



Analisi dei Rischi con CRAMM

28 Ottobre 2004

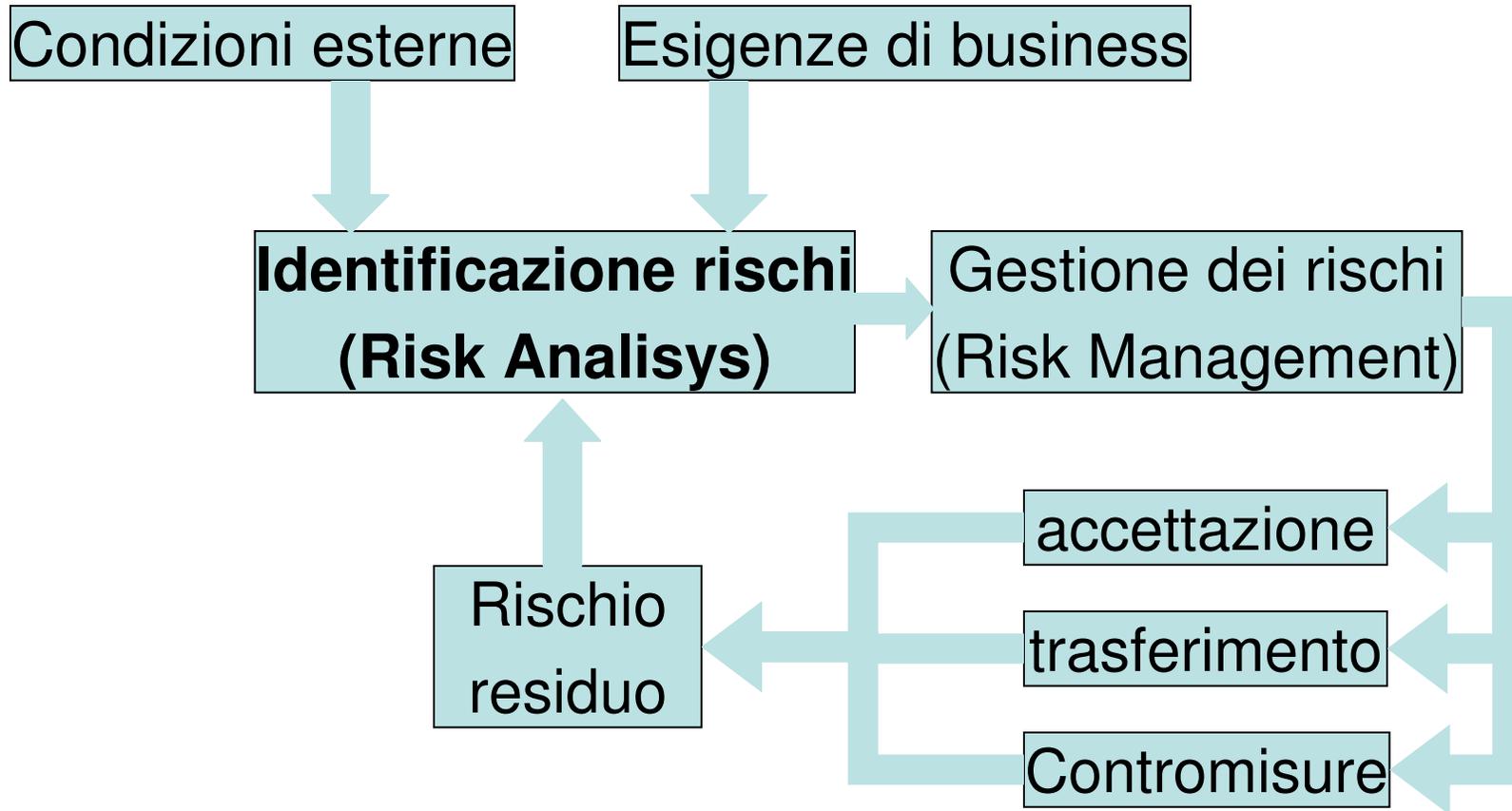
(a cura di **Carla Trincherò – Unisys**)



INDICE DELLA PRESENTAZIONE :

1. La sicurezza in azienda
2. Gestione del rischio in un'azienda
3. Risk Analysis
4. Perché il CRAMM?
5. I moduli della progettazione
6. Perimetro dell'analisi
7. Individuazione degli asset da proteggere
8. Scenari
9. Impatti
10. Vulnerabilità
11. Minacce
12. La Misura del rischio
13. I risultati del CRAMM
14. Benefici della soluzione

Gestione del rischio in un'azienda :



Risk Analysis

“L’analisi del rischio è un processo volto ad identificare e valutare il danno causabile da un incidente e, quindi, a individuare le contromisure adeguate al bene da proteggere”

Gli obiettivi:

- **Quantificare l’impatto in relazione ai possibili scenari**
- **Identificare vulnerabilità e minacce**
- **Individuare il bilanciamento ottimale tra l’impatto e il costo delle misure di sicurezza necessarie a ridurre il rischio**

Perché il CRAMM?

