

FRAMEWORK NAZIONALE PER LA CYBERSECURITY E LA DATA PROTECTION

TUTORIAL – PARTE 3/6
INTRODUZIONE AL FRAMEWORK

Pisa, 12-02-2019

info@cybersecurityframework.it



SAPIENZA
UNIVERSITÀ DI ROMA



CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY



cini
Cyber Security National Lab

INTRODUZIONE DEI “PROTOTIPI DI CONTESTUALIZZAZIONE”

- Le contestualizzazioni sono poco adatte a cogliere esclusivamente alcuni aspetti
 - leggi/regolamenti
 - standard di settore
 - best practices specifiche
- Il problema deriva dal fatto che la contestualizzazione, per sua natura, tende ad essere strettamente legata al **dominio** in cui viene definita
 - i **livelli di maturità** sono legati alla realtà organizzativa che li definisce sulla base delle proprie strategie di implementazione del framework
- Le **guide per l'applicazione** includono controlli, anche molto specifici, che sono strettamente legati all'ambito applicativo considerato

PROTOTIPO DI CONTESTUALIZZAZIONE

Prototipi di contestualizzazione – I prototipi di contestualizzazione sono un nuovo strumento introdotto nel Framework per permettere la definizione di template utilizzabili per la contestualizzazione in specifici settori

I prototipi possono essere utilizzati, ad esempio, per cogliere attraverso il Framework:

- specifiche **normative** che richiedono l'attuazione di determinate pratiche indirizzate alla cybersecurity o alla data protection;
- **regolamenti tecnici** e di attuazione che indicano puntuali controlli legati alla cybersecurity o alla data protection;
- **best practice** di settore inerenti alla cybersecurity o alla data protection.

PROTOTIPO DI CONTESTUALIZZAZIONE

Introduzione dei “**prototipi di contestualizzazione**”

Un prototipo:

- per ogni subcategory del Framework core definisce la relativa classe di implementazione: obbligatoria, consigliata, libera
- per ogni subcategory può definire un livello di priorità per la relativa implementazione

PROTOTIPO DI CONTESTUALIZZAZIONE

Viene inoltre accompagnato da una guida all'implementazione, un documento che descrive:

- Il contesto di applicazione del prototipo
- Ulteriori vincoli sulla selezione delle subcategory
- la definizione dei livelli di priorità
- Un elenco di controlli di sicurezza, per le subcategory considerate, che andranno, in fase di implementazione del prototipo in una contestualizzazione, opportunamente organizzati nei diversi livelli di maturità eventualmente previsti.

PROTOTIPO DI CONTESTUALIZZAZIONE

Il processo di implementazione di un prototipo in una contestualizzazione, avviene seguendo i seguenti passi:

