ITHUM
it's for human

Approved by
academy ict

GIOVEDÌ 20 FEBBRAIO 2025 - ORE 17:00

Intelligenza Artificiale NIS2 e buone pratiche UNI

Con la partecipazione tecnica di

Maurizio GENNA
ICT Product Manager

Valentina MUSSI
National Market Leader - Cybersecurity & Digital

BUREAU VERITAS 1828
BUREAU VERITAS

Agenda:

- **17:00** Presentazione
- **17:10** Speech *Ciclo di vita per Intelligenza Artificiale – ISO 42001*
- **17:30** Speech *Considerazioni AI rispetto a NIS2 e buone prassi UNI*
- **17.50** Feedback / Prossime iniziative
- **18:00** Dibattito - Q&A
- **18:15 (circa)** Saluti

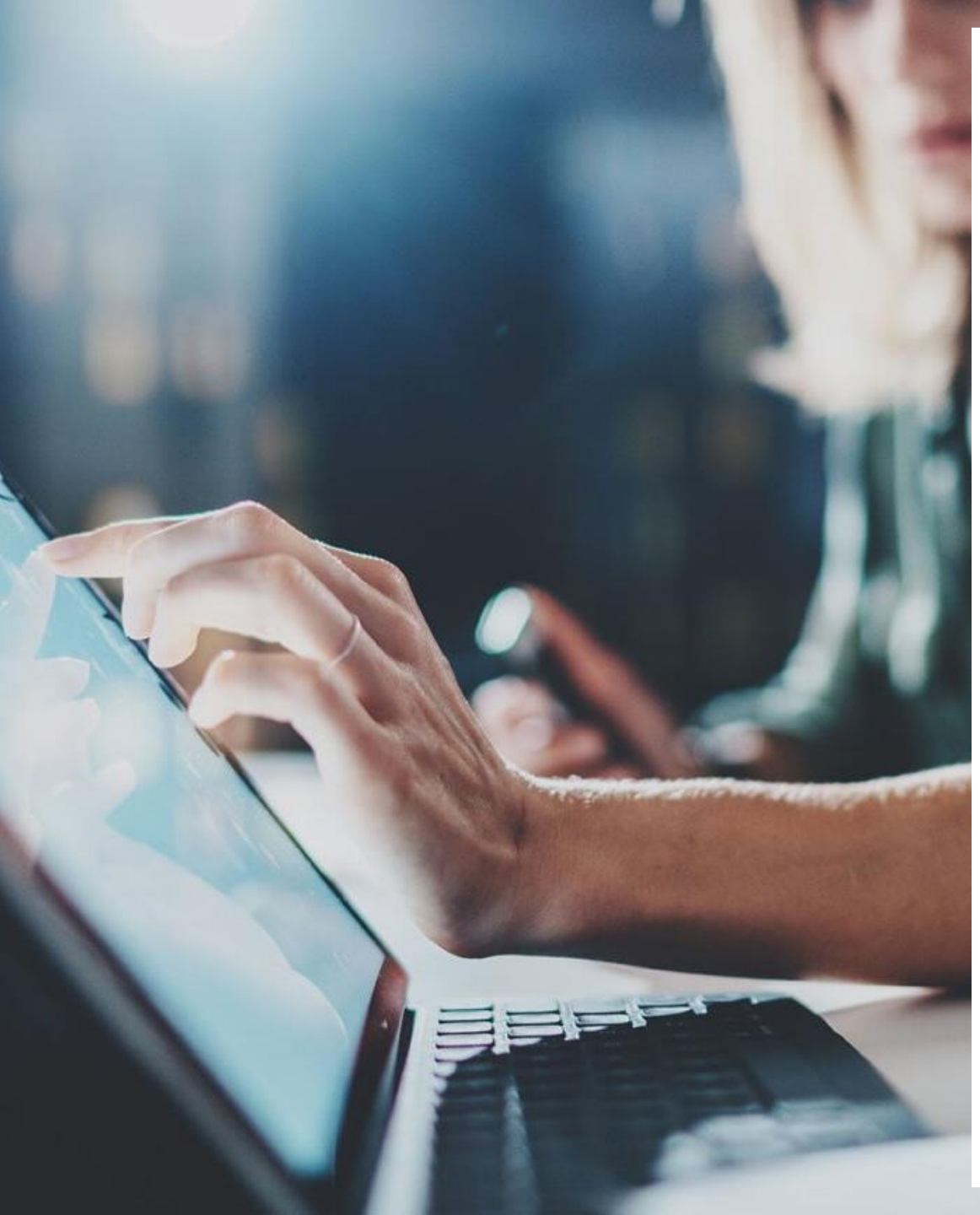
Relatori:

Maurizio GENNA - **ICT Product Manager** – LinkedIn

Valentina MUSSI – **National Market Leader - Cybersecurity & Digital** LinkedIn

Presenta e Modera: Marco CIAMPI – LinkedIn

Evento LinkedIn



SISTEMA DI GESTIONE DELL'INTELLIGENZA ARTIFICIALE ISO/IEC 42001:2023

20 FEBBRAIO 2025

INTERVENGONO

Maurizio GENNA

› ICT Product Manager

Valentina MUSSI

› National Market Leader - Cybersecurity & Digital

BUREAU VERITAS NEL MONDO

€5.9

miliardi

FATTURATO 2023

83.000

dipendenti*

400.000

clienti

~1.600

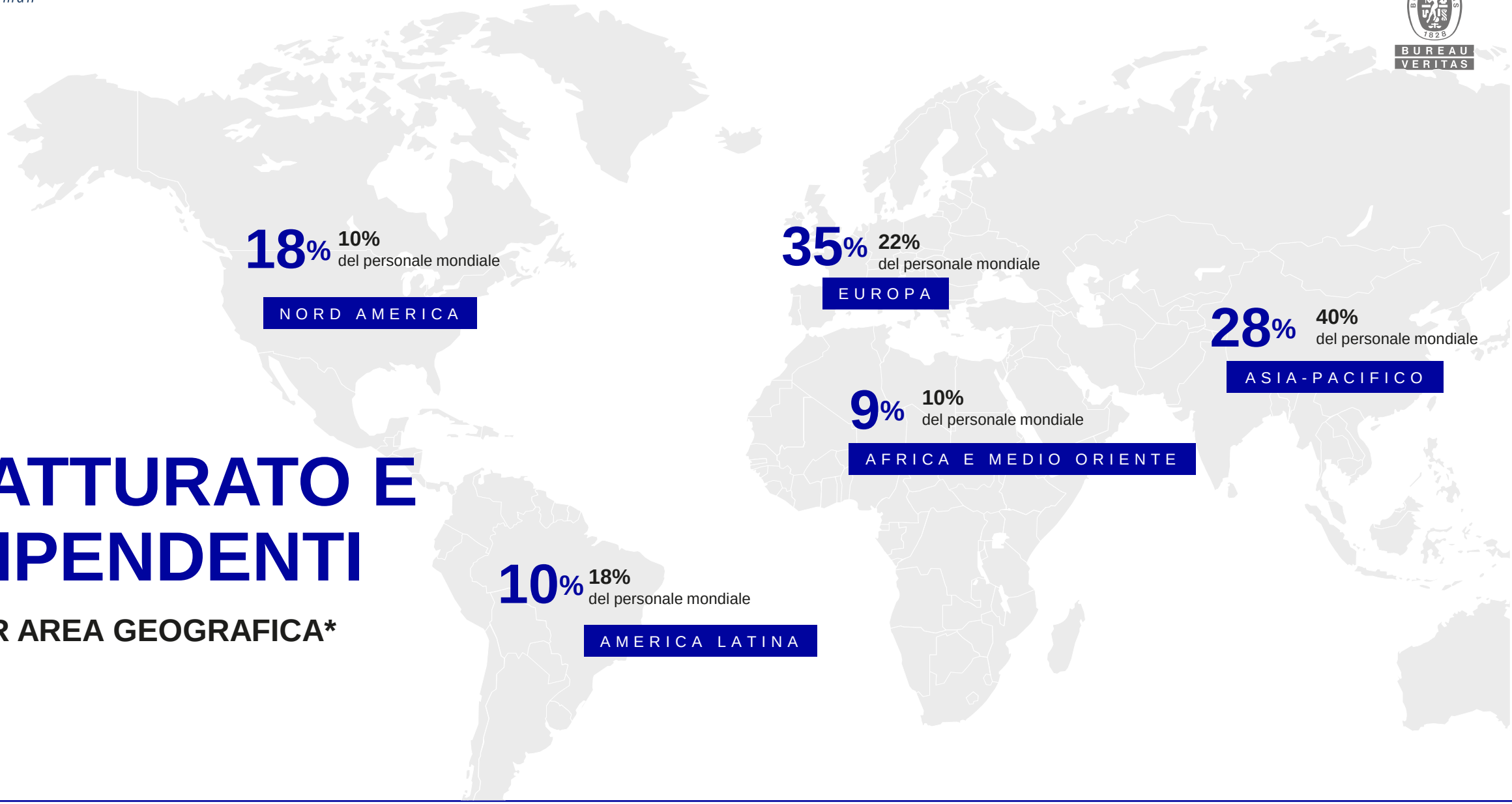
uffici e laboratori

IN 140 PAESI

* Al 31 Dicembre 2023

FATTURATO E DIPENDENTI

PER AREA GEOGRAFICA*



18% 10% del personale mondiale

NORD AMERICA

35% 22% del personale mondiale

EUROPA

28% 40% del personale mondiale

ASIA-PACIFICO

9% 10% del personale mondiale

AFRICA E MEDIO ORIENTE

10% 18% del personale mondiale

AMERICA LATINA

* Al 31 Dicembre 2023

BUREAU VERITAS IN ITALIA

PRESENTE DAL 1839

VALORE DELLA PRODUZIONE

