CYBER RESILIENCE

Linee guida per l'acquisizione dei sistemi IT e OT, con implementazione dei processi orientati al «Security by Design»

La NAV-50-4217-0010-13-00B000

CF Gianluca Maria MARCILLI

Facendo un po' di sintesi

CYBER RESILIENCE

L'acquisizione di Navi e Sistemi «Secure by Design»

La NAV-50-4217-0010-13-00B000

CF Gianluca Maria MARCILLI

La sicurezza cibernetica

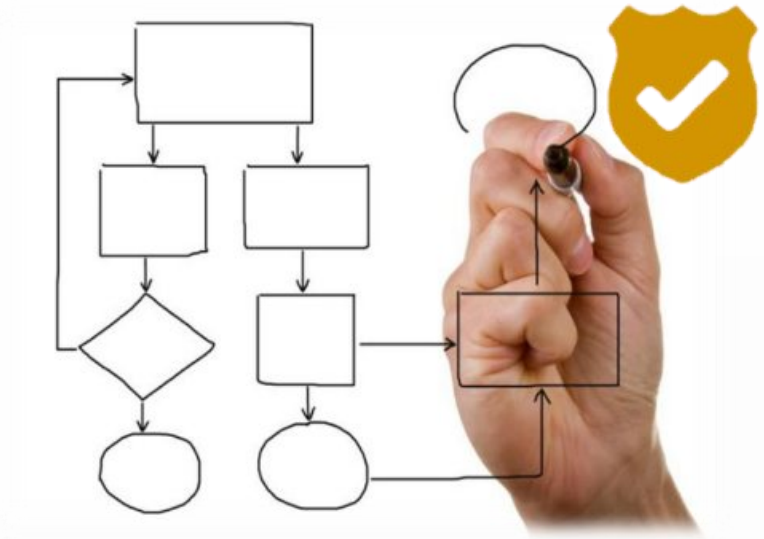
Scelte tecniche

COMITATO ELETTROTECNICO ITALIANO

ISO International Organization for Standardization

UNI ENTE ITALIANO DI NORMAZIONE

Valutazione del fattore umano



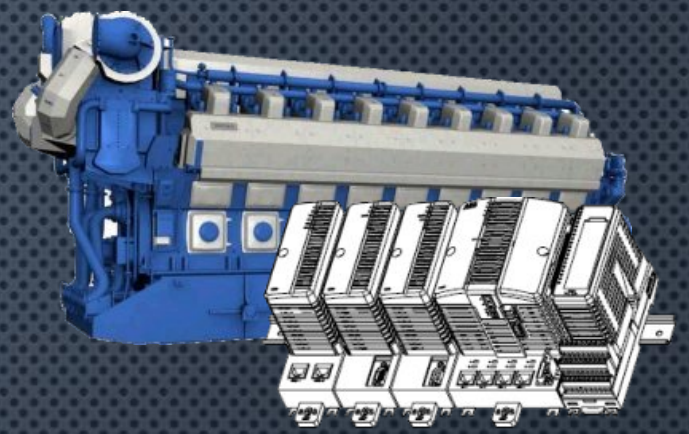
Scelte organizzative e procedurali

https://www.facebook.com/vitadainformatici/

CYBER SECURITY E RISK MANAGEMENT

Valutazione Tecnica

Strategie di mitigazione



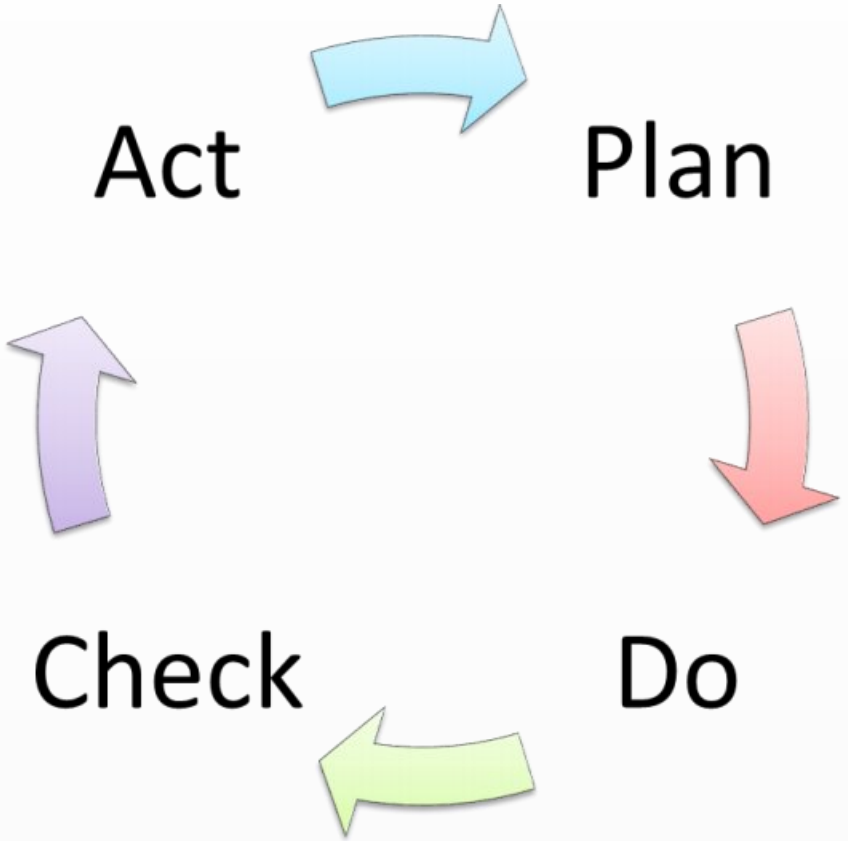
IT vs OT

- Confidenzialità
- Integrità
- Disponibilità

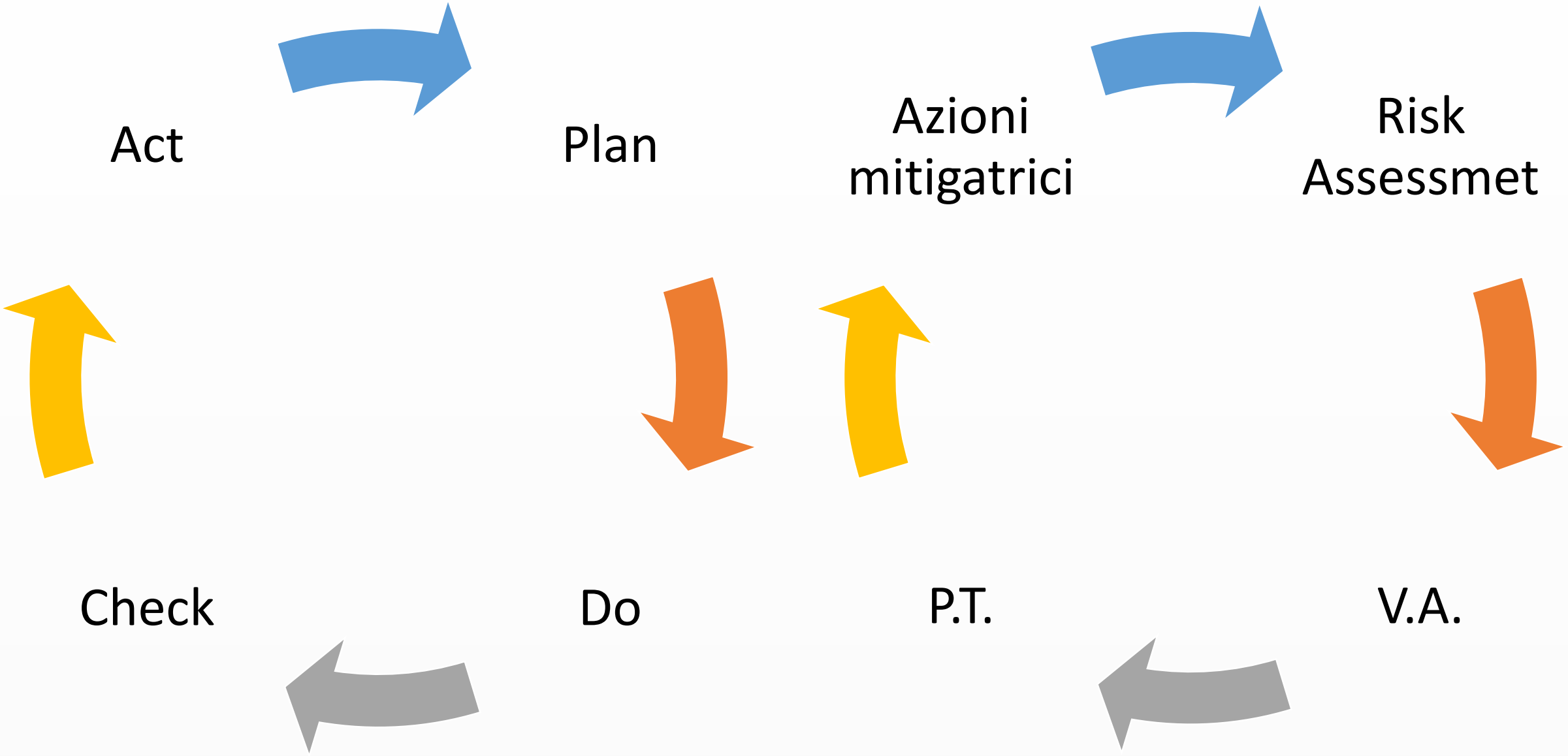
- Disponibilità
- Integrità
- Confidenzialità

