

# Kick Off Gruppo di Lavoro AIC

## *"Cyber Security Framework for Supply Chain"*

Roma 8 giugno 2016

**Raffaella D'Alessandro e Giuseppe Russo**

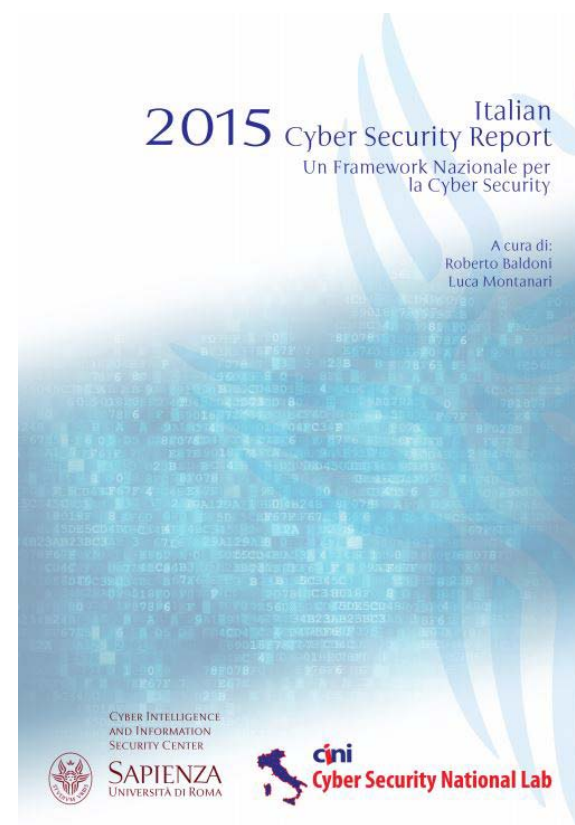


# Agenda

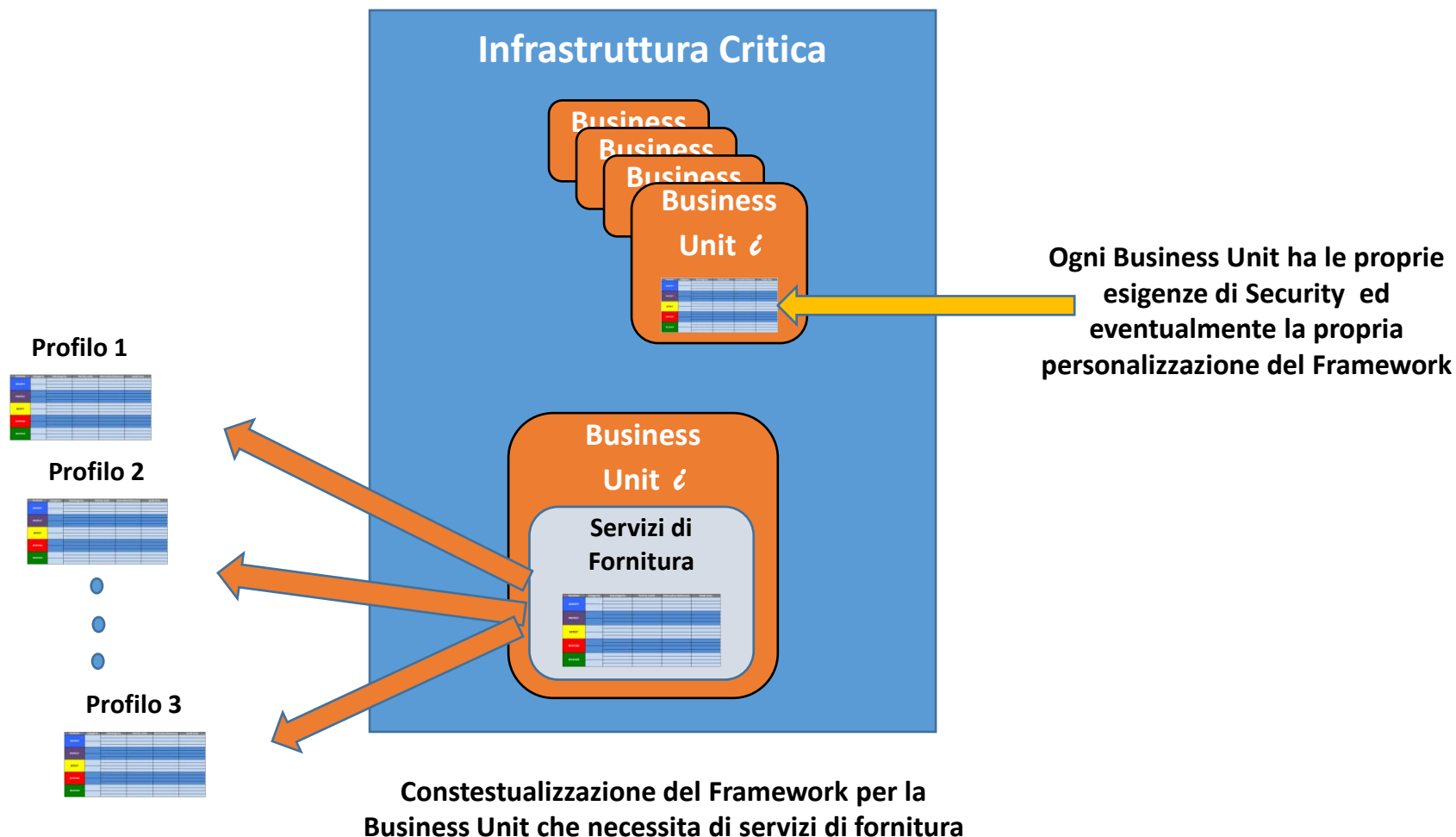


- Obiettivi del gruppo di lavoro
- Approccio metodologico
- Attività proposte
- Risultati attesi
- Organizzazione del Gruppo di lavoro
- Tempi

- Definire una **contestualizzazione** del *Cyber Security Framework Nazionale* da applicare alla fornitura di uno specifico servizio della azienda IC
- Sviluppare **ulteriori esempi** di profili di Cyber Security per la fornitura di servizi alle IC
- Sviluppare **Linee Guida** per definire ed applicare ai propri fornitori il Profilo di Cyber Security dei servizi
- Promuovere la **diffusione dei risultati del gruppo di lavoro**



# Approccio metodologico: Contestualizzazioni e profili nell'ambito della metodologia



La contestualizzazione del Cyber Security Framework Nazionale verrà condotta *al fine di definire*, per le tipologie di servizio individuate, il relativo **profilo di Cyber Security da garantire da parte del fornitore in termini di:**

- Funzioni, Category e subcategory (anche nuove)
- Informative Reference
- Linee Guida di Riferimento per ciascuna subcategory
- Livelli di Priorità
- Livelli di Maturità

# La contestualizzazione del Framework da applicare ai servizi di fornitura delle IC



Functions	Categories	Subcategories	Priority Levels	Maturity Levels				Informative References	Guide Lines
				M1	M2	M3	M4		
IDENTIFY									
PROTECT									
DETECT									
RESPOND									
RECOVER									