- Quantitativo/Qualitativo, rigoroso e generale
- Risk analysis & management
- Business Processes
- Metodo suddiviso in tre moduli e supportato da tool sw
- Orientato agli impatti, alle minacce ed ai rischi



Perché il CRAMM? Un po' di storia

- **1985: CCTA si pose l'obiettivo di sviluppare una metodologia per l'analisi e la gestione dei rischi**
- **1986: sviluppo di un metodo manuale**
- **1987: lancio della prima versione SW**
- **1992: versione 2.0**
- **.....**
- **2003: Versione 5.0**

Perché il CRAMM? Un po' di storia

Standard & Information Source

- British Standard on Information Security Management (BS 7799)
- Information Technology Security Evaluation Criteria (ITSEC)
- Computer Security Evaluation Criteria (TCSEC) and Common Criteria
- HMG Manual of Protective Security
- CISCO's white paper on setting up routers
-

Perché il CRAMM? Un po' di storia

- 113 tipi di HW, 21 di SW
- 9 scenari per la valutazione degli asset
- 27 Impatti
- 37 tipi di minacce e vulnerabilità predefinite (ciascuna applicabile ad un a determinata tipologia di asset)
- 3100 Contromisure (di cui 1500 relative ai controlli del BS 7799)
- Giustificazione delle CM tecniche (ITSEC: Security Target) ed organizzative (ISO 17799/BS 7799)

Perché il CRAMM?

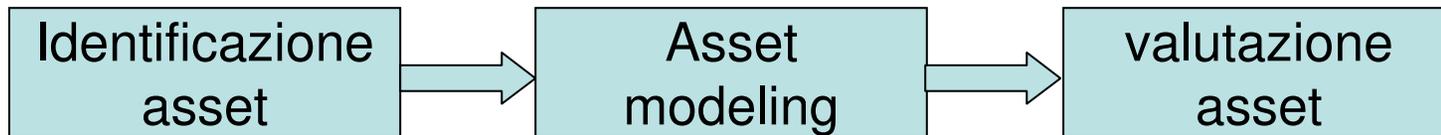
Caratteristiche principali

- **Consistenza:** sistemi simili, soggetti a simili rischi ottengono soluzioni simili
- **Flessibilità:** soluzioni più dettagliate
- **Rigore:** rischi non abbattuti e che
- **Efficienza:** le spese per la sicurezza possono essere giustificate
- **Audita:** correttamente e in modo idoneo
- **Awareness:** la revisione contribuiscono ad aumentare la consapevolezza dei problemi di sicurezza dei dati

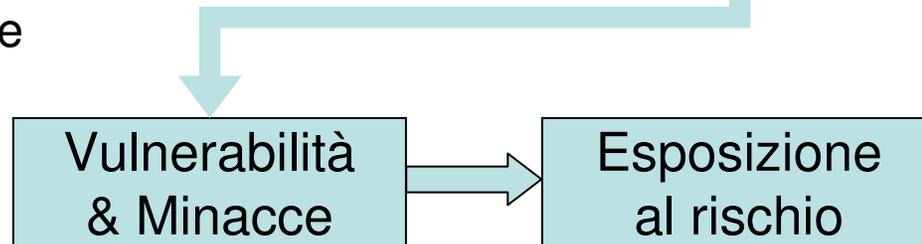
La caratteristica più importante è che il CRAMM fornisce una metodologia attraverso la quale le spese per la sicurezza possono essere giustificate

I moduli della progettazione

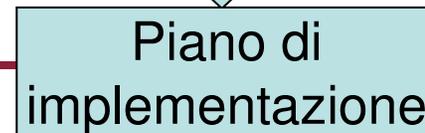
Identificazione & Valutazione asset



Analisi Vulnerabilità e Minacce



Risk Management



Scenari



- Sicurezza personale
- Privacy e dati personali
- Obblighi di legge
- Law enforcement
- Interessi economici e commerciali
- Perdite finanziarie
- Ordine pubblico
- Management e business
- Perdita di immagine