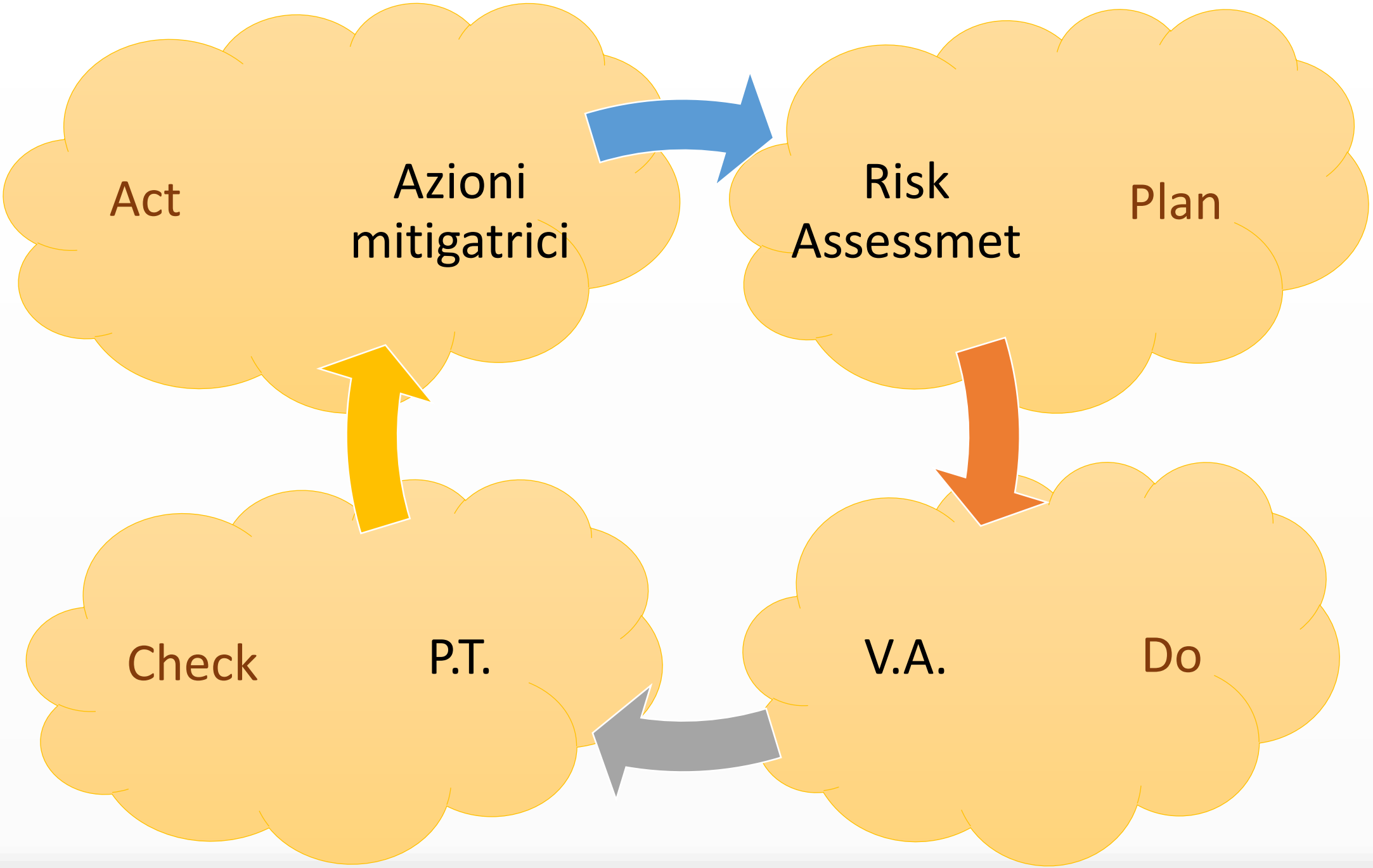
Windows Lyfe Cycle VS Ship

Il modello di gestione della ISO27001 - 27002



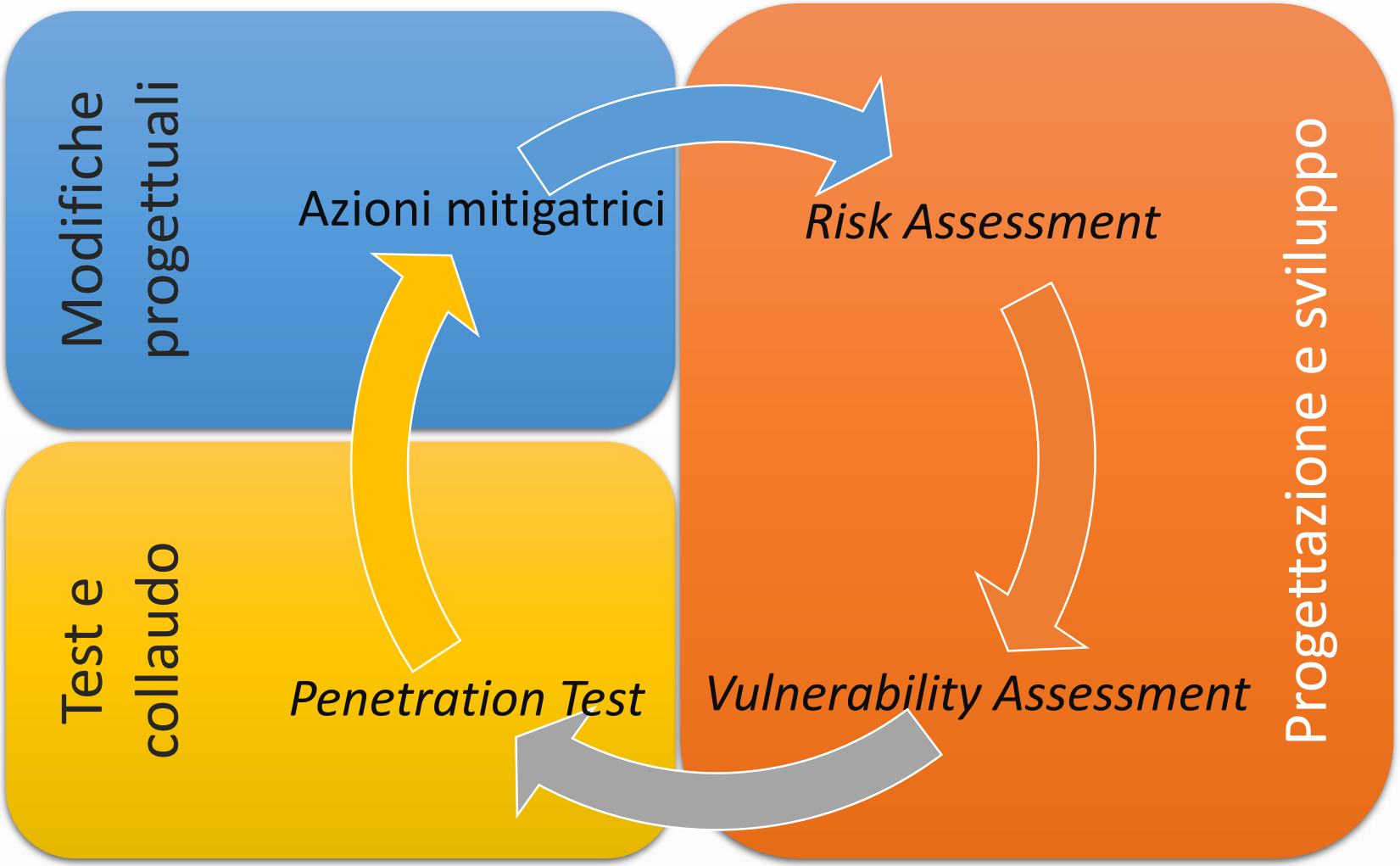
ISO
International Organization for Standardization


Act
Plan
Azioni mitigatrici
Risk Assessmet
Check
Do
P.T.
V.A.