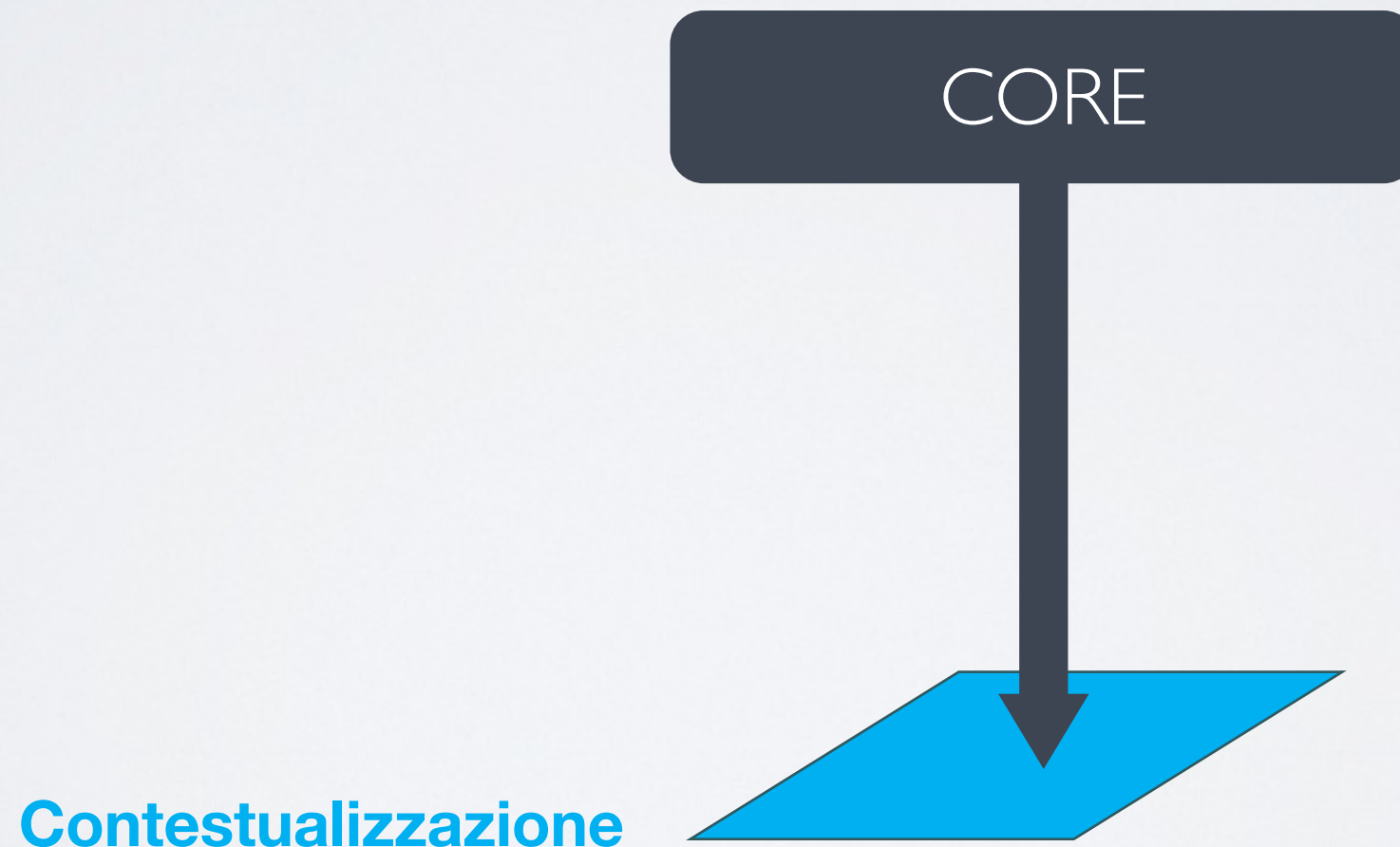
- tutte le subcategory indicate come **obbligatorie** nel prototipo vengono selezionate nella contestualizzazione
- la selezione nella contestualizzazione delle subcategory indicate come **consigliate** nel prototipo deve essere attentamente valutata in considerazione delle specifiche caratteristiche dell'ambito applicativo previsto per la contestualizzazione
- gli eventuali **ulteriori vincoli** sulla selezione delle subcategory documentati nella guida di applicazione del prototipo devono essere applicati

PROTOTIPO DI CONTESTUALIZZAZIONE

- per ogni subcategory selezionata a seguito dei precedenti passi deve essere indicato nella contestualizzazione un **livello di priorità**, preferibilmente almeno pari o superiore a quello indicato nel prototipo, tenendo conto di eventuali vincoli documentati nella guida di applicazione del prototipo
- gli eventuali **controlli di sicurezza** documentati nella guida di applicazione del prototipo possono essere integrati nelle linee guida all'applicazione della contestualizzazione

