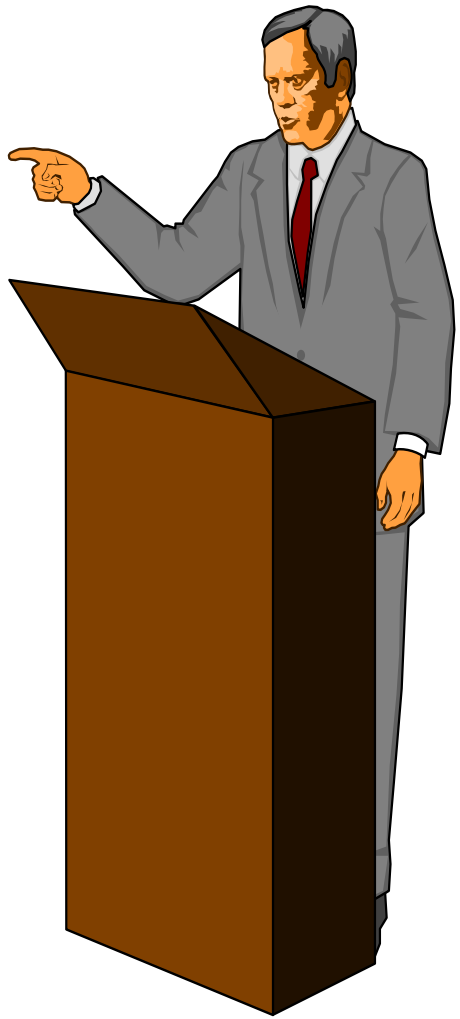
Risk Analysis
&
Risk Management

Prof. Ing. Claudio Cilli, CIA, CISA, CISSP, CISM
c.cilli@isacaroma.it

Risk Analyisis: Il problema

- Perdita di riservatezza
- Perdita di fiducia
- Perdita di disponibilità
- Perdita totale del bene
- Requisiti normativi e legali



Security Program Profile

Fase 1
Risk Analysis

Il processo di determinazione delle perdite potenziali correnti

Fase 2
Risk Management

Il processo di determinazione e verifica delle perdite potenziali

Perché effettuare una Risk Analysis?

- Fornire informazioni critiche al Management
- E’ un prerequisito per la Risk Management
- Rispettare leggi e regolamenti
- Ridurre le perdite provocate dalle minacce

Obiettivi della Risk Analysis

- Determinare quali beni sono critici
- Identificare e valutare le contromisure esistenti
- Identificare le minacce possibili
- Determinare le vulnerabilità
- Calcolare le perdite previste
- Raccomandare le azioni correttive

Metodologie di Risk Analysis

- **Quantitative**
  - Assegnare valutazioni economiche ai rischi
  - Inizialmente più costose e complesse
  - Vantaggio a lungo termine: ripetibili e confrontabili
- **Qualitative**
  - Vantaggiose quando i beni o i dati non sono facilmente valutabili in termini economici
  - Vantaggiose quando la criticità della missione e importante
  - Influenzano in misura minima la funzionalità della missione
  - Bassi costi di esecuzione

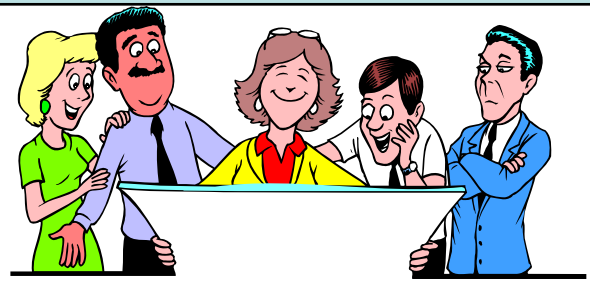
Risk Analysis Team

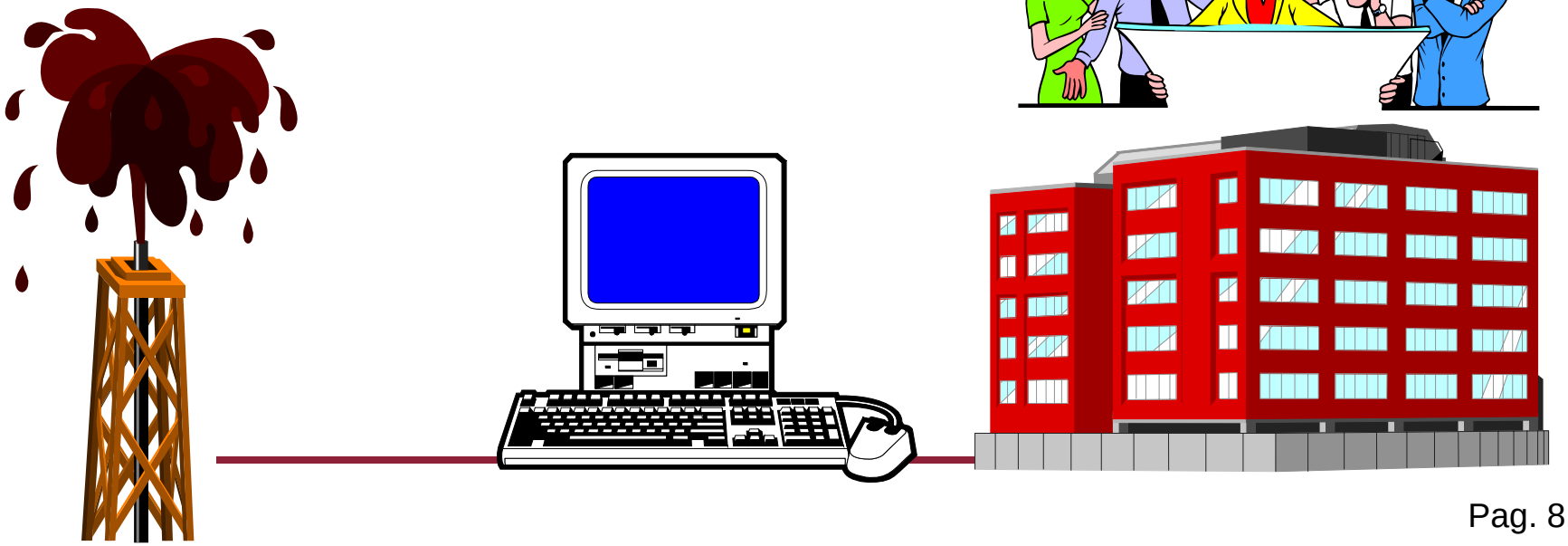
- Team Leader
- Proprietari dei dati
- Sistemisti e programmatori
- Responsabile della Sicurezza Fisica
- Internal Auditor
- Esperti delle varie tecnologie

