istituto e il ruolo che ricoprono al suo interno.

Management body

- **Funzionamento** – il “Management body” deve definire appropriate modalità e procedure di funzionamento interno per la sua organizzazione e funzionamento e fare in modo che tali pratiche siano rispettate e periodicamente riviste per eventuali miglioramenti. In particolare:
 - ✓ **valutazione del funzionamento** - il “Management body” deve valutare l’efficacia e l’efficienza delle sue attività sia a livello individuale che collettivo ed il funzionamento dei comitati interni;
 - ✓ **il Presidente** - gioca un ruolo cruciale nel garantire un corretto funzionamento del “management body”, lo guida ed è responsabile del suo effettivo funzionamento complessivo. In un sistema monistico il Presidente ed il Chief Executive Officer non devono coincidere. Nei casi contrari, è importante che l’istituto disponga di misure che minimizzino i potenziali pregiudizi sui controlli e sugli equilibri;
 - ✓ **Comitati** – nel creare dei Comitati specifici si deve tenere conto della dimensione e della complessità dell’istituto; i comitati sono composti da membri del Management body (all’occorrenza possono essere invitati anche altre persone qualora la loro esperienza specifica o i loro suggerimenti siano rilevanti per la trattazione di alcuni argomenti). I poteri di delega attribuiti a tali Comitati non esonerano il Management body come organo di supervisione dai suoi doveri e responsabilità ma possono costituire un supporto su tematiche per facilitare lo sviluppo e l’implementazione delle pratiche e delle decisioni di buon governo societario (i.e. Comitato Audit e Comitato Rischi).

Management body

- **Valori di governo societario e codice di condotta** - il "Management body" deve implementare e promuovere standards altamente etici e professionali.
- **Conflitti di interesse** - Il "Management body" deve stabilire, implementare e mantenere in vigore politiche atte ad individuare e conflitti di interesse attuali o potenziali in modo da prevenirli. Se i conflitti di interesse non possono essere prevenuti, devono quantomeno essere appropriatamente gestiti.
- **Procedure di alert interno** - Il "Management body" deve implementare appropriate procedure di alert interno che il personale possa utilizzare per richiamare l'attenzione su preoccupazioni legittime e significative inerenti fatti connessi alla governance interna.
- **Outsourcing** - il "Management body" deve approvare e rivedere con regolarità le politiche di outsourcing dell'istituto. Le politiche di outsourcing devono valutare l'impatto dell'outsourcing sugli affari della banca ed i rischi che esso comporta (come i rischi operativi, reputazionali e di concentrazione). La policy deve contenere gli accordi di reporting e monitoraggio implementati in tutta la durata del contratto. L'istituto resta interamente responsabile di tutti i servizi e le attività dati in outsourcing e delle decisioni del management che derivano da essi.
- **Politiche di retribuzione** - Il management body in qualità di organo di supervisione deve mantenere, approvare e supervisionare i principi della politica remunerativa del proprio istituto. Il "Management body", in qualità di organo di supervisione, deve mantenere, approvare e supervisionare i principi della politica remunerativa del proprio istituto.
- **Valutazione del sistema di governance interna** - il "Management body" deve monitorare e valutare periodicamente l'efficacia del sistema di governance interna dell'istituto.

Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparenza



Risk Management

- **La cultura del rischio** – Un istituto deve implementare una cultura del rischio integrata e incentrata sull'azienda, basata sulla piena consapevolezza dei rischi da fronteggiare e su come gli stessi vengono gestiti, tenendo conto della propria risk tolerance/appetite.
- **Allineamento delle retribuzioni al profilo di rischio** - le politiche e le practices retributive dell'istituto devono essere compatibili con il suo profilo di rischio e promuovere un'effettiva gestione dello stesso.
- **Framework di Risk Management** - deve comprendere le politiche, le procedure, i limiti ed i relativi controlli, la tempistica e la costante identificazione, misurazione o valutazione, monitoraggio, mitigazione e reporting dei rischi associati alle attività di ciascuna business line e dell'istituto nel suo complesso.
- **Nuovi prodotti** - un istituto dovrebbe disporre di una policy di approvazione dei nuovi prodotti (NPAP), deliberata dal "Management body", che indirizzi lo sviluppo di nuovi mercati, prodotti e servizi e i cambiamenti significativi rispetto alla situazione attuale/esistente.



Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparency

Internal Control - focus

- **Il framework dei controlli interni** – un istituto deve implementare e mantenere un framework dei controlli interni robusto e comprensibile, che comprenda specifiche funzioni di controllo indipendenti con appropriate caratteristiche/standing per adempiere alla propria mission.

Il framework dei controlli interni di un istituto deve garantire:

- ✓ interventi efficaci ed efficienti,
- ✓ un adeguato controllo dei rischi,
- ✓ una condotta del business prudente,
- ✓ affidabilità delle informazioni finanziarie e non finanziarie riportate sia all'interno che verso l'esterno,
- ✓ la conformità alla legge, alla normativa regolamentare e degli organi di supervisione e rispetto ai ruoli ed alle decisioni interne dell'azienda.

Il sistema dei controlli interni deve coprire l'intera organizzazione, incluse le attività di tutto il business, di supporto e delle unità di controllo. Lo schema dei controlli interni deve essere appropriato rispetto al business dell'azienda, in linea con le politiche amministrative e con le procedure di contabilità.

Le funzioni di controllo comprendono la Funzione Controllo Rischi, la Funzione di Compliance e l'Internal Audit.

Le funzioni di controllo devono essere organizzate secondo livelli gerarchici e riportare direttamente al Management body.

Internal Control - focus

- **La Funzione Controllo Rischi** – un istituto deve predisporre una Funzione Controllo Rischi (FCR) comprensibile e indipendente.
 - ✓ la FCR deve garantire che tutti i rischi rilevanti siano identificati e gestiti in modo appropriato, attraverso la disponibilità di informazioni consistenti ed indipendenti, analisi e giudizi di esperti sulle esposizioni al rischio, e consigli sulle proposte e sulle decisioni sul rischio fatte dal Management body e dalle Unità di business o di supporto in modo che siano coerenti con la risk tolerance/appetite dell'istituto;
 - ✓ la FCR occupa un ruolo centrale nello schema organizzativo, in modo che possa implementare le politiche di rischio e controllare il sistema di risk management;
 - ✓ la FCR deve essere indipendente dalle unità di business e di supporto controllate ma non deve essere isolata dagli stessi. Deve possedere una sufficiente conoscenza delle tecniche e delle procedure di gestione del rischio e dei mercati e dei prodotti. L'interazione tra le funzioni operative e la FCR facilita la responsabilizzazione di tutto il personale aziendale nella gestione dei rischi.

Internal Control - focus

- **Il ruolo della FCR** – la FCR deve essere coinvolta attivamente nella fase iniziale dell'elaborazione della risk strategy aziendale e nelle decisioni inerenti la gestione di tutti i rischi che si sono manifestati. Essa ricopre un ruolo chiave nel garantire che l'istituto metta in piedi un processo efficace di gestione dei rischi. In particolare:
- ✓ *strategie e processo decisionale* - la FCR deve supportare il Management body nella definizione del livello di risk tolerance/appetite di istituto e della risk strategy, fornendo tutte le informazioni inerenti i rischi rilevanti (i.e. attraverso analisi tecniche sulle esposizioni ai rischi)
 - ✓ *relazioni con parti correlate* - la FCR garantisce che le operazioni con parti correlate siano riviste e che i rischi, attuali o potenziali, che esse implicano siano identificati e adeguatamente valutati
 - ✓ *complessità della struttura legale* - la FCR dovrebbe fornire supporto nell'identificazione dei rischi materiali derivanti dalla complessità della struttura legale dell'istituto (carenza nella trasparenza del management, rischi operativi derivanti da strutture complesse e interconnesse, ecc)
 - ✓ *cambiamenti rilevanti* - prima di prendere alcuna decisione relativa ad operazioni importanti quali fusioni, acquisizioni, ingresso in nuovi mercati o nuovi prodotti, la FCR dovrebbe valutare l'impatto dei cambiamenti sostanziali e delle operazioni straordinarie sul profilo di rischio dell'istituto e/o del gruppo;
 - ✓ *misurazione e valutazione* - la FCR deve garantire che la misurazione interna dei rischi dell'istituto e la loro valutazione coprano una appropriata gamma di scenari e non siano basati su assunzioni troppo ottimistiche riguardanti le dipendenze e le correlazioni.

