

**SECURITY & SAFETY in Banca:
opportunità o ulteriori vincoli per uno
sviluppo sostenibile ?**

Dr. Ing. Franco del Conte

Segretario Generale ANIAB

Associazione Nazionale Ingegneri e Architetti Bancari

TRATTATO DI MAASTRICHT (1992) – art. 2

LA COMUNITA' HA IL COMPITO DI PROMUOVERE
UNO SVILUPPO ARMONICO ED EQUILIBRATO
DELLE ATTIVITA' ECONOMICHE, UNA
CRESCITA SOSTENIBILE, NON INFLAZIONISTICA
E CHE RISPETTI L'AMBIENTE, IL MIGLIORAMENTO
DEL TENORE E DELLA QUALITA' DELLA VITA

Dalla sicurezza costa ... alla sicurezza paga

Sicurezza: quanto mi costi!

Per le banche il primo obiettivo non è risparmiare sui sistemi di sicurezza, ma contenere il peso degli oneri ripetitivi e non previsti di esercizio e manutenzione attribuibili spesso ad una scarsa integrazione progettuale. Ma per pervenire ad un tale obiettivo serve un vero progetto aziendale.

f. del conte - BANCAFORTE 1997

Decennale di BANCAFORTE

... Bancaforte si fa volano di un nuovo concetto di sicurezza. Vale a dire la sicurezza come asset da valorizzare nelle strategie di governance delle banche. Sia come protezione dei dipendenti e dei clienti, sia in termini di tutela dei sistemi informativi e di continuità del business.

... Senza perdere di vista l'ottimizzazione organizzativa
Editoriale – M. Iaconis

DILEMMA BANCARIO: sviluppo sostenibile o inerzia strategica ?

L'attività d'impresa deve testimoniare al mercato non più solo il proprio valore economico ma anche il livello di *customer satisfaction* raggiunto tramite le ricadute positive della propria attività nei confronti degli altri stakeholder

- » Ritorno economico
Bilancio d'esercizio – qualità economica
- » Partecipazione
 - Fiducia
 - Immagine
 - Audit
- » **Bilancio sociale – qualità etica**

Corporate governance

Non c'è sviluppo senza sicurezza - A. Ciampi

Il nuovo modello di *governance*, che risponda anche alla crescente domanda di trasparenza da parte della società civile, opera tra

- Complessità degli scenari possibili
- Proliferazione normativa
- Globalizzazione
- Dematerializzazione dei valori d'impresa
- Scandali finanziari
- Trasparenza e visibilità diritti clientela

Creare il valore d'impresa

Creare valore per gli *stakeholder* che, come portatori di interessi molteplici e differenziati di tipo

1. Economici, patrimoniali, finanziari (Azionisti, soci, CEO, CDA)
 2. Competitivi vs. clienti interni – esterni (Management, dipendenti, clientela, fornitori, partner, istituzioni)
 3. Sociali, etici, ambientali (Territorio, comunità locali, mass media, opinion maker, OOSS),
- contribuiscono alla realizzazione della missione aziendale
 - sono in grado di influenzare con le loro molteplici decisioni (di spesa, di investimento, di collaborazione, di controllo, di regolamentazione) il raggiungimento degli obiettivi aziendali
 - vengono influenzati dalle scelte e dalle attività dell'impresa

Quali valori d'impresa

gestione integrata del rischio e *corporate governance*

- Illeciti ed incidenti indeboliscono il valore
- Compliance contro i rischi legali per violazioni di leggi (privacy, reati societari, reati contro la PA) aumentano la fiducia
- Avere strategie trasparenti di prevenzione, contenimento e di attenuazione degli effetti negativi crea valore d'impresa
- Security, safety, sociale creano valore

S&S: strumento d'integrazione

Il contenimento della spesa corrente, obiettivo comune di ogni azienda, deve enfatizzare e attivare ogni strumento aziendale che promuova il coordinamento, che stimoli le potenziali **sinergie** in modo che, a parità di investimenti, si ottenga sempre il miglior rapporto costi benefici in un continuo controllo della spesa corrente. La cultura aziendale del perseguire **efficienza** nelle singole spese deve, assai più strategicamente, tendere alla ricerca della maggiore **efficacia** del sistema, risultato complessivo dell'attività dei singoli sottosistema componenti (safety, security, quality, environment), che invece risultano spesso gravati da spese one-shot, parcellizzate e fuori controllo.

