DIH
Digital Innovation Hub

# Cybersecurity

*assessment*

SISTEMI FORMATIVI CONFINDUSTRIA
FEDERMANAGER
4.MANAGER
CONFINDUSTRIA
Industria 4.0 Veneto

# *Cybersecurity Maturity Assessment* per le PMI

INIZIATIVA DI:

Sistemi Formativi Confindustria

Rete dei *Digital Innovation Hub*

- Nell'ambito dell'elaborazione del "Piano di sviluppo dei DIH" è stato costituito un Gruppo di Lavoro dedicato allo sviluppo del *modello di Assessment per la valutazione del livello di Cybersecurity delle PMI.*

- Il ***Cybersecurity Maturity Assessment*** segue i riferimenti del **Framework Nazionale per la Cybersecurity e Data Protection (FNCS)**, che discende a sua volta dal **framework NIST**, National Institute of Standards and Technology americano, e dello standard **ISO/IEC 27001**.

- Poiché per le micro, piccole e medie imprese implementare una gestione del rischio *Cyber* basata sul *Framework* nazionale può risultare troppo complesso e oneroso è stato deciso di semplificarlo in modo da renderlo applicabile anche fascia delle micro, piccole e medie imprese

- Per questo motivo è stato stilato un elenco di ***controlli essenziali di Cybersecurity*** che rappresentano un insieme minimo di pratiche di sicurezza dalla quale parti

# *Cybersecurity Maturity Assessment* per le PMI

INIZIATIVA DI:

Sistemi Formativi Confindustria

Rete dei *Digital Innovation Hub*

- Il ***Cybersecurity Maturity Assessment*** nasce quindi per aiutare il management aziendale Nnel processo di comprensione dell'importanza della protezione dai rischi *Cyber* e promuovere la *Data Protection*.

- Ha quindi l'obiettivo di ***aumentare la consapevolezza delle aziende sul tema della Cybersecurity*** e ***fornire una fotografia del livello di maturità*** basata su *standard* di riferimento nazionali e internazionali.

- E' un insieme di linee guida che aiutano ad introdurre una ***cultura di gestione del rischio*** all'interno dell'azienda e intende aiutare le aziende nella definizione di un percorso di ***miglioramento progressivo*** per implementare in azienda una gestione della Cyber sicurezza

I vantaggi nell'utilizzo del framework sono:

- ***identificare*** i rischi legati alla Cyber sicurezza
- ***valutare*** i livelli di Cyber sicurezza in uno specifico momento
- ***abilitare*** l'implementazione delle misure di sicurezza
- ***monitorare e valutare*** l'efficacia delle misure adottate

# *Il processo di assessment*

**INDIVIDUAZIONE PROFILO DI RISCHIO**

Lo strumento individua il profilo di rischio dell'impresa andando a individuare un **livello di maturità *target*** da raggiungere

**IL *Cyber assessment* si adatta allo specifico contesto**

**MISURAZIONE DEL LIVELLO CYBER**

Lo strumento misura il livello *Cybersecurity* che raggiunge l'impresa e indica se il **livello di maturità minimo** è superato o meno

**Il *Cyber assessment* fornisce la postura di sicurezza dell'organizzazione analizzandola**

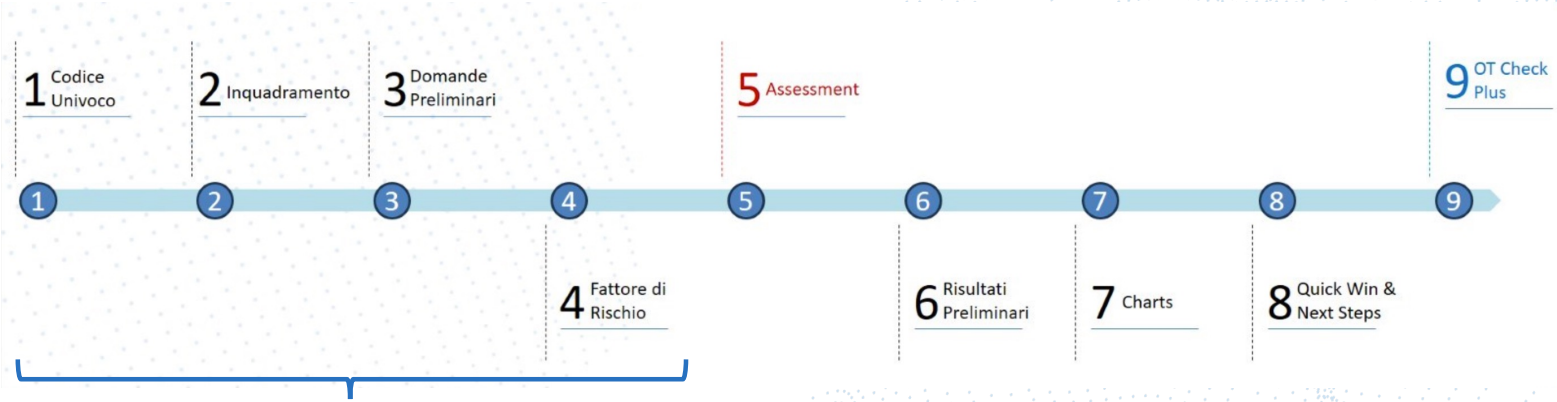
**- a livello generale -**
**- per category -**
**- per function -**