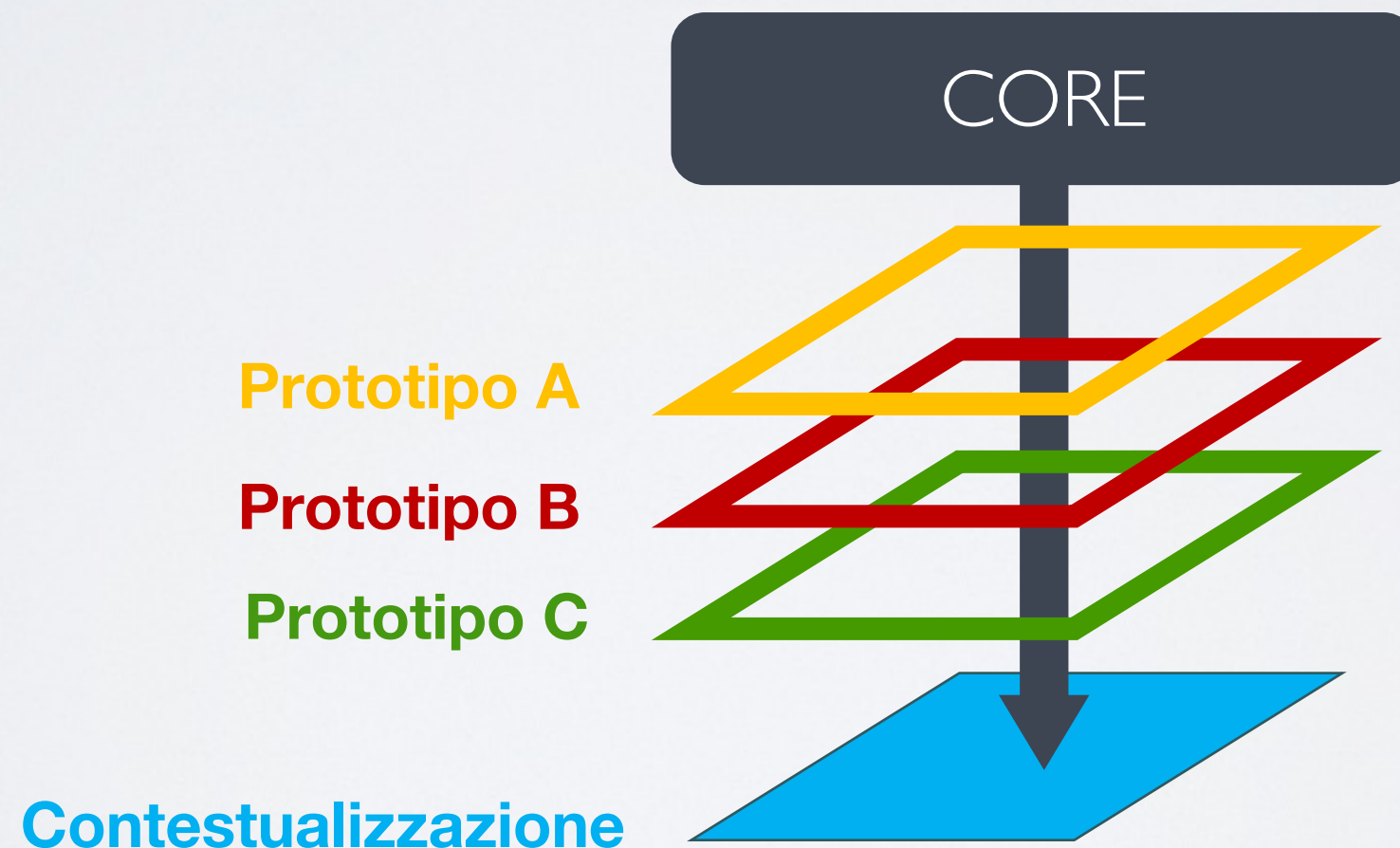
USO DEI PROTOTIPI

- Metodologia framework 1.0



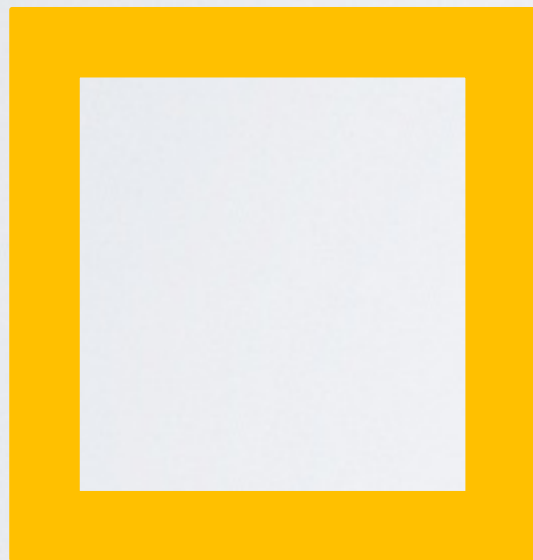
USO DEI PROTOTIPI

- Più prototipi possono essere implementati in fase di contestualizzazione per cogliere aspetti diversi