Act
Azioni mitigatrici
Risk Assessmet
Plan
Check
P.T.
V.A.
Do

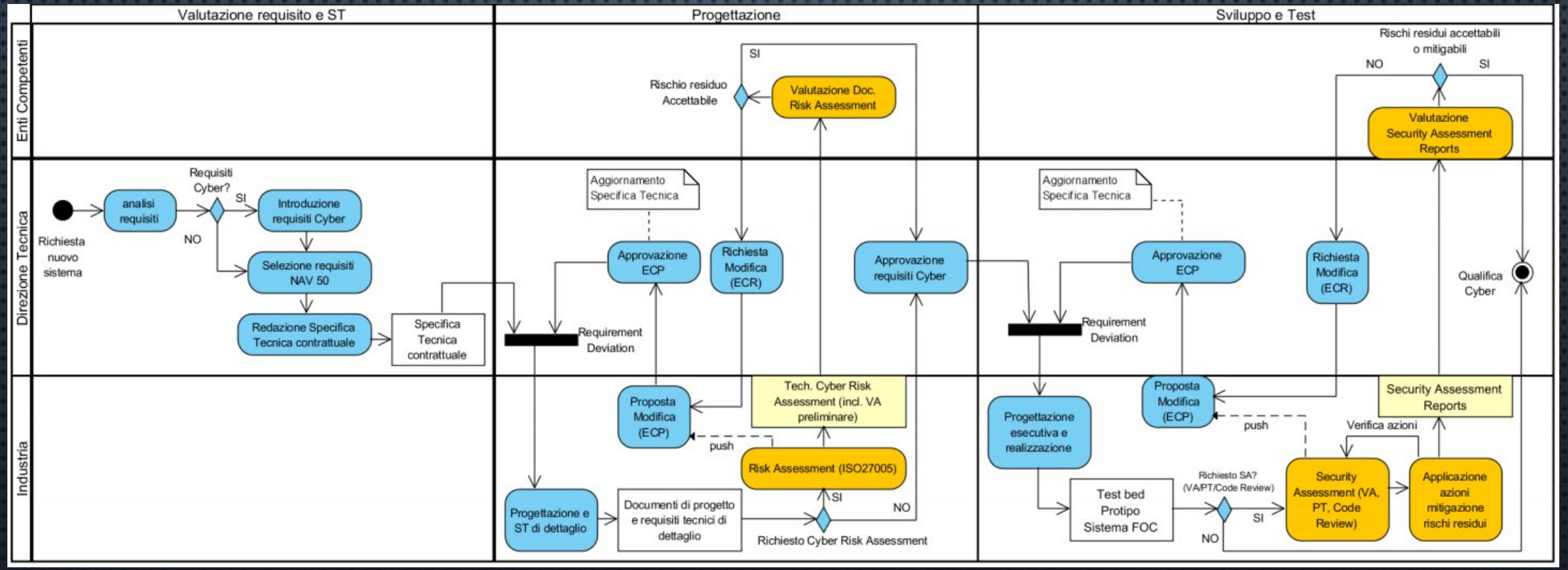

Act
Azioni mitigatrici
Risk Assessment
Plan
ISO
International Organization for Standardization
ISO27001
ISO27002
Check
Penetration Test
Vulnerability Assessment
Do

