

L'analisi delle contromisure ai fini di garantire la disponibilità, l'integrità e la riservatezza delle informazioni

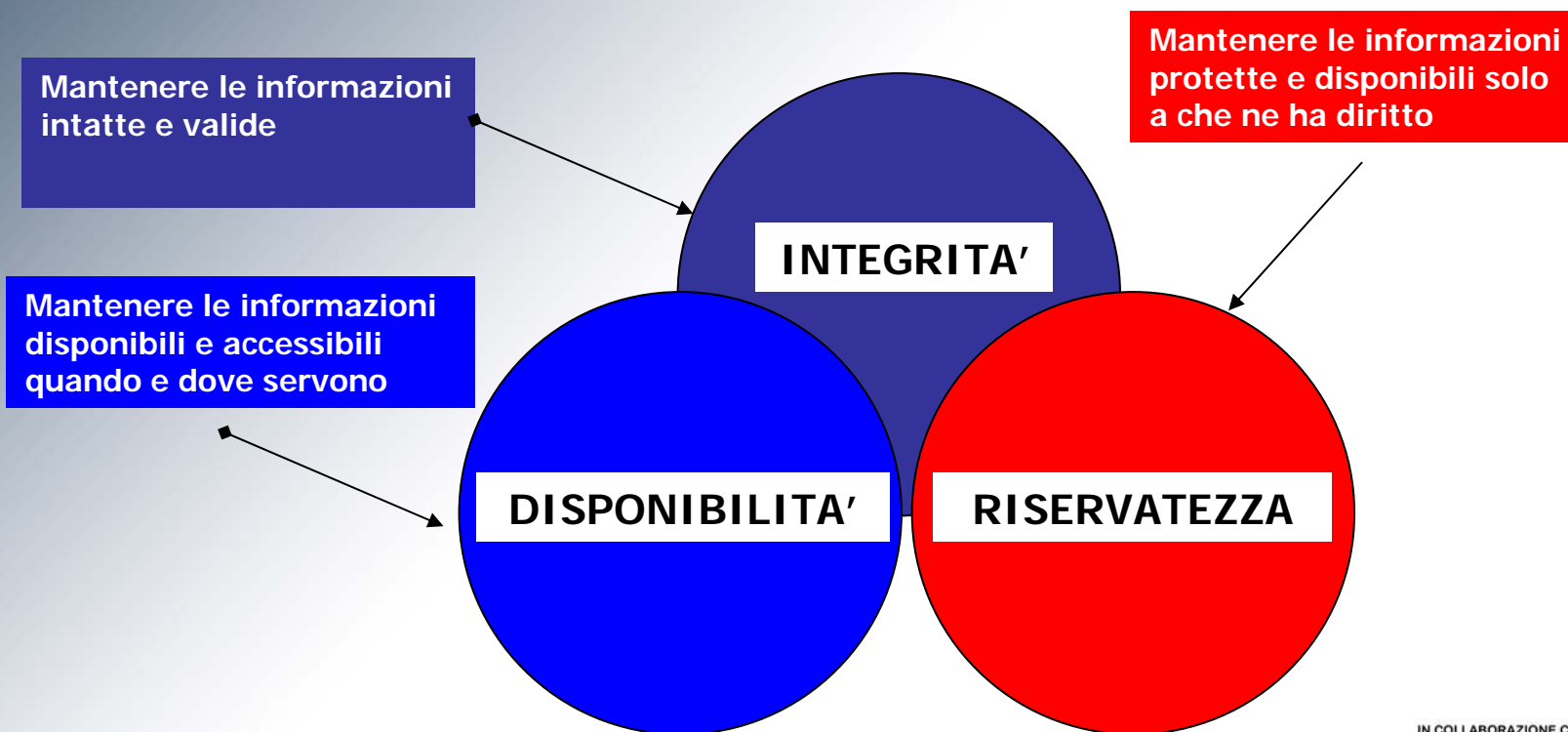
Ing. Michele Tassinari (Auditor CERMET per la ISO 27001)

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

La Sicurezza delle Informazioni si caratterizza nella prevenzione e protezione di tre parametri fondamentali



IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani



Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 13335-1:2004]

La riservatezza si riferisce a quei servizi richiesti per proteggere l'informazione dalla divulgazione non autorizzata. Nella categoria delle informazioni che devono essere protette dall'accesso pubblico possono essere inglobate alcune informazioni come: records sul personale, reports di ricerca e sviluppo, strategie di mercato, cartelle cliniche, ecc.