Passo 1: Identificare gli Assets

- I beni (asset) rappresentano qualunque cosa di valore che necessita di essere protetto o salvaguardato

Dettagli sugli asset
- *Determinare il valore*
- *Verificare se condivisi con altre risorse*
- *Determinare se critici per l'organizzazione o la funzione*
- *Proprietà*
- *Locazione fisica*
- *Parte dell'inventario?*





Passo 2: Identificare le minacce

- Identificare le minacce applicabili e la loro frequenza di accadimento
- Le minacce sono eventi o azioni che possono potenzialmente avere impatto sugli asset

- Eventi naturali
- Errori umani
- Incendi
- Furti
- Alimentazione elettrica
- Problemi hardware
- Problemi software
- Abuso di privilegi da parte degli utenti

Dettagli sulle minacce

Giustificazione

- *Perché sono possibili*
- *Perché sono frequenti*

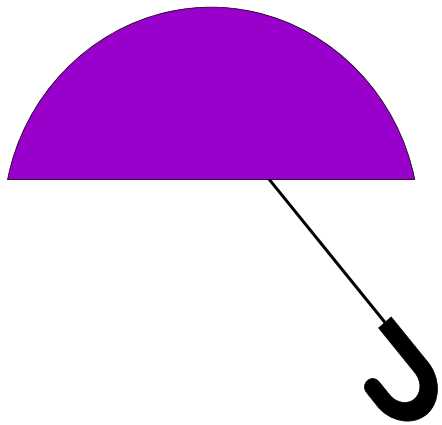
Frequenza di accadimento

- *Record storici*
- *Conoscenze empiriche*

Passo 3: Contromisure esistenti

- Identificare le contromisure attualmente esistenti
- Le contromisure sono apparati, processi, azioni e/o procedure in grado di ridurre le vulnerabilità

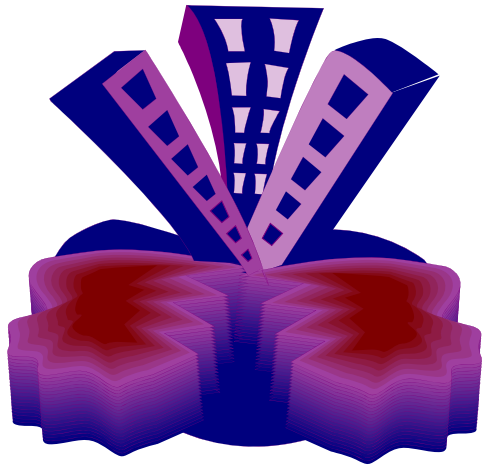
- Procedure organizzative
- Supporto del Management
- Contingency plan
- Metal Detector
- Antivirus software
- Difese perimetrali
- Training
- UPS
- Condizionamento
- Procedure di backup
- Controllo accessi
- CCTV
- Guardie



Valgono solo se opportunamente installate!

Passo 4: Vulnerabilità

- Determinare le vulnerabilità
- Le vulnerabilità rappresentano una condizione di debolezza



Esempi di vulnerabilità

Suscettibilità a:

- Accessi non autorizzati
- Eventi naturali
- Instabilità dell'alimentazione elettrica
- Attività terroristica
- Dipendenza da una sola persona
- Errori degli utenti o degli operatori
- Incendio
- Furto di risorse

Quantificare le vulnerabilità

- *I livelli di vulnerabilità sono calcolati basandosi sulle contromisure attualmente esistenti*
- *Il processo di risk analysis deve identificare le aree di vulnerabilità e i loro livelli*

Una debolezza può consentire alle minacce di avere impatto sugli asset

Passo 5: Calcolo delle perdite

- Calcolo delle perdite stimate:

$(V_L * Asset_{Cost} * T_V) = SLE$

And, SLE * $Threat_{Multiplier}$ = ALE

Dove:

V_L= Livello di vulnerabilità

T_v= Valore della minaccia (Threat Value)