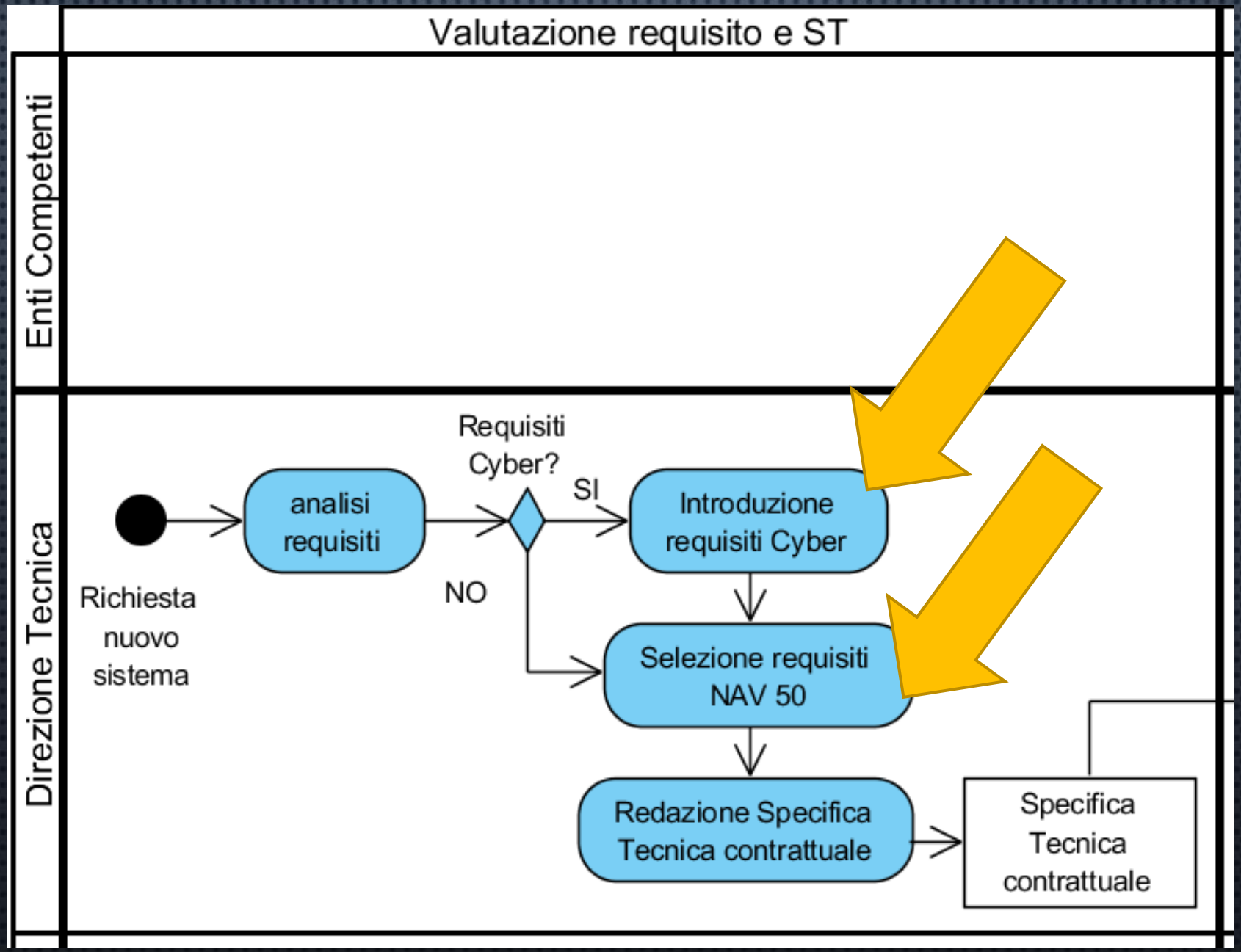
Sicurezza Cyber nel procurement



su **prototipi** e/o in ambiente **simulato**

LA PROPOSTA DI PROCESSO



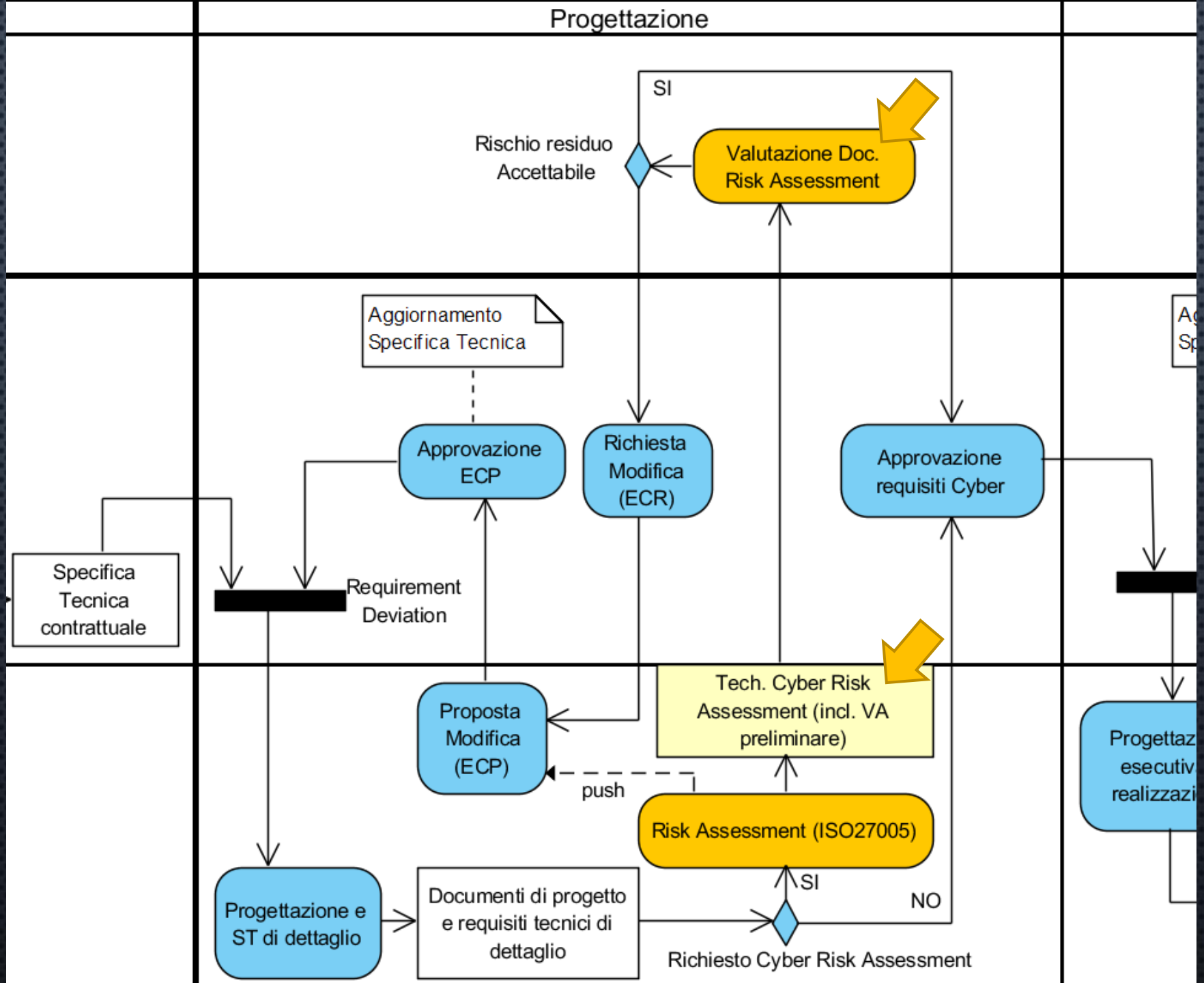

Valutazione requisito e ST
Enti Competenti
Direzione Tecnica
Richiesta nuovo sistema
analisi requisiti
Requisiti Cyber?
SI
NO
Introduzione requisiti Cyber
Selezione requisiti NAV 50
Redazione Specifica Tecnica contrattuale
Specifica Tecnica contrattuale

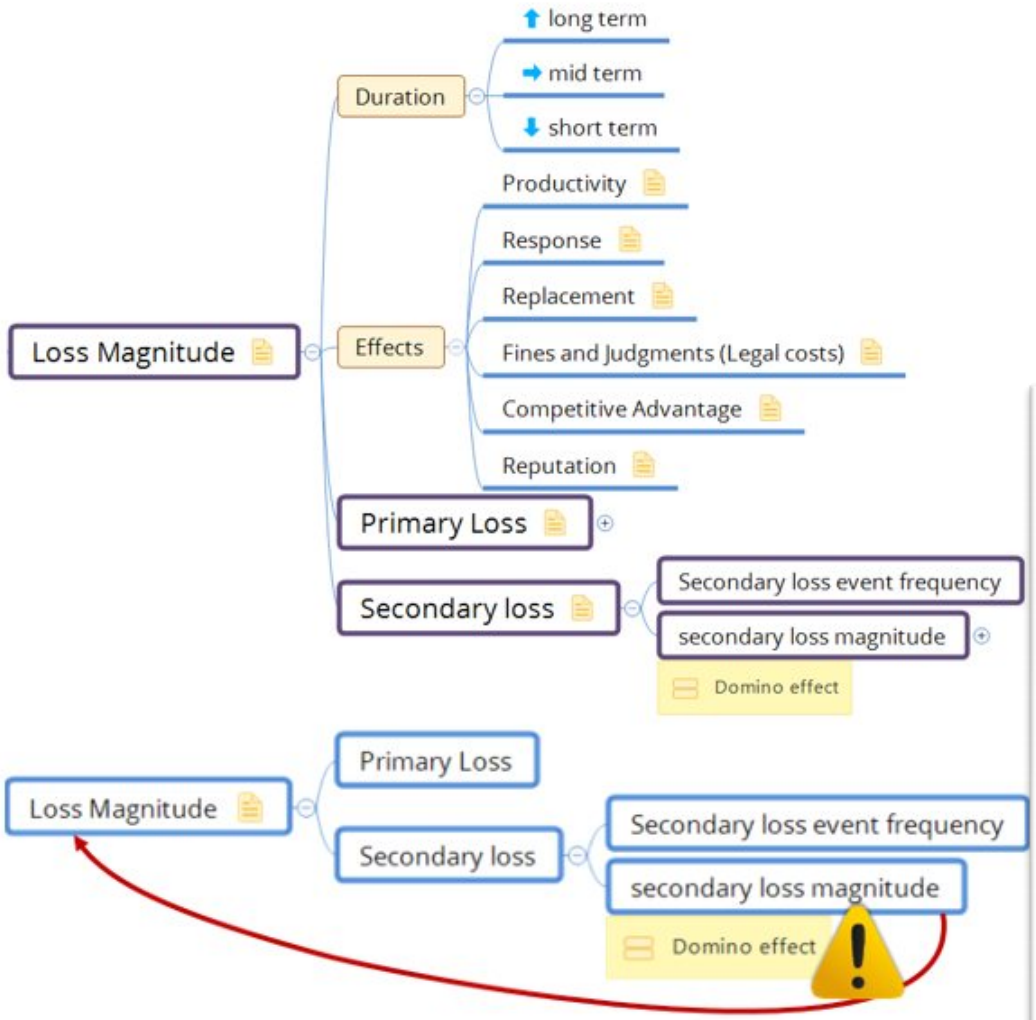
2.4.2 Sistemi di Gestione degli accessi

Per una corretta gestione degli accessi ad un sistema IT e OT dovrebbe essere attuato un processo formale di registrazione e de-registrazione degli utenti per abilitare e disabilitate l'assegnazione dei diritti di accesso.

minimale	Dal punto di vista implementativo per i sistemi complessi è importante l'utilizzo di ***user* ID univoche** per consentire il collegamento tra gli utenti e le loro azioni, in modo da garantire la corretta corrispondenza fra operazioni effettuate e responsabile dell'attività (***accountability***); l'uso di indentificativi condivisi, come ad esempio password di amministrazione o accesso a sistemi distribuiti (IOT), è permesso solo quando per ragioni tecniche od operative non sia altrimenti possibile, o quando il rischio derivante sia ritenuto comunque accettabile. In questi casi potranno essere previste procedure di controllo aggiuntive e/o procedure di aggiornamento delle credenziali (es. cambio *password* periodico e condizionato all'avvicendamento del personale responsabile) specifiche per il modello di impiego previsto per il sistema/sottosistema.
minimale	In caso di avvicendamento del personale o di modifica delle attribuzioni gli *account* nominativi dovranno essere disabilitati. Questo non implica la rimozione dei dati personale. Dove possibile è preferibile la disabilitazione degli *account* e/o il cambio delle *password*, invece della loro cancellazione per evitare di perdere dati storici sulle operazioni effettuate sugli *asset software* e *hardware* del sistema da parte degli "operatori protempore" (esigenze forensi/ gestione in configurazione del sistema).
avanzato	Nei sistemi complessi e ove ritenuto necessario, per gli utenti con alti privilegi sarà richiesta la registrazione di tutte le modifiche dei privilegi stessi, in modo da permettere la ricostruzione delle autorizzazioni protempore e il possibile riconoscimento di ***privilege escalation*** non autorizzate.
minimale	La strutturazione dei ruoli deve rispecchiare quanto più possibile l'organizzazione funzionale corrispondente agli incarichi assegnati al personale che impiegherà i sistemi. Questo potrà rendere più semplice la gestione delle autorizzazioni all'accesso ai sistemi in fase di cambio incarico, in caso di sostituzione temporanea o di ristrutturazione gerarchica dell'organizzazione.

Requisiti in appendice alla norma da poter usare o richiamare nella specifica tecnica contrattuale.