Basilea 2 - *Total capital ratio*

Total Capital Ratio, quale indicatore della adeguatezza del capitale di vigilanza che le banche devono accantonare per far fronte alle tre tipologie di rischio individuate:

1. Rischio di mercato: perdite sostenute dalla banca e originate da variazioni sfavorevoli dei prezzi degli strumenti finanziari (tassi di interesse, di cambio, corsi obbligazionari, etc.).
2. **Rischio operativo: perdite derivanti da errori umani, problemi tecnici o di procedura, e comunque non attribuibili al comportamento dei debitori o agli eventi di mercato.**
3. Rischio di credito: perdite future su un credito per insolvenza del debitore, rischio di non recupero, rischio di esposizione o deterioramento della "qualità" del debitore, deve essere non inferiore al 8% del rapporto tra il totale delle attività svolte e detti rischi.

Basilea 2 - Rischio operativo

Rischio operativo stimato per maggiori costi o minori performance riconducibili a:

- processi interni (ruoli e responsabilità definite e assegnate; procedure; modelli e metodologie di monitoraggio e controllo dei rischi; violazione della sicurezza informatica; out-sourcing);
- risorse umane (negligenze, frodi, errate decisioni manageriali, azioni incoerenti o conflittuali, errori, insoddisfazione, incompetenza, inosservanza delle leggi ossia rischio legale);
- fattori tecnologici (malfunzionamento dei sistemi operativi, errori di programmazione e progettazione, interruzioni nei servizi, scarsa disponibilità operativa, innovazione tecnologica non adeguata);
- eventi esogeni (vulnerabilità politiche e istituzionali del contesto in cui la banca opera, attività criminali come furti, atti di terrorismo ed, infine, eventi naturali come terremoti o inondazioni).

Valori aziendali di S&S

Benefici aziendali

- Riduzione illeciti interni ed esterni
- Riduzione rischi sulle persone
- Riduzione costi per sanzioni, penali e no-quality
- Miglioramento immagine e reputazione
- Aumento senso di appartenenza e motivazione
- Diminuzione turnover, assenteismo, incidenti
- Miglioramento clima aziendale

Benefici stakeholder

- Miglioramento valore economico e di mercato
- Aumento cultura aziendale e controllo sociale
- Miglioramento dialogo con PA
- Trasparenza
- Tutela dei posti di lavoro
- Salvaguardia dell'ambiente e del territorio
- Riduzione criminalità
- Recupero di fiducia e fidelizzazione

Dal Risk Management alla CSR

da Gestire il rischio su base normativa (qualità esplicita che sono disposto a pagare): Crisis, Safety, Security, Privacy

a Creare valore su base volontaria (qualità implicita che se c'è è meglio ma non sono disposto a pagare): fiducia, reputazione, eticità, sicurezza, equità, ascolto e attenzione ai portatori d'interesse, proattività

Dai **vincoli** d'impresa agli **asset** competitivi

L' esigenza cogente di tutela (security & safety) non deve essere invasiva

- né per il cittadino (privacy)
- né per il lavoratore (tutela collettiva L. 300)
- né per il dipendente (safety 626)

La sicurezza della collettività deve essere garantita dalla collettività stessa tramite gli **STAKEHOLDER** che meglio la rappresentano

NUOVO APPROCCIO

Da una gestione **deterministica** (ingegnere) ad una gestione **probabilistica** (project manager) dove la gestione del rischio si limita a tenere sotto controllo la probabilità residua dell'evento negativo.

La **Norma UNI 10459** - Funzioni e profilo del professionista della security aziendale - fornisce un importante riferimento quando afferma che l'attività manageriale PUO' essere svolta anche attraverso il ricorso alle tecniche di gestione per la qualità, per il contributo che esse possono dare sia alla riduzione dei costi, sia alla qualità di prodotti e servizi.

Approccio aziendale proattivo

1. valutare i rischi connessi alle proprie attività,
2. definire i processi, le responsabilità e gli obiettivi

La **security** sostenibile

Security come sistema di strategie, attività, operazioni finalizzate alla tutela dei processi critici d'impresa e delle risorse immateriali e materiali ad essi correlate nell'ottica di garantire la Business Continuity e tutelare il Valore dell'Azienda, proteggendo i fattori chiave di successo, la capacità competitiva e di creazione del valore d'impresa. Attenuazione nei rischi patrimoniali e nei processi aziendali.