€ 182
milioni

UFFICI

21

DIPENDENTI

~ 1.000

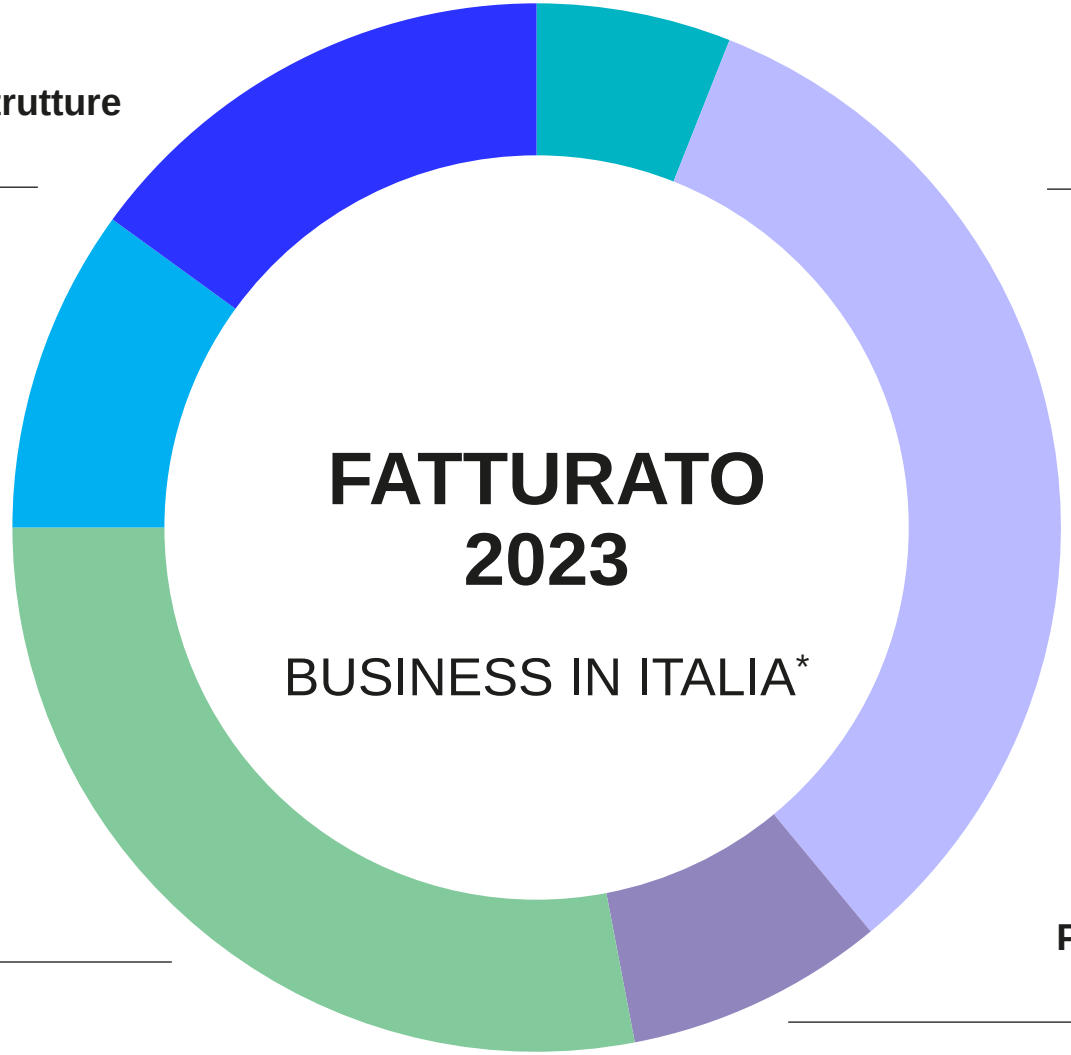
TECNICI E VALUTATORI

~ 900

CLIENTI

20.000

* Al 31 dicembre 2023



15% Edilizia e infastrutture

10% Marine & Offshore

28% Certificazione

Agroalimentare e materie prime **6%**

Industria **33%**

Prodotti di consumo **8%**

* Al 31 dicembre 2023
Le percentuali si riferiscono al valore del fatturato dell'attività di core business

00

Introduzione

DEFINIZIONE DI AI:

Non esiste una definizione unica di AI

L'Intelligenza Artificiale (AI) è il campo della scienza informatica che si occupa di creare computer o sistemi software in grado di compiere compiti che altrimenti richiederebbero l'intelligenza umana.

Questi compiti possono includere il riconoscimento di immagini, la comprensione del linguaggio, la risoluzione di problemi e la presa di decisioni. In sostanza, l'AI cerca di far svolgere ai computer attività intelligenti simili a quelle svolte dagli esseri umani.

