Industria 4.0
Veneto

CONFINDUSTRIA
Veneto SIAV S.r.l.

Confindustria Veneto SIAV alle Imprese

ASSESSMENT DI CYBER SICUREZZA

Assessment di Cyber sicurezza

1. Introduzione: quali sono i rischi Cyber per le imprese
2. Modello per l'assessment di Cyber sicurezza
3. Descrizione della piattaforma e relative fasi operative
4. Il report di restituzione
   - AS-IS & TO-BE
   - Conclusioni, Quick Wins & Next Steps
   - Assessment OT (Operational Technologies) e Industrial IoT
5. La direttiva NIS2

Introduzione: quali sono i rischi Cyber per le imprese

Industria 4.0
Veneto

Quali sono i rischi Cyber per imprese?

1. **Pagamenti errati su IBAN falsificati** (furto di identità, "man-in-the-middle")

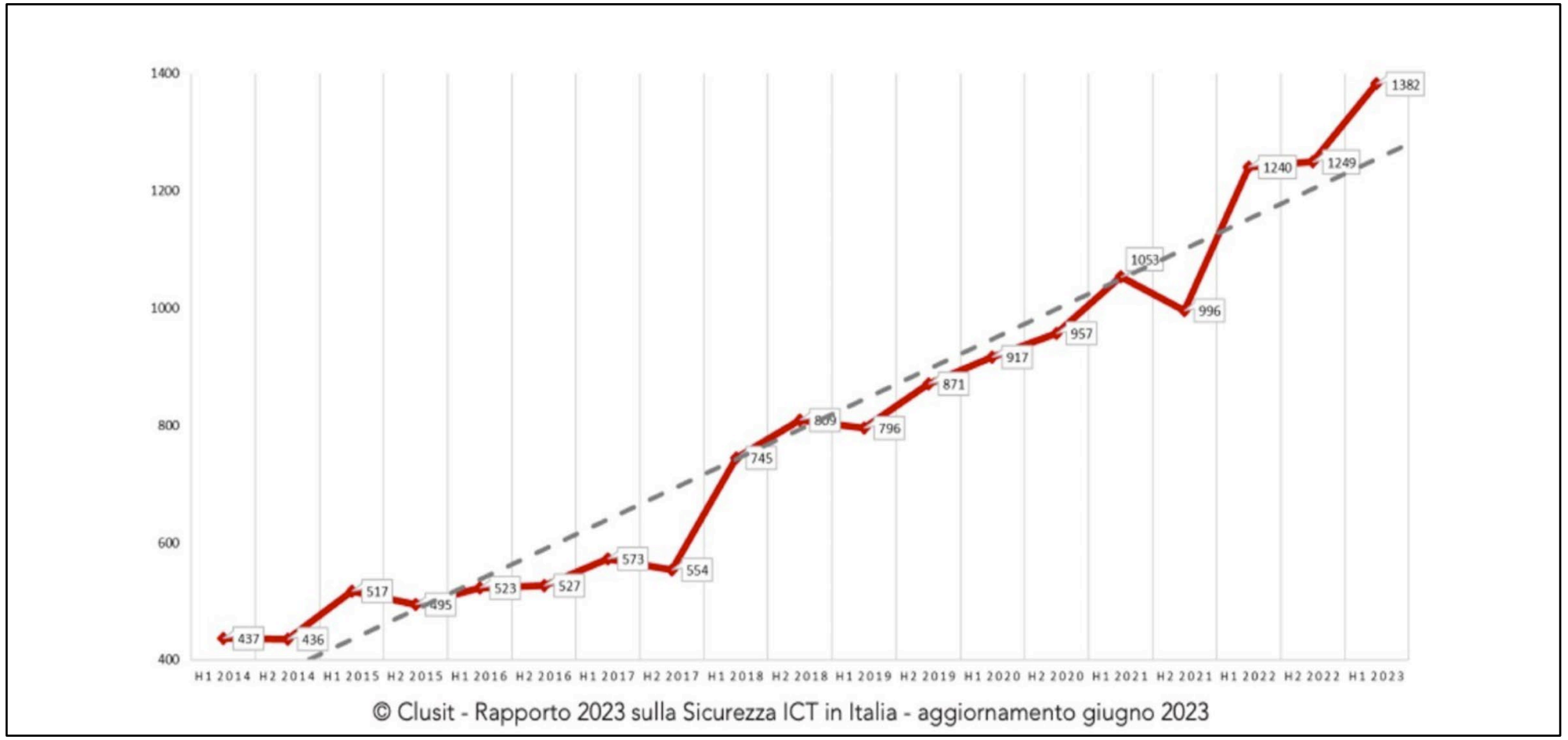
2. **Cryptolocking delle infrastrutture ICT**
   - Fermo dell'azienda (giorni, settimane) – ripartenza non garantita
   - Pagamento del riscatto (fermo dell'azienda lungo, costo importante, illecito penale)
   - Impossibilità di recuperare i dati aziendali

3. **Ransomware e furto delle informazioni aziendali**
   - Furto di dati di clienti e fornitori (GDPR!)
   - Furto di dati sensibili (relativi ai prodotti, ai progetti, ai contratti, ecc.)

4. **Danno reputazionale e normativo**
   - Immagine dell'azienda nel mercato/territorio
   - Verso i propri clienti (supply-chain dei fornitori) – es. NIS2, Tisax, ecc.

