CSI your digital partner

Torino 10 Maggio

SICURI di essere SICURI?

Le misure di sicurezza adeguate: dalla teoria alla pratica

Valutare le misure con la DPIA:

integrazione con la BIA -Business Impact Assessment-

e con il Cybersecurity Framework aziendale

Stefano Luca Tresoldi - stefano.tresoldi@tresoldi.net
Componente associazione Centro Studi di Informatica Giuridica di Ivrea Torino

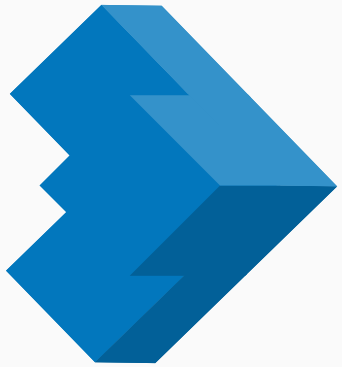
Indice

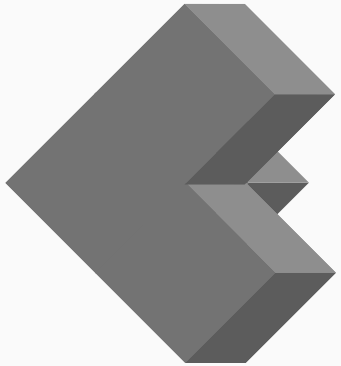
- DPIA, BIA e Cybersecurity Framework
- Documenti e materiali per approfondimenti

Cos’è

La DPIA è un processo volto a

- **descrivere il trattamento** e a
- **valutarne necessità e proporzionalità** nonché
- i relativi **rischi** (per i diritti e le libertà delle persone fisiche), allo **scopo di approntare misure idonee** ad affrontarli.
- E’ una procedura che permette di valutare e **dimostrare la conformità** con la norma





Quando è necessaria

È necessario eseguire una DPIA per i trattamenti che potrebbero comportare un **rischio elevato per i diritti e le liberta delle persone**.

Consultazione del DPO - Raccomandazioni del WP29 al titolare

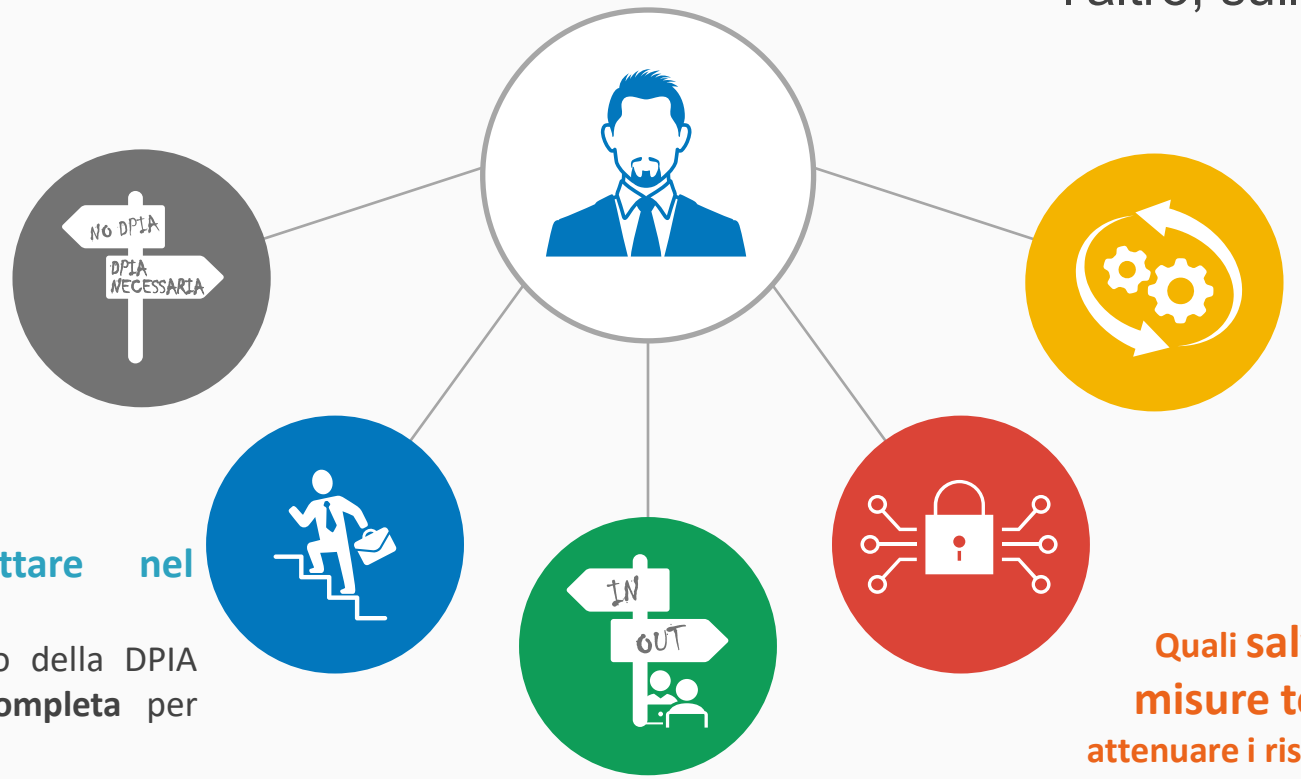
Il Gruppo di lavoro WP29 raccomanda che **il titolare** del trattamento **si consulti con il DPO**, fra l'altro, sulle seguenti tematiche