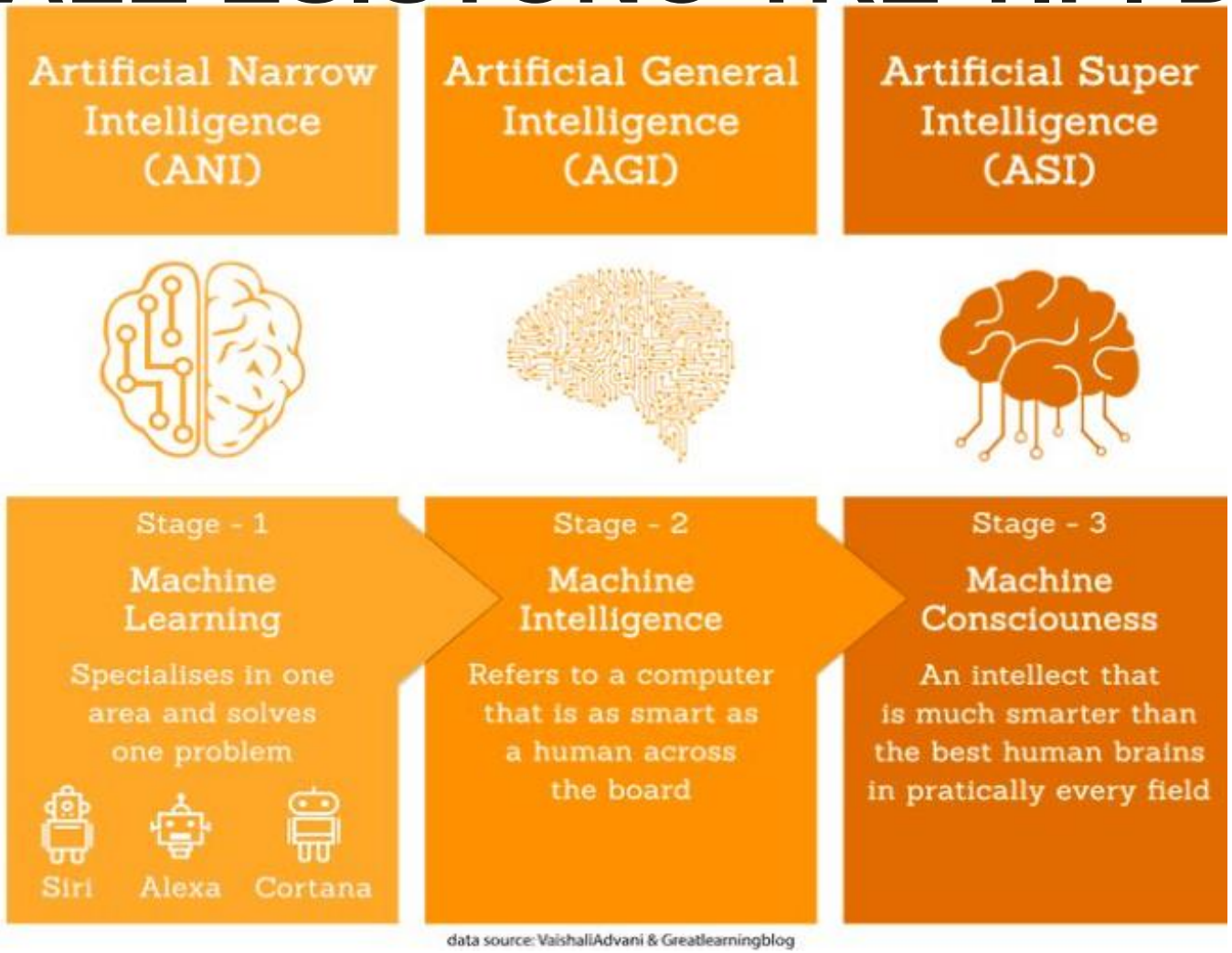
DIFFERENZA TRA I TERMINI AI E MACHINE LEARNING

Non esiste una definizione unica di AI

- AI (Intelligenza Artificiale) è un termine generale che si riferisce a tutte le tecnologie che permettono a una macchina di simulare il comportamento umano intelligente, come prendere decisioni, riconoscere immagini, comprendere il linguaggio e altro.