5. **Impatti assicurativi, organizzativi,…**

Gli attacchi Cyber in Italia stanno crescendo in maniera molto significativa



… e le cose stanno continuando a peggiorare

Rapporto Clusit 2024

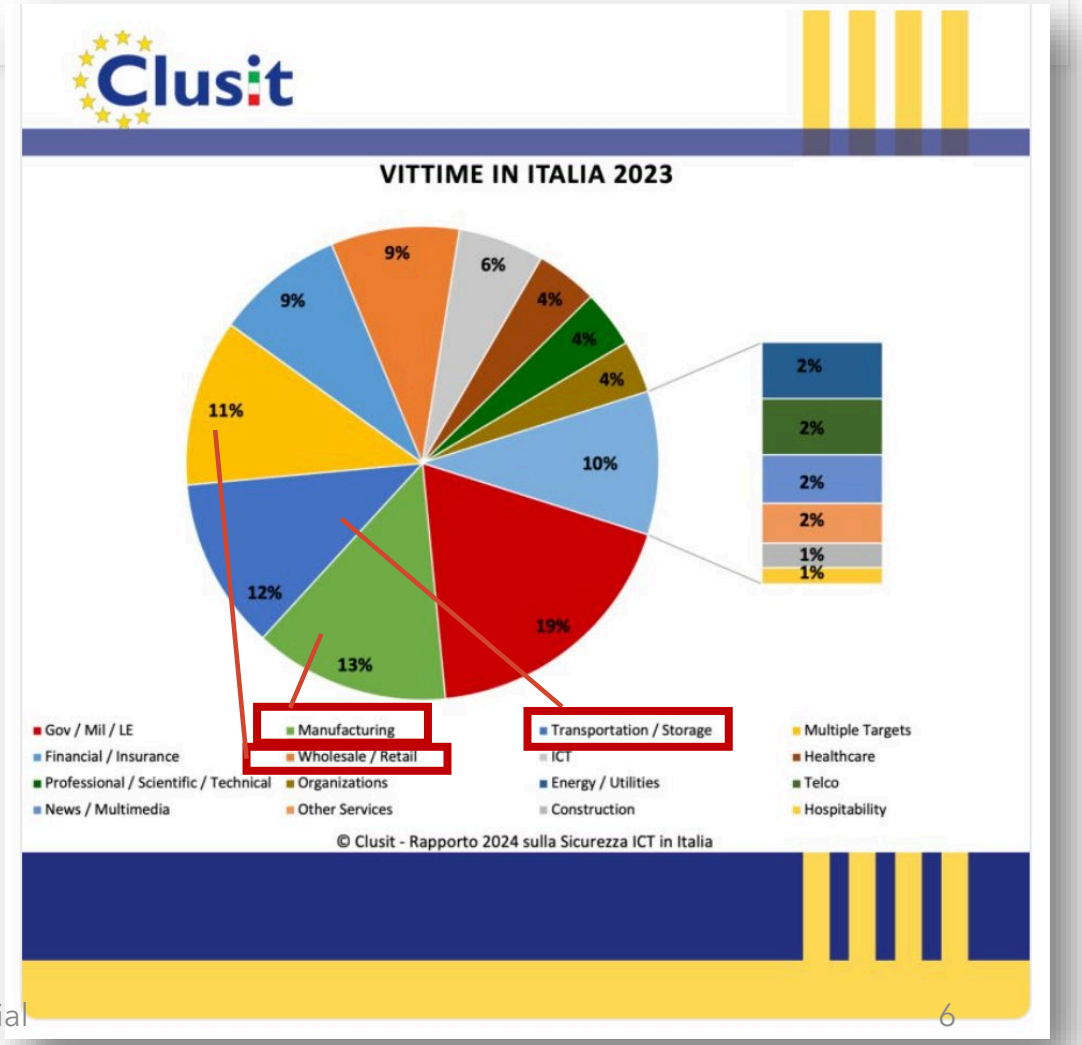
❗Con 2.779 incidenti gravi analizzati a livello globale da #Clusit, il 2023 restituisce **una fotografia nettamente peggiorativa rispetto ai dodici mesi precedenti**, continuando a descrivere una curva degli #attacchi **in inesorabile crescita**, che registra un +12% sul 2022.

IT Mensilmente è stata rilevata una media di 232 attacchi, con un picco massimo di 270 nel mese di aprile, che rappresenta anche il valore massimo misurato negli anni.

Il nostro Paese appare sempre più nel mirino del #cybercrimine: lo scorso anno in Italia è andato a segno l'11% degli attacchi gravi globali mappati dal Clusit (crescita del 65% rispetto al 2022)

❗**Oltre la metà degli attacchi - il 56% - ha avuto conseguenze di gravità critica o elevata**.

Con uno sguardo agli ultimi cinque anni, emerge inoltre che **oltre il 47% degli attacchi totali censiti in Italia dal 2019 si è verificato nel 2023.**



Modello per l'assessment di Cyber sicurezza

Industria 4.0
Veneto

Modello per l'assessment nazionale di Cyber sicurezza

Assessment di Cyber sicurezza - Come nasce - Cos'è

Il modello dell'assessment segue i riferimenti del NIST (*National Institute of Standards and Technology* americano) da cui discende il ***Framework Nazionale per la CyberSecurity e data protection (FNCS),*** e dallo standard internazionale **ISO/IEC 27001** (e ISO 27002)

Il framework è un insieme di linee guida che aiutano ad introdurre una cultura di gestione del rischio all'interno dell'azienda per combattere la minaccia Cyber.

Il framework è stato semplificato in modo da renderlo applicabile anche alle medie, piccole e micro imprese, introducendo ***15 controlli essenziali di Cyber sicurezza***

Lo strumento, a partire dalla verifica dei 15 controlli essenziali, ha integrato 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'implementare misure di sicurezza
- **monitorare** e valutare l'efficacia delle misure adottate

L'assessment implementa rigorose misure di «*non-disclosure*» e trattamento confidenziale delle informazioni

Modello per l'assessment nazionale di Cyber sicurezza

Assessment di Cyber sicurezza - Come si sviluppa

L'assessment si basa su 2 profili di riferimento in materia di Cyber sicurezza dell'azienda:

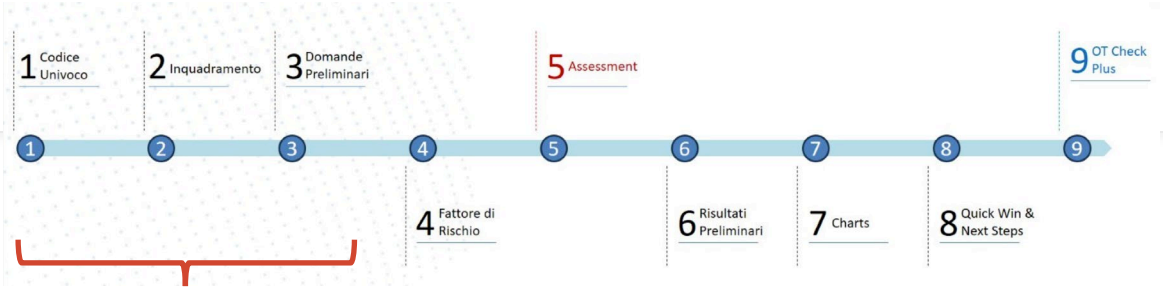
PROFILO TARGET (TO-BE) che offre l'opportunità all'azienda di valutare quale potrebbe essere un livello minimo di maturità Cyber richiesto all'azienda e come i processi aziendali, le tecnologia utilizzate, la formazione delle persone possano evolvere per raggiungere un approccio strutturato alla Cyber sicurezza.
Questo profilo viene definito tenendo conto dello specifico contesto di business dell'azienda stessa e del livello di sicurezza desiderato (base-medio-avanzato)

PROFILO ATTUALE (AS-IS) che fornisce all'azienda una metrica sul proprio stato dell'arte attuale in materia di Cyber sicurezza (aree critiche).

Lo scopo è quello di fornire all'azienda una "fotografia" del suo attuale livello di esposizione al rischio in materia di Cyber sicurezza e Protezione delle Informazioni.

Anche questa "fotografia" viene scattata tenendo conto dello specifico contesto di business dell'azienda stessa e del grado di maturità tecnico-organizzativa in ambito Cyber dell'azienda

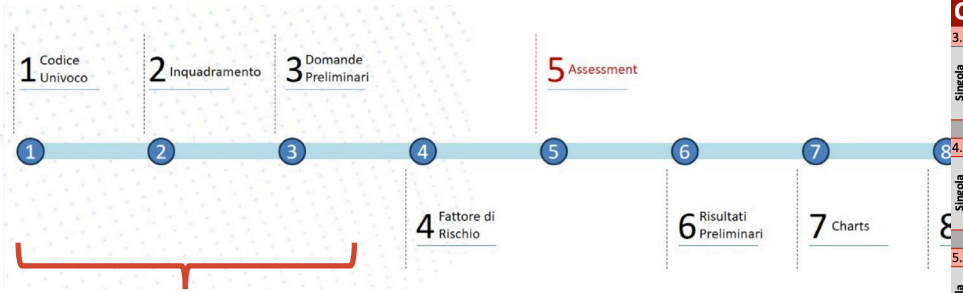
Assessment di Cyber Sicurezza



L'assessment si costituisce di 4 fasi:

1. **Adesione da parte dell'azienda e firma dei documenti di NDA**

Assessment di Cyber Sicurezza



2. Raccolta di informazioni di inquadramento dell'azienda (ca. 1 ora 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 di profilo di rischio di Cyber Sicurezza dell'azienda (molto basso-basso-medio-alto-critico) contestualizzato allo specifico contesto di business dell'azienda.