Progettazione nella **security**

L'esigenza di **SECURITY** rappresenta la prima vera attuazione di una progettazione integrata

Storicamente in campo per interfacciare opere edili (sicurezza passiva) con impianti elettromeccanici ed elettronici (sicurezza attiva) sperando di aver già integrato tra loro, gli impianti tecnologici convenzionali, opere elettriche, climatizzazione, telecomunicazione, elaborazione dati, oggi il *system integrator* deve essere fortemente orientato al *customer care*

La *safety* sostenibile

- Safety per la tutela dei lavoratori
- Safety per la tutela della clientela
- Etica per presidiare e difendere i valori fondanti dell'impresa, in cui si riconosce, per rafforzarne l'identità e promuovere coerenza nei comportamenti all'interno ed all'esterno dell'azienda
- CSR sistema di gestione strategica dell'impresa integrata con tutti gli stakeholder aziendali

Progettazione nella *safety*

Come norma cogente, la **SAFETY** non ha mai preteso integrazioni.

L'approccio tradizionale degli anni '50 ricercava la **mera e più riduttiva conformità** (approccio deterministico o di compliance) alla norma (misure minime), solo negli anni '90 la sicurezza del lavoro assume il taglio **probabilistico** del risk management, individuando con l'articolo 6 del decreto 626/94 le responsabilità più ampie del progettista per assicurare la sicurezza del posto di lavoro.

Alla deontologia del progettista si chiede di definire i livelli di prestazione degli apprestamenti di sicurezza e di salute, nel rispetto della norme cogenti (**conoscenza**), delle norme raccomandative (**coscienza**), delle norme comportamentali che derivano dalla propria personale esperienza e sensibilità (**competenza**).

Clima aziendale

I programmi di benessere aziendale possono generare per le aziende un ritorno sugli investimenti anche del 400%. Uno studio condotto nel Regno Unito sottolinea anche come uno staff in cattive condizioni fisiche lavori mediamente un giorno alla settimana in meno rispetto ai colleghi in condizioni migliori.

Infatti, per ogni sterlina investita in programmi di benessere, si registrano 3,73 sterline in benefici per l'organizzazione, mentre la produttività delle persone in cattive condizioni fisiche (*) è del 18% inferiore rispetto a quella delle persone in salute.

(*) Tra le altre conclusioni dello studio, emerge come gli uomini single molto difficilmente riescano a migliorare il proprio stato fisico se non sono sottoposti a programmi di benessere

Approccio aziendale proattivo

3. tracciare le attività di un sistema dove
le **tecnologie innovative** non siano la soluzione,
le **compliances** non siano esercitazioni,
le **certificazioni** non siano un fardello,
le **norme** siano stimolo organizzativo.

Non innamoriamoci delle soluzioni ... appassioniamoci ai risultati !!

La validità tecnica delle soluzioni adottate si traduce in reali opportunità di sviluppo aziendale unicamente quando la struttura organizzativa (risorse umane e procedure) è messa in grado di utilizzare al meglio le **opportunità offerte dalle tecnologie.**

La vera innovazione consiste, nel saper gestire ed utilizzare ciò che la tecnologia propone sul mercato.

Le tecnologie innovative

Lo strumento tecnologico è neutro, spesso utile può essere a volte molto dannoso dipende dall'uso che se ne fa, non è né una medicina, né un antidoto, né una droga

THE RIGHT TOOL FOR THE RIGHT JOB

da solo non è mai la soluzione, è sempre e solo uno strumento, ma come tale lo si deve saper adoperare

I costi della tecnologia

In un impianto di sicurezza l'hardware e la componentistica non incidono più del 25% sul costo globale

Eventuali economie non possono né devono essere perseguite sul costo d'acquisto dei materiali ma su

- integrazione
- semplicità di gestione
- oneri esercizio e manutenzione
- efficacia

