

**Integrazione dei Sistemi di Gestione volontari
con quelli obbligatori con particolare riferimento
per la Sicurezza delle Informazioni**

**Analisi del rischio come strumento di integrazione
dei sistemi di gestione**

Maggio 2008

DPCM 3/02/2006 – capo VIII
(Sicurezza dei Sistemi EAD Classificati)

D.Lgs. 196/03

Analisi del rischio

D.Lgs. 231/01

ISO/IEC 27001

Normativa Bancaria

Individuare i rischi cui una determinata azienda o parte di essa è esposta ed intervenire in modo da ridurli entro limiti accettabili.

- ❑ Analisi a priori: volta ad individuare le caratteristiche che un sistema (ancora da realizzare) deve soddisfare,
- ❑ Analisi a posteriori: volta a verificare che un sistema (già realizzato) soddisfi determinate caratteristiche,
- ❑ Analisi continua: volta a monitorare che le caratteristiche di un certo sistema siano in grado di abbattere il rischio.

CONFLITTO: Applicazione dei medesimi requisiti di sicurezza con modalità diversificate

SOLUZIONE: Applicazione del requisito di sicurezza che presenta un più alto grado di robustezza

Realizzazione di una infrastruttura per l'analisi e la gestione del rischio e per l'analisi della conformità

L'infrastruttura MIGRA è stata realizzata in modo da:

- ❑ adattarsi alle diverse realtà FNM,
- ❑ affrontare aspetti di sicurezza sia di tipo fisico che logico,
- ❑ supportare l'adeguamento aziendale a diversi Standard/disposizioni normative.

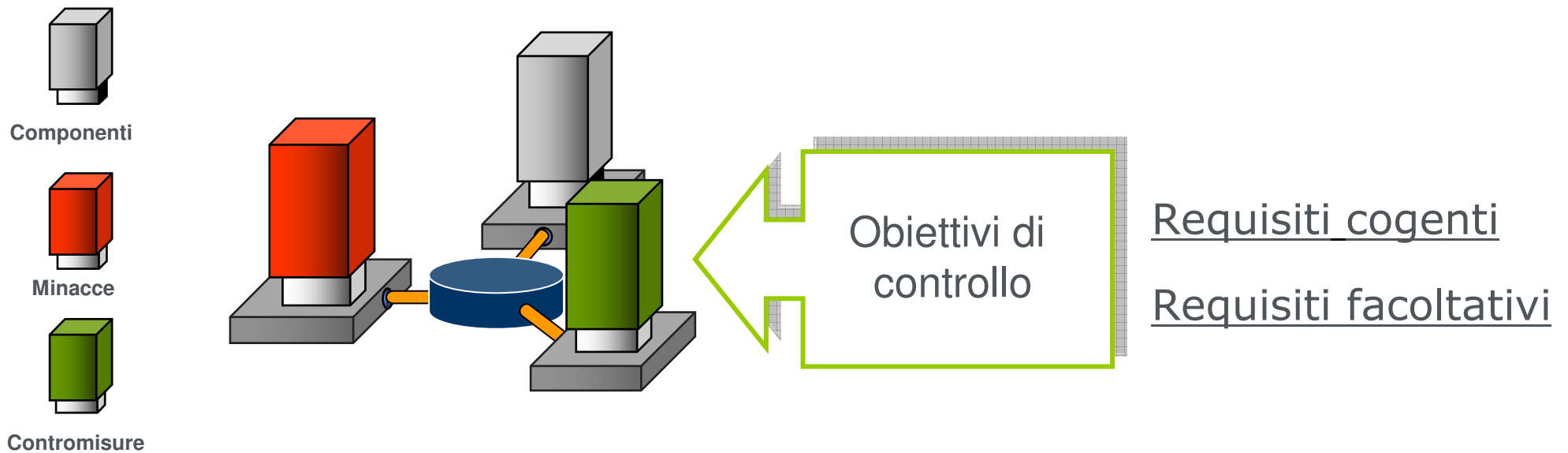
1. Utilizzo di una Base di Conoscenza (che mette in relazione Asset, Minacce/Attacchi e Contromisure) editabile e aggiornabile tramite un Software (KBB);

2. Approccio per **perimetri** (ambiti più piccoli rispetto all'intera azienda). La modellizzazione per perimetro può essere realizzata considerando:


- Processi,
- Servizi erogati,
- Insedimenti fisici,
- Aree geografiche,
- Aree di Business,
-;

3. Riduzione burocrazia con conseguente abbattimento delle tempistiche di analisi (es. unica intervista);
4. Risoluzione conflitti tra le diverse disposizioni normative tramite:
 - ❑ applicazione del requisito di sicurezza con grado di robustezza più alto,
 - ❑ utilizzo di reportistica a supporto delle decisioni del management;
5. Implementazione e mantenimento di un sistema di Gestione con attribuzione di ruoli e responsabilità (governance);

6. Storicizzazione analisi effettuate;
7. Indicazione gap da colmare per adeguamento a nuovi requisiti cogenti o facoltativi;



- ❑ Costoso in termini di utilizzo di risorse al primo approccio in relazione al livello di maturità del SGSI presente;
- ❑ Forte commitment per le persone coinvolte.