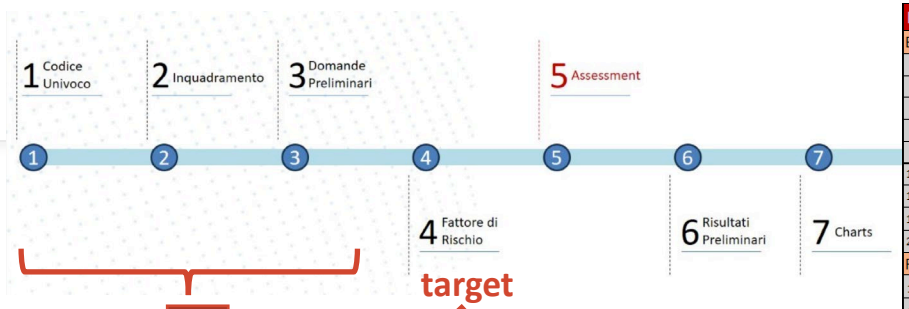
CONTESTO

3. L'IMPRESA HA SEDI ESTERE?		
Singola	1	No
	2	Sì, in Europa
	3	Sì, in paesi extra UE
	4	Sì, sia in paesi UE che in paesi extra UE
4. FATTURATO DELL'AZIENDA		
Singola	1	MAGGIORE DI 50 MILIONI
	2	MAGGIORE O UGUALE A 10 MILIONI E MINORE DI 50 MILION
	3	MAGGIORE O UGUALE A 2 MILIONI E MINORE DI 10 MILIONI
	4	MINORE DI 2 MILIONI
5. NUMERO DI DIPENDENTI TOTALI		
Singola	1	MAGGIORE DI 250 DIPENDENTI
	2	TRA 50 E 250 DIPENDENTI
	3	TRA 10 E 49 DIPENDENTI
	4	MINORE DI 10 DIPENDENTI
6. SETTORE DI RIFERIMENTO		
Multipla	1	Industria alimentare, delle bevande e del tabacco
	2	Industria tessile, dell'abbigliamento e della pelle (escluso fashi
	3	Industria chimica e farmaceutica
	4	Industria petrolchimica e del carbone
	5	Industria della gomma e della plastica
	6	Industria dei metalli
	7	Industria dei veicoli a motore e di altri mezzi di trasporto
	8	Industria elettromeccanica, dei macchinari e delle attrezzatur
	9	Industria elettronica, elettrica ed ottica
	10	Industria della carta e della stampa
	11	Industria del legno e dei mobili
	12	Industria dei materiali da costruzione
	13	Industria del vetro
	14	Altra industria manifatturiera
	15	Industria della difesa (o affini)
	16	Pubblica amministrazione (locale, regionale)
	17	Pubblica amministrazione centrale
	18	Healthcare/Medicali/Aziende sanitarie
	19	Banking/Finance
	20	Digital service provider (software & web)
	21	Energy (esclusi petrolchimica e carbone)
	22	ICT & Telco (hardware, reti, dispositivi, connettività e telecom
	23	Educazione/Ricerca
	24	Media/Intrattenimento
	25	Posta/Corrieri
	26	Gestione, distribuzione e trattamento delle acque
	27	Altro
7. L'azienda fa parte di una o più delle seguenti filiere produttive?		
Multipla	1	Agribusiness
	2	Chimica
	3	Costruzioni
	4	Difesa/Aeronautica
	5	Energia
	6	Finanza
	7	ICT
	8	Meccanica
	9	Mediatico/Audiovisivo
	10	Metallurgia/siderurgia
	11	Mezzi di traporto

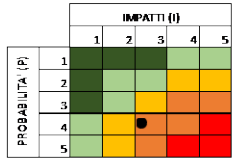
DOMANDE PRELIMINARI

Negli ultimi 3 anni sono stati rilevati eventi di sicurezza cibernetica accidentali o di natura intenzionale, compresi TENTATIVI di attacco reiterati			
ad esempio: (malfunzionamenti sistemici, data breach, attacchi cibernetici, intrusioni, accessi non autorizzati, truffe, phishing etc.)			Select 1
Singola	1	No (0 eventi/incidenti)	
	2	1 Incidente	
	3	tra 2 e 5 eventi	X
	4	tra 6 e 10 eventi	
	5	più di 10 eventi	
Quali tra questi impatti sono stati registrati in seguito agli attacchi?			Select +
Multipla	1	Perdita/Cancellazione/Modifica permanente di dati	
	2	Inaccessbilità dei dati per periodi di tempo prolungati	
	3	Inaccessibilità dei dati per periodi di tempo limitati	
	4	Pubblicazione di dati NON rilevanti/confidenziali/personali	X
	5	Pubblicazione di dati rilevanti/confidenziali/personali	
	6	Nessuna perdita economica	X
	7	Perdita economica limitata dovuta a danni emergenti o lucro cessante	
	8	Perdita economica significativa dovuta a danni emergenti o lucro cessante	
Quale tra queste tipologie di incidente è stata registrata?			Select +
Multipla	1	Malfunzionamento IT/OT (non meglio specificato)	
	2	Data Breach (accesso dati e/o sistemi da parte di attori esterni e/o pubblicazione dei dati)	
	3	Intrusioni a sistemi aziendali con eventuale modifica di dati	
	4	DDoS/DoS (negazione di un servizio web / saturazione dei sistemi)	
	5	Ransomware (cifratura e inaccessibilità dei dati e richiesta di riscatto)	
	6	Phishing/Social Engineering/Spam/Scam/Fraud (tentativi di truffa, furto di informazioni o invio di allegati contenenti malware a mezzo mail/telefonico/chat)	X
	7	Frode bancaria/catena di fornitura (p.e: richieste di bonifici da parte di falsi fornitori)	X
	8	Infezioni da Malware/Virus (non meglio specificato)	
Qual è per l'azienda il livello di criticità dell'infrastruttura IT/OT in termini di disponibilità e integrità dei servizi e dei dati?			Select 1
Singola	1	In caso di interruzione/indisponibilità/compromissione dei sistemi e/o dei dati non viene intaccata l'operatività dell'azienda (l'azienda può riorganizzare erogazione dei servizi e produzione entro 1 ora e/o nessuna perdita economica)	
	2	In caso di interruzione/indisponiblità/compromissione dei sistemi e/o di dati si prevedono impatti di bassa entità per l'azienda, con la possibilità di garantire la piena operatività mediante strumenti non IT/OT (l'azienda può riorganizzare erogazione dei servizi e produzione entro 4 ore e/o possibile perdita economica non significativa)	
	3	In caso di interruzione/indisponibilità/compromissione dei sistemi e/o dei dati si prevedono impatti di media entità per l'azienda, con la possibilità di garantire l'operatività parziale mediante strumenti non IT/OT (l'azienda può riorganizzare erogazione dei servizi e produzione entro 24 ore e/o perdita economica certa, ma non significativa)	X
	4	In caso di interruzione/indisponibilità/compromissione dei sistemi e/o dei dati si prevedono impatti gravi per l'azienda (l'azienda può riorganizzare erogazione dei servizi e produzione entro 48 ore e/o perdita economica certa con un rientro inferiore ai 6 mesi)	