Innovazione - Il rischio

- Come nel Risk Management, non è il **pericolo** che deve far paura ma il **rischio** ovviamente inteso quale probabilità che il pericolo individuato causi poi effettivamente un danno e la severità del danno stesso
- Così l'innovazione tecnologica ed organizzativa, i risultati della ricerca e sviluppo prima di essere implementati in azienda richiedono una attenta analisi del **rischio connesso all'innovazione** stessa sia in termini di tipologia del rischio innovazione: tempi di attuazione, durata, costo, qualità, quantità accettabile sia per le ricadute potenziali sugli aspetti organizzativi nelle diverse fasi del processo produttivo aziendale: progettazione, costruzione, gestione, dismissione, investendo quindi le poche e limitate risorse sulla gestione del solo **rischio residuo**.
- Se la documentazione e la registrazione in sistema qualità dell'analisi del rischio in un approccio safety avviene proprio tramite la redazione del documento valutazione del rischio (DVR) cosa avviene nella security?

innovazione - l'opportunità

- l'innovazione deve portare più efficienza nella gestione del processo, di qualsiasi processo organizzativo, non può sostituire o definire esso stesso il processo
- il costo dell'innovazione è giustificato solo dalla rivalutazione del processo, dal suo riesame per il dimagrimento organizzativo e procedurale (**la fabbrica snella**), procedure di audit e reporting meno costose ma sempre adeguate allo scopo, mai ridondanti e sovrabbondanti rispetto alle effettive esigenze
- costante riprogettazione del processo di creazione del valore
- la qualità, quella percepita, è il vero valore da perseguire nella sicurezza
- la qualità commerciale è invece quella che ti viene riconosciuta e pagata
- l'innovazione determinata dal DVR nella 626, dal DPS nella privacy (norme cogenti) dalla certificazione qualità (volontaria) deve essere vista come opportunità di razionalizzazione dei flussi informativi, di identificazione dei process owners aziendali, di ridefinizione dei processi di valorizzazione dei codici etici e deontologici da considerare come vere e proprie nuove fonti del diritto
- nel recente editoriale del decennale di Bancaforte,
 - la sicurezza,
 - la tecnologia
 - l'innovazione
 - l'ottimizzazione organizzativa
- sono gli **asset** da valorizzare nelle strategia di governance delle banche.

Le certificazioni

NON E' SUFFICIENTE la valutazione di compliance come rischio di conformità o rischio di inadeguatezza per la redditività d'impresa che può essere determinato dalle **violazioni o non conformità** con legislazioni, norme, regolamenti, prassi e standard prescrittivi, con le politiche interne e procedure o con eventuali standard etici.

La certificazione, infatti, non più **semplice compliance** come furono viste le ISO precedenti alla Vision, ma come certificazione di **best practice** e di miglioramento continuo.

Leggi, norme, regolamenti

vincoli nella loro applicazione iniziale, nella diffusa resistenza al cambiamento, nell'inerzia a modificare le proprie abitudini e le prassi consolidate nel tempo

stimoli in una visione proattiva, dovendo cambiare rivaluto integralmente i processi organizzativi aziendali sia quelli produttivi di valore aggiunto (*core business*) sia quelli accessori di puro costo (*outsourcing*)

da necessità ad opportunità di sviluppo solo se, come in tutti i paesi europei di sperimentata democrazia, la nuova legge è preceduta dal dibattito e dalla consultazione. Quindi gli organi preposti effettuano le scelte e la discussione si chiude. Quando una nuova legge viene promulgata e pubblicata la si applica e basta. Da noi, invece, solo quando la legge viene pubblicato sulla G.U. si comincia a discutere sulla possibilità di disapplicarla invece che applicarla e basta!

I quesiti della SICUREZZA

Un'auto sicura?

- A - Non si ferma mai
- B - Nessuno te la ruba
- C - In caso d'incidente non ti fai male

Ma allora cos'è la sicurezza?

- PREVENZIONE - PROTEZIONE - ORGANIZZAZIONE

Antincendio

- Sistemi di rilevazione o sistemi di estinzione?

Tutto finalizzato al dopo evento

- Cosa vogliamo che rimanga: dopo un incendio?
- Cosa vogliamo aver salvato: dopo la rapina?
- Cosa avremmo voluto aver protetto: dopo un'intrusione?

Tre quesiti chiave

- Cosa posso fare? (mitigazione o minimizzazione del rischio).
- Quanto mi "costa"? (in termini economici, ma anche di risorse, capacità, mezzi).
- Ne vale la pena?