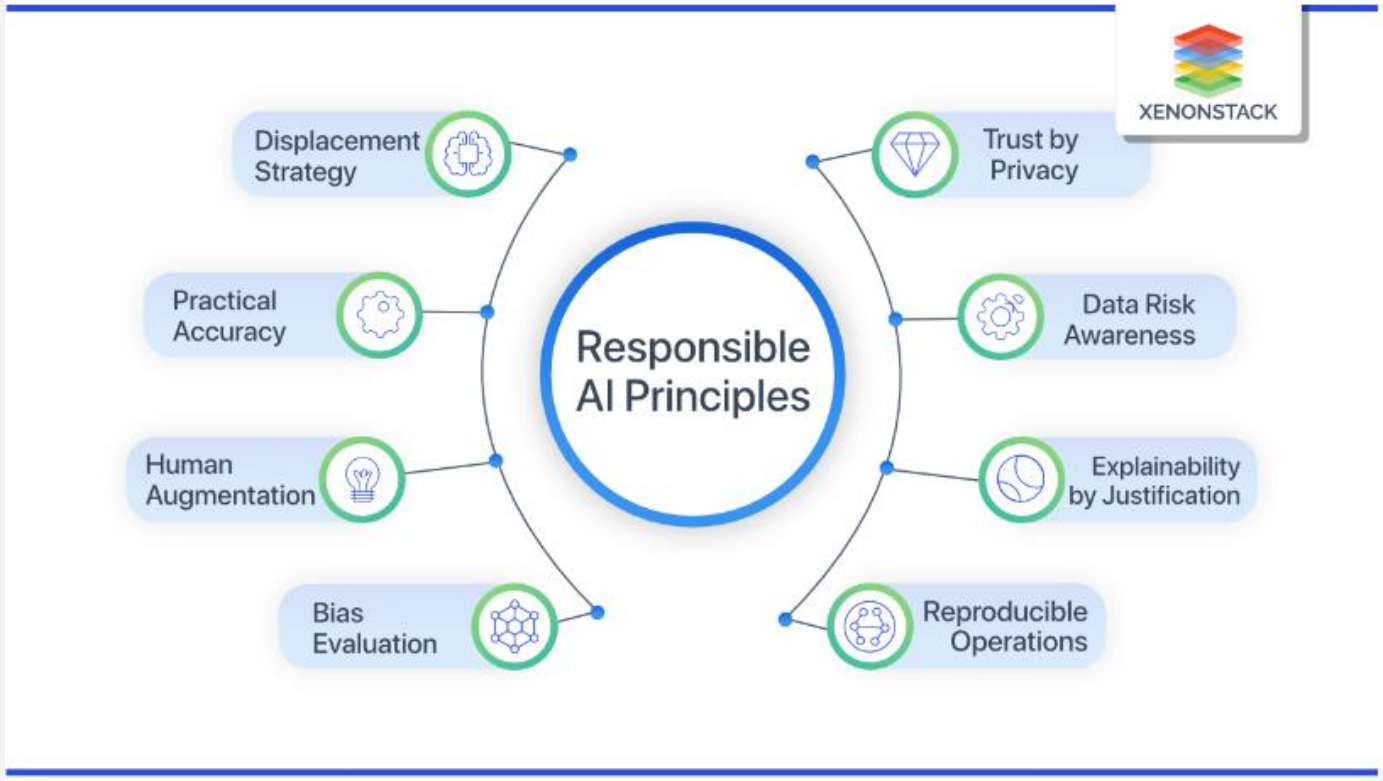
- ML (Machine Learning) è una parte dell'AI che si concentra su algoritmi e modelli matematici che permettono alle macchine di "imparare" dai dati e migliorare nel tempo, senza essere programmate esplicitamente per ogni compito.

IN GENERALE ESISTONO TRE TIPI DI AI:



I PRINCIPI DELL'AI:

- Dignita e supervisione umana;
- Robustezza e sicurezza;
- Privacy e governance dei dati;
- Trasparenza;
- Diversità, non discriminazione ed equità;
- Benessere sociale e ambientale;
- Accountability



01

Sfide e Opportunità Implementazione Norma ISO 42001

LA NORMA ISO 42001

Alcune caratteristiche dell'IA, come la sua capacità di apprendere e migliorare in modo continuo, oppure la sua mancanza di trasparenza e spiegabilità, possono sollevare preoccupazioni aggiuntive rispetto ai metodi tradizionali di svolgimento dei compiti. In questi casi, potrebbero essere necessarie garanzie supplementari per garantire un utilizzo responsabile e sicuro della tecnologia.

L'adozione di un sistema di gestione dell'IA per estendere le strutture gestionali esistenti non è solo una mossa operativa, ma anche una decisione strategica per un'organizzazione. Tale passo richiede un'analisi approfondita delle implicazioni, comprese le sfide e le opportunità che l'IA porta con sé. È fondamentale per le organizzazioni comprendere come integrare efficacemente l'IA nel loro contesto operativo, assicurandosi che sia implementata in modo etico, sicuro e trasparente.

LA NORMA ISO 42001

Il sistema di gestione dell'IA dovrebbe essere integrato con i flussi operativi dell'azienda e la struttura manageriale complessiva. Le tematiche specifiche relative all'IA devono essere considerate durante la progettazione dei processi, dei sistemi informativi e dei meccanismi di controllo. Esempi essenziali di tali processi gestionali includono:

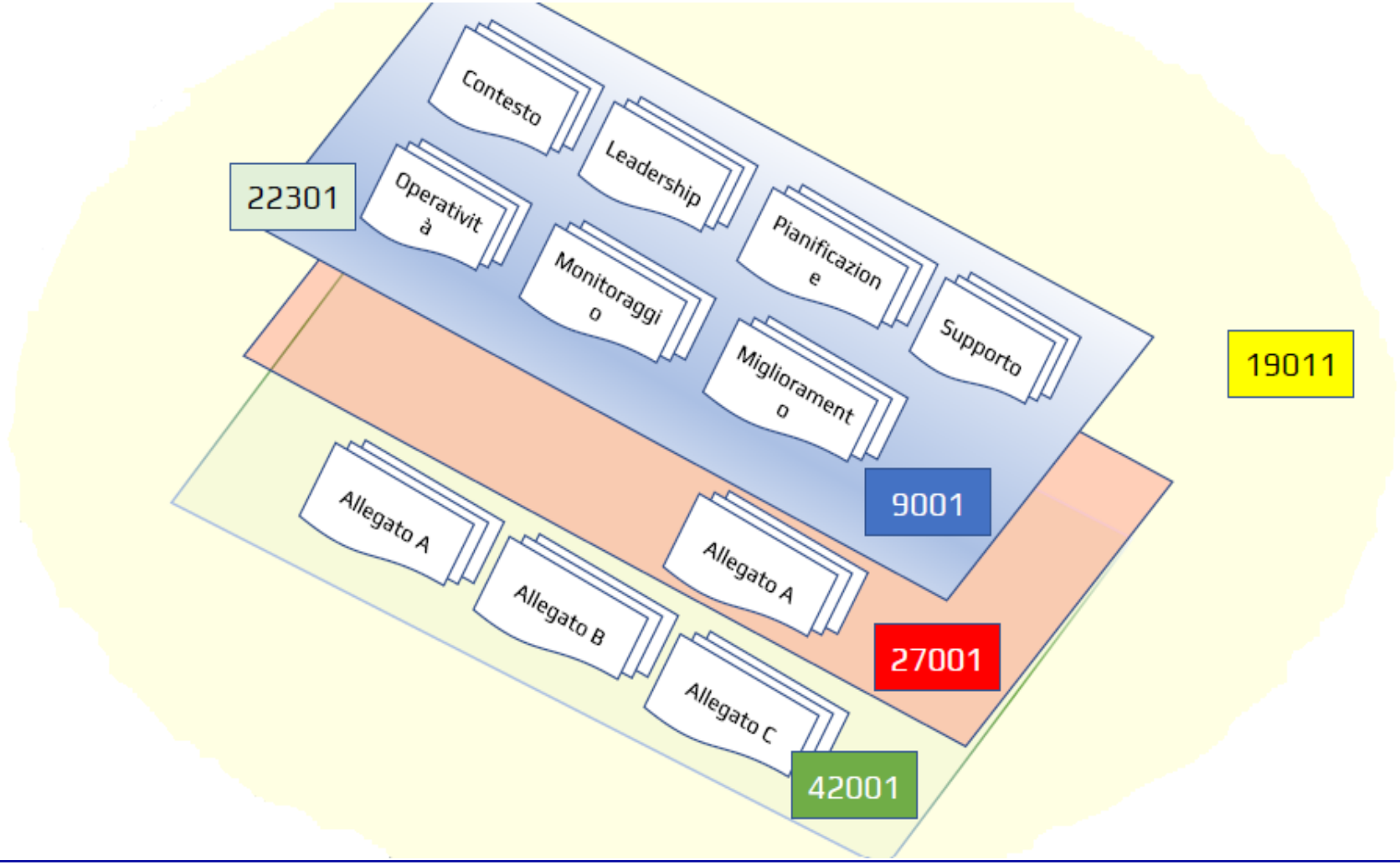
definizione degli obiettivi aziendali, coinvolgimento delle parti interessate e formulazione della politica organizzativa;

gestione dei rischi e delle opportunità;

procedure per gestire le problematiche legate all'affidabilità dei sistemi di intelligenza artificiale, come sicurezza, equità, trasparenza e qualità dei dati, lungo tutto il loro ciclo di vita;

modalità di gestione dei fornitori, dei partner e delle terze parti che forniscono o sviluppano sistemi di IA per l'organizzazione.

LA NORMA ISO 42001



LA NORMA ISO 42001

STANDARD ISO 42001

Lo standard ISO/IEC 41001:2022 Information technology - Artificial intelligence - Management system definisce i requisiti per pianificare, attuare, verificare e migliorare un sistema di gestione per l'Intelligenza Artificiale.

INTERNAZIONALITA’

Lo standard IS0 42001 è uno standard volontario riconosciuto a livello mondiale.

APPLICABILITA'

Lo standard ISO 42001 si applica a tutte le realtà di ogni natura (pubblico e privato), tipologia e dimensione.

LA NORMA ISO 42001

CERTIFICABILITA’

I sistemi di gestione per la sicurezza delle informazioni sviluppati in conformità allo standard ISO 42001 sono certificabili da un ente terzo (organismo di certificazione) accreditato.

Non è ancora uscita la Circolare Accredia perchè attendevano la pubblicazione della ISO 42006.

LA NORMA ISO 42001

Corpo principale della Norma punti 4-10 HLS e.....

ALLEGATO A Tabella requisiti come Annex A ISO 27001 dove è speicifcato che “Not all the control

objectives and controls listed in Table 4.1 are required to be used, and the organization can design and implement their own controls ”

ALLEGATO B Guida per l’implementazioen dei controlli AI anche a livello di integrazione con altri Sistemi di Gestione.

ALLEGATO C Principali obiettivi e fattori di analisi dei rischi da tenere in considerazione in ambito per AI (potential organizational objectives, risk sources and descriptions that can be considered by the organization when managing risks).