Per stimare il valore di riservatezza di una specifica risorsa informativa, si deve cercare di ipotizzare ciò che qualcuno o l'organizzazione è disposto a pagare per ottenere l'informazione, oppure il danno che la compagnia può subire se l'informazione dovesse cadere in mani sbagliate.

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani



Integrity: The property of safeguarding the accuracy and completeness of asset. [ISO/IEC 13335-1:2004]

La *integrità* si riferisce a quei servizi che sono richiesti per assicurare che l'informazione sia corretta, completa e autentica quando viene elaborata, trasmessa, presentata e memorizzata. L'integrità dell'informazione può essere a volte molto più importante della sua riservatezza.

Availability: The property of being accessible and usable upon demand by authorized entity. [ISO/IEC 13335-1:2004]

La *disponibilità* delle risorse di rete, dei servizi e dell' informazione continua a crescere per importanza al crescere dell' espansione delle reti.

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

1. Identificazione degli asset

Asset: Anything that has value to the organisation [ISO/IEC 13335-1:2004]

Output: Il risultato di questa fase è un inventario contenente tutti i principali “assets” all’interno del ISMS considerato, la loro locazione e il loro gestore (“owner”)

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

2. Valutazione degli asset

Output: Il risultato di questa fase l’assegnazione di un valore, ad esempio sulla base della **riservatezza, disponibilità, e integrità**, o in base ad altri criteri se applicabili, ad ognuno degli asset identificati nel passo prima.

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

3. Identificazione dei requisiti di sicurezza

Output: Il risultato di questa fase è l'identificazione delle minacce e vulnerabilità, oltre ai requisiti cogenti e contrattuali o interni, per ciascuno degli asset individuato.

Threat: a potential cause of an unwanted incident, which may result in harm to a system or organisation

Vulnerability: a weakness of an asset or group of asset, which can be exploited by a threat.

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

4. Valutazione dei requisiti di sicurezza

Output: Come per la valutazione degli assets, il risultato di questa fase è l'assegnazione di un valore, sulla base della metodologia di analisi del rischi scelta, ai requisiti di sicurezza

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

5. Calcolo del rischio

Output: Il risultato di questa fase è il calcolo del rischio per ciascun asset all'interno del campo di applicazione del ISMS in termini di divulgazione, modifica non disponibilità e distruzione.

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

6. Identificazione ed
valutazione di
contromisure per il
trattamento del
rischio

Output: Il risultato di questa fase è l'identificazione e documentazione delle contromisure adottate a seguito della valutazione dei rischi.

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

6. Identificazione ed
valutazione di
contromisure per il
trattamento del
rischio

Eliminare il rischio: Ad esempio:

- Non Conducendo certe attività;
- Rimuovendo gli asset da un area fisica ad un'altra;
- Non processando certe informazioni in quanto non può essere garantita l'adeguata protezione.

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

6. Identificazione ed
valutazione di
contromisure per il
trattamento del
rischio

Trasferire il rischio: Ad esempio:

- Assegnando in outsourcing assets critici;
- Gestendo adeguate coperture assicurative

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

7. Selezionare adeguati controlli

Output: Il risultato di questa fase è la riduzione di tutti quei rischi identificati con la necessità di un trattamento

Ridurre il rischio: rischi che si possono ridurre operando sulla limitazione del danno con l'adozione di sistemi di controllo e prevenzione

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)

7. Selezionare adeguati controlli

Output: Il risultato di questa fase è la riduzione di tutti quei rischi identificati con la necessità di un trattamento

Accettare il rischio: rischi il cui danno probabile è inferiore al costo di gestione e di trasferimento