Assessment di Cyber Sicurezza



ID	PARAMETRO	SCORE	PESO
ESPOSIZIONE ALLA MINACCIA (PROBABILITA')			
18	L'azienda ha sedi estere	4	
24	Fatturato dell'azienda	4	
30	Numero di dipendenti	4	
36	Settore/i di Riferimento	2	
65	Filiera/e produttive	1	
103	Canali web e social	4	
111	Stampanti e dispositivi removibili	5	
138	Servizi cloud e web	5	
210	Numero di incidenti registrati	3	
RILEVANZA DEGLI ASSET (IMPATTI)			
119	Dati confidenziali	4	
125	Dati personali	3	
131	Infrastruttura Server interna	4	
145	Infrastruttura Client/Ufficio	3	
151	Sviluppo Software	1	
156	Siti produttivi e OT	3	
218	Impatti registrati a seguito degli incidenti	3	
238	Continuità operativa IT/OT	3	
245	Servizi critici	1	



FATTORE DI RISCHIO (NORMALIZZAZIONE P*I)		LEGENDA PROFILO DI SICUREZZA E LIVELLO DI MATURITA'		
		MISURE MINIME DI SICUREZZA	PROFILO DI SICUREZZA INTERMEDIO	PROFILO DI SICUREZZA AVANZATO
MOLTO BASSO	1	INITIAL	MANAGED	MANAGED
BASSO	2	MANAGED	MANAGED	DEFINED
MEDIO	3	MANAGED	DEFINED	QUANTITATIVELY MANAGED
ALTO	4	DEFINED	DEFINED	QUANTITATIVELY MANAGED
CRITICO	5	DEFINED	QUANTITATIVELY MANAGED	OPTIMIZED

LIVELLI DI MATURITA'

FATTORE DI RISCHIO	4	ALTO
PROFILO DI SICUREZZA TARGET	MISURE MINIME DI SICUREZZA	
LIVELLO DI MATURITA' MINIMO RICHIESTO	DEFINED	

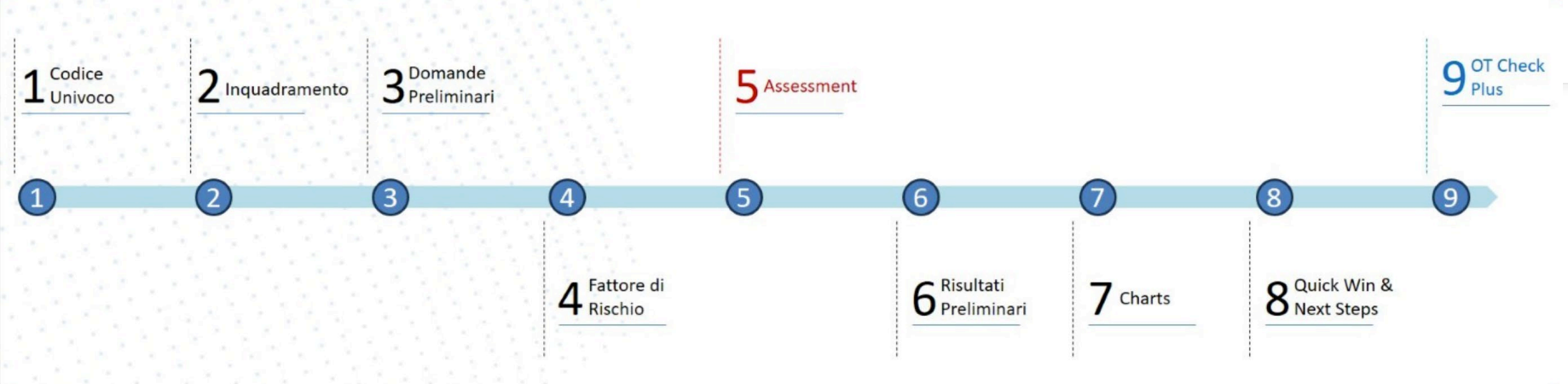
2. Raccolta di informazioni di inquadramento dell'azienda (ca. 1 ora di tempo dell'azienda, via webmeeting)

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 di profilo di rischio di Cyber Sicurezza dell'azienda (molto basso-basso-medio-alto-critico) contestualizzato allo specifico contesto di business dell'azienda.

Mettendo poi in relazione questo profilo di rischio con il livello di misure che l'azienda intende adottare in ottica Cyber (base-medio-avanzato), ne conseguirà il profilo di rischio «target»

MATURITY LEVEL	SCORE	TITLE	DESCRIPTION
INCOMPLETE	0	Ad hoc and unknown	Incomplete approach to meeting the intent of the Practice Area. May or may not be meeting the intent of any practice. Work may or may not get completed.
INITIAL	1	Unpredictable and reactive	Initial approach to meeting the intent of the Practice Area. Not a complete set of practices to meeting the full intent of the Practice Area Work gets completed but is often delayed and over budget.
MANAGED	2	Managed on the project level	Subsumes level 1 practices. Simple, but complete set of practices that address the full intent of the Practice Area. Does not require the use of the organizational assets. Projects are planned, performed, measured, and controlled.
DEFINED	3	Proactive, rather than reactive.	Builds on level 2 practices. Uses organizational standards and tailoring to address project and work characteristics. Projects use and contribute to organization assets. Organization-wide standards provide guidance across projects, programs, and portfolios.
QUANTITAVELY MANAGED	4	Measured and controlled	Organization is data-driven with quantitative performance improvement objectives that are predictable and align to meet the needs of internal and external stakeholders.
OPTIMIZED	5	Stable and flexible	Organization is focused on continuous improvement and is built to pivot and respond to opportunity and change. The organization's stability provides a platform for agility and innovation.

Assessment di Cyber Sicurezza



3. Assessment (ca. 3 ore, in presenza)

Durante questa fase (30 titoli/domande incrementali) vengono raccolte informazioni più dettagliate atte a definire la postura "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 "Quick Wins" e "Next Steps" che saranno contenuti nel report di restituzione

Assessment di Cyber Sicurezza

FNCS CATEGORY	Domanda	REQUISITI LIVELLO DI MATURITA' MINIMO	Traccia per il Mentor	RISPOSTE ASSESSOR (COMPILARE LE CELLE IN GIALLO)	MATURITY LEVEL
Asset Management	**Domanda 1 | Inventario hardware e software** È presente un inventario dei dispositivi hardware (HW) e software (SW) (anche gratuiti)? È mantenuto aggiornato, con appositi strumenti, quando nuovi dispositivi approvati vengono collegati in rete?	OBBLIGATORIO	Valutare l'esistenza, anche parziale di un inventario degli asset aziendali. Sono definiti asset: hardware, equipaggiamento fisico dell'azienda - computer, server, router o firewall software, programmi e applicativi che l'impresa utilizza per gestire le proprie attività dati, patrimonio informativo aziendale utenti, ovvero tutti i soggetti che possono interagire nella gestione delle risorse	Sì	
			Valutare se l'inventario esistente è aggiornato, occasionalmente o con periodicità definita. Per periodicità definita è da intendersi anche		
Information Protection Processes and Procedures	**Domanda 7| Backup & Disaster Recovery (DR)** Avete copie di backup che riguardino sistemi operativi, applicazioni software e dati? Quante copie conservate? Esistono sistemi o piani per le attività di Disaster Recovery?	OBBLIGATORIO	Verificare se sono effettuati i Backup (anche parziali)	Sì	
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se esiste una politica di gestione dei backup o una prassi consolidata	Sì	
Information Protection Processes and Procedures	**NOTE Domanda 7|**	OBBLIGATORIO	*Verificare se la politica di backup è stata formalizzata e se è resa disponibile ed è consultabile dai responsabili incaricati e/o dalla popolazione aziendale*	Parziale	
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se i backup periodici vengono effettuati automaticamente mediante un SW specifico	Sì	
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se i backup sono effettuati periodicamente (secondo schedulazioni predefinite)	Sì	
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se il SW utilizzato per la gestione dei backup restituisce un alert in caso di backup fallito	Parziale	
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se sono conservate almeno 2 copie di sicurezza dei backup	Sì	
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se esiste almeno una copia di backup in cloud remoto (datacenter proprietario o in outsourcing con distanza > 20 km dal sito primario) che comprenda almeno le informazioni critiche e che sia predisposta con parametri adatti a un ripristino dei sistemi in tempi utili al mantenimento della continuità operativa	Parziale	DEFINED
Information Protection Processes and Procedures		OBBLIGATORIO	Verificare se esistono almeno tre copie di backup (principale in sede, locale in un edificio separato e in cloud remotizzato)	Sì	
Information Protection Processes and Procedures	*Inserire nota (max 200 caratteri)*	OBBLIGATORIO	Le copie di backup sono protette mediante l'utilizzo di protocolli crittografici	No	