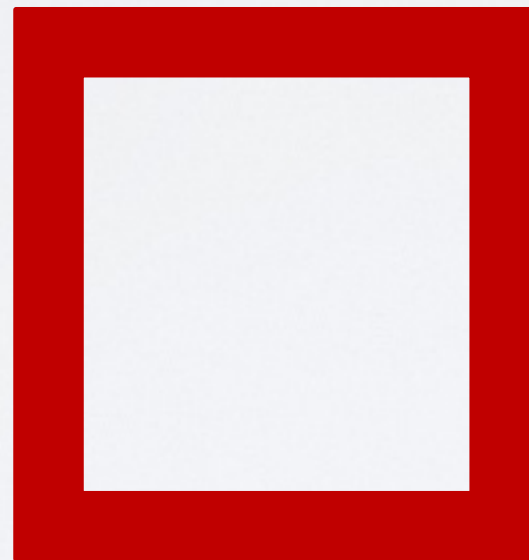


USO DEI PROTOTIPI

- Più prototipi possono essere implementati in fase di contestualizzazione per cogliere aspetti diversi



Prototipo GDPR



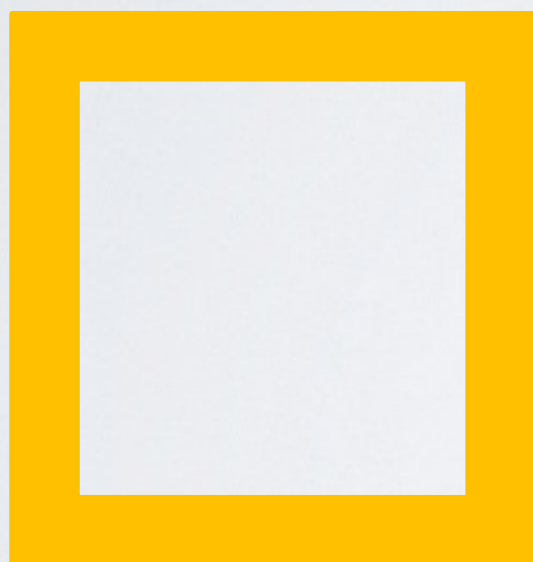
Prototipo NIS



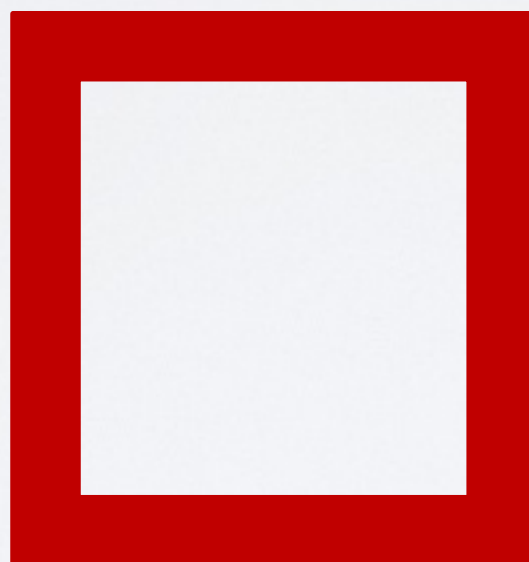
Prototipo CCS-CSC

LIVELLI DI PRIORITA'