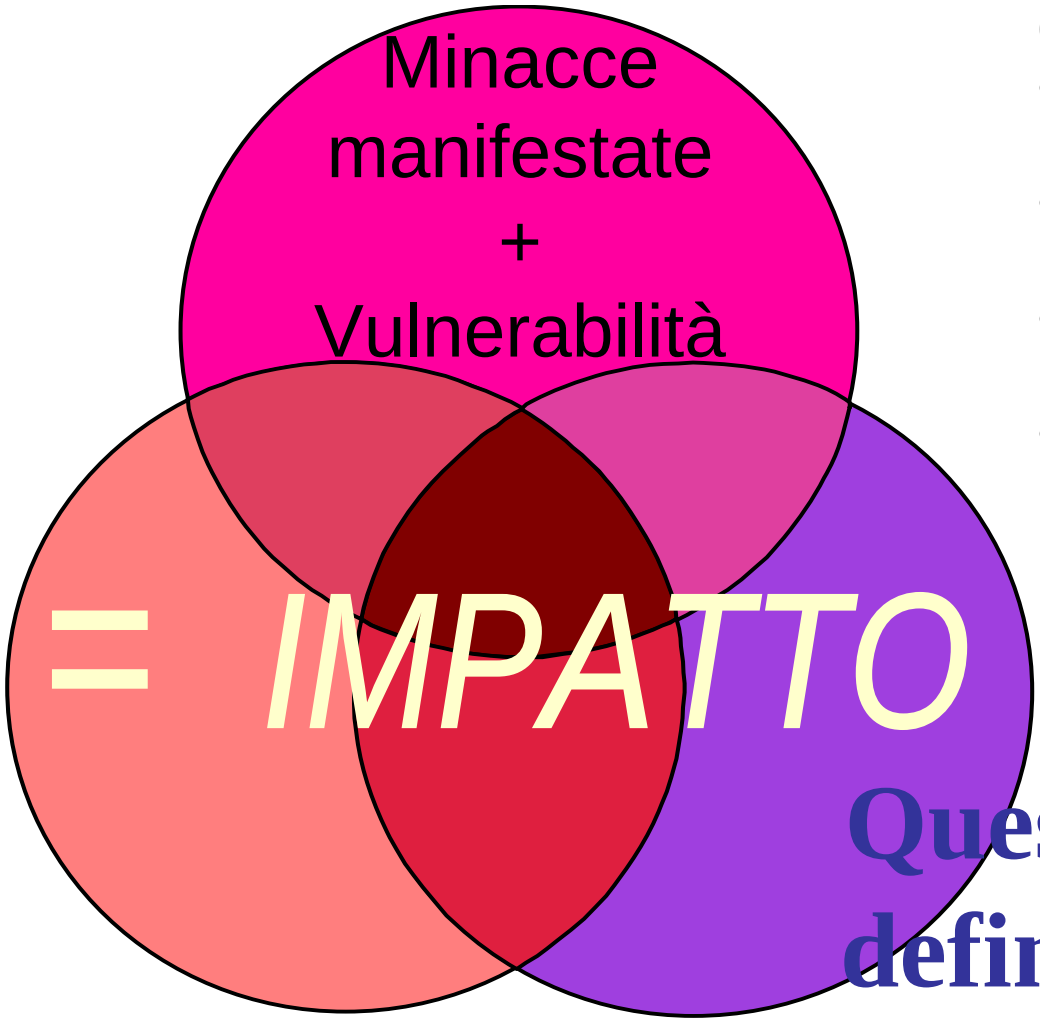
SLE= Single Loss Expectancy

ALE= Annual Loss Expectancy

La perdita (loss) è una misura dell'impatto su un bene da parte di una o più minacce

L'impatto è un ben preciso valore, calcolato e determinato

Impatto



Categorie di impatto:

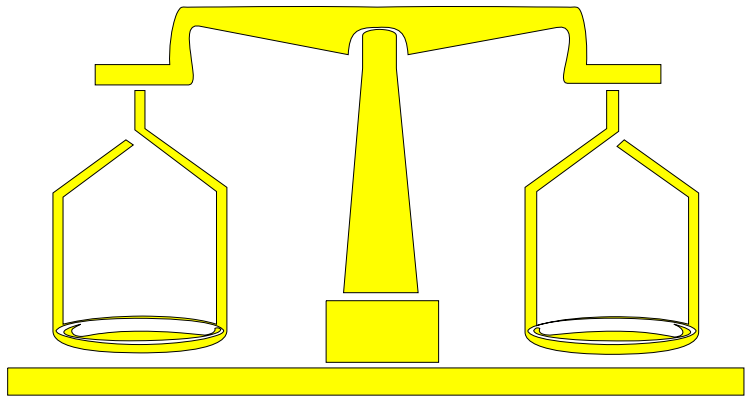
- *Divulgazione (perdita di riservatezza)*
- *Distruzione (perdita completa del bene)*
- *Perdita di fiducia (Asset disponibile, ma inaffidabile)*
- *Negazione del servizio (Asset indisponibile)*

Questo è ciò che si definisce "rischio"

Passo 6: Raccomandazioni

Raccomandare le opportune azioni correttive

- *Vi sono molti modi per ridurre la perdita attesa dovuta a una contromisura*
- *Sono necessarie negoziazioni economiche in fase operativa e di acquisizione*
- *Alcune contromisure sono imposte da norme e regolamenti*
  - *Contingency plan*
  - *Security training*
- *Alcune contromisure sono discrezionali*

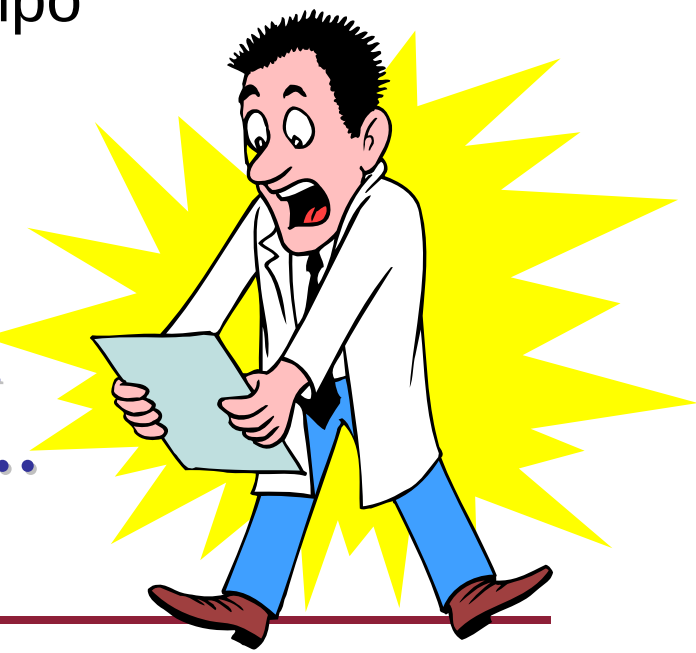


Ogni azione correttiva è una contromisura

Processi comuni

– Sia se automatici o manuali, in ogni risk analysis devono essere completati i medesimi passi…
  - Devono essere allocate delle risorse
  - Deve essere speso del tempo

E, come in ogni processo, il management deve decidere…



Il paradigma dell'automazione

- Una metodologia valida consente di completare tutti i passi con:
  - Meno impiego di risorse interne
  - Procedure più consistenti
  - Risultati ripetibili
  - Risultati più accettabili
  - Meno tempo
  - Costi inferiori

Assioma 1

- Esiste sempre la stessa popolazione di minacce
  - Postulato: La popolazione di minacce è infinita in numero e varietà. Ogni minaccia si manifesterà con frequenza indeterminata e incontrollata. La stessa popolazione di minacce esiste per ogni sistema in ogni luogo. Solo il comportamento apparente delle minacce varia