Elaborazione: Score delle domande

1 Visualizzazione della Function e della Category del FNCS associate alle domande.

2 Elenco delle domande.

3 I pesi associati alle dimensioni People, Process & Technology indicano il livello di impatto che le attività implicate dalla domanda possono avere su ogni singola dimensione. I pesi sono basati su una scala da 1 a 10 e sono stati associati a ciascuna domanda a partire da un'analisi della ISO 27002.

4 Livello e score di Maturità raggiunto dall'azienda per ogni domanda (basato sul punteggio delle tracce).

FUNCTION	CATEGORY	DOMANDA	PEOPLE	PROCESS	TECHNOLOGY	MATURITY LEVEL	MATURITY SCORE
IDENTIFY	Asset Management	**Domanda 1 | Inventario hardware e software** È presente un inventario dei dispositivi hardware (HW) e software (SW) (anche gratuiti)? È mantenuto aggiornato, con appositi strumenti, quando nuovi dispositivi approvati vengono collegati in rete?	5	8	7	INITIAL	1
IDENTIFY	Asset Management	**Domanda 2 | Servizi web** I servizi web (social network, cloud computing, posta eletronica, spazio web, ecc.) offerti da terze parti a cui si è registrati e le informazioni su essi condivise, sono quelli stretamente necessari? NOTA: (Da completare solo se risposta affermativa alla domanda 4 RISCHIO INERENTE)	6	7	6	INCOMPLETE	0
IDENTIFY	Asset Management	**Domanda 3 | Gestione informazioni** Sono individuati e classificati le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti?	4	8	8	INCOMPLETE	0
IDENTIFY	Asset Management	**Domanda 4 | Responsabile monitoraggio normative** Avete un responsabile che si occupi di monitoraggio delle normative, aggiorni le policies di sicurezza e le distribuisca all'interno dell'organizzazione?	8	8	3	INCOMPLETE	0
PROTECT	Information Protection Processes and Procedures	**Domanda 5 | Utilizzo e ciclo di vita degli asset** Esistono regolamenti per l'utilizzo degli asset da parte dei dipendenti e per la loro gestione durante il loro intero ciclo di vita (consegna, gestione dell'obsolescenza, riconsegna, sanificazione e dismissione)?	5	8	8	INCOMPLETE	0

Elaborazione: Score delle categories

1 Visualizzazione della Function e della Category del FNCS associate alle domande.

3 I pesi associati alle dimensioni People, Process & Technology in questo caso riportano la media ponderata dei risultati di ogni Category sulla base delle domande che la compongono.

4 Il livello di maturità associato alle category è caclolato come media ponderata dei livelli delle domande che la compongono utilizzando come pesi le dimensioni PPT.

FUNCTION	CATEGORY	PEOPLE	PROCESS	TECHNOLOGY	AVERAGE OVERALL SCORE	MATURITY LEVEL
IDENTIFY	Asset Management	0,3	0,3	0,4	0	INCOMPLETE
PROTECT	Information Protection Processes and Procedures	0,1	0,1	0,1	0	INCOMPLETE
IDENTIFY	Governance	0,1	0,1	0,1	0	INCOMPLETE
IDENTIFY	Risk Management Strategy	0,1	0,1	0,1	0	INCOMPLETE

Elaborazione: Score Functions & Overall Score

TARGET MATURITY LEVEL	MANAGED	2
DETECTED MATURITY LEVEL	INCOMPLETE	0

FUNCTION	PEOPLE	PROCESS	TECHNOLOGY	AVERAGE OVERALL SCORE	MATURITY LEVEL
IDENTIFY	0,132608696	0,138709677	0,14375	0	INCOMPLETE
PROTECT	0,1	0,1	0,1	0	INCOMPLETE
DETECT	0,1	0,1	0,1	0	INCOMPLETE
RESPOND & RECOVER	0,1	0,1	0,1	0	INCOMPLETE

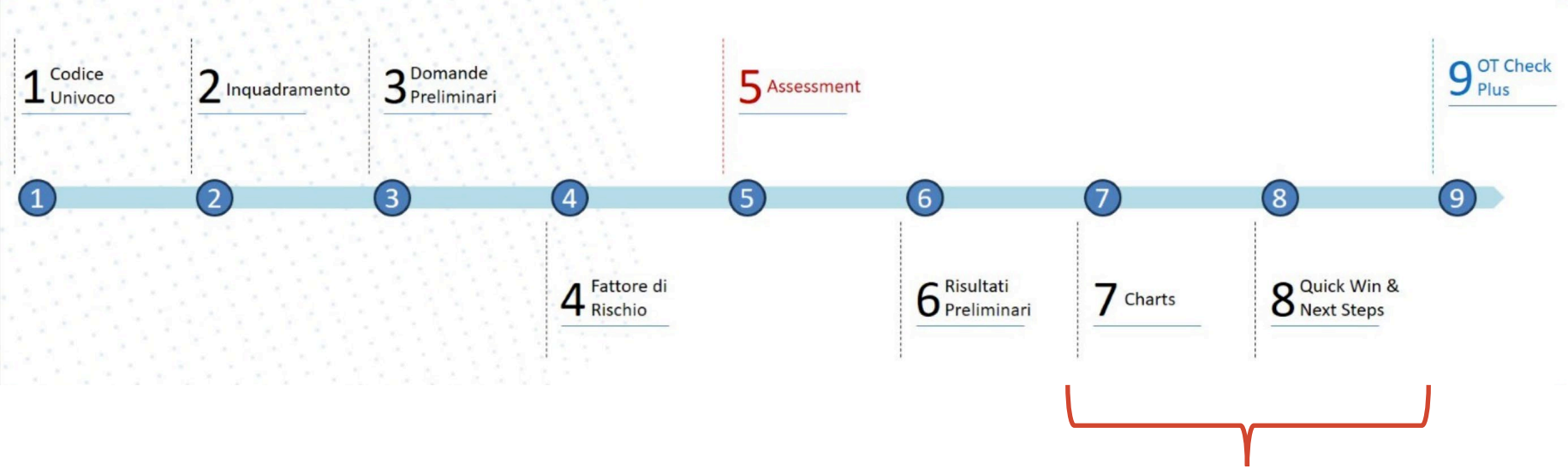
1 La terza tabella mostra i risultati medi complessivi raggiunti dall'azienda in relazione al livello di maturità desiderato. Il livello di maturità desiderato rappresenta l'obiettivo che deve essere raggiunto su ciascuna domanda.