Internal Control - focus

➤

- ✓ *Monitoraggio* - La FCR deve garantire che tutti i rischi identificati siano efficacemente monitorati dalle business units, essa deve monitorare regolarmente l'attuale profilo di rischio ed esaminarlo rispetto agli obiettivi strategici aziendali, alla risk tolerance/appetite. La FCR deve analizzare i trends e riconoscere i nuovi potenziali rischi derivanti dai cambiamenti esterni ed interni in modo che i rischi effettivi siano regolarmente rivisti (i.e. back testing) per valutare e migliorare l'accuratezza e l'efficacia del processo di risk management.
- ✓ *Esposizioni non approvate* - la FCR deve essere adeguatamente coinvolta in ogni cambiamento alla strategia aziendale, alla risk tolerance/appetite approvate e ai limiti. In caso di violazioni - anche se dovuta a cambiamenti degli scenari esterni - essa deve analizzarne le cause e proporre gli interventi correttivi
- ✓ L'istituto deve intraprendere le azioni appropriate contro i *comportamenti fraudolenti interni e esterni* e contro le violazioni della disciplina (i.e. violazioni delle procedure interne, violazione dei limiti).

Internal Control - focus

- **Il Chief Risk Officer** – Un istituto deve incaricare una persona (il CRO) che abbia la responsabilità esclusiva della FCR e del monitoraggio del sistema di risk management aziendale nell'ambito dell'intera organizzazione. Il CRO (o una posizione equivalente) è responsabile di garantire informazioni sui rischi che siano vaste, comprensive e bene interpretate, tali da mettere in grado il Management body di comprendere il profilo complessivo di rischio dell'azienda;
deve avere una sufficiente competenza, un'esperienza operativa, indipendenza e anzianità per promuovere (o mettere un veto) decisioni che influenzano l'esposizione al rischio di un istituto;
deve comunicare direttamente con il Management body o con i Comitati;
la risk policy deve prevedere i casi di veto del CRO e la natura dei suoi interventi/suggerimenti;
qualora le caratteristiche di un istituto – per la sua dimensione, organizzazione e natura della sua attività – non giustificano l'attribuzione di tale responsabilità ad una persona designata, la funzione può essere ricoperta da un altro senior manager interno all'istituto, a patto che non vi sia conflitto di interesse;
l'istituto deve avere processi formalizzati per l'assegnazione della posizione al CRO e per la definizione delle sue responsabilità. Se il CRO viene sostituito ciò deve essere fatto previa approvazione del management body nella sua funzione di supervisione. In genere la rimozione o l'assegnazione dell'incarico al CRO viene resa nota e l'autorità di vigilanza viene informata delle ragioni che hanno portato alla scelta.

Internal Control - focus

- **La Funzione di Compliance** – Un istituto deve avere una policy di Compliance e istituire una Funzione di Compliance permanente ed efficace che la gestisca e designare una persona responsabile per tutto l'istituto (Compliance Officer). La Funzione di Compliance informa il management body sulle leggi, i regolamenti, la normativa e gli standards che l'istituto è tenuto a rispettare e valuta il possibile impatto di ciascun cambiamento a livello legale e regolamentare dell'operatività dell'istituto.

La Funzione di Compliance deve altresì verificare che i nuovi prodotti e le nuove procedure siano conformi al quadro normativo vigente e a ciascun futuro cambiamento conosciuto della legislazione, dei regolamenti e dei requisiti di vigilanza.

- **La Funzione Interna Audit** - la funzione di Internal Audit (IA) deve valutare se la qualità del sistema di controlli interni di un istituto è sia efficace che efficiente.

L'IA è responsabile della valutazione dell'adeguatezza del sistema di controlli interni e deve avere accesso illimitato a tutti i documenti e alle informazioni rilevanti relativi a tutte le unità operative e di controllo.

Il lavoro dell'IA deve essere svolto in base a un piano strategico di audit e di programmi dettagliati di audit che seguono l'approccio "risk based".

L'IA deve riferire dei suoi accertamenti e suggerimenti per i miglioramenti dei controlli interni direttamente al Management body e/o al suo Comitato audit (dove esiste). Tutte le raccomandazioni dell'audit devono essere sottoposte a una procedura di follow up ai rispettivi livelli del management in modo da assicurarsi della loro attuazione e riportare la loro risoluzione.

Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparenza



Systems and continuity

➤ **Il Sistema informativo e di comunicazione** – Un istituto deve avere un sistema informativo e di comunicazione efficace e attendibile che copre tutte le attività significative. Le decisioni prese dal management potrebbero essere influenzate negativamente da informazioni non attendibili e fuorvianti fornite da sistemi scarsi e mal controllati. Ciò premesso è elemento critico per l'istituto predisporre e mantenere sistemi informativi tali da coprire l'intera gamma delle sue attività.

➤ **Business Continuity Management** - Un istituto deve predisporre un piano di continuità degli affari in modo da garantire la sua capacità di operare quotidianamente e limitare le perdite nel caso di eventi catastrofici.

Il business di un istituto si basa su determinate risorse cruciali (es. sistema IT, sistema di comunicazione, edifici). Lo scopo del Business Continuity Management è quello di ridurre le conseguenze operative, finanziarie, legali, reputazionali e materiali derivanti da un disastro o da una prolungata interruzione di tali risorse e dalla conseguente distruzione causata alle procedure di business ordinarie utilizzate dall'azienda. Altre misure di mitigazione di risk management devono essere finalizzate a ridurre la probabilità di tali incidenti o a trasferire il loro impatto finanziario/economico a parte terze (i.e. attraverso polizze assicurative).

I piani di contingency e business continuity devono essere predisposti in modo da fare in modo che l'istituto reagisca in modo appropriato alle emergenze e sia in grado di mantenere le sue principali attività di affari nel caso in cui si verifichi la distruzione delle sue procedure ordinarie di business.

Un istituto deve disporre di piani di recupero/emergenza per le risorse cruciali in modo da consentirgli di ritornare all'operatività normale in un giusto lasso temporale. Ciascun rischio residuo derivante dalle potenziali distruzioni del business devono essere coerenti con la risk tolerance/appetite dell'istituto.

Indice

- Importance of internal governance & purpose of the Guidebook
- Concepts used in the Guidebook
- Implementation of the Guidebook
- Principles:
 - ✓ Corporate Structure and Organisation
 - ✓ Management Body
 - ✓ Risk Management
 - ✓ Internal Control
 - ✓ Systems and continuity
 - ✓ Trasparenza

Trasparenza

- **Responsabilizzazione** – Le strategie e le policies devono essere comunicate a tutto il personale dell'istituto.
- **Trasparenza della governance interna** - il sistema di internal governance di un istituto deve essere trasparente in modo da fornire a tutti gli stakeholders rilevanti le informazioni chiave necessarie ad esprimere un giudizio sull'efficacia del management body nel governare l'istituto. Un istituto deve rappresentare la sua posizione corrente e le prospettive future in modo chiaro, bilanciato, accurato e tempestivo. Un istituto deve fare disclosure delle informazioni che descrivono la governance interna nel suo complesso sia a livello di gruppo che individuale, in modo comprensibile e significativo, la disclosure al pubblico deve coprire almeno i seguenti punti:
 - ✓ la struttura di governo e le policies, compresi gli obiettivi, la struttura organizzativa, gli accordi di governance interna, la struttura e l'organizzazione del management body, compresa la frequenza degli incontri e la struttura degli incentivi e della remunerazione dello stesso;
 - ✓ la natura, il perimetro, lo scopo e la tipologia dell'operatività con le controllate e le parti correlate e una spiegazione di come esse possano influenzare l'intera organizzazione;
 - ✓ le modalità con cui vengono stabiliti il business e la risk strategy aziendale (compreso il grado di coinvolgimento del management body) ed i fattori di rischio prevedibili;
 - ✓ il sistema dei controlli interni e come sono organizzate le funzioni di controllo, i principali obiettivi che perseguono, come è monitorata la loro prestazione dal management body e ogni pianificazione di cambiamenti sostanziali di tali funzioni;
 - ✓ le informazioni rilevanti sui risultati finanziari/economici e operativi.