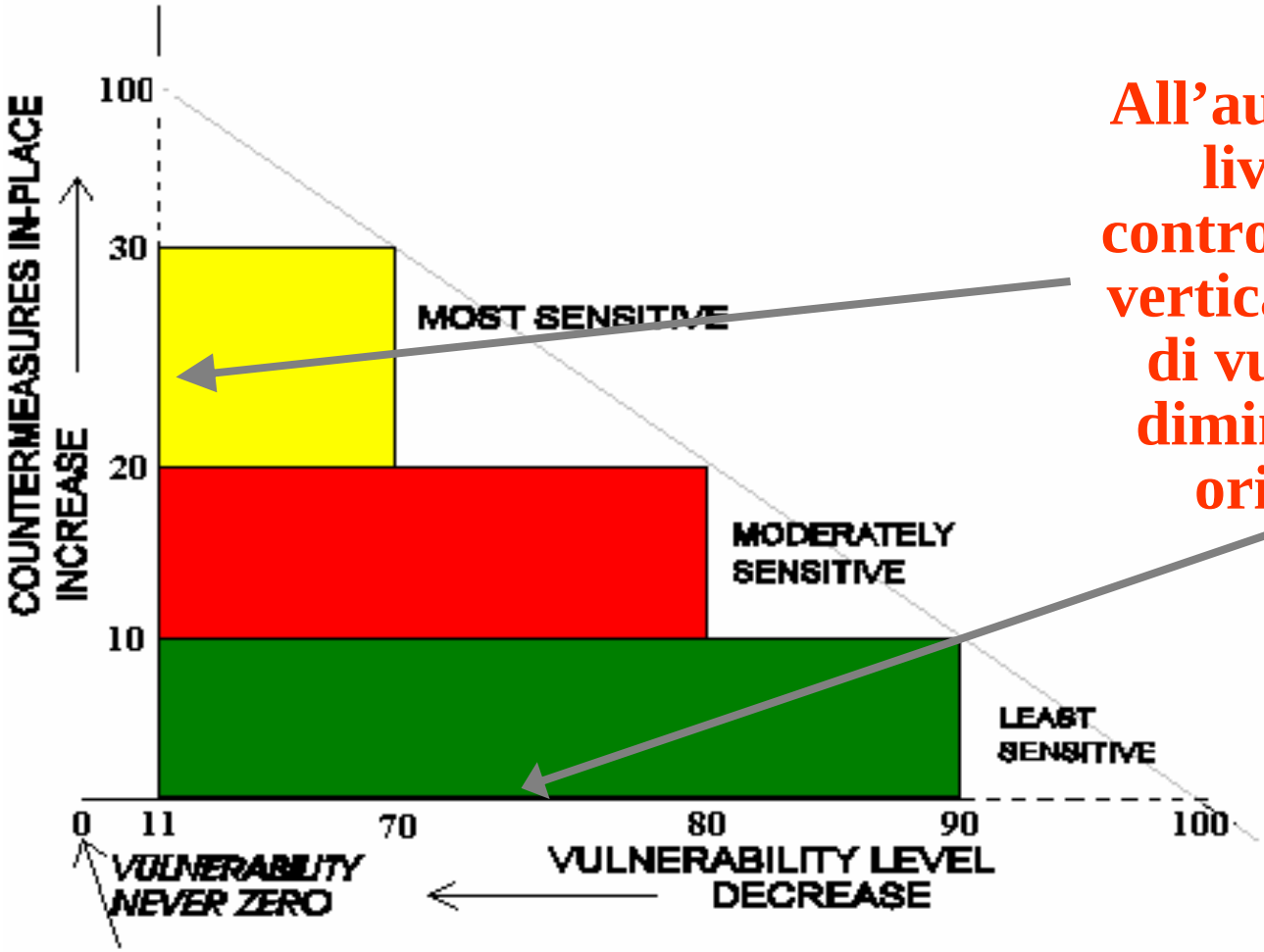
Assioma 2

- La frequenza di occorrenza di una minaccia non può essere alterata
  - Postulato: Le alterazioni apparenti della frequenza di occorrenza delle minacce sono, in realtà, contromisure. Queste contromisure riducono il livello di vulnerabilità alla specifica minaccia, non quanto spesso questa si manifesta

Assioma 3 (Primario)

- All’aumentare del livello delle contromisure presenti, diminuisce la vulnerabilità
  - Postulato: Il livello di vulnerabilità alle minacce si riduce adottando le contromisure. Alcune contromisure sono più efficaci per modificare la vulnerabilità di altre. Il livello di vulnerabilità e il valore di ogni contromisura indicata per ridurlo possono essere espressi numericamente

Contromisure vs. vulnerabilità



All'aumentare del livello delle contromisure (asse verticale), il livello di vulnerabilità diminuisce (asse orizzontale)

Assioma 4

- Tutte le contromisure presentano vulnerabilità
  - Postulato: Un livello di vulnerabilità ZERO non può mai essere ottenuto poiché tutte le contromisure hanno esse stesse delle debolezze. Data una contromisura, possono essere identificate una o più vulnerabilità

Assioma 5

- L’impiego di contromisure può consentire di ottenere un livello accettabile di vulnerabilità
  - Postulato: Esiste una combinazione di contromisure che consente di ottenere un qualunque arbitrario livello di vulnerabilità. Aggiungendo contromisure, il livello di vulnerabilità può essere portato a un livello commisurato all’importanza, sensibilità o livello di classificazione delle informazioni elaborate