**SUGGERIMENTI PRATICI: *QUICK WINS* e *NEXT STEPS***

Lo strumento fornisce suggerimenti per orientare una ***gap analysis*** e definire azioni per superare il livello di maturità *target* e implementare una ***roadmap* di *remediation***

**Il *Cyber assessment* restituisce *quick wins* e *next steps***

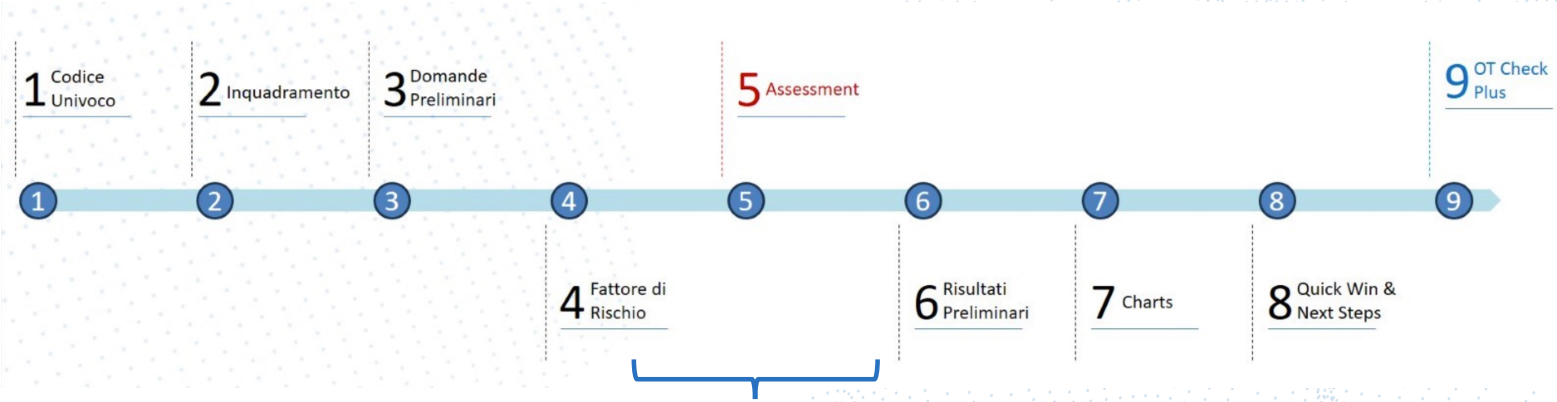
# *Il processo di assessment*




***1. Raccolta di informazioni di inquadramento dell'azienda (ca. 30' di tempo dell'azienda, via webmeeting)***

Durante questa fase vengono raccolte alcune informazioni preliminari sull'azienda (codice Ateco, settore, numero dei dipendenti, presenza all'estero, ecc.) che servono a definire un **«Profilo Target»** di rischio di Cybersecurity dell'azienda (molto basso-basso-medio-alto-critico) ***contestualizzato allo specifico contesto di business dell'azienda.***