Indice

- BCBS 168 – Comitato di Basilea – *Principles for enhancing corporate governance* 4 oct 2010
 - ✓ *modalità operative del "Board"*
 - ✓ *Senior Management*
 - ✓ *Risk Management e funzioni di controllo*
 - ✓ *Remuneration policies*
 - ✓ *strutture di corporate complesse*
 - ✓ *disclosure e trasparenza*

- CEBS – *High Level Principles for Risk Management*

Principles for enhancing corporate governance – key areas

Il Comitato di Basilea si era già mosso a marzo del 2010 con il documento di consultazione *Principles for enhancing corporate governance* le seguenti aree di intervento:

➤ **Modalità operative del Consiglio di Amministrazione:**

- il CdA ha la responsabilità complessiva della Banca ivi compresa la definizione/approvazione delle strategie di business e di rischio, organizzative, di politica finanziaria e di governance. Il CdA deve anche svolgere un effettivo controllo sull'attività dell'Alta Direzione (AD);
- per adempiere a tali responsabilità il CdA
 - Effettua valutazioni oggettive ed ha e mantiene adeguate qualifiche e competenze,
 - Persegue pratiche di "buon governo" al suo interno
 - È supportato da funzioni di controllo dei rischi – sui quali il CdA effettua una supervisione – competenti, robuste e indipendenti.

➤ **Alta Direzione (Senior Management):**

- sotto la supervisione del CdA, l'AD assicura che le attività bancarie sono coerenti con le strategie di business, la propensione al rischio e le politiche approvate dallo stesso CdA.

➤ **Risk Management e controlli interni:**

- la banca deve avere una funzione di Risk Management indipendente (ivi compreso un Chief Risk Officer (CRO) o equivalente) con sufficiente autorevolezza, importanza, autonomia, adeguate risorse e diretti accesso al CdA;
- i rischi devono essere identificati e monitorati costantemente sia a livello globale che su base individuale e la complessità del Risk Management e delle infrastrutture di controllo interno deve essere adeguata ai cambiamenti del profilo di rischio della banca (insiti nel suo processo di crescita) e in base agli scenari esterni di riferimento;
- una concreta gestione del rischio non può prescindere da una chiara e tempestiva comunicazione interna alla Banca – garantita sia da una struttura organizzativa adeguata che da un sistema idonea di reportistica al CdA e all'AD.

Principles for enhancing corporate governance – key areas

➤ **Remunerazioni:**

- le Banche devono adeguarsi al documento del Financial Stability Board *Principles for Sound Compensation Practises* (che stabilisce compensi adeguati ad obiettivi della banca di lungo termine).

➤ **Strutture di corporate complesse e poco trasparenti:**

- il CdA e l'AD devono conoscere, capire e guidare la governance aziendale e la sua evoluzione, assicurando che la struttura organizzativa sia idonea e non ci siano complessità organizzative non giustificate o inappropriate;
- l'AD, e il CdA per la parte di sua competenza, deve conoscere la mission di ciascuna struttura organizzativa e le attività che potrebbero essere di ostacolo alla trasparenza e deve porre attenzione agli specifici rischi che tali strutture potrebbero generare cercando di mitigarli.

➤ **Disclosure e trasparenza:**

- la trasparenza è uno strumento di supporto per implementare e rafforzare una sana governance aziendale



Indice

➤ BCBS 168 – Comitato di Basilea – *Principles for enhancing corporate governance* 4 oct 2010

- ✓ *modalità operative del "board"*
- ✓ *Senior Management*
- ✓ *Risk Management e funzioni di controllo*
- ✓ *Remuneration*
- ✓ *strutture di corporate complesse*
- ✓ *disclosure e trasparenza*

➤ CEBS – *High Level Principles for Risk Management*

- ✓ *governance e cultura del rischio*
- ✓ *risk appetite e risk tolerance*
- ✓ *il ruolo del CRO e della funzione di risk management*
- ✓ *modelli di rischio e integrazione delle aree di risk management*
- ✓ *policy e pratiche di approvazione di nuovi prodotti*

High Level Principles for Risk Management

Il CEBS, a seguito di un'analisi condotta sulle linee guida del risk management esistenti, ha disciplinato le tematiche per le quali erano stati riscontrati dei gaps normativi. Questa regolamentazione è contenuta nel guidebook *High level principles for risk management* (febbraio 2010). I principi contenuti nel guidebook devono servire sia agli Organi di Vigilanza (SREP) che agli istituti (ICAAP) per l'implementazione del Pillar 2 (entro dicembre 2010). Il documento individua le seguenti aree di intervento:

➤ **Governance e cultura del rischio:**

- ✓ una robusta cultura del rischio è elemento chiave per un efficace risk management ed uno dei prerequisiti per la creazione di una cultura del rischio è l'esistenza di una **funzione di risk management indipendente e che copra tutte le tipologie di rischio (e tutte le business lines), sotto la diretta responsabilità del CRO o di un senior manager** (in base al criterio di proporzionalità)
- ✓ il management body è pienamente responsabile della supervisione del senior management e definisce le pratiche di business e i piani strategici, nel fare ciò deve comprendere a pieno la tipologia del business e i rischi ad esso associati
- ✓ ogni membro dell'organizzazione deve essere consapevole della sua responsabilità inerente l'identificazione e il reporting dei rischi rilevanti
- ✓ gli istituti devono favorire la cultura del rischio e stabilire il sistema di governo dei rischi attraverso una policy appropriata
- ✓ La governance dei rischi deve essere formalizzata ed aggiornata. Il sistema di risk management deve essere soggetto a revisione da parte di un organo indipendente.

High Level Principles for Risk Management

➤ **Risk appetite e risk tolerance:**

- ✓ il risk appetite o la risk tolerance non devono tener conto solo dell'avversione al rischio dell'istituto, ma anche della situazione finanziaria vigente e della direzione strategica dell'istituto stesso. Per garantire la sicurezza ai depositanti, questi limiti tengono conto in particolare della composizione del capitale e di requisiti di liquidità;
- ✓ gli istituti possono esprimere la loro risk tolerance/appetite in vari modi, compreso i rating del credito o dei tassi obiettivo del ROE; l'essenziale è che i target fissati siano coerenti tra di loro e coerenti con l'obbligo dell'istituto di tutelare i propri depositanti;
- ✓ i target di risk tolerance/appetite devono tener conto dei rischi rilevanti per l'azienda (inclusi quelli derivanti dalle operazioni "fuori bilancio")
- ✓ il management body e l'alta direzione sono responsabili di fissare suddetti limiti
- ✓ il ruolo del management body e dell'alta direzione di supervisionare i rischi deve essere chiaramente formalizzato
- ✓ l'alta direzione è responsabile della gestione dei rischi su base giornaliera, sotto la supervisione del management body. Inoltre, a causa della volatilità della tipologia di business del settore bancario e dello sviluppo economico in generale, è necessario che i metodi di misurazione dei rischi siano rivisti periodicamente anche in funzione degli obiettivi strategici dell'istituto. In particolare ci si deve assicurare che i limiti al rischio di trading, credito, liquidità e altri rischi siano coerenti con il risk appetite e la risk tolerance complessiva dell'azienda, anche nel caso di un andamento economico "stressato".

High Level Principles for Risk Management

➤ **Il ruolo del Chief Risk Officer e delle funzioni di risk management**

- ✓ l'istituto deve incaricare una persona responsabile della funzione Risk Management di tutta l'organizzazione, di solito questa persona è il Chief Risk Officer (tuttavia nei casi di aziende di piccole dimensioni il Responsabile dei controlli interni può anche essere Responsabile della funzione Risk Management)
- ✓ il CRO (o equivalente) deve avere una sufficiente indipendenza e anzianità da renderlo in grado di cambiare (o mettere eventuali veti) il processo decisionale dell'istituto.
- ✓ il CRO deve avere le competenze (skills e esperienza) compatibili col profilo di rischio dell'istituto; egli, infatti, gioca un ruolo chiave nel far capire al management body ed all'alta direzione il profilo di rischio complessivo dell'istituto;
- ✓ anche la funzione di Risk Management deve avere le competenze idonee al profilo di rischio aziendale (essa gioca un ruolo chiave nell'identificare, misurare e valutare i rischi complessivi dell'istituto). La FRM è responsabile di supervisionare e approvare i sistemi rating interni, i modelli di valutazione dei rischi e l'analisi dei rischi insiti nei nuovi prodotti o nelle operazioni eccezionali.
- ✓ la FRM deve essere coinvolta nella fase iniziale di determinazione del piano strategico e nel processo decisionale delle attività di business
- ✓ la FRM è indipendente dalle unità operative
- ✓ la gestione dei rischi non deve essere esclusivo appannaggio della FRM
- ✓ il management body e l'alta direzione devono garantire l'allocazione di risorse idonee (sia per numero che per qualifica) alla FRM.