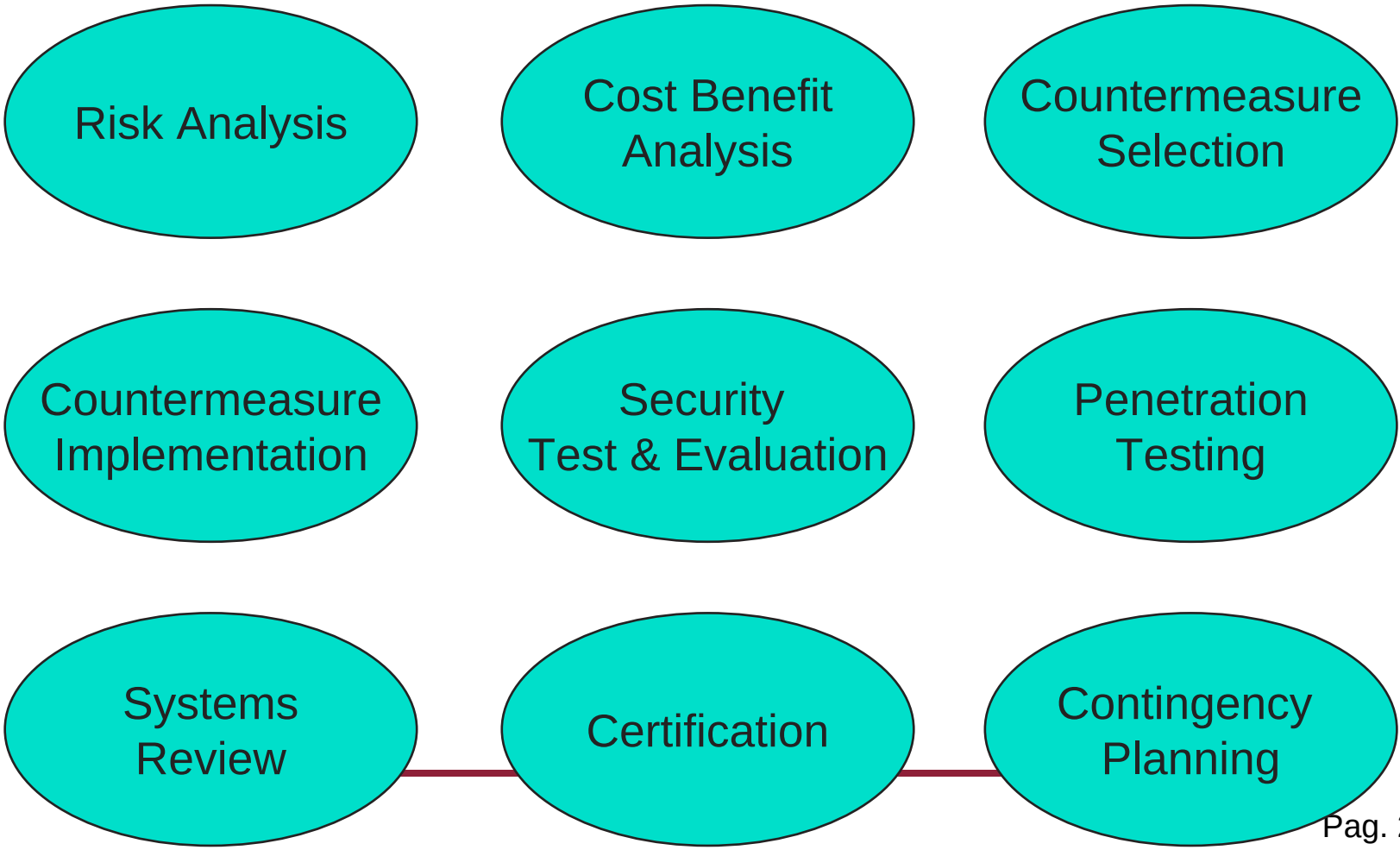
Risk Management

Processo relativo all’identificazione, valutazione, controllo e riduzione dei rischi nei sistemi informativi