2 La quarta tabella mostra i valori medi relativi al punteggio di maturità associato ad ogni Function del FNCS. I risultati sono ottenuti effettuando il calcolo della media dei valori associati ad ogni category che compone una Function.

Il report di restituzione

Industria 4.0
Veneto

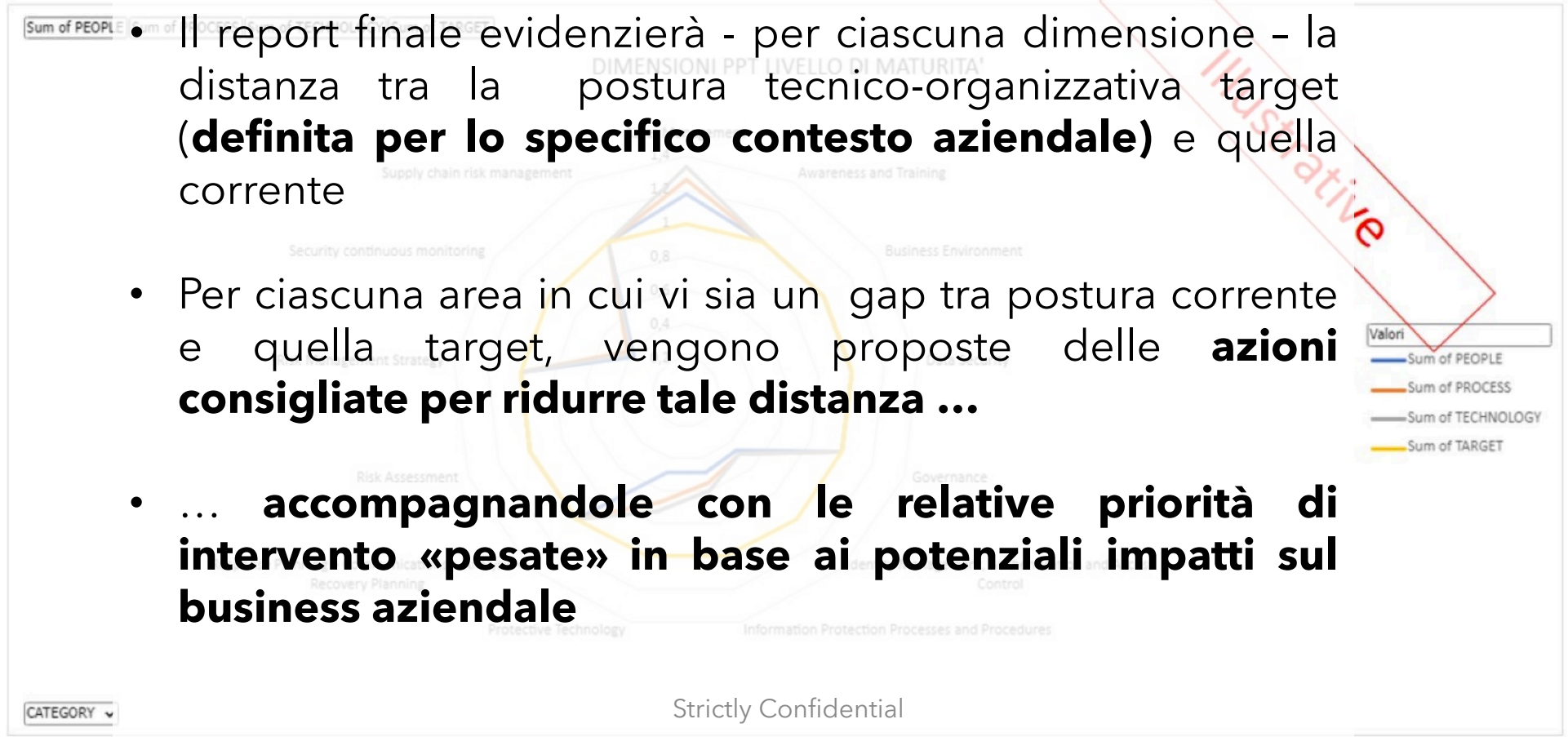
Assessment di Cyber Sicurezza



4. 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 – qualora fosse necessario - la gestione della sicurezza, sia dal di vista dei processi aziendali impattati, sia da quello tecnologico, nonchè per definire la priorità per le eventuali azioni di rimedio.

Il reporto di restituzione



- Il report finale evidenzierà - per ciascuna dimensione – la distanza tra la postura tecnico-organizzativa target (**definita per lo specifico contesto aziendale)** e quella corrente

- 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 priorità di intervento «pesate» in base ai potenziali impatti sul business aziendale**

Il reporto di restituzione

ID	CATEGORY	QUICK WIN
1	Asset Management	Si suggerisce di assicurare che i servizi web e cloud utilizzati siano funzionali esclusivamente all'attività lavorativa.

TABELLA QUICK WIN

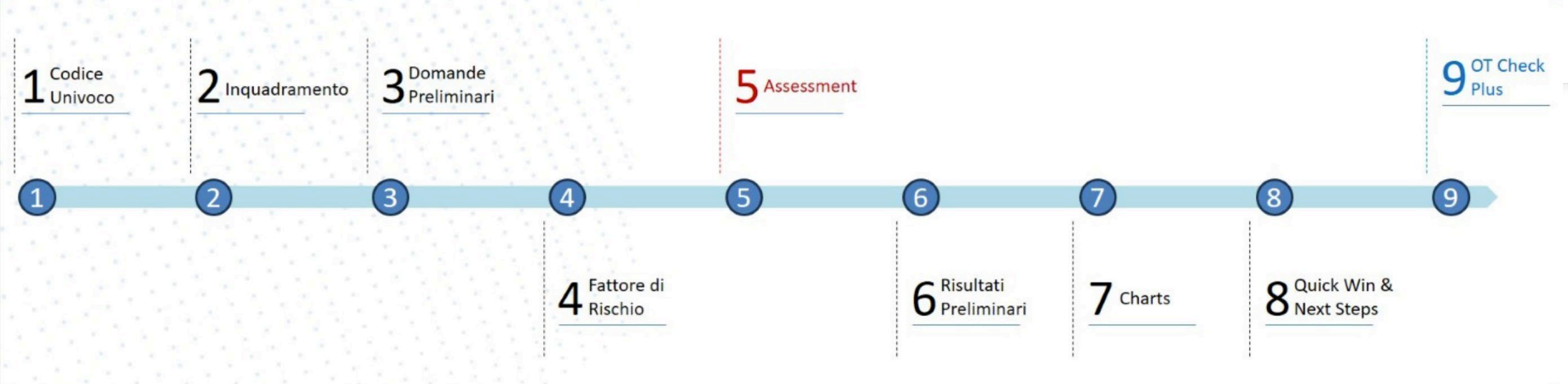
La prima tabella visualizza in ordine casuale, non prioritizzato, i consigli utili per raggiungere il livello di maturità desiderato.