Il Risk Manager in BASILEA 2

- La crescente complessità nella gestione delle imprese moderne, vuoi per la nascita di nuovi fattori di rischio vuoi per l'acuirsi di problematiche già esistenti, non consente più un approccio semplificato per la valutazione della qualità delle infrastrutture di produzione.
- Se si analizza p.e. il Basilea 2, si nota che tra i rischi operativi si trovano inseriti anche "il rischio di perdite derivanti da disfunzioni a livello di procedure, personale e sistemi interni, oppure da eventi esogeni": individuando i **pericoli operativi**
- associando i pericoli d'impresa correlati con la security e la safety, la probabilità di accadimento ed il valore loro associato avremo individuato le **classi di rischio** specifico che ciascun risk manager, secondo proprie personali valutazioni e le proprie competenze tecniche, farà bene a tenere in vista sul proprio **cruscotto aziendale**.

INDICATORI

- La **disponibilità** (MDT) di un sistema complesso infatti non va interpretata semplicisticamente come **affidabilità** (MTBF) dei suoi moduli, bensì come capacità di corretta ed economica gestione. In sostituzione di parametri di riferimento più tradizionali (Vitruvio ne esaltava la Venustas, la Utilitas, la Firmitas) oggi vale la Direttiva 89/106/CEE). Flessibilità d'uso ed economicità di gestione forniscono per l'infrastruttura di riferimento un parametro di stima assai apprezzato e, specie se certificato in **due-diligence** come un diritto reale di godimento, assume anche una chiara ed oggettiva validazione del valore patrimoniale.

Gli indicatori di qualità

Oggi si assiste ad una costante ricerca degli indicatori di qualità, confezionati ad hoc per ogni specifica esigenza di valutazione e reporting che, come strumenti di management, aiutino il manager a disporre ed utilizzare strumenti di supporto alle decisioni (Decision Support System), a costruire cruscotti operativi, sempre più oggettivi e trasparenti; peraltro ciò avviene in linea con uno dei requisiti fondamentali della Norma UNI EN ISO 9004 che, in solo otto principi esemplifica gli strumenti di qualità per il management e, tra questi otto, individua a pieno titolo quello di *decisioni prese sulla base di dati oggettivi e misurabili*.

CORE BUSINESS vs OUTSOURCING

- La tendenza attuale di ricercare sempre e solo l'ottimizzazione del profitto, a scapito di quello sostenibile, riduce l'attenzione degli asset aziendali al solo *core business*. Con le tecniche di *outsourcing* più spinte tutte le aziende sono sempre più orientate alla terziarizzazione con un maggiore sviluppo di contratti prestazionali basati sui risultati (Global Service – UNI 10685).
- L'individuazione all'esterno di **responsabilità professionali delegabili** per legge (Servizi di Prevenzione e Protezione – D.L.vo 626/94, Coordinatore per la Sicurezza – D.L.vo 494/96, Terzo responsabile dell'energia – L.10/91) fa sì che si tenda ad esternalizzare non solo la competenza ma, con essa, anche lo stesso *up-grading* tecnologico delle infrastrutture, degli immobili e degli impianti tecnologici in esso ricompresi: l'aggiornamento normativo o per obsolescenza o per migliori prestazioni delle apparecchiature più specialistiche, tipiche per esempio nel settore security, nell'EDP e nelle comunicazioni, viene affidato all'impresa partner come *all-inclusive* del canone pattuito.
- outsourcing professionale: ulteriore rischio da gestire!

BEST PRACTICE

1. il Protocollo sullo Sviluppo Sostenibile e Compatibile del Sistema Bancario del 16 giugno 2004, tra ABI e OOSS
2. Verbale di accordo del 5 aprile 2006 tra Banca Intesa S.p.A. e le OO.SS.LL. sullo sviluppo sostenibile
3. Commissione Nazionale per la Sicurezza ABI-OOSS
4. SGSL - Inail

Norma A90001720

In inchiesta pubblica

Gestione del rischio

SOMMARIO

La norma definisce i termini di base relativi al processo di gestione del rischio e costituisce un riferimento generale applicabile a tutte le organizzazioni, indipendentemente da tipologia, dimensione ed attività svolta, al fine di promuovere un approccio coerente per la descrizione del processo di gestione del rischio e l'utilizzo della terminologia pertinente.