[WP 243 rev. 01]

Se condurre o meno una DPIA

Quale metodologia adottare nel condurre una DPIA

La metodologia per lo svolgimento della DPIA deve risultare **sufficientemente completa** per garantire il rispetto del GDPR



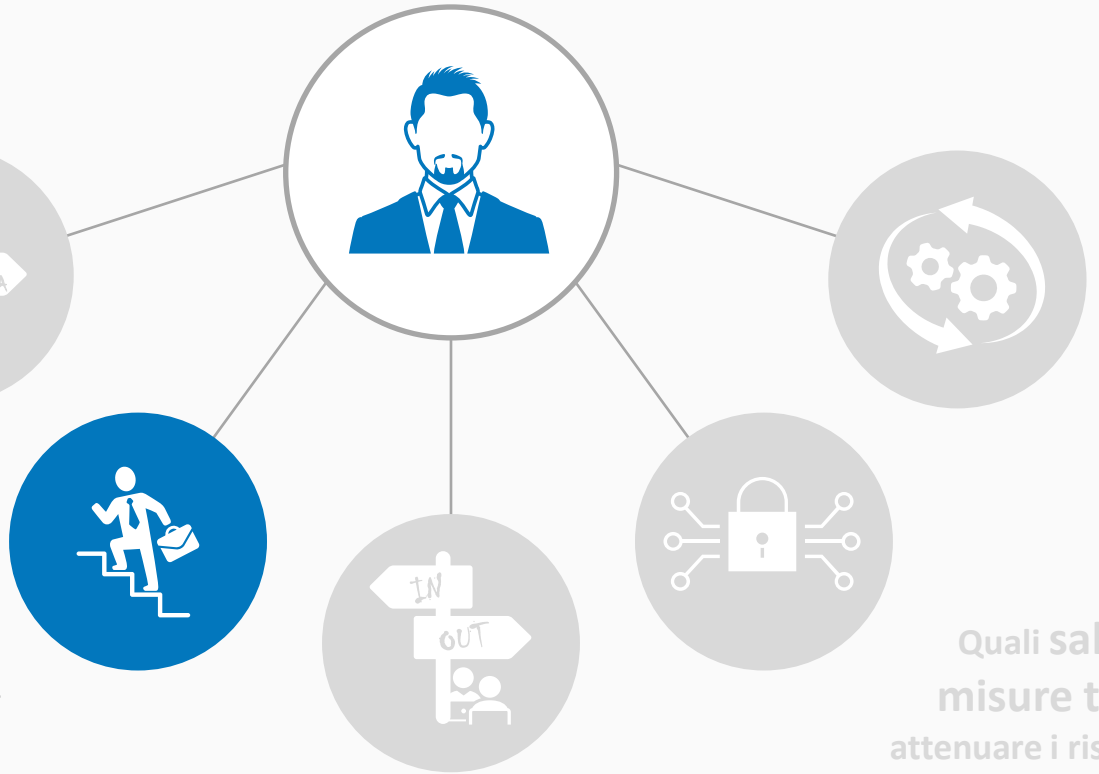
Se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) **siano conformi al GDPR**

Quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate

Se condurre la DPIA con le risorse interne ovvero esternalizzandola

Consultazione del DPO - Raccomandazioni del WP29 al titolare

Quale metodologia adottare per condurre una **DPIA**



Se condurre o meno una DPIA

Se la DPIA sia stata **condotta correttamente** o meno, e se le **conclusioni** raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) **siano conformi** al GDPR