ID	CETEGORY	NEXT STEPS
1	Asset Management	Si raccomanda di identificare hardware e software critici la cui compromissione può compromettere l'attività aziendale.
2	Asset Management	Si suggerisce di effettuare una mappatura o inventario, anche parziale, dei dati archiviati (ad esempio, mappatura delle cartelle di rete/SharePoint)
3	Asset Management	Si suggerisce di designare un referente, interno o esterno, responsabile della compliance normativa e delle politiche interne in ambito cybersecurity e/o privacy.

TABELLA NEXT STEPS

La seconda tabella visualizza in ordine casuale, non prioritizzato, i consigli relativi alle misure che potranno essere implementate in futuro per incrementare il livello di maturità dell'azienda oltre a quello desiderato.

Assessment di Cyber Sicurezza - recap



L'assessment si costituisce di 4 fasi:

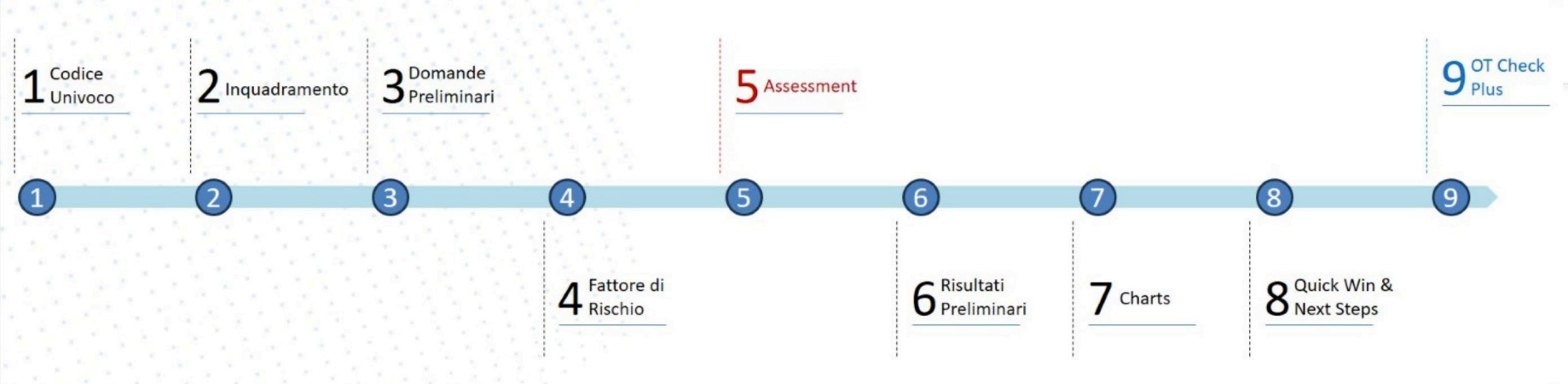
1. Adesione da parte dell'azienda e firma dei documenti di NDA
2. Raccolta di informazioni di inquadramento dell'azienda (ca. 1 ora di tempo dell'azienda, via webmeeting)
3. Assessment (ca. 3 ore, in presenza)
4. La consegna in azienda dei risultati dell'assessment (ca. 2 ore di tempo, in presenza)

5. (opzionale) OT Assessment Check Plus

Assessment OT (Operational Technologies) e Industrial IoT

Industria 4.0
Veneto

Assessment di Cyber Sicurezza



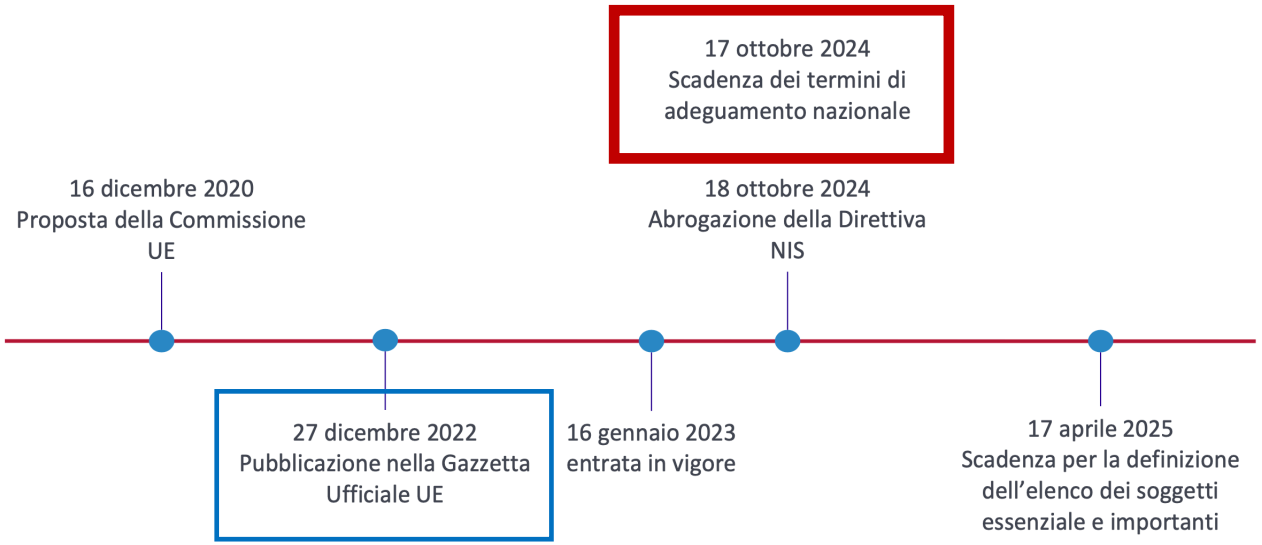
5. (opzionale) OT assessment di Cyber sicurezza

- 34 titoli/domande incrementali
- È consigliabile farlo assieme all'assessment di Cyber sicurezza
- richiede all'azienda un tempo aggiuntivo di ca. 2 ore per lo svolgimento dell'assessement specifico e ca. 1 ora per la presentazione dei risultati specifici

La direttiva NIS2

Industria 4.0
Veneto

NIS2 – La direttiva EU



- ❑ Migliorare il livello di **consapevolezza del rischio** nelle organizzazioni e nelle aziende
- ❑ Aumentare il livello di **resilienza** delle organizzazioni e delle aziende
- ❑ Estendere lo **scope** della precedente normativa NIS, sia dal punto di vista dei settori impattati che da quello delle dimensioni delle aziende
- ❑ Stabilire **chiare responsabilità e sanzioni**

NB: la direttiva stabilisce un riferimento normativo **minimo,** ciascun paese dovrà recepirla entro la scadenza prefissata ma potrà anche inserire requisiti più restrittivi e/o estenderne lo scope (es. Germania)

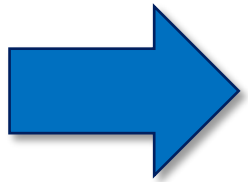
NIS2: cosa richiede

Policy: adozione di un insieme di policies di information system e analisi del rischio

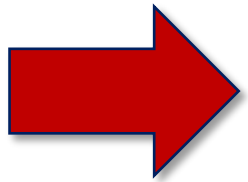
Gestione degli incidenti Cyber: obblighi di segnalazione predefiniti (e stringenti)

Adozione di misure di **business continuity, disaster recovery** e gestione della crisi

Adozione di **maggiori misure tecniche di sicurezza** quali ad es. crittografia e autentificazione a più fattori