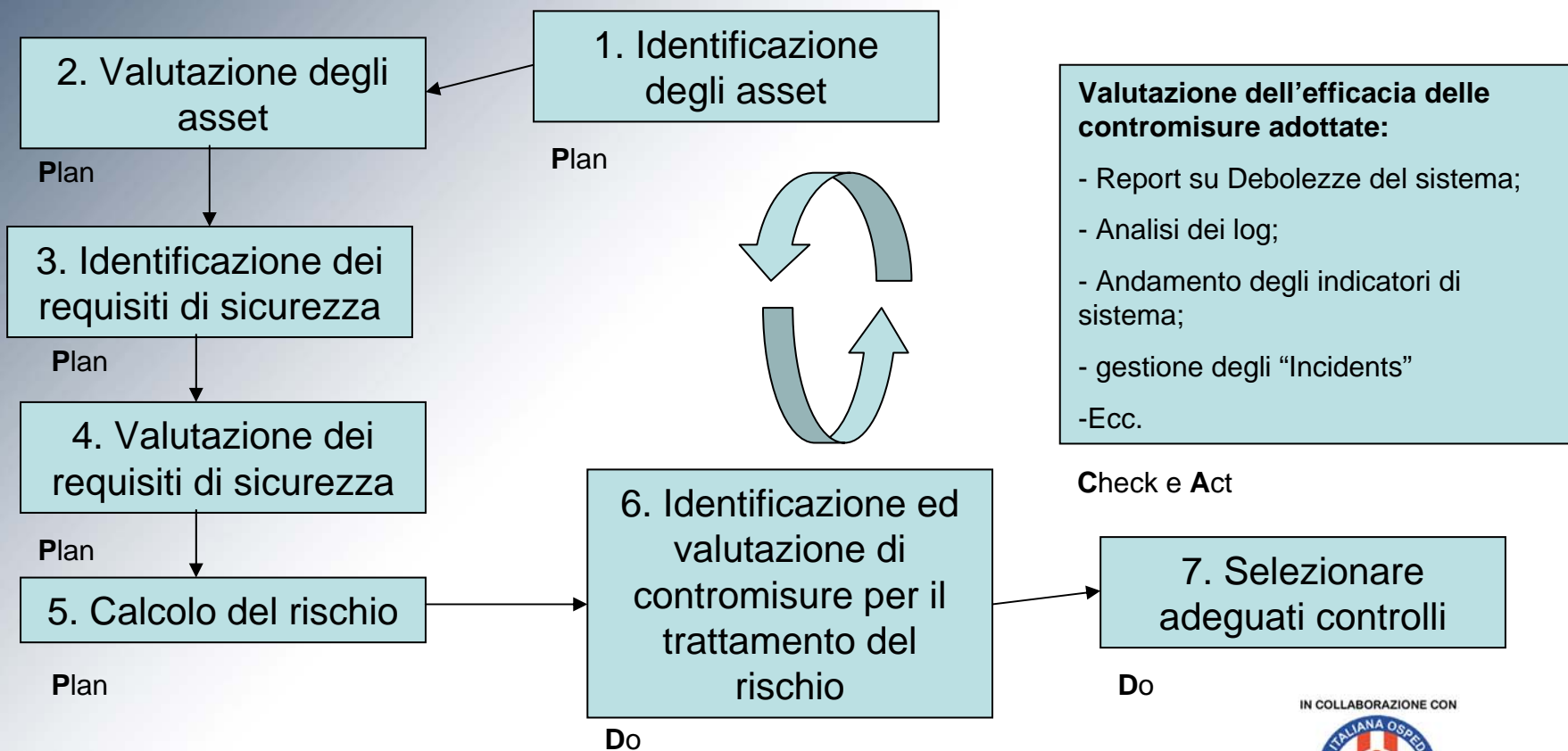
IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani

“Principali fasi del risk assessment

(Fonte documento BSI PD 3002:2002)



L'analisi delle contromisure ai fini di garantire la disponibilità, l'integrità e la riservatezza delle informazioni

Ing. Michele Tassinari (Auditor Cermet per la Iso 27001)

IN COLLABORAZIONE CON



Consulta Nazionale Aiop Giovani