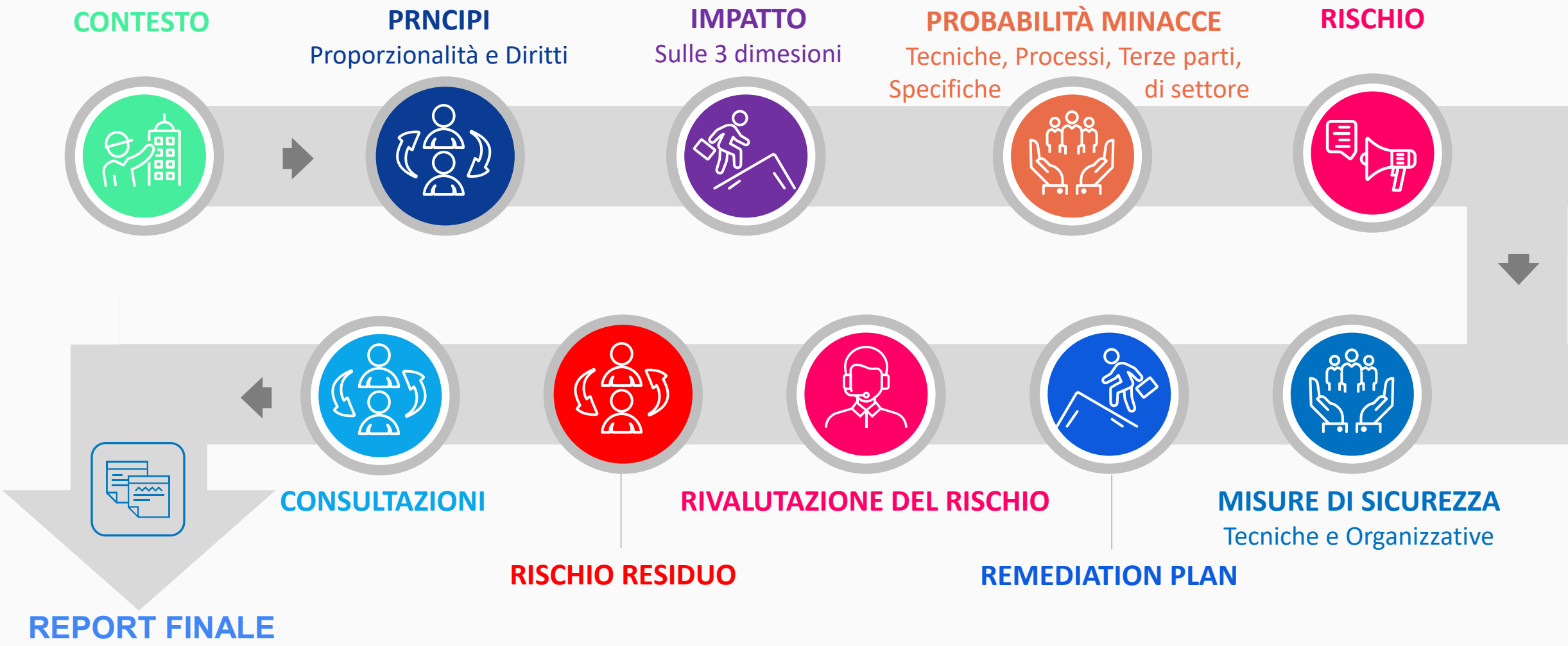
Quale metodologia adottare nel condurre una DPIA

La metodologia per lo svolgimento della DPIA deve risultare **sufficientemente completa** per garantire il rispetto del GDPR

Quali **salvaguardie** applicare, comprese **misure tecniche** e **organizzative**, per attenuare i rischi per i diritti e gli interessi delle persone interessate

Se condurre la DPIA con le **risorse interne** ovvero **esternalizzandola**

Elementi principali di una metodologia DPIA



Elementi principali di una metodologia DPIA

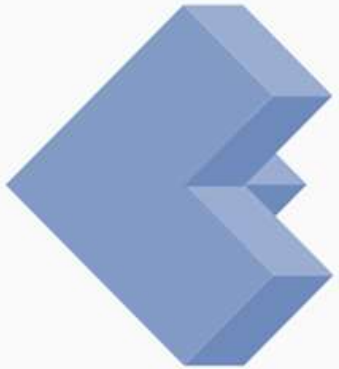
Il set delle misure di sicurezza

Business Impact Analysis: Cos'è e a cosa serve

Cos'è

La BIA –Business Impact Anaysis- è un processo di analisi volto a

- **determinare l'impatto e le ricadute sul business** aziendale derivanti da eventi che causano l'interruzione dell'erogazione di servizi o della produzione di beni
- individuare e valutare i **processi aziendali rilevanti** ai fini della continuità operativa