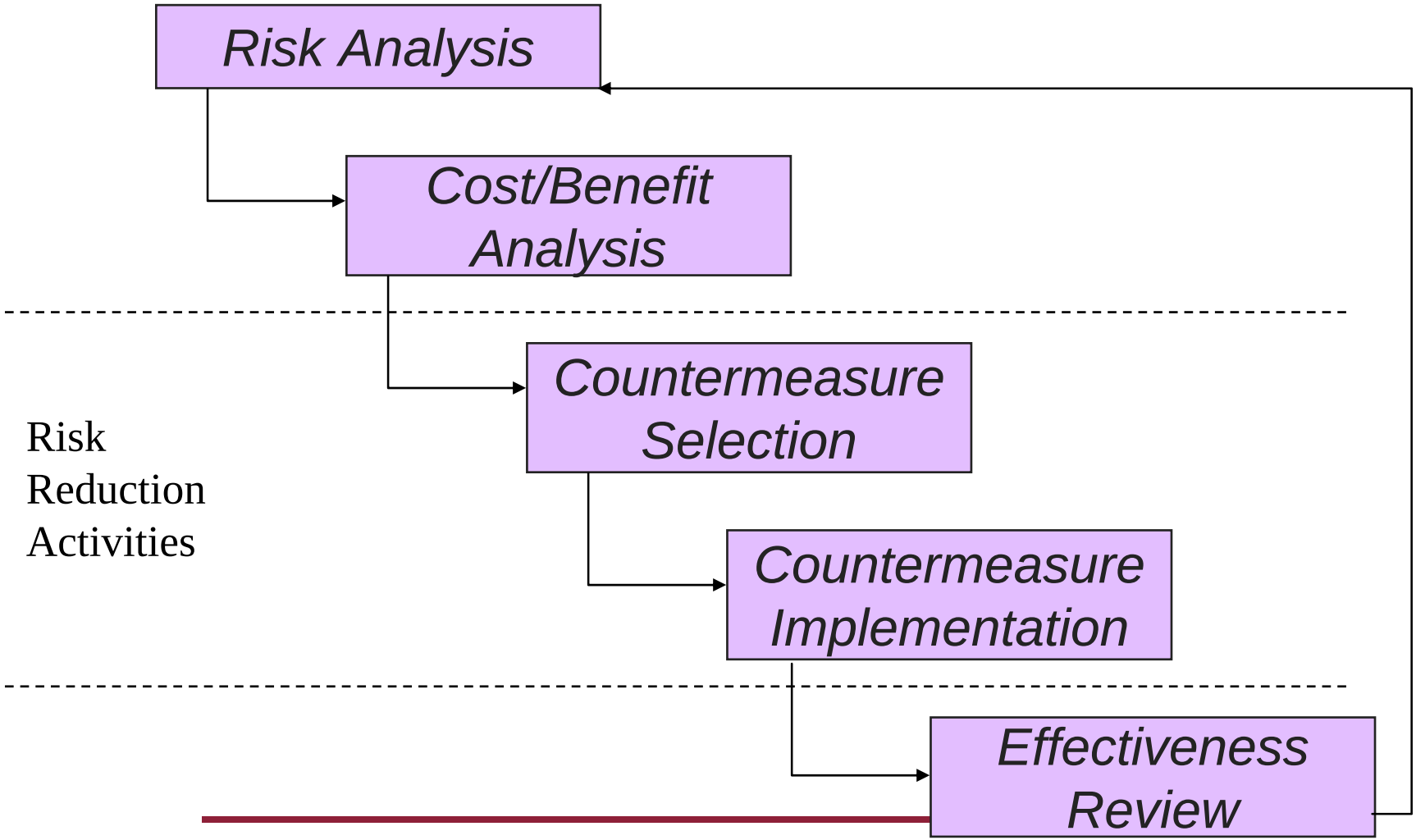
Obiettivi del Risk Management

- Identificare aree specifiche dove le protezioni sono necessarie per prevenire deliberate o accidentali divulgazioni non autorizzate, modifiche, uso non autorizzato delle informazioni, o negazione del servizio
- Utilizzo dell'approccio basato sul rischio
- Conduzione di risk assessment
  - In ogni caso almeno ogni tre anni
  - Modifiche significative dell'ambiente IS

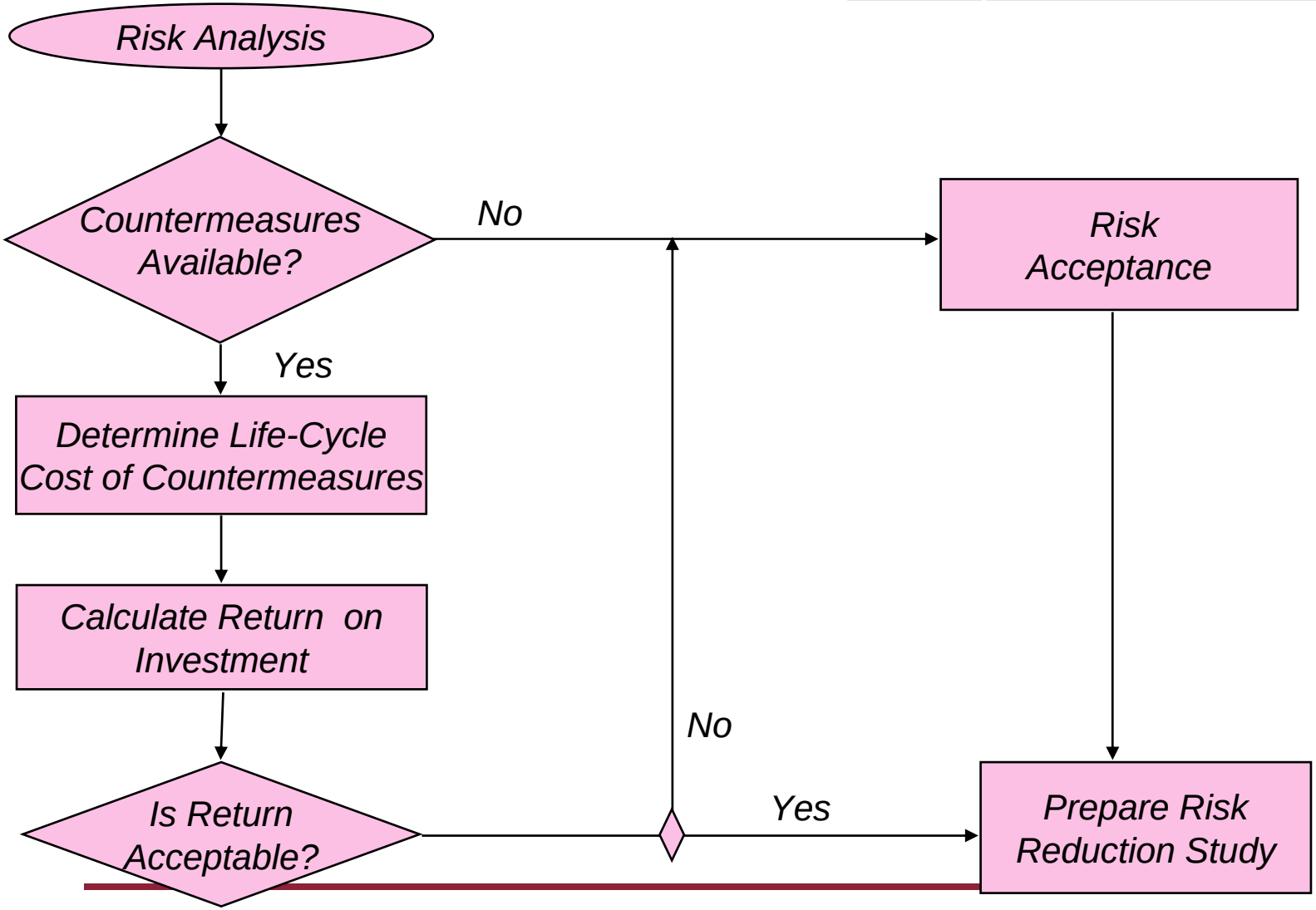
Quadro di sintesi del Risk Management



Metodologia di Risk Management



Analisi Costi/Benefici



Matrice di identificazione delle contromisure

Obiettivo di Controllo / Tipo di Controllo	Preventive	Rivelatrici/ Deterrenti	Correttive
Amministrative			
Fisiche			
Tecniche			

Life-Cycle Cost delle contromisure

- Costi di investimento
- Costi di implementazione
- Costi operativi e di manutenzione
- Costi diretti e indiretti