Progettazione
SI
Rischio residuo Accettabile
Valutazione Doc. Risk Assessment
Aggiornamento Specifica Tecnica
Approvazione ECP
Richiesta Modifica (ECR)
Approvazione requisiti Cyber
Specifica Tecnica contrattuale
Requirement Deviation
Proposta Modifica (ECP)
Tech. Cyber Risk Assessment (incl. VA preliminare)
push
Risk Assessment (ISO27005)
SI
NO
Progettazione e ST di dettaglio
Documenti di progetto e requisiti tecnici di dettaglio
Richiesto Cyber Risk Assessment



Indicazioni pratiche su come valutare i rischi

2.2 Valutazione della probabilità di un evento

Per la magnitudo può essere impiegato anche un criterio oggettivo come il costo in attività come la riparazione di un guasto, per le spese legali, per la perdita di fatturato o similari. Per la probabilità il rischio di stima condizionata dalla percezione del valutatore diventa ancora più alto. Per questo motivo, la tassonomia proposta parte da quella indicata dalla metodologia FAIR, suggerendo alcune domande di esempio utili a determinare, con maggiore dettaglio, parametri di valutazione numerica a partire da considerazioni obbiettivamente qualitative.

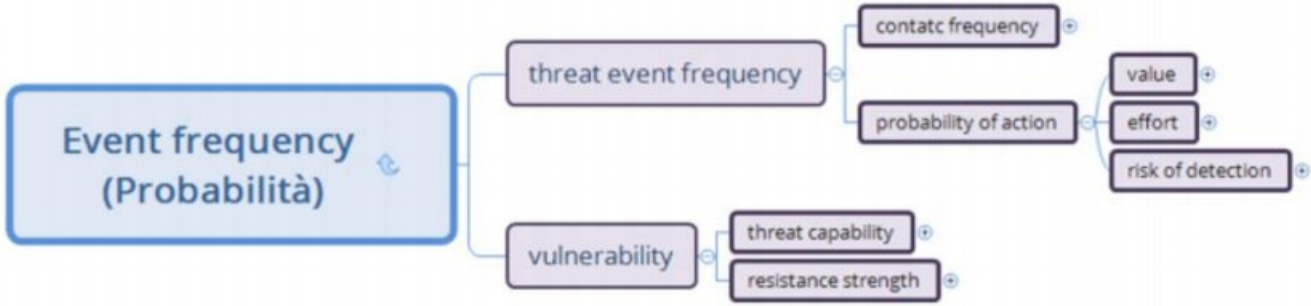
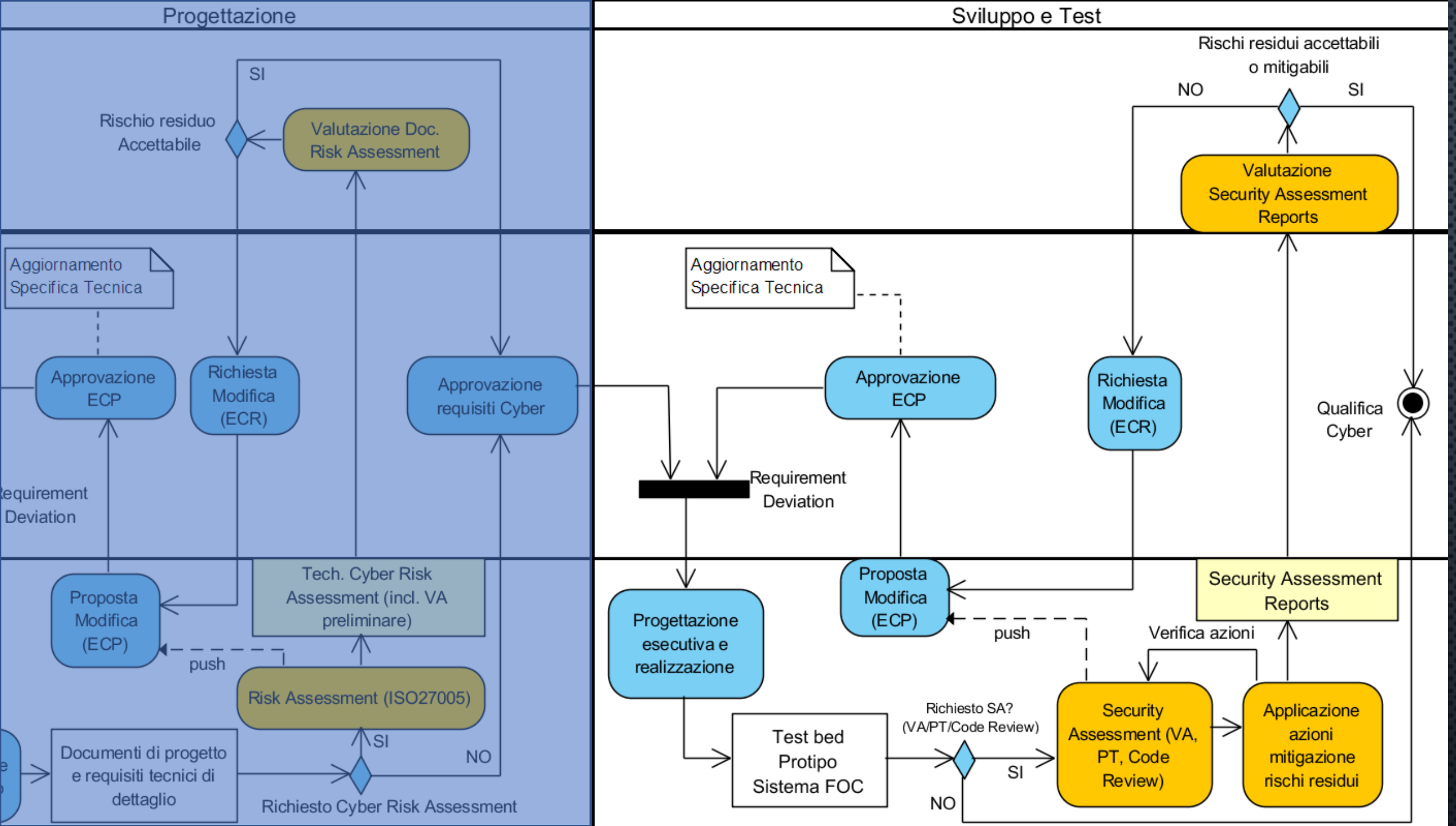


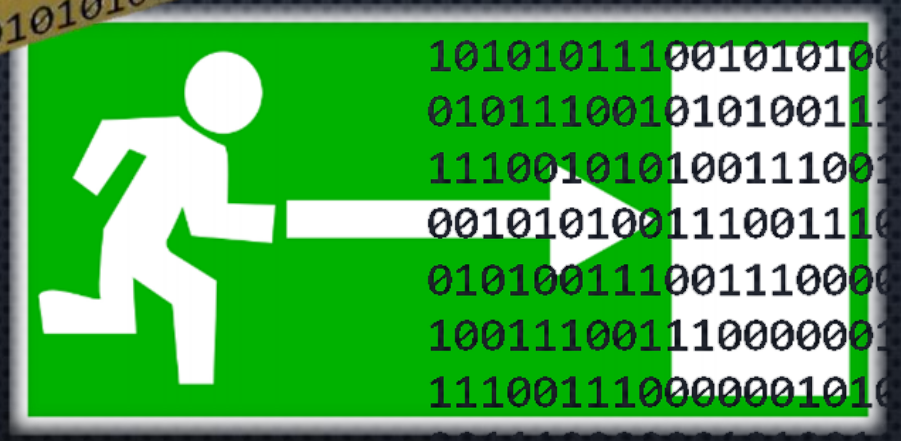
Figura 9 - Probabilità come stima di frequenza di un evento dannoso


Progettazione
Sviluppo e Test
SI
Rischio residuo Accettabile
Valutazione Doc. Risk Assessment
Rischi residui accettabili o mitigabili
NO
SI
Valutazione Security Assessment Reports
Aggiornamento Specifica Tecnica
Approvazione ECP
Richiesta Modifica (ECR)
Approvazione requisiti Cyber
Aggiornamento Specifica Tecnica
Approvazione ECP
Richiesta Modifica (ECR)
Qualifica Cyber
equirement Deviation
Requirement Deviation
Proposta Modifica (ECP)
Tech. Cyber Risk Assessment (incl. VA preliminare)
push
Risk Assessment (ISO27005)
SI
NO
Documenti di progetto e requisiti tecnici di dettaglio
Richiesto Cyber Risk Assessment
Progettazione esecutiva e realizzazione
Proposta Modifica (ECP)
push
Security Assessment Reports
Verifica azioni
Test bed Protipo Sistema FOC
Richiesto SA? (VA/PT/Code Review)
SI
NO
Security Assessment (VA, PT, Code Review)
Applicazione azioni mitigazione rischi residui