# Attività proposte per il Gruppo di Lavoro

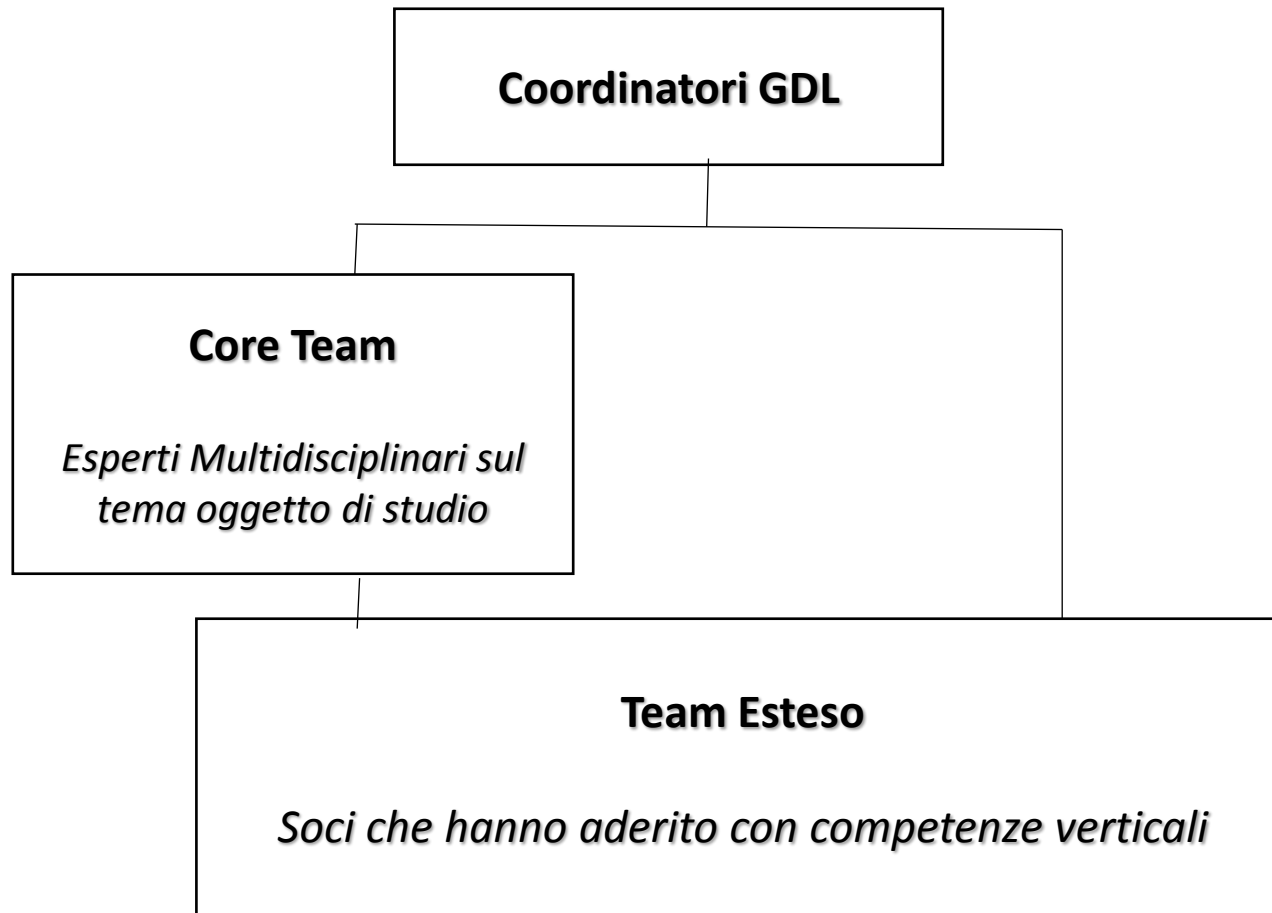


1. Analisi del Profilo Cyber per la **Contestualizzazione del Framework** alla Supply Chain nelle IC
  - a) Studiare bene il framework, anche attraverso sessioni di approfondimento e condivisione, al fine di enucleare i principali elementi da tenere in considerazione nella sua applicazione alla Supply Chain
  - b) Condividerne l'ambito di applicazione alle IC selezionando le tipologie di fornitura e di supply chain per le quali contestualizzare il framework
  - c) Analisi delle Vulnerabilità di Settore applicabili al contesto in cui opera la IC e identificazioni di ulteriori metodologie disponibili in ambito Sicurezza della Supply Chain
2. Selezione della **Tipologia di Servizio di Fornitura** per il quale sviluppare la Contestualizzazione su cui valutare il profilo di rischio attuale
3. Selezione delle **sottocategorie del Framework Core** che meglio si adattano alla Supply Chain nelle IC
4. Definizione dei relativi **Livelli di Priorità** per l'implementazione per le Subcategory selezionate
5. Specificare i **Livelli di Maturità** per le Subcategory a priorità alta.
6. A valle della contestualizzazione sviluppare le **Linee guida** per l'applicazione da parte della azienda IC ai propri fornitori