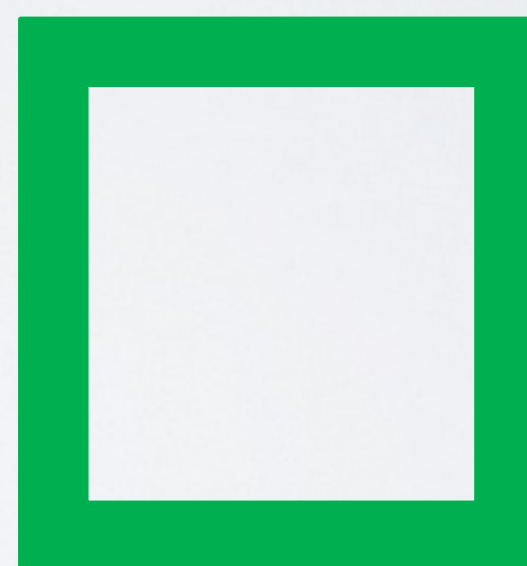
- Definizione dei livelli di priorità
 - Se è coinvolto un livello di priorità alto il Nuovo livello di priorità deve essere posto ad alto
- Negli altri casi sono possibili 2 opzioni
 - **Risk based**: assegnare il Massimo tra gli n livelli di priorità
 - **Cost based**: assegnare il minimo tra gli n livelli di priorità