DAL FISICO AL DIGITALE

- Il parallelismo con la sicurezza sul lavoro e la lotta antincendio

Consegnare sistemi con una relazione tecnica di valutazione del rischio

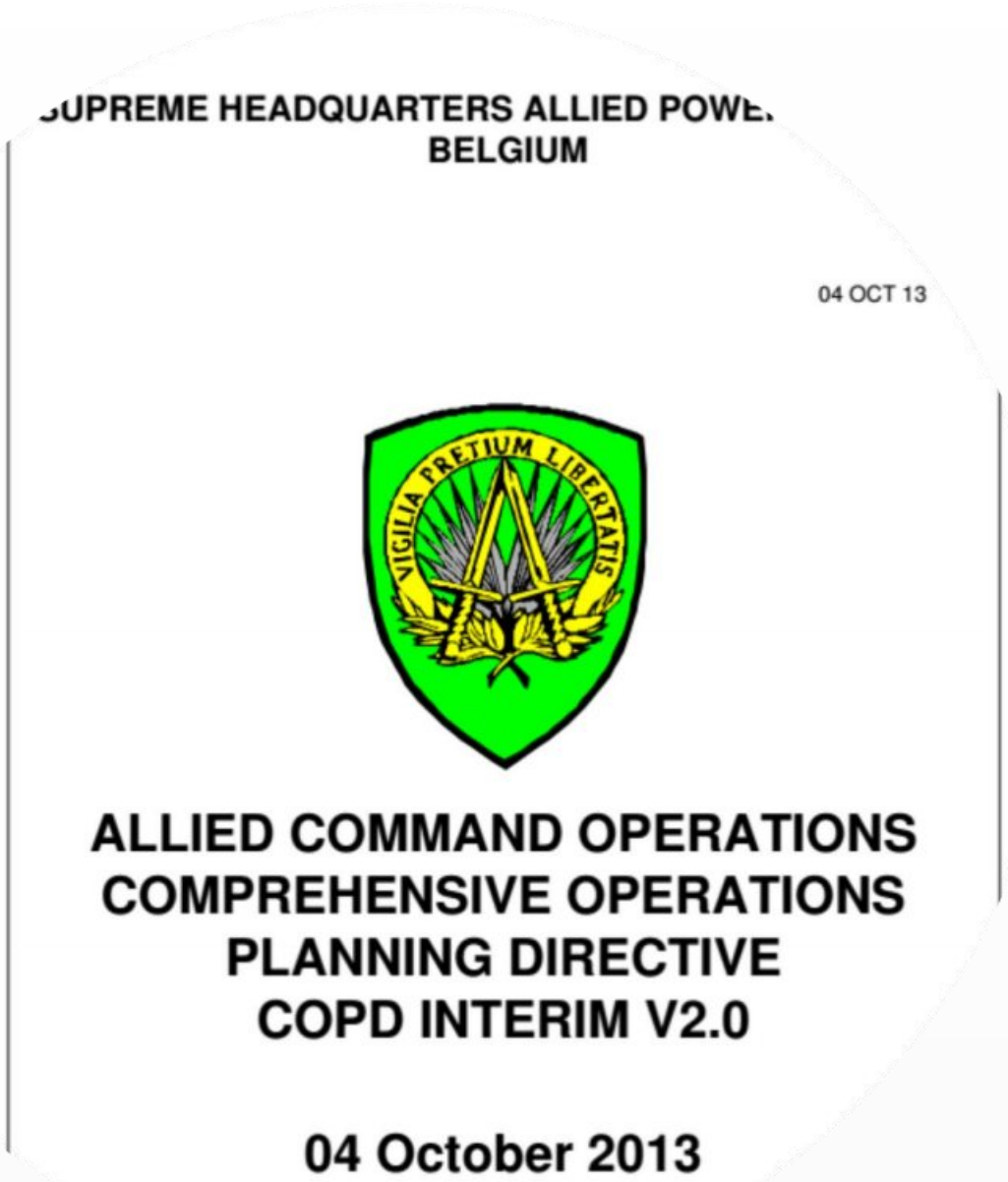


Siamo pronti per un DVR – C?

- Documento di Valutazione del Rischio Cibernetico

A differenza del mondo “safety” Ricordiamo che il contesto della security è di tipo “adversary”

Quale approccio metodologico?



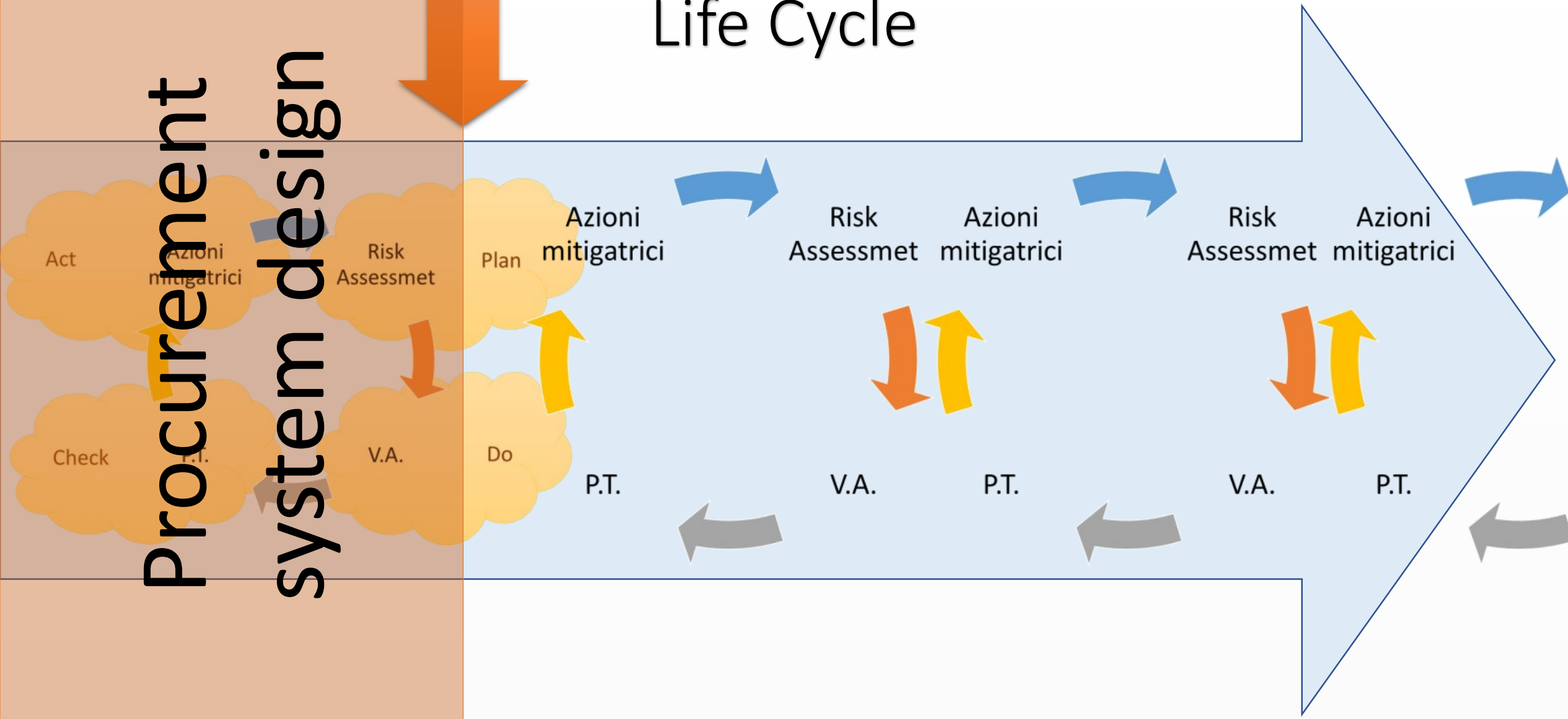
Dal **Red Teaming** all'**analisi multidimensionale.**

Un valido riferimento metodologico che viene dall'esperienza nella pianificazione operativa e dalla dottrina militare.