Metodi di calcolo del costo

- Quantitativi ($$$)
  - ALE (Annual Loss Exposure)
  - SOL (Single Occurrence Loss)
- Qualitativi
  - Analisi del rischio sommari
    - Fuzzy metrics
    - No risk/Very high risk
    - Rank 1 to 10

Calcolo del Ritorno dell'Investimento

- Benefici economici:
  - ROI = ALE originale – ALE dopo l'applicazione delle contromisure
  - Costo annuale delle contromisure
- Benefici non economici
  - Migliore gestione
  - Migliori consapevolezza e fiducia sulla sicurezza
  - Costi futuri evitati
  - Livello di integrità dei dati migliorato

Studio della riduzione del rischio

- L'obiettivo è di presentare al management le contromisure necessarie alla riduzione del rischio
- Comprende:
  - Risultati della Risk Analysis
  - Raffigurazioni degli ipotetici scenari minaccia/vulnerabilità
  - Risultati dell'analisi costi/benefici
  - Configurazioni alternative delle contromisure

Selezione delle contromisure

- Necessità reali di protezione per l'organizzazione
- Valore delle informazioni vs. rischio di perdita
- Determinazione del livello di accettazione del rischio
- Identificazione delle vulnerabilità da eliminare
- Valutazione del ritorno dell'investimento
- Determinazione delle contromisure cost-effective da implementare
- Allocazione delle risorse economiche

Opzioni quando si selezionano le contromisure

- Riduzione dei rischi
- Prevenzione da perdita
- Limitazione delle perdite
- Trasferimento delle perdite
- Rischio accettabile

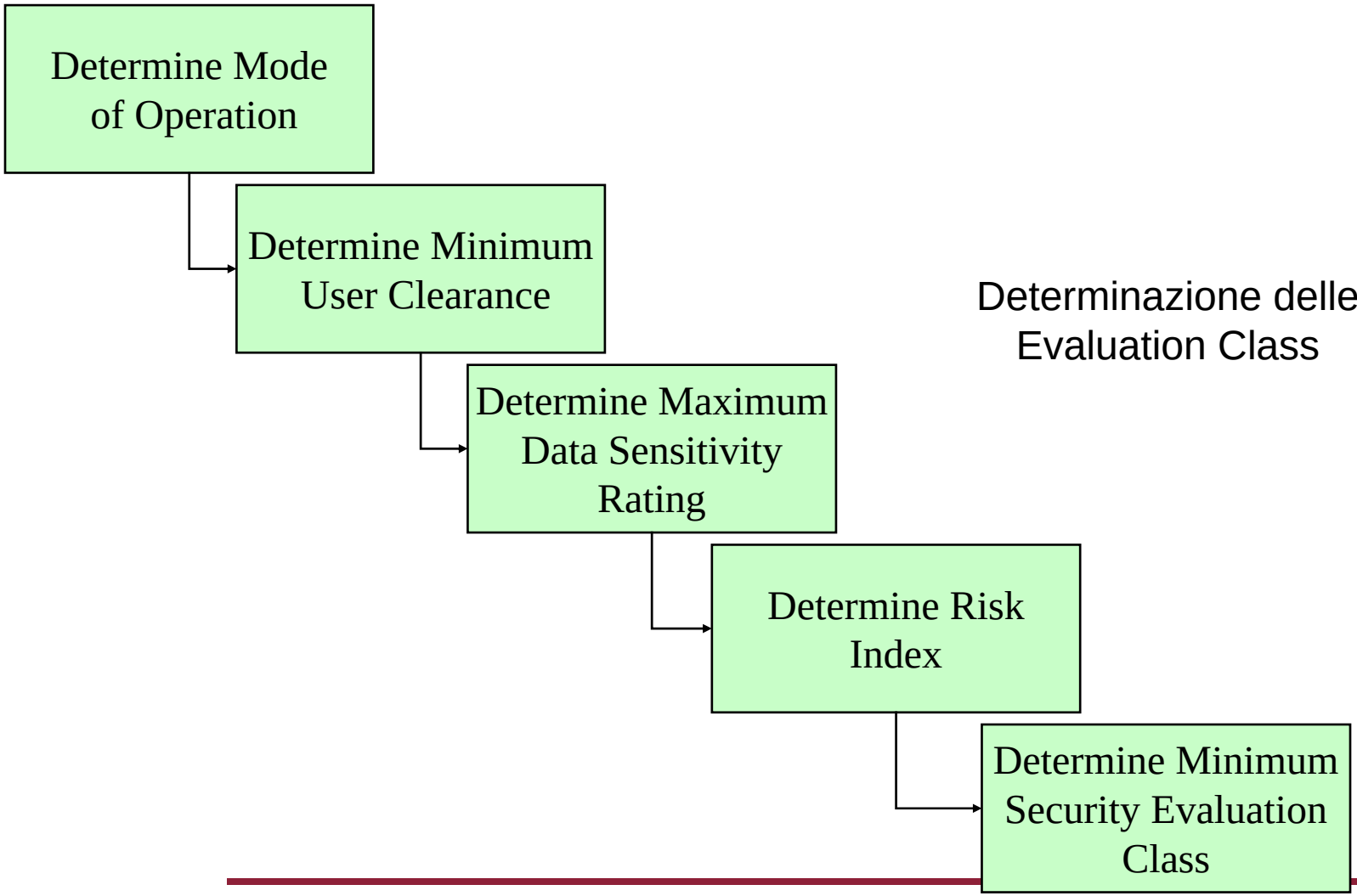
“Absolute security is achieved only at unlimited cost”