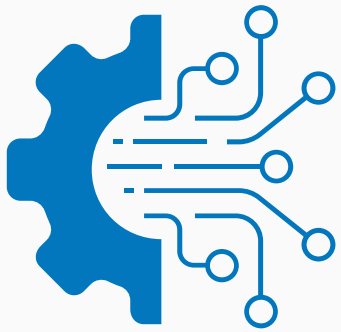
A cosa serve

- Identificare le **attività critiche** per l'operatività, i **rischi** e gli **impatti** derivanti dalla loro mancata disponibilità
- Sviluppare strategie e misure di continuità del business
- **Minimizzare gli impatti negativi derivanti da eventuali interruzioni delle attività**
- definire le priorità di ripristino in caso di interruzione

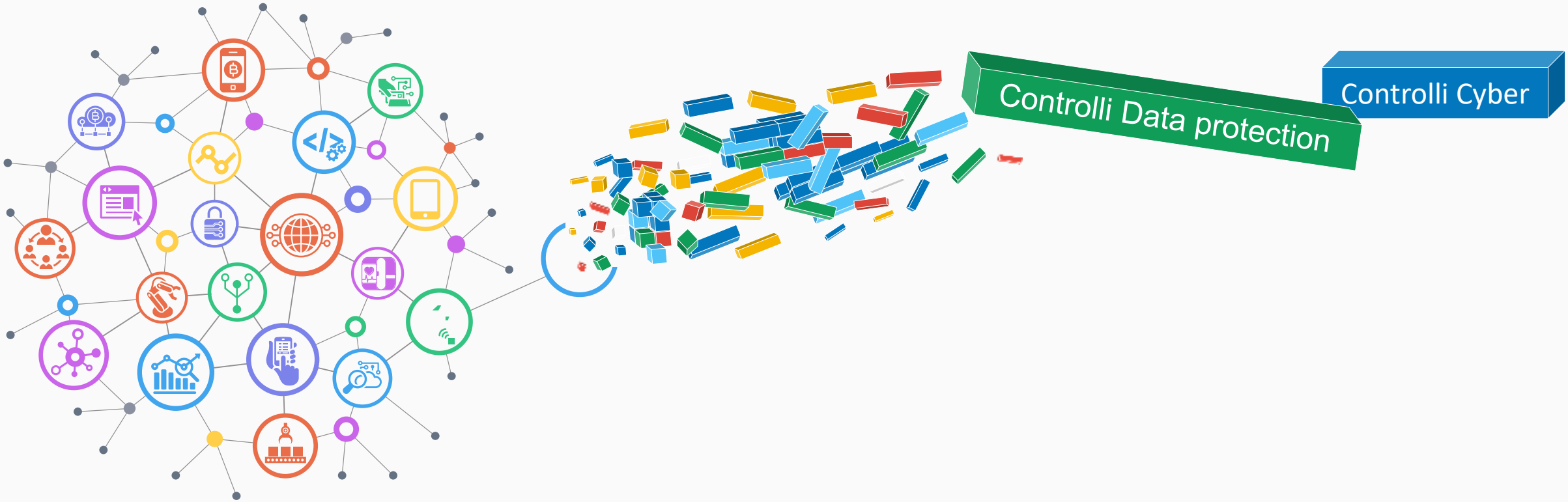
Grandi multinazionali

Esigenza delle grandi multinazionali era dotarsi di una **Metodologia DPIA ad hoc** che potesse risultare **Omogenea** e **raffrontabile** per tutte le società del gruppo in tutte le country.