# *Il processo di assessment*



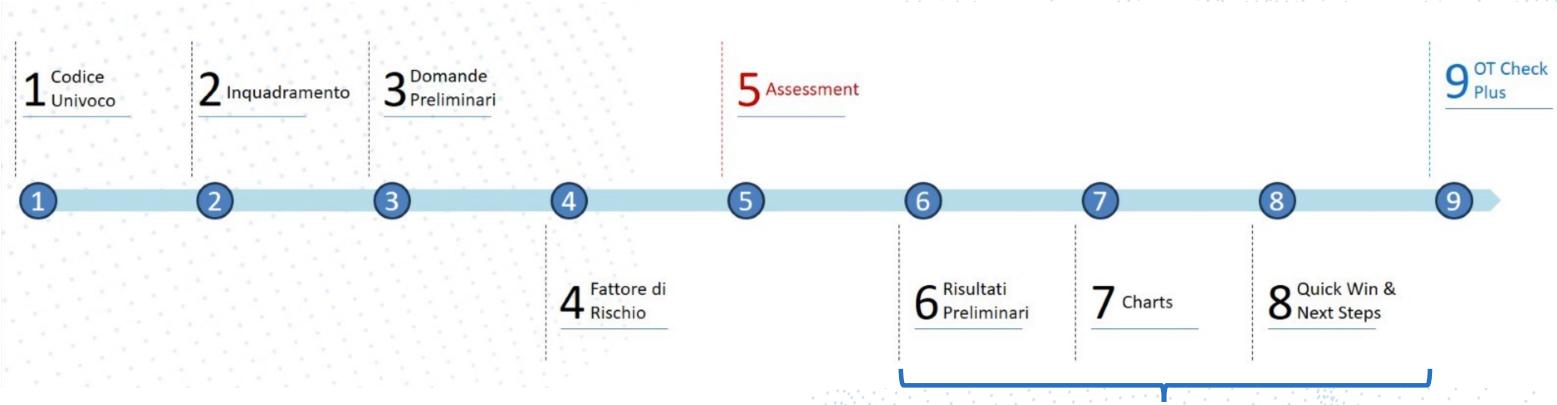

***2. Assessment (ca. 2,5 ore, in presenza)***

Durante questa fase (30 titoli/domande incrementali) vengono raccolte informazioni più dettagliate atte a definire il "***Profilo corrente***" in ambito Cyber dell'azienda.

Questa sarà poi oggetto di confronto con il *"Profilo Target"* per definire la distanza tra il posizionamento attuale e quello consigliato …

… e definire conseguentemente le azioni di rimedio consigliate che saranno contenuti nel report di restituzione

# *Il processo di assessment*



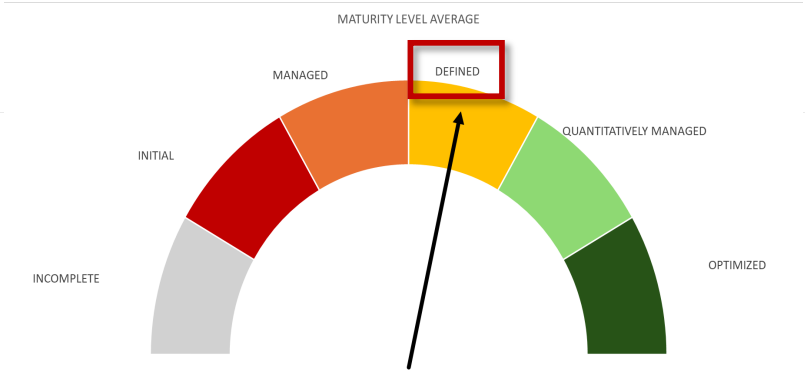

***3. La consegna in azienda dei risultati dell'assessment (ca. 2 ore di tempo dell'azienda, in presenza)***

*Questa fase prevede la consegna all'azienda di alcuni report e consigli pratici per migliorare – laddove necessario - la gestione della sicurezza, sia dal di vista dei processi aziendali impattati, sia da quello tecnologico, nonchè per definire eventuali azioni di rimedio sul breve e sul medio termine.*

# *Il report di restituzione*

- Livello complessivo di maturità Cyber dell'azienda rilevato mediante l'assessment

- Indicazioni di eventuali gap esistenti secondo le category definite nel modello:
  - *Il report finale evidenzierà - per ciascuna dimensione – la distanza tra la postura Cyber corrente e target, definita per lo specifico contesto aziendale*
  - *Per ciascuna area in cui vi sia un gap tra postura corrente e quella target, vengono proposte delle azioni consigliate per ridurre tale distanza, accompagnandole con le relative indicazioni di intervento*




# *Il report di restituzione*

- Livello complessivo di maturità Cyber dell'azienda rilevato mediante l'assessment