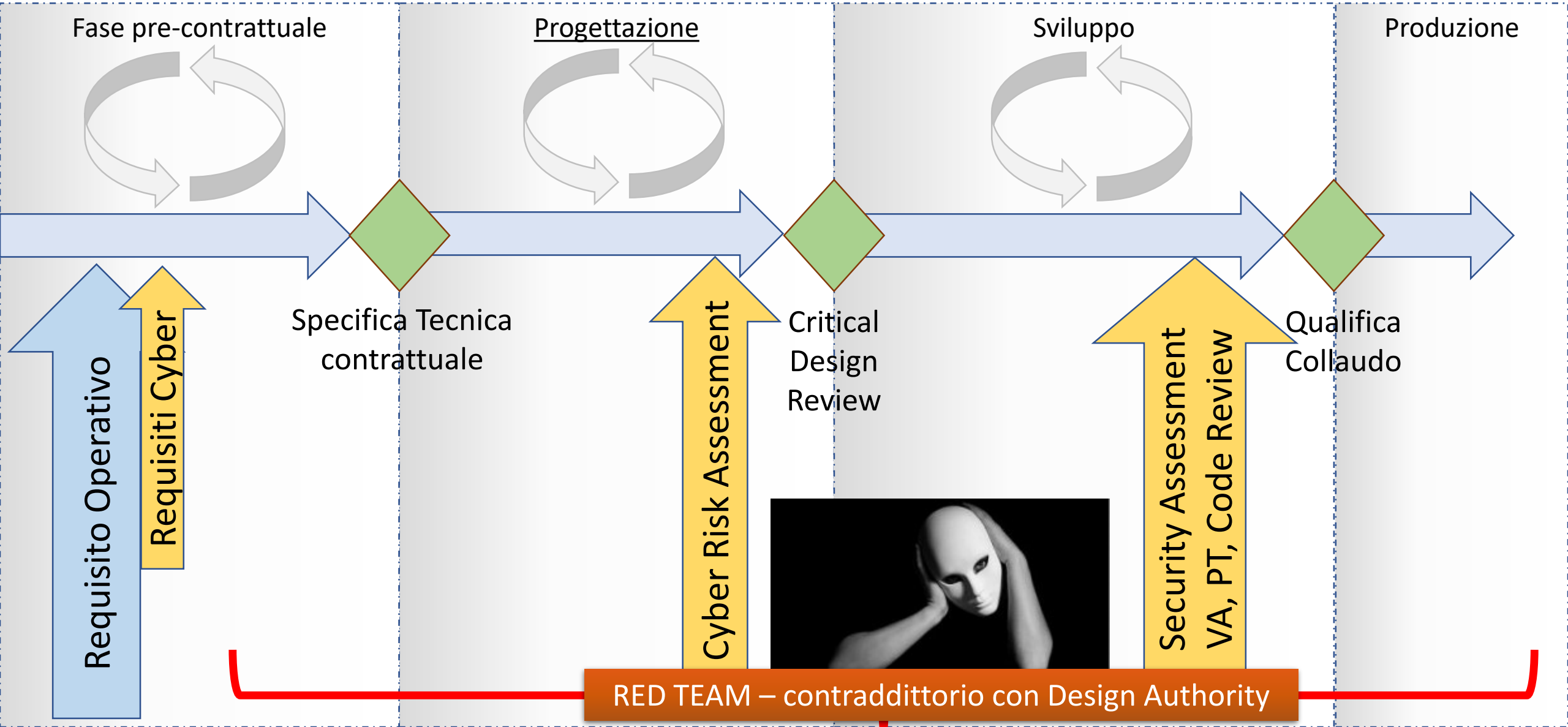
Acquisizione del sistema

Life Cycle

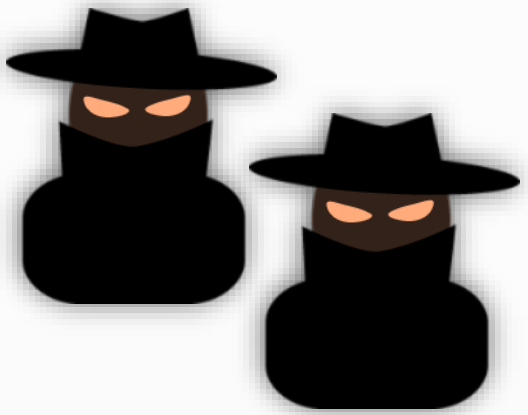
Procurement system design



Il processo della NAV50-4217

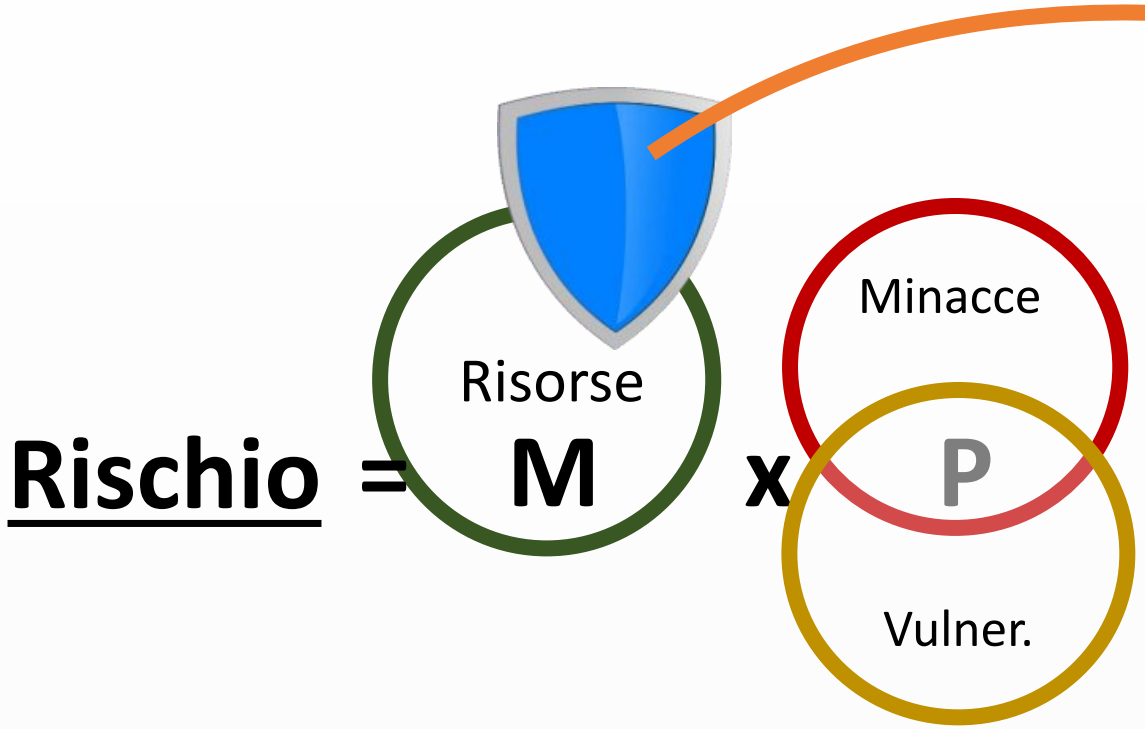


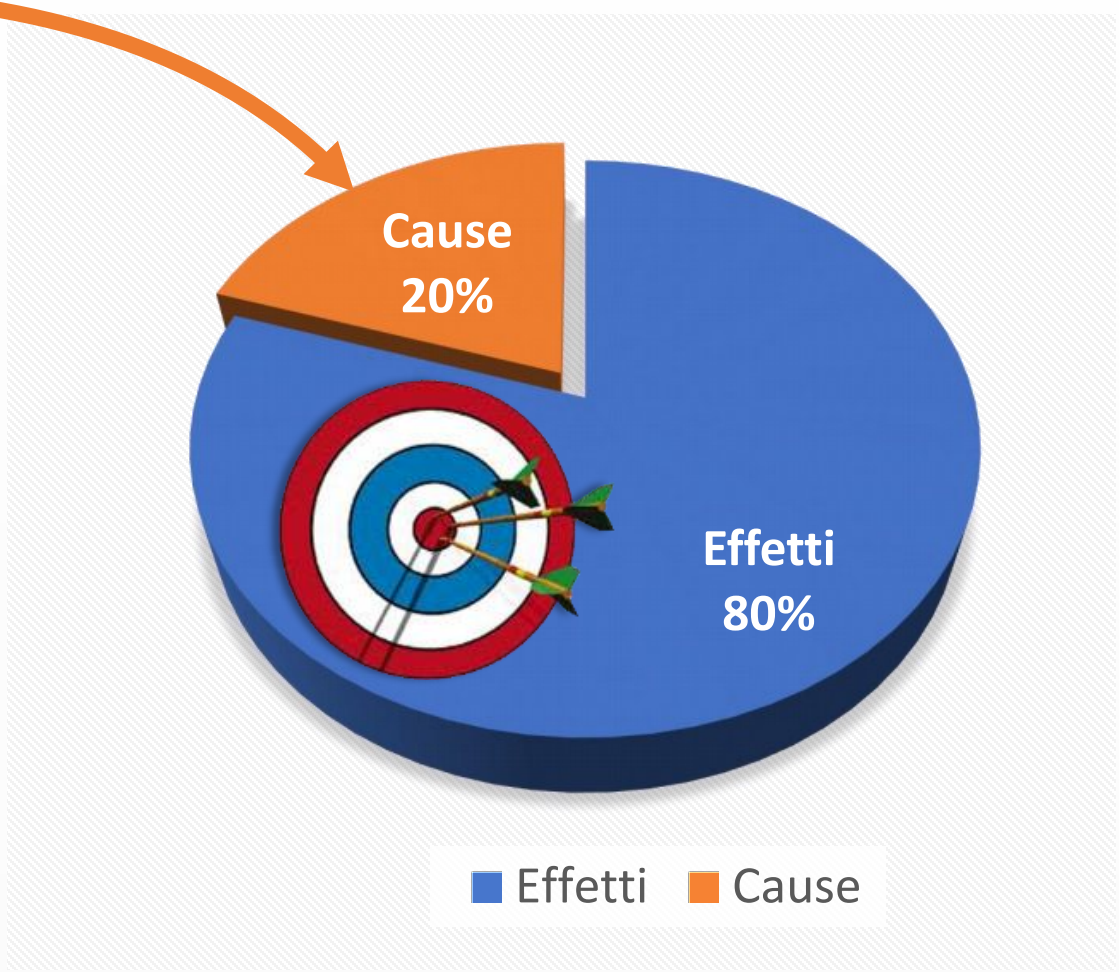
Contraddittorio:
pensare come gli attaccanti