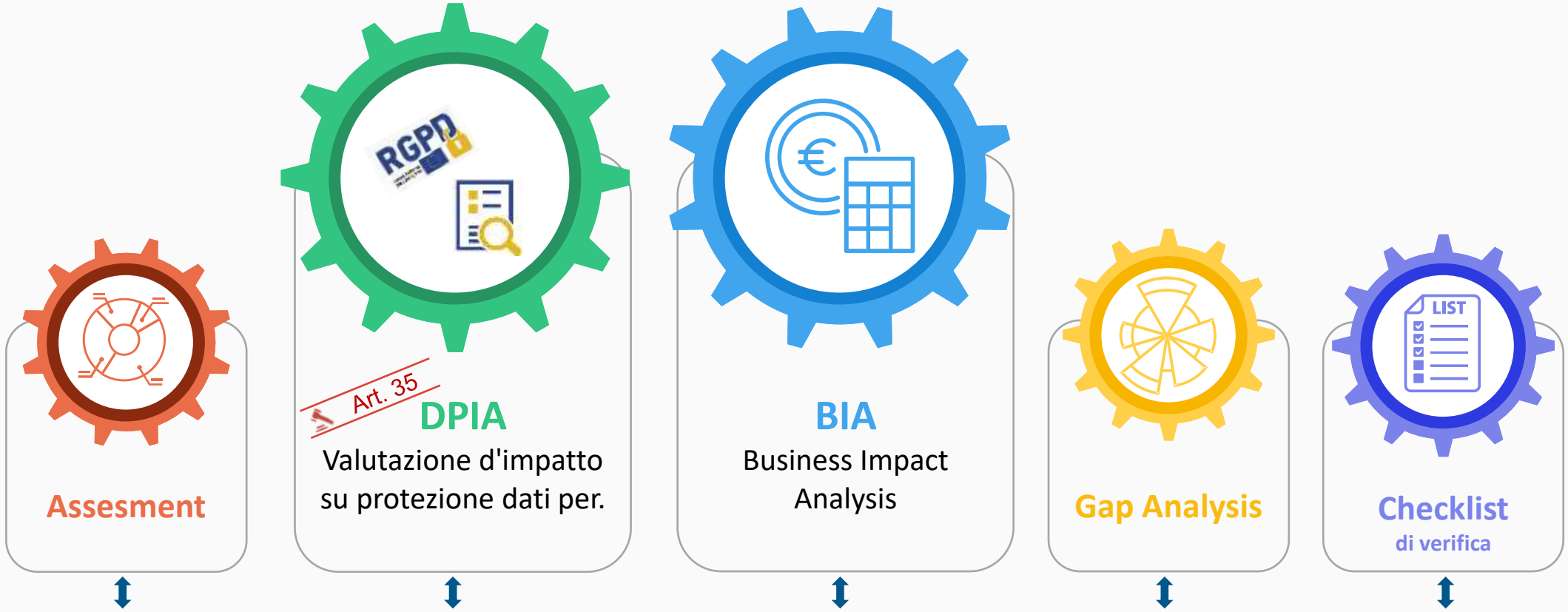
e che risultasse **integrata** con i framework aziendali esistenti ovvero iniziare a creare un framework aziendale cyber di riferimento (es. DPIA, BIA e controlli cyber)



Framework aziendale di riferimento

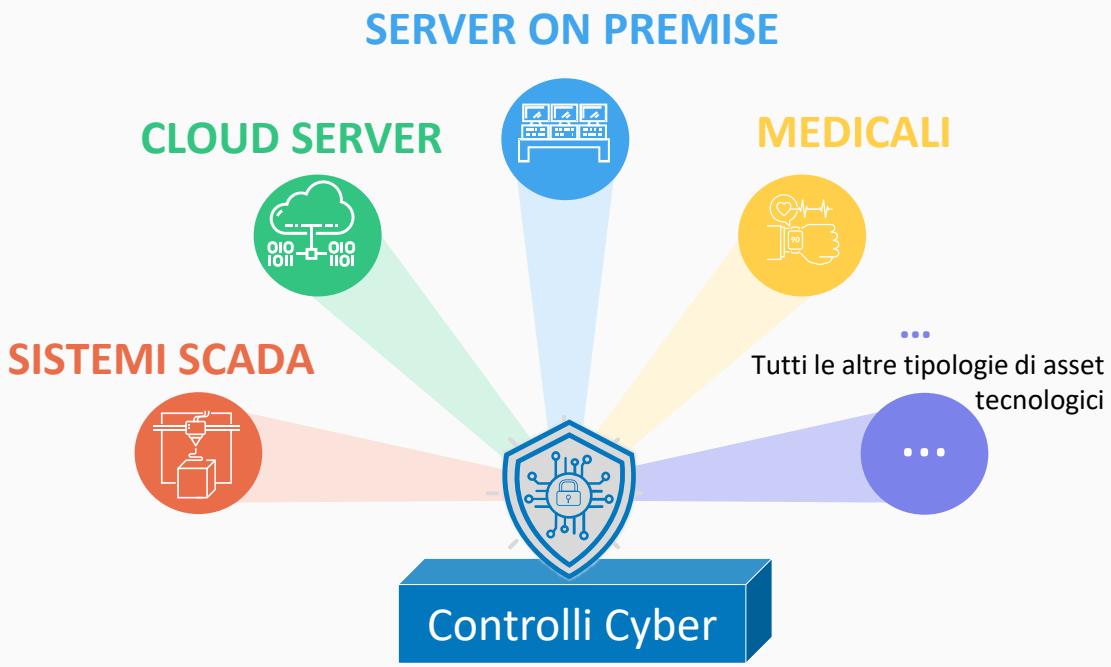


I vantaggi di un framework aziendale di riferimento che utilizza set di controlli comuni