Impatti

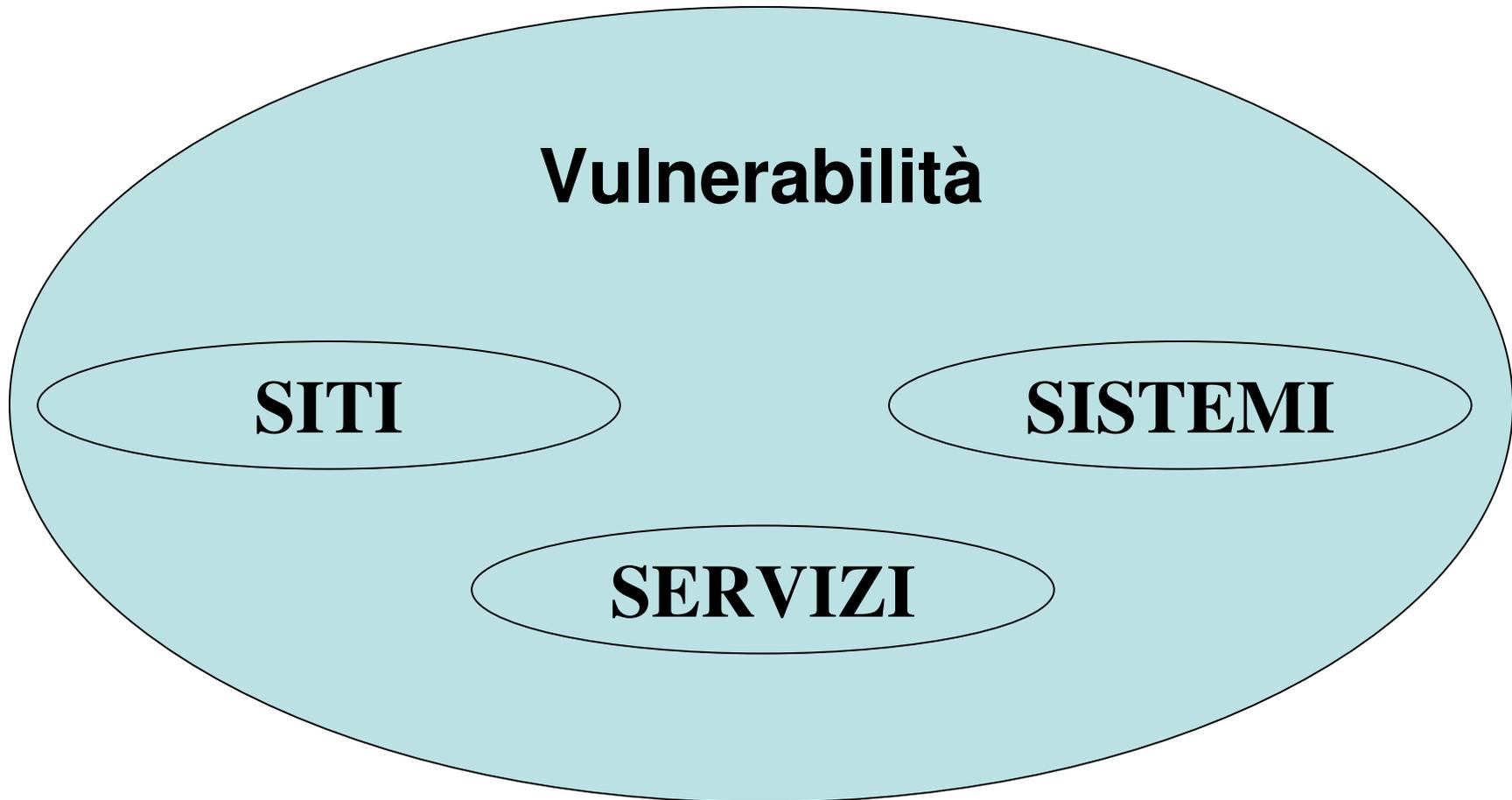
➤ Perdita, relativa ad uno o più scenari, conseguente al verificarsi di un incidente.