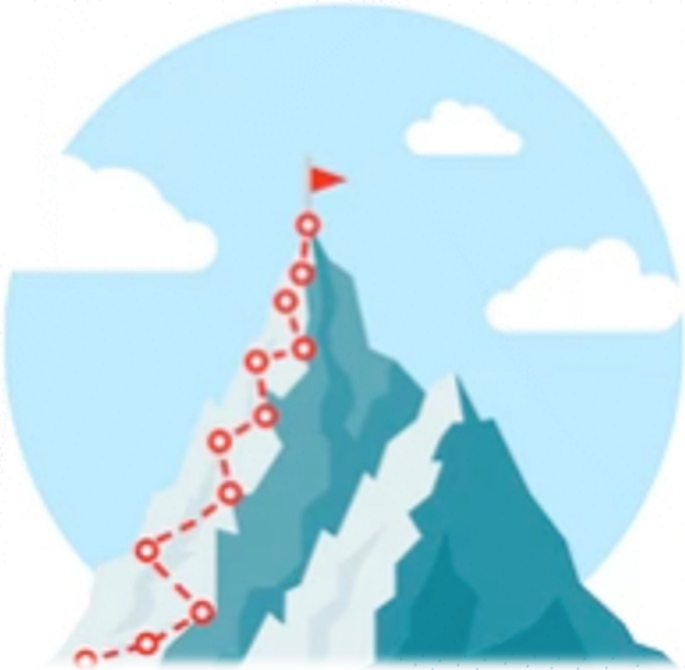
- Indicazioni di eventuali gap esistenti secondo le category definite nel modello

- Azioni di rimedio consigliate nel breve (*«Quick Wins»*) e nel medio termine (*«Next Steps»*)

| ID | CATEGORY | QUICK WIN |
|---|---|---|
| 7 | Information Protection Processes and Procedures | Si consiglia di affidare la gestine della sicurezza dei servizi critici ad una risorsa dedicata, interna o esterna, per garantire una supervisione continua e competente delle pratiche di sicurezza applicate ai servizi critici |
| 8 | Information Protection Processes and Procedures | Si suggerisce di designare formalmente un referente, interno o esterno, responsabile della compliance normativa e delle politiche interne in ambito cybersecurity e/o privacy (ad es. DPO) - vedasi anche NIS2 |
| 9 | Governance | Si consiglia di assegnare ruoli e responsabilità specifici per la gestione della sicurezza informatica (vedasi NIS2) |
| 10 | Business Environment | Si raccomanda di formalizzare politiche e procedure in ambito cybersicurezza, aggiornarle periodicamente e renderle accessibili e consultabili da parte della popolazione aziendale interessata, al fine di promuovere una cultura della sicurezza e della privacy all'interno dell'organizzazione (vedasi NIS2) |
| 11 | Risk Management Strategy | Si consiglia di allocare proattivamente un budget specifico per la cybersecurity, definendo spese ad hoc a discrezione dei responsabili designati dall'alta direzione |

| ID | CATEGORY | NEXT STEPS |
|---|---|---|
| 1 | Information Protection Processes and Procedures | Si raccomanda di mantenere almeno tre copie di backup: una principale in sede, una locale in un edificio separato e una in cloud remotizzato, per una maggiore sicurezza dei dati. |
| 2 | Information Protection Processes and Procedures | Si raccomanda di avere una copia di backup in cloud remoto per le informazioni critiche e di predisporre i parametri adatti al ripristino dei sistemi e politiche di DR (ad es. RTO/RPO, ecc.) |
| 3 | Risk Assessment | Si raccomanda di adottare una metodologia specifica per la valutazione dei rischi o degli impatti che includa aspetti di information/cyber security, per un'analisi approfondita delle vulnerabilità aziendali. |
| 4 | Response Planning + Communications + Analysis + Recovery Planning | Si consiglia di stabilire piani, procedure, linee guida o prassi consolidate per la gestione degli incidenti informatici e per la continuità operativa, al fine di prepararsi efficacemente a eventuali emergenze (vedasi NIS2) |
| 5 | Awareness and Training | Si suggerisce di prevedere attività di formazione periodiche dedicate alla gestione degli incidenti, per preparare adeguatamente il personale ad affrontare situazioni di emergenza. |
| 6 | Information Protection Processes and Procedures | Si raccomanda di effettuare aggiornamenti anche sui dispositivi Operational Technology (OT)/di controllo industriale in base alle segnalazioni dei reparti IT/Operation interni o dei produttori. |

# *Il percorso di difesa per la Cybersecurity*



- Accompagnare le aziende con attività di ***assessement*** *finanziati* nell'ottica di percorso di miglioramento della consapevolezza e di un miglioramento progressivo nei confronti dei rischi di Cybersicurezza

ma anche ….

- aiutandole a comprendere il loro posizionamento nei confronti di eventuali obblighi normativi (con ***servizi consulenziali post-assessment,*** anch'essi *finanziati*)

- Supportandole nel definire ed implementare percorsi di rimedio nei confronti dei rischi di Cybersecurity sempre mediante ***servizi consulenziali post-assessment*** (anch'essi *finanziati).*

Ad esempio formazione dei dipendenti in ambito Cyber, definizione di Analisi dei Rischi, redazione di Piani di Risposta ad eventuali attacchi Cyber, ecc.

# Contatti


Massimo Colorio

dih-veneto@siav.net

www.siav.net