High Level Principles for Risk Management

➤ **I modelli di gestione del rischio e l'integrazione delle tematiche di risk management:**

- ✓ gli istituti devono identificare e gestire tutti i rischi rilevanti sia a livello di portafoglio delle singole business line che di gruppo
- ✓ si deve evitare ogni eccessiva dipendenza (fiducia) da specifici metodologie e modelli di gestione del rischio
- ✓ Le decisioni inerenti la determinazione del livello di rischio "preso" non devono tener conto solo di informazioni quantitative o dei risultati dei modelli adottati ma anche delle limitazioni pratiche e concettuali delle metriche e dei modelli che utilizzano approcci qualitativi (comprese le valutazioni di esperti e le analisi critiche)
- ✓ gli istituti devono adottare un trattamento integrato di tutti i rischi rilevanti
- ✓ deve essere predisposto un meccanismo di comunicazione regolare e trasparente all'interno dell'organizzazione (tra il management body, le business line, la FRM e le altre funzioni di controllo)
- ✓ le procedure interne ed i sistemi informativi devono essere tali da consentire a tutte le fonti di rischio di identificare, misurare e monitorare gli stessi su base aggregata e, all'occorrenza, anche per ciascuna entità, business line o portafoglio.

➤ **Le politiche ed i processi per l'approvazione di nuovi prodotti**

- ✓ un istituto deve formalizzare una politica per l'approvazione di nuovi prodotti, che comprenda anche i cambiamenti delle caratteristiche dei prodotti già esistenti.

Principles for enhancing corporate governance **Focus su aree di miglioramento nel RM**

Processi

- **Coinvolgere** attivamente ed in modo efficace il **senior management** nella gestione del rischio
- **Garantire l'indipendenza del risk management** ed un adeguato sistema di **incentivi**
- Discutere e condividere il **risk appetite** a partire dal top management
- Predisporre processi di gestione **"cross risks"**
- **Porre rigore e disciplina** nell'applicazione delle **regole** (es standards di sottoscrizione, gestione dei collaterali)
- **Preparare contingency plans**