ALLEGATO D Settori principali e più critici dove applicata AI (Use of the AI management system across domains or sectors)

SFIDE NELLA GESTIONE RESPONSABILE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE

1. Valutazione degli impatti dei sistemi di IA (A.5.1 - A.5.6): Valutare e documentare gli impatti dei sistemi di IA su individui, gruppi, e sulla società nel suo complesso è una sfida complessa. Potrebbe essere difficile prevedere tutti i possibili impatti e garantire che le valutazioni siano esaustive e accurate.

2. Processi per lo sviluppo responsabile della progettazione di sistemi di IA (A.6.1.2): Definire e implementare processi per lo sviluppo responsabile dei sistemi di IA richiede una comprensione approfondita delle implicazioni etiche, sociali e legali dell'IA. Potrebbe essere difficile integrare adeguatamente questi processi in tutte le fasi del ciclo di vita dello sviluppo.

3. Verifica e convalida del sistema IA (A.6.2.3): La verifica e la convalida dei sistemi di IA possono essere complesse a causa della natura dinamica e non deterministica dell'IA. Potrebbe essere difficile stabilire criteri definiti per la verifica e la convalida e garantire che siano soddisfatti in modo adeguato.

SFIDE NELLA GESTIONE RESPONSABILE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE

4. Funzionamento e monitoraggio del sistema IA (A.6.2.5): Mantenere il funzionamento e il monitoraggio continuo dei sistemi di IA può essere impegnativo, specialmente considerando la necessità di aggiornamenti regolari, riparazioni e gestione delle prestazioni nel tempo.

Risolvere queste sfide richiederà un impegno significativo da parte delle organizzazioni nell'implementare processi solidi per gestire responsabilmente i sistemi di IA.

CATEGORIE DI AZIENDE COINVOLTE NELLA ISO 42001 (DA ISO 42006)

- AI PRODUCER
- AI DEVELOPER E PROVIDER
- AI USER
- MULTIPLE ROLES

CATEGORIE DI AZIENDE COINVOLTE NELLA ISO 42001 (DA ISO 42006)

Fattori di incremento

- Sensitive context of AI system(s)
- Non-sensitive context of AI system(s)
- Data complexity with reference to the managed AI system(s)
- Risk assessment with reference to the managed AI system(s)
- more than one legal framework to manage
- Number of outsourced services used in the scope of the AIMS
- AIMS running in more than one company location
- Number of Disaster Recovery Sites
- Diversity of technology
- Number of all documented controls needed to satisfy ISO/IEC 42001 requirements

AMBITO DELLA CERTIFICAZIONE ISO 42001 PER I PRODOTTI DI AI

Ambito della certificazione: La norma ISO 42001 definisce un sistema di gestione che governa i processi e i prodotti di intelligenza artificiale controllati dall'azienda.

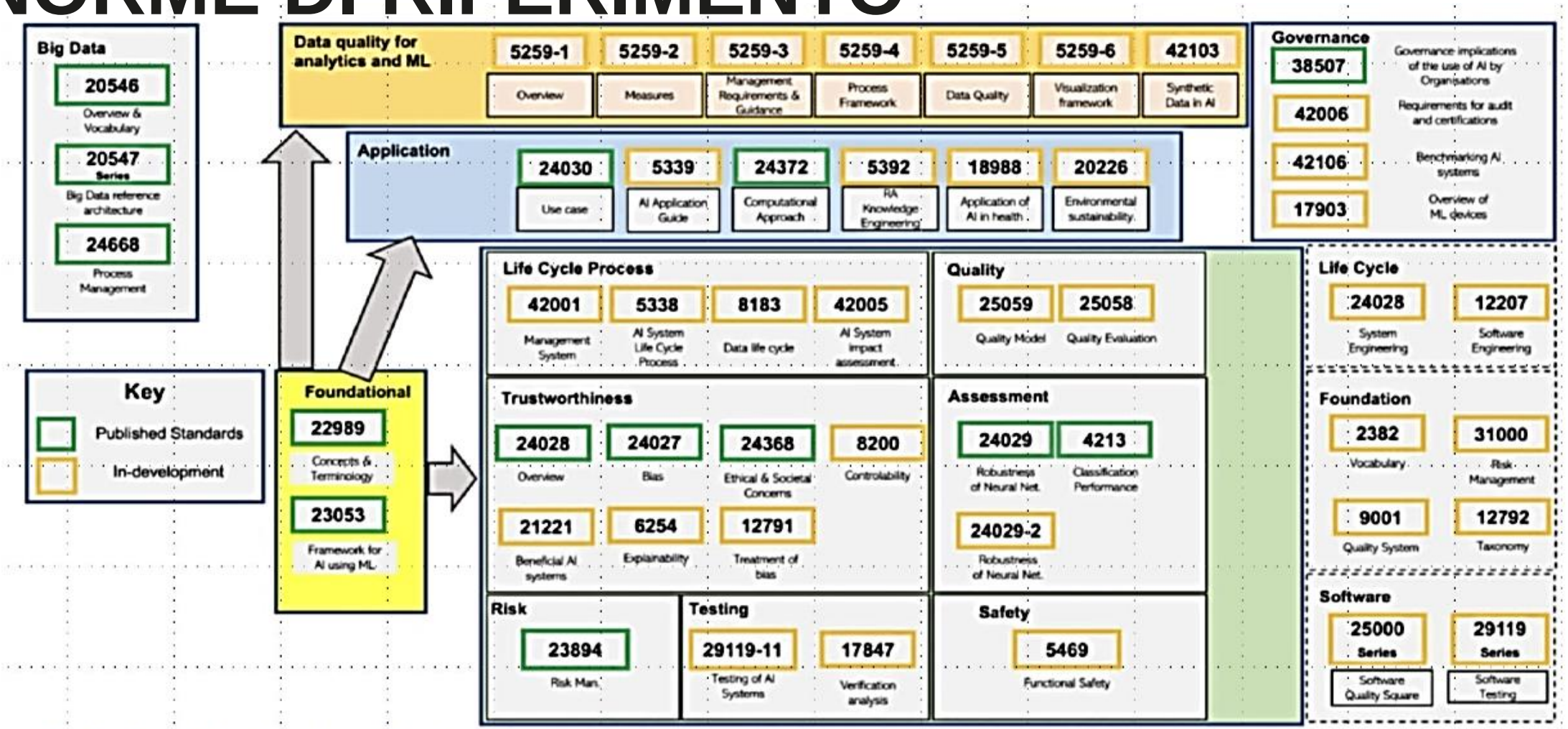
Esclusione dei servizi esterni: Non è possibile certificare come "prodotto AI" i servizi che utilizzano terze parti, come OpenAI, se i dati sono elaborati su server esterni e non controllabili direttamente dall'azienda.