Dennis Steinauer, NIST

Revisione dell'efficacia

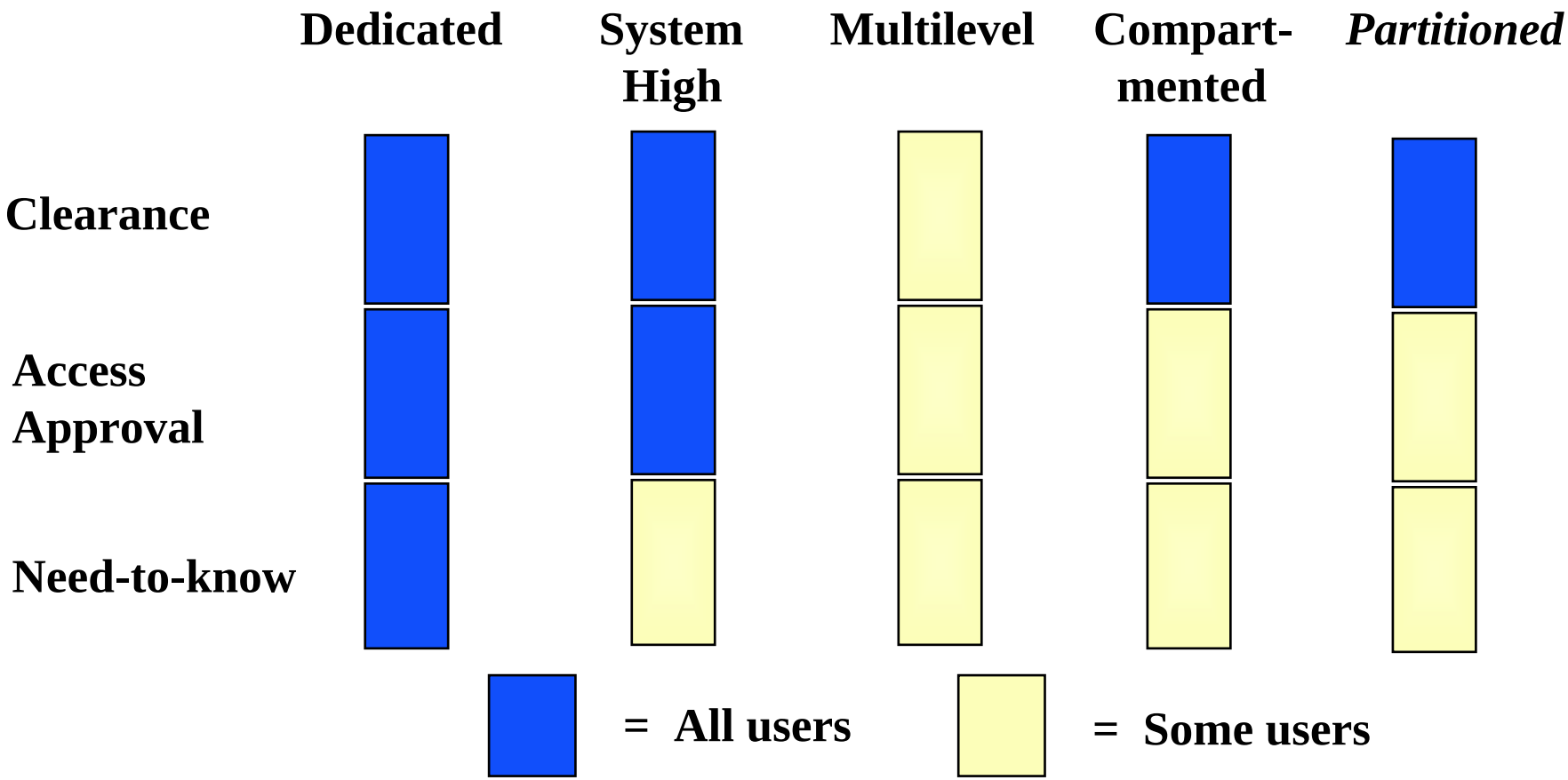
- Valutazione periodica delle contromisure a seguito di:
  - Modifiche nei processi operativi
  - Tipi di applicazioni
  - Modifica degli obiettivi del Management
  - Nuove tecnologie
- Il Risk Management deve essere applicato il tutto il System Life-Cycle

Esempio di Risk Analysis: Orange Book



Determinazione delle Evaluation Class

Orange Book: Modes of Operation



Orange Book: Minimum User Clearance

MINIMUM USER CLEARANCE	RATING (R_{min})
Uncleared (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)/Current Background Investigation (BI)	4
Top Secret (TS)/Current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

Orange Book: Maximum Data Sensitivity

Maximum Data Sensitivity Ratings Without Categories	**RATING (R_{max})**	**Maximum Data Sensitivity With Categories**	**RATING (R_{max})**
Unclassified	0	Not Applicable	
Not Classified but Sensitive	1	N With One or More Categories	2
Confidential	2	C With One or More Categories	3
Secret	3	S With One or More Categories With No More Than One Category Containing Secret Data	4
		S With Two or More Categories Containing Secret Data	5
Top Secret	5	TS With One or More Categories With No More Than One Category Containing Secret or Top Secret Data	6
		TS With Two or More Categories Containing Secret or TS Data	7

Orange Book: Calcolo del Risk Index

- **If Rmin < Rmax**
  - Risk Index = Rmax - Rmin
- **If Rmin > Rmax**
  - Risk Index = 1, if there are categories on the system to which some users are not authorized access
  - 0, otherwise

R_{max} = *System's maximum data sensitivity*
R_{min} = *System's minimum user clearance*

Orange Book:
Minimum Security Evaluation Class

RISK INDEX	Mode of Operation	Minimum Criteria Class for Open Environments	Minimum Criteria Class for Closed Environments
0	Dedicated	No Prescribed Min	No Prescribed Min
0	System High	C2	C2
1	Compartmented, Multilevel	B1	B1
2	Compartmented, Multilevel	B2	B2
3	Multilevel	B3	B2
4	Multilevel	A1	B3
5	Multilevel	*	A1
6	Multilevel	*	*
7	Multilevel	*	*

Penetration Test & Automated Risk Analysis Tools

- Test di sicurezza nei quali i valutatori cercano di eludere le protezioni di sicurezza di un sistema informativo basandosi sulla loro comprensione del sistema stesso e della sua implementazione
- NIST Special Publication 500-174
  - “Guide for selecting automated tools”
- Processo di selezione degli strumenti automatici
  - Assegnazione delle persone
  - Definizione dei requisiti
  - Preparazione di una checklist per la selezione
  - Richiesta di una dimostrazione dei sistemi candidati
  - Valutazione delle alternative
  - Selezione del package