Valutiamo anche i processi

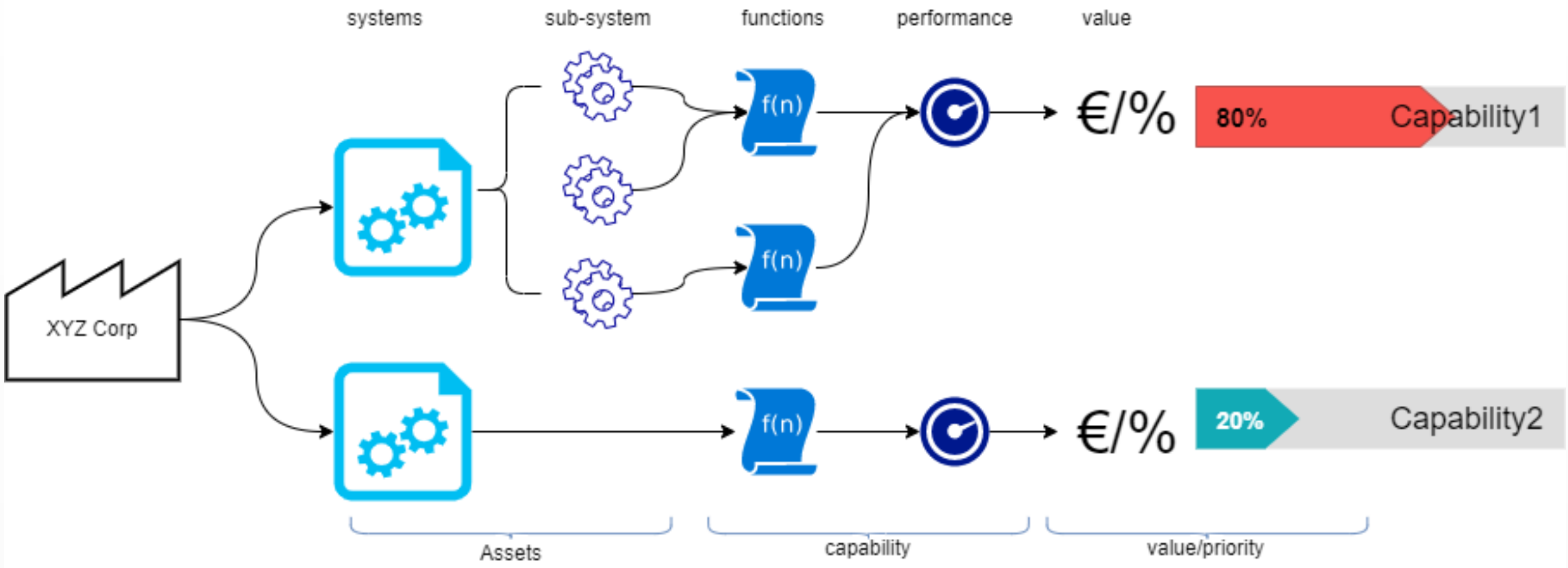
Individuare le risorse da proteggere



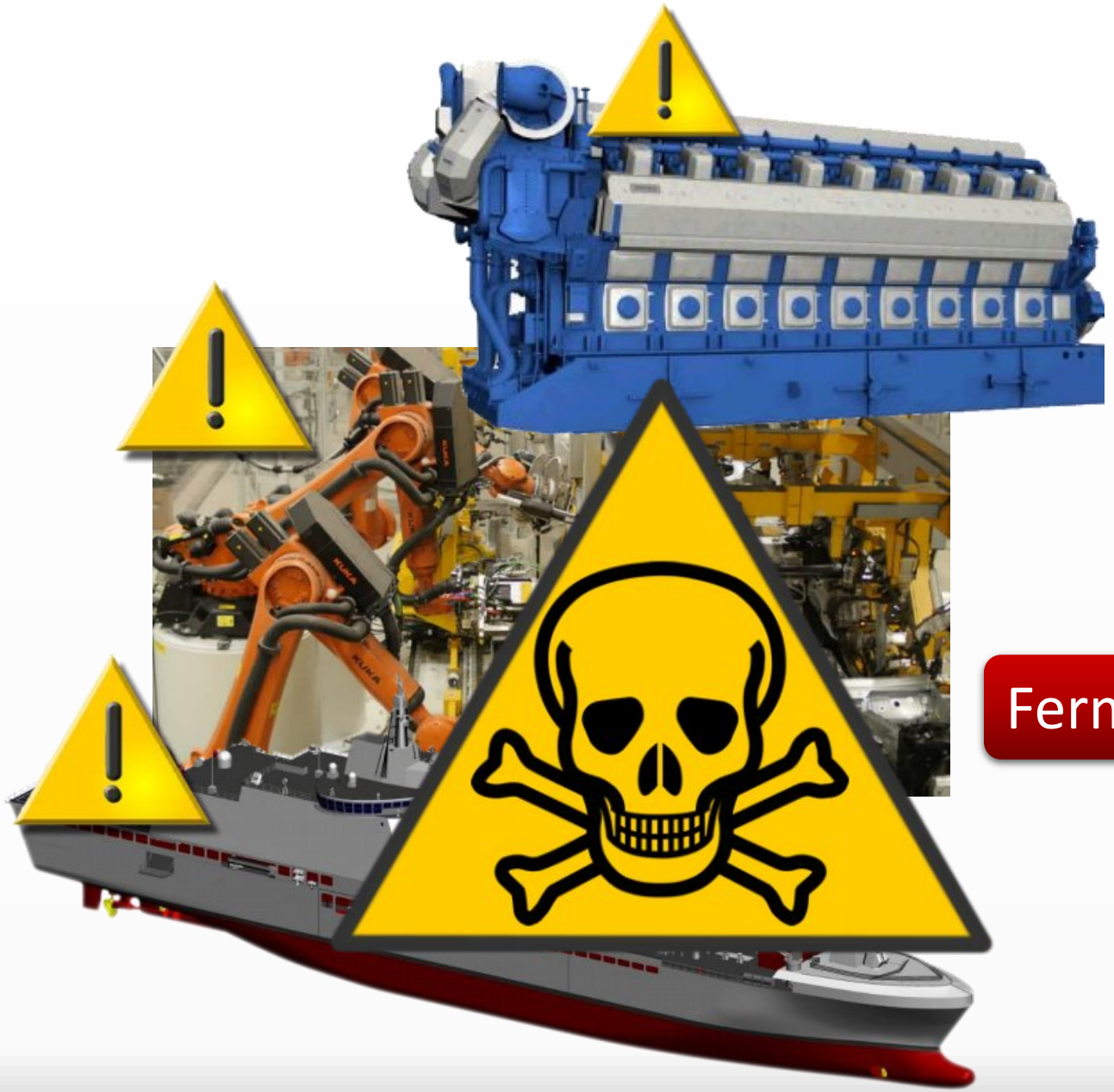


Concentrarsi sui valori più importanti

Definire i sistemi critici.



Misurare l’impatto



Ripristino capacità

€+...

Fermo macchina

€€

Fermo impianto
Fermo nave

€€€€

Conclusioni


Ministero della Difesa

NAV-50-4217-0016-13-00B000

ATTO DI APPROVAZIONE

Approva la seguente Pubblicazione:

- LINEE GUIDA PER LA REDAZIONE DELLA DOCUMENTAZIONE CONTRATTUALE AFFERENTE LE FORNITURE DI SISTEMI IT E OT DESTINATI A BORDO DELLE UU.NN. CHE PREVEDONO REQUISITI DI SICUREZZA CIBERNETICA

Roma, lì 17 DIC. 2019

Requisiti di sicurezza cibernetica nelle ST contrattuali

Cyber Risk Assessment come documento di progetto

Approccio in contraddittorio RED TEAMING con la “*design authority*”