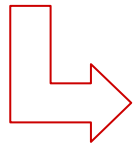


**Integrazione dei Sistemi di Gestione volontari
con quelli obbligatori con particolare riferimento
per la Sicurezza delle Informazioni**

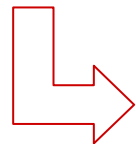
**Analisi del rischio come strumento di integrazione
dei sistemi di gestione (Aspetti pratici)**

Maggio 2008

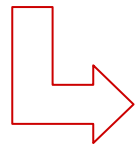
Modellazione Perimetro



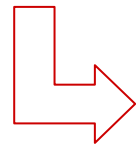
Individuazione Asset



Classificazione criticità



Analisi e Gestione
del Rischio

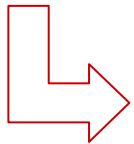


Report

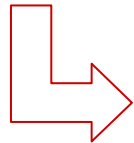
Funzionalità di MIGRA



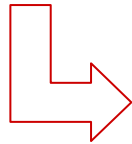
Modellazione Perimetro



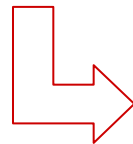
Individuazione Asset



Classificazione criticità



Analisi e Gestione
del Rischio



Report

Cogente
(es. D.Lgs.196/03)

Conformità

Facoltativo
(es. ISO/IEC 27001)

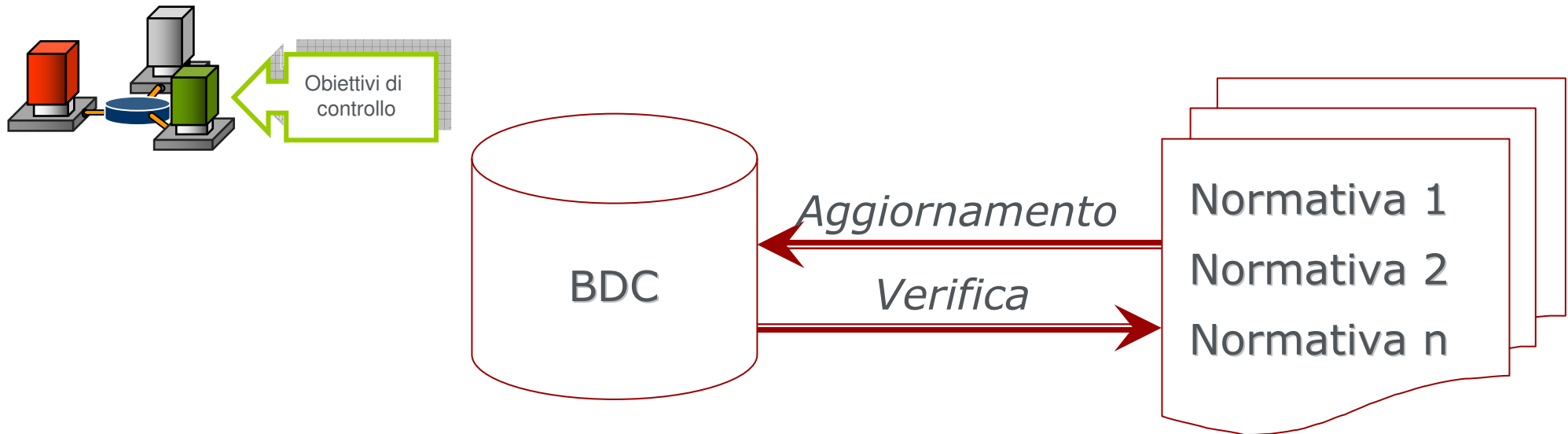
Cogente (es. D.Lgs.196/03)

L'adeguamento si ha solo se si implementa una specifica **graduazione di una contromisura,**

Facoltativo (es. ISO/IEC 27001)

L'adeguamento si ha se si implementa una **contromisura.**

L'adeguamento può essere più o meno soddisfacente a seconda della graduazione della contromisura implementata.



Aggiornamento: L'entrata in vigore di una nuova normativa può richiedere l'aggiornamento della Base di Conoscenza MIGRA,

Verifica: Prima di procedere all'aggiornamento occorre verificare che i nuovi requisiti di sicurezza non siano in contrasto con i precedenti.