- **Divulgazione**
- **Distruzione**
- **Indisponibilità**
- **Modifica**
- **Ripudio**



IMPATTO

Vulnerabilità



Minacce



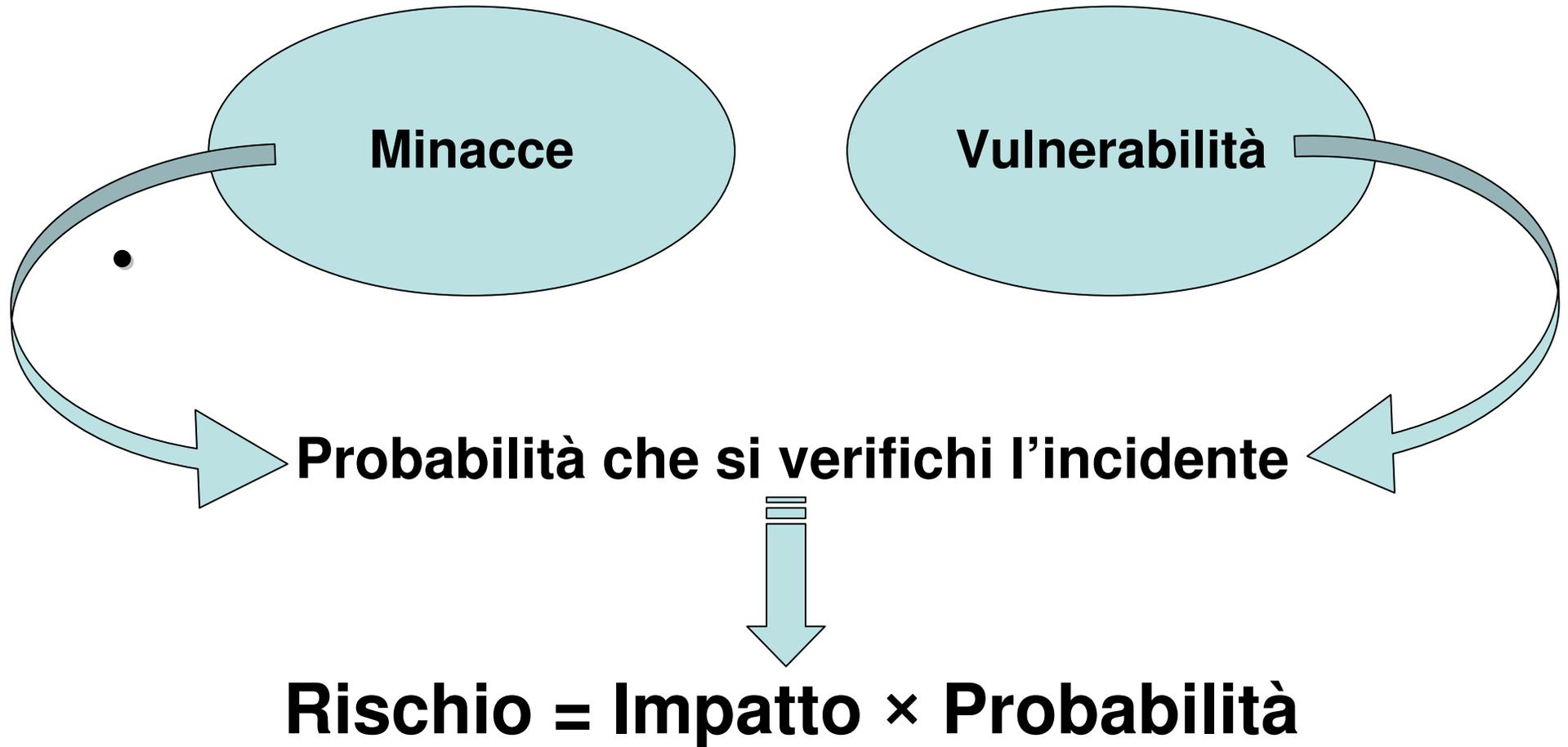
- La minaccia, invece, è definita come l'eventualità che la vulnerabilità sia sfruttata da un soggetto o da un'entità al di fuori del controllo dell'organizzazione per produrre effetti deleteri in termini economici o di perdita d'immagine.



Errori/omissioni
Introduzione SW illegale
Furti
Eventi naturali
Modifica/copia di informazioni
Manomissione
Vandalismo

.....

Misura del rischio



Contromisure



- Dalle informazioni contenute nella misura del rischio CRAMM estrapola un set di contromisure.
 - **Sul personale**
 - **Fisiche**
 - **HW/SW**
 - **Procedurali/organizzative**



Benefici della soluzione

- Ottenere una visione oggettiva dei rischi e delle priorità
- Giustificare la spesa per la sicurezza
- Supporto al risk management
- Soluzioni conformi agli standard della sicurezza