Svolgimento di **audit** e **test** di Cyber sicurezza

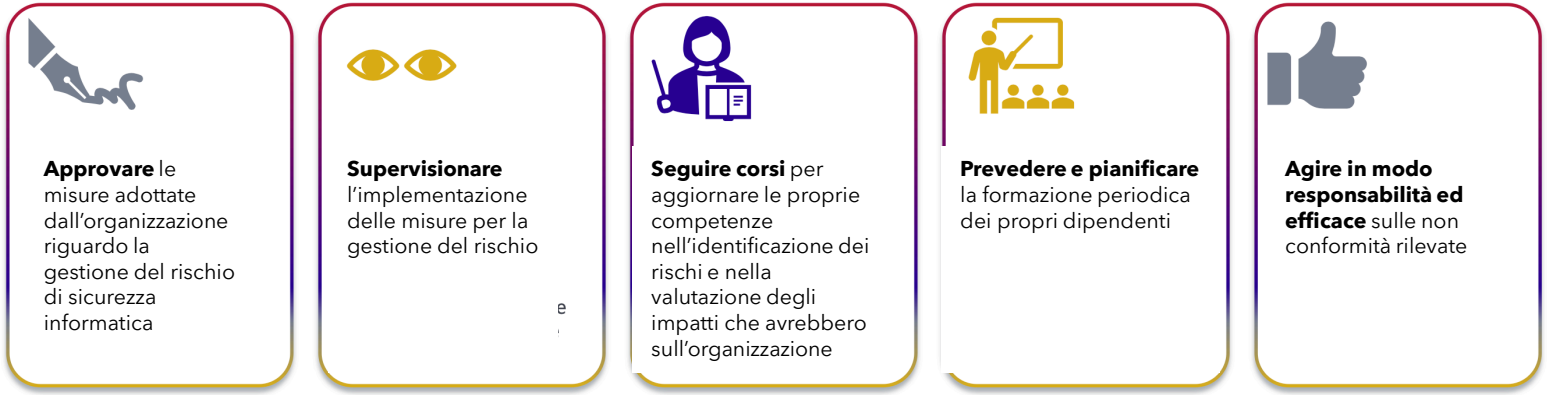


Gli obblighi di Cyber sicurezza **devono coinvolgere tutta la Supply Chain !**

NIS2: Responsabilità del Top Management

Caratteristiche salienti della normativa:

- **Analisi e Gestione del Rischio** (sulla linea del GDPR)
- **Responsabilità diretta del Top Management** (CdA)
- **Obbligo di segnalazione degli incidenti**
- **Vigilanza diretta e ispezioni dagli organi di controllo**
- **Sanzioni per non conformità**



NIS2: classificazione delle organizzazioni

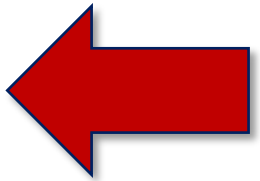
Per differenziare il livello di supervisione ed il regime sanzionatorio delle organizzazioni vigilate

- **ENTITA' GRANDI** *(Large Entities)* : **>= 250** dipendenti **o >= 50 M Euro** Fatturato
- **ENTITA' MEDIE** *(Medium Entities)* : **50 - 249** dipendenti **o 10 - 49 M Euro** Fatturato
- **ENTITA' PICCOLE** *(Small & Micro Entities)* : **< 49** dipendenti **e <10 M Euro** Fatturato

- **ESSENZIALI** *(Essential)* : **Supervisione continua – Sanzioni** 10 MEuro / 2% Fatturato globale
- **IMPORTANTI** *(Important)* : **Supervisione a campione / in caso di incidenti – Sanzioni** 7 M Euro / 1,4% Fatturato globale
- **ESCLUSE** *(Not in scope)* : **Nessuna supervisione**

NIS2: settori impattati

- Fabbricazione di dispositivi medici e medico-diagnostici in vitro,
- Fabbricazione di computer e prodotti di elettronica e ottica,
- Fabbricazione di apparecchiature elettriche,
- Fabbricazione di macchinari e apparecchiature n.c.a. (*Non Classificate Altrove),*
- *Fabbricazione* di autoveicoli, rimorchi e semirimorchi,
- Fabbricazione di altri mezzi di trasporto



Settori **critici:**

12. Servizi postali e di corriere
13. Gestione dei rifiuti
14. Fabbricazione, produzione e distribuzione di sostanze chimiche
15. Produzione, trasformazione e distribuzione di alimenti
16. Fabbricazione (di disp. medici, computer, prodotti di elettronica e ottica, apparecchiature elettriche, macchinari e apparecchiature n.c.a., autoveicoli, rimorchi, semirimorchi e altri mezzi di trasporto)
17. Fornitori di servizi digitali
18. Ricerca

e Comunicazione)

10. Pubblica Amministrazione centrale e regionale
11. Spazio

NIS2: soggetti impattati – settori ad alta criticità

		Grandi imprese	Medie imprese (*)	Piccole e micro imprese
ENERGIA	Energia elettrica, teleriscaldamento e teleraffreddamento, petrolio, gas, idrogeno	Essenziale	Importante	Non applicabile
TRASPORTO	Trasporto aereo, ferroviario, per vie d'acqua, su strada	Essenziale	Importante	Non applicabile
	Trasporto pubblico: **solo** se indicato dalla CER	Essenziale	Importante	Non applicabile
BANCARIO	Istituti di credito (attenzione al regolamento DORA)	Essenziale	Importante	Non applicabile
MERCATI FINANZIARI	Sedi di negoziazione, controparti centrali(attenzione al regolamento DORA)	Essenziale	Importante	Non applicabile

(*) Media Impresa = occupa da 50 a 250 persone e realizza un fatturato annuo che non supera I 50 M€

NIS: soggetti impattati – settori critici

	Grandi imprese	(*) Medie imprese	Piccole e micro imprese
SERVIZI POSTALI E DI CORRIERE	Importante	Importante	Non applicabile
GESTIONE DEI RIFIUTI	Importante	Importante	Non applicabile
Solo se attività principale			
SOSTANZE CHIMICHE			
Fabbricazione, produzione e distribuzione	Importante	Importante	Non applicabile
ALIMENTARE			
Produzione, trasformazione e distribuzione	Importante	Importante	Non applicabile

(*) Media Impresa = occupa da 50 a 250 persone e realizza un fatturato annuo che non supera I 50 M€

NIS: soggetti impattati – settori critici

		Grandi imprese	(*) Medie imprese	Piccole e micro imprese
FABBRICAZIONE	Dispositivi medico-diagnostici in vitro, elettronici, ottici, computer, apparecchiature elettriche, macchinari, mezzi di trasporto	Importante	Importante	Non applicabile
FORNITORI DI SERVIZI DIGITALI	Mercati online, motori di ricerca, piattaforme di social network	Importante	Importante	Non applicabile
RICERCA	Organizzazioni di ricerca	Importante	Importante	Non applicabile

(*) Media Impresa = occupa da 50 a 250 persone e realizza un fatturato annuo che non supera I 50 M€

NIS2: come possiamo aiutare

1. Identificare, valutare e mitigare i rischi di Cyber sicurezza dell'azienda
2. Valutare la postura di sicurezza (assessment di Cyber sicurezza)
3. Rafforzare le difese organizzative e tecnologiche dell'azienda
4. Formare il personale dell'azienda creando consapevolezza riguardo la Cyber sicurezza
5. Formalizzare un piano di risposta agli incidenti Cyber
6. Monitorare la Supply Chain

Contatti

Massimo Colorio

dih-veneto@siav.net

www.siav.net