Portafoglio/Policies

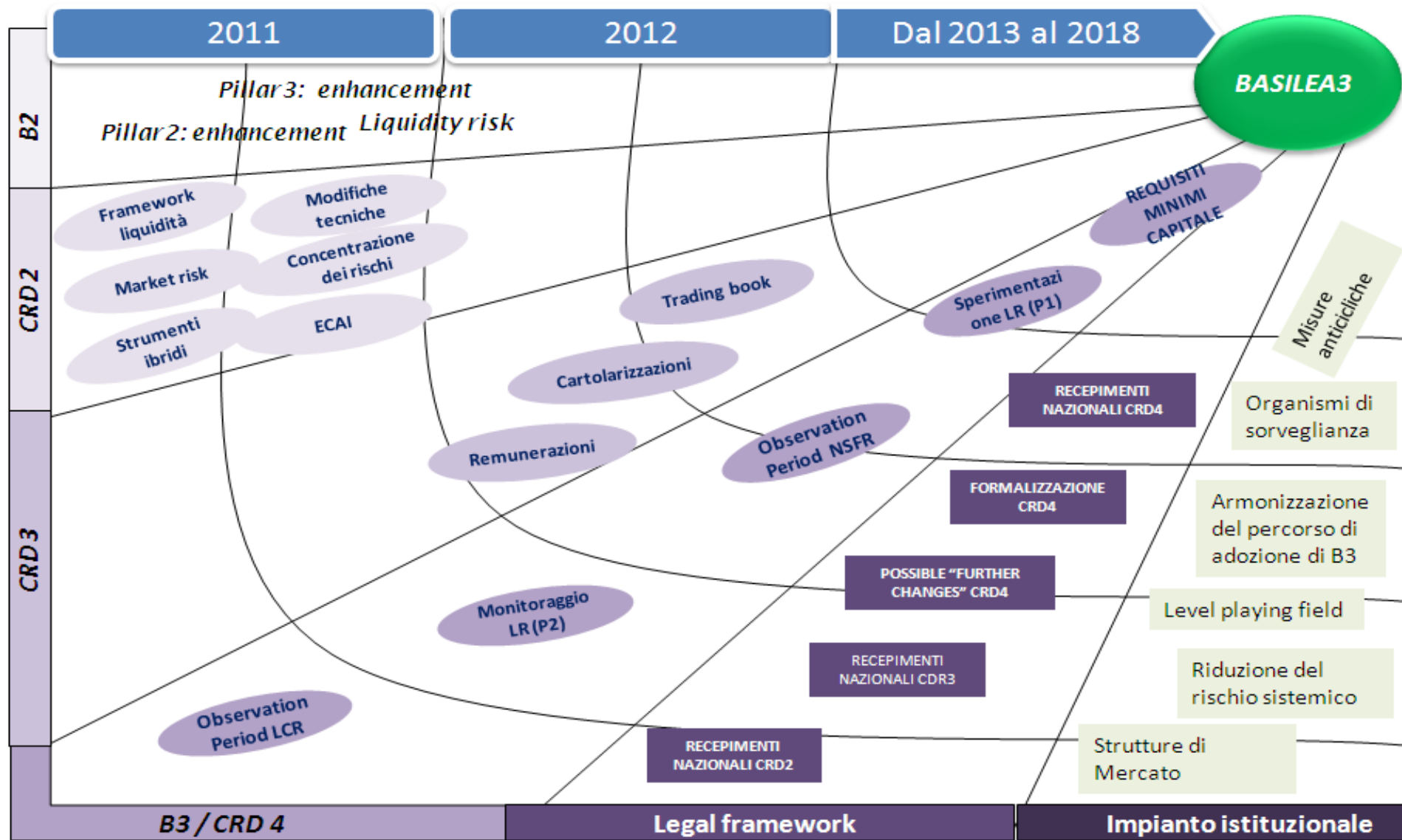
- Rafforzare le **politiche di funding**
- **Riconsiderare** la piena fiducia nei **modelli** (es. VAR, pricing) e potenziare lo stress/shock testing
- Ampliare il ruolo del **portfolio management** (es. sulla concentrazione del rischio, regole di rischio/rendimento, diversificazione)
- Applicare con disciplina le regole in fase di **erogazione e copertura**
- Aumentare la **trasparenza**

IT

- Investire in un **ambiente IT robusto**
- Investire in sistemi di **MIS**

Approccio
olistico ed
applicazioni ERM

CASSA DI RISPARMIO DI SAN MINIATO



Processo di risk management

- Risk assessment
- Valutazione dei rischi
- Aggregazione
- Misurazione e controllo
- Monitoraggio e reporting

Mapa dei rischi

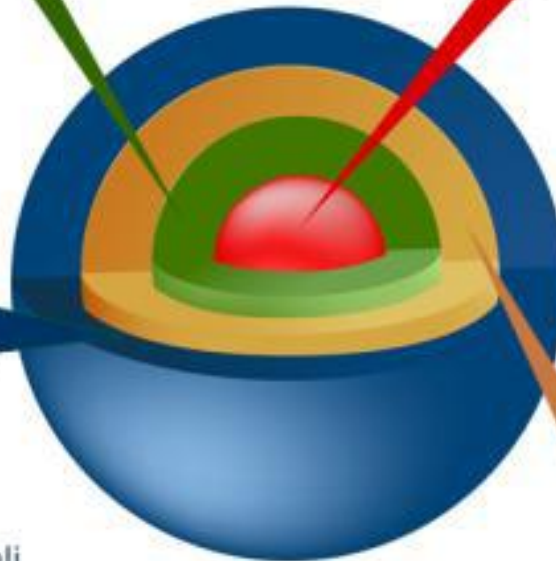
- Identificazione del perimetro e degli obiettivi
- Identificazione di rischi e opportunità
- Classificazione dei rischi

Governance

- Ruoli e responsabilità
- Profilo di rischio
- Risk management policy
- Integrazione processi decisionali
- Valutazione e review dell'ambiente di controllo

Risk intelligence

- Data quality
- Dashboards
- Modelli



Il governo dei rischi dovrà appoggiarsi su di uno schema che ne consenta la valutazione anche attraverso le modalità con le quali essi interagiscono e renda più robuste le scelte strategiche attraverso l'integrazione con i processi di pianificazione e gestionali

Grazie per l'attenzione

p.palliola@crsm.it