Prototipo GDPR

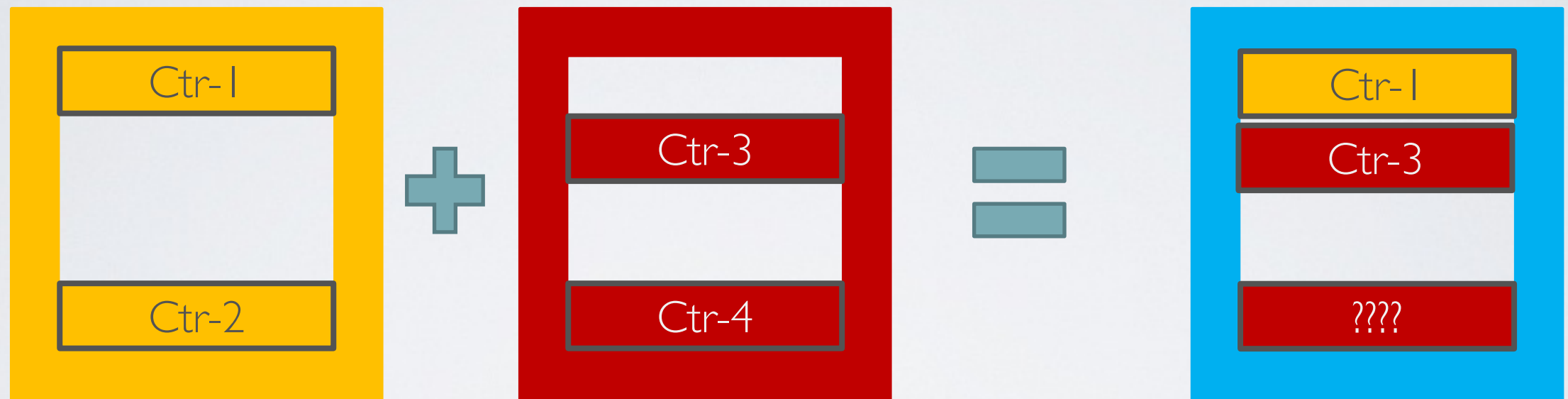


Prototipo NIS



Prototipo CCS-CSC

LIVELLI DI MATURITA' / CONTROLLI DI SICUREZZA



Prototipo A

Prototipo B

Contestualizzazione

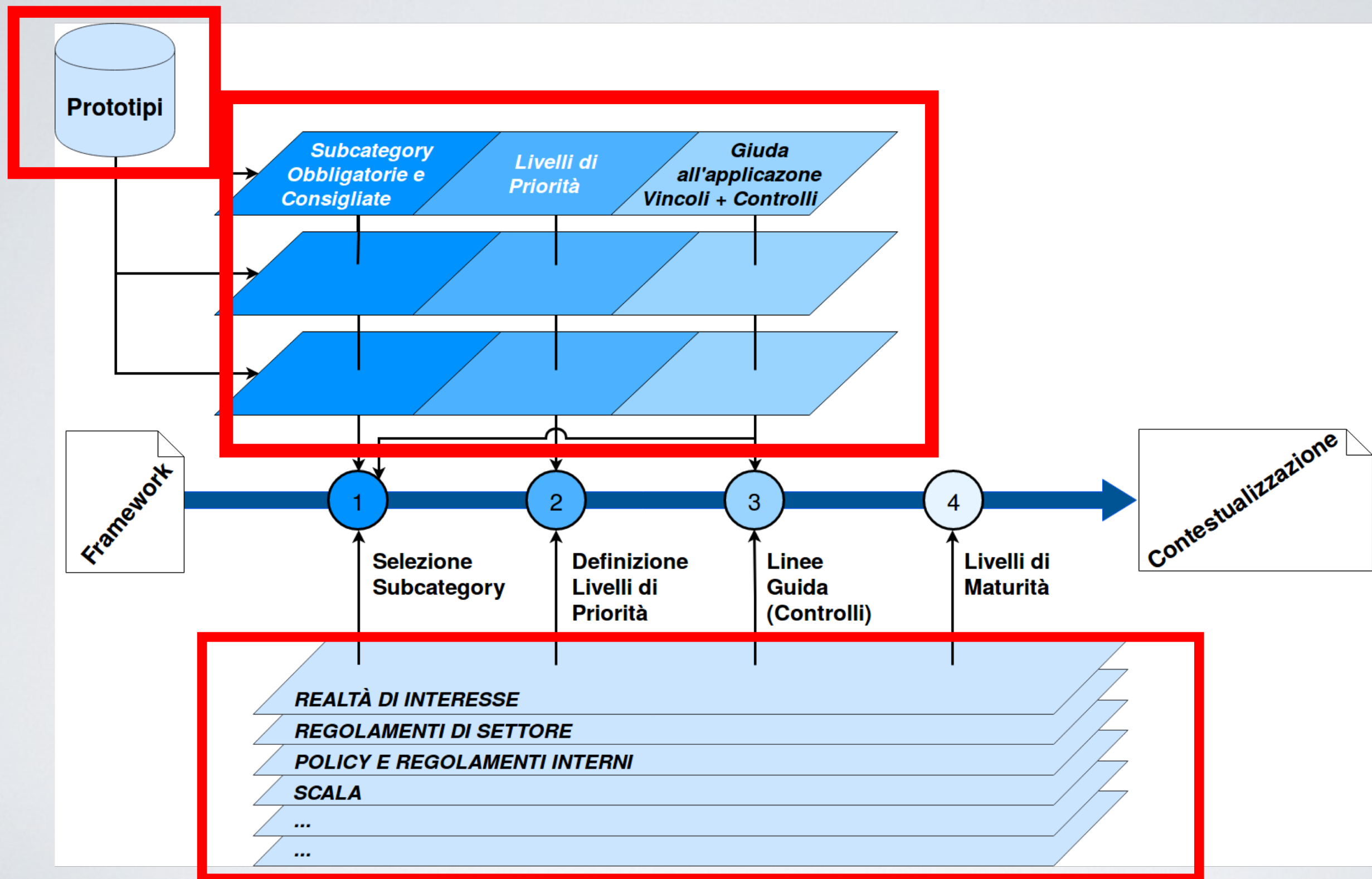
Ctr-# == controllo di sicurezza

Gestire l'integrazione tra i controlli derivanti da prototipi diversi

PROTOTIPI DI CONTESTUALIZZAZIONE

A valle di questo processo di implementazione, ripetuto per tutti i prototipi di interesse, la contestualizzazione risultante può essere ulteriormente specializzata, laddove se ne ravveda la necessità.

PROTOTIPO DI CONTESTUALIZZAZIONE



METODOLOGIA DI UTILIZZO

A. Identificare una contestualizzazione del Framework

B. Definire priorità e ambito

C. Identificare sistemi e asset

D. Determinare il profilo corrente

E. Analizzare il rischio

F. Determinare il profilo target

G. Determinare il gap rispetto al profilo target

H. Definire e attuare una roadmap per raggiungere il profilo target

I. Misurare le performance