Come costruire un framework aziendale per i controlli cyber

- Individuazione degli **asset tecnologici** aziendali
- Classificare gli asset tecnologici in **classi tecnologiche** distinte in base alle differenti specificità degli stessi



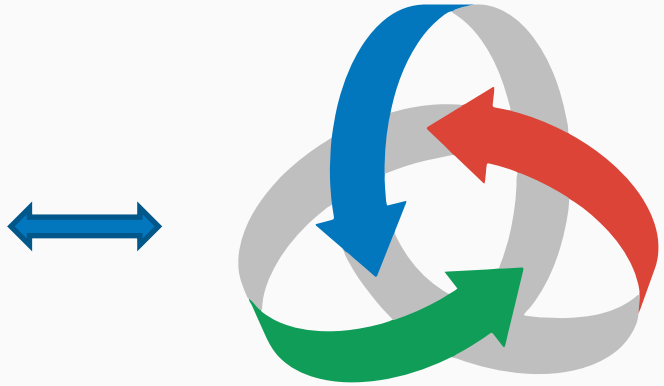
- Individuazione di un **set globale di 'controlli cyber'** di riferimento es. ISO 27001, ISO… e altri controlli
- **Mappatura** dei controlli del set globale di riferimento su ciascuna delle classi degli asset tecnologici creando quindi un **sub set di controlli specifico per ciascuna classe** degli asset tecnologici
- Per ciascun subset di controlli, specifici per le singole tipologie di asset tecnologici individuati, creare una **Baseline di riferimento** (Target) e una **Better Practice Line**
- Integrare nei tools aziendali i subset dei controlli creati in modo da poterli, di volta in volta, usare in base alle specificità di ciascuno degli asset tecnologici che si andranno a considerare e valutare.

Influenze reciproche tra DPIA e BIA

Art. 35

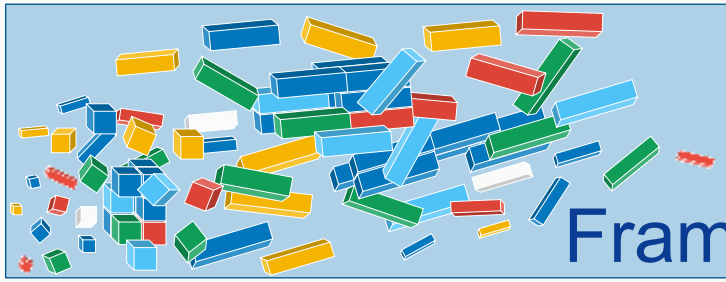
DPIA

Valutazione d'impatto su protezione dati per.



BIA

Business Impact Analysis



Controlli Data protection

Controlli Cyber

Framework aziendale di riferimento

Quale metodologia?

Una **metodologia DPIA** deve risultare, sufficientemente **completa** e **adeguata al settore industriale** dell'azienda, ma non solo.

Si deve **integrare** con gli esistenti **processi e procedure aziendali** come

- Cybersecurity Framework aziendale
- BIA - Business impact Assessment

Documenti

e materiali per approfondimenti

Documenti e materiali per approfondimenti

WP29- Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248rev.01) adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Garante Privacy - Applicare il GDPR. Le linee guida europee (2019) [doc. web n. 9277035] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9277035

Garante Privacy - Valutazione d´impatto sulla protezione dei dati. https://www.garanteprivacy.it/regolamentoue/DPIA

Centro Studi di Informatica Giuridica di Ivrea-Torino (CSIG) è un' associazione indipendente interdisciplinare senza finalità di lucro attiva dal 2005 (rivolta a giuristi, informatici, ricercatori, studenti..etc.)

Thanks!

Contatti:

Stefano Luca Tresoldi

stefano.tresoldi@tresoldi.net

Centro Studi Informatica Giuridica

CSIG

Ivrea - Torino