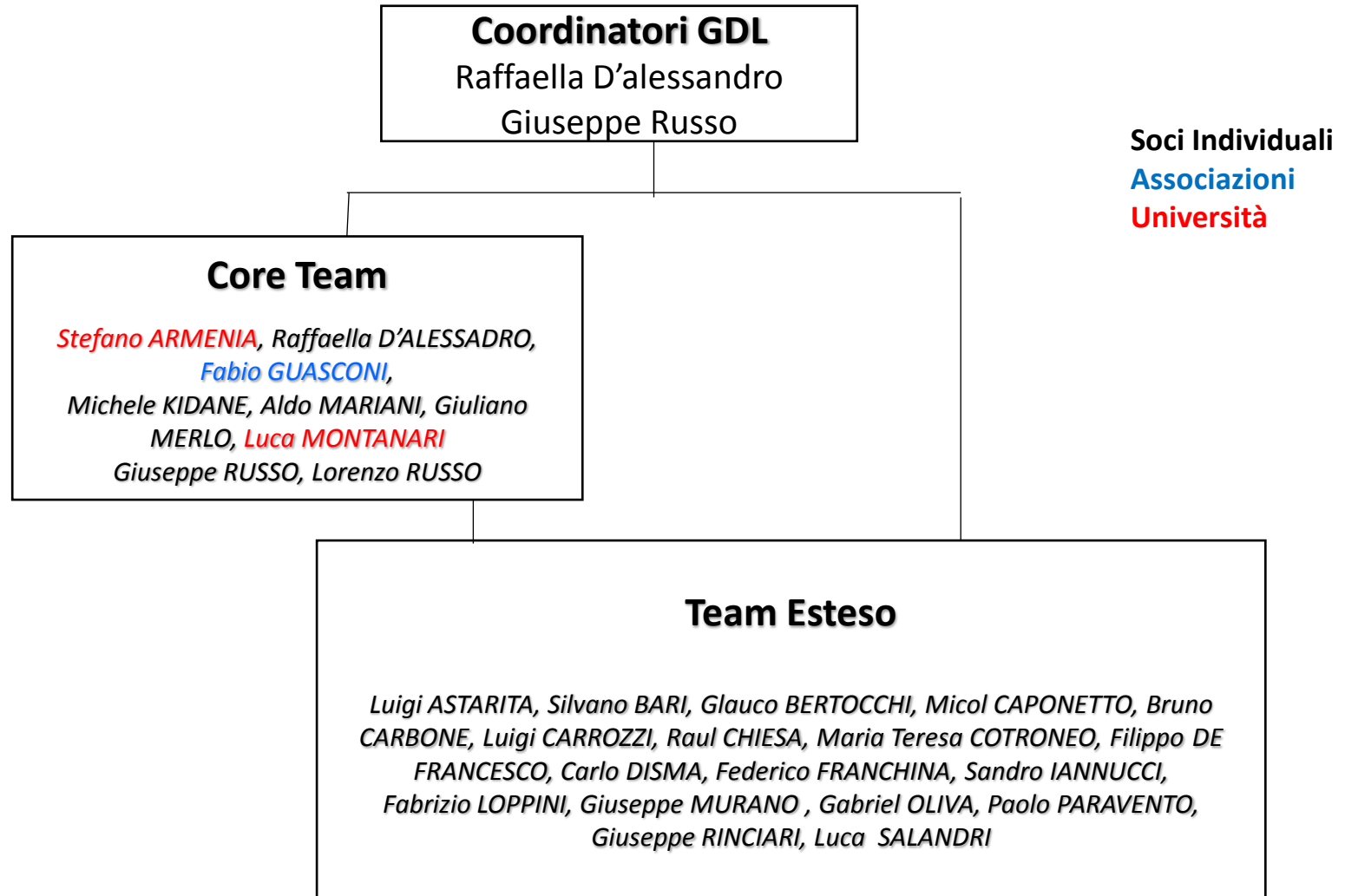
- Esempi di **contestualizzazione** del Cyber Security Framework Nazionale **con esempi di profili associati** per i servizi di fornitura della supply chain di una Infrastruttura Critica presa come caso di studio
- Documento contenente **le linee guida metodologiche per la contestualizzazioni del Cyber Security Framework Nazionale per i servizi di fornitura e relativi profili per i fornitori**
- Interventi di **sensibilizzazione e formazione** in merito all'applicazione della contestualizzazione del Cyber Security framework Nazionale ai fornitori delle supply chain delle IC



# Struttura Organizzativa del Gruppo di Lavoro



# Struttura Organizzativa del Gruppo di Lavoro



	Giugno	Luglio	Agosto	Settembre	Ottobre	Novembre
1	■					
2				■		
3					■	
4					■	
5					■	
6						■

1. Analisi del Profilo Cyber per la **Contestualizzazione del Framework** alla Supply Chain nelle IC
  - a) Studiare bene il framework, anche attraverso sessioni di approfondimento e condivisione, al fine di enucleare i principali elementi da tenere in considerazione nella sua applicazione alla Supply Chain
  - b) Condividere l'ambito di applicazione alle IC selezionando le tipologie di fornitura e di supply chain per le quali contestualizzare il framework
  - c) Analisi delle Vulnerabilità di Settore applicabili al contesto in cui opera la IC e identificazioni di ulteriori metodologie disponibili in ambito Sicurezza della Supply Chain
2. Selezione della **Tipologia di Servizio di Fornitura** per il quale sviluppare la Contestualizzazione su cui valutare il profilo di rischio attuale
3. Selezione delle **sottocategorie del Framework Core** che meglio si adattano alla Supply Chain nelle IC
4. Definizione dei relativi **Livelli di Priorità** per l'implementazione per le Subcategory selezionate
5. Specificare i **Livelli di Maturità** per le Subcategory a priorità alta.
6. A valle della contestualizzazione sviluppare le **Linee guida** per l'applicazione da parte della azienda IC ai propri fornitori

## Giugno kick-off del WG

# Q&A