Controllo sui dati: La certificazione è valida solo per prodotti di IA dove l'azienda mantiene il controllo diretto su tutte le fasi di gestione e trattamento dei dati.

Etica.....

Tutta da disciplinare in futuro con Norme specifiche (AI Act ha approcciato in modo light)

NORME DI RIFERIMENTO



ALTRE NORME DI RIFERIMENTO

NORME DI RIFERIMENTO

Alcune delle norme elencate sono ancora in versione Draft o DIS

ISO/IEC 24028 Information technology - Artificial intelligence - Overview of trustworthiness in artificialintelligence.

ISO/IEC 24027 Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making.

ISO/IEC 24368 Information technology - Artificial intelligence - Overview of ethical and societal concerns.

ISO/IEC 4213 Information technology - Artificial intelligence - Assessment of machine learning classification performance.

ISO/IEC 5259 1-5 Data quality for analytics and machine learning (ML). ISO/IEC 5339

ISO/IEC 5469 Artificial intelligence - Functional safety and AI systems.

ISO/IEC 6254 Information technology - Artificial intelligence - Objectives and approaches for explainability of ML models and AI systems.

ISO/IEC 23053 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML).

ISO/IEC 23894 Information technology - Artificial intelligence - Guidance on risk management.

ISO/IEC 38507 Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations.

NORME DI RIFERIMENTO

Alcune delle norme elencate sono ancora in versione Draft o DIS

- ISO/IEC WD 22989: Concetti e terminologia dell'intelligenza artificiale
- ISO/IEC NP TR 24027: Tecnologia dell'informazione - Intelligenza artificiale (AI) - Pregiudizio nei sistemi di IA e processo decisionale assistito dall'IA
- ISO/IEC 42005 - Tecnologia dell'informazione - Intelligenza artificiale (AI) Valutazione d'impatto dei sistemi IA
- ISO/IEC NP TR 24028: Tecnologia dell'informazione - Intelligenza artificiale (AI) - Panoramica del
- ISO/IEC NP TR 24029-1: Intelligenza Artificiale (AI) - Valutazione della robustezza delle reti neurali Parte 1: Panoramica
- ISO/IEC NP TR 24030: Tecnologia dell'informazione - Intelligenza artificiale (AI) - Casi d'uso
- ISO/IEC NP 23894: Tecnologia dell'informazione - Intelligenza artificiale - Gestione del rischio
- ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements
- NIST AI 100-1 Artificial Intelligence Risk Management Framework (AI RMF 1.0)
- REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

02

NIS 2 Aggiornamenti
La nuova UNI PdR CSF

IL DECRETO ITALIANO E GLI ATTORI COINVOLTI

DIRETTIVA EUROPEA NIS 2 (2022/2555)

DECRETO ITALIANO 138/2024

AGENZIA DI CYBERSICUREZZA NAZIONALE

AZIENDE

TOP MANAGEMENT

ORGANIZZAZIONE

ENTRO QUANDO?

I soggetti che si riconocono in uno dei settori/sottosettori/tipologie **DOVRANNO:**

REGISTRAZIONE PORTALE DI ACN	CONFERMA DA ACN	TERMINE PER RAGGIUNGERE COMPLIANCE NIS 2
		
•**Entro il 17 gennaio 25:** fornitori di servizi di sistema dei nomi di dominio, i gestori di registri dei nomi di dominio di primo livello, i fornitori di servizi di registrazione dei nomi di dominio, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, nonché i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network •**Dal 1 gennaio 25 al 28 febbraio 25:** Tutti gli altri soggetti	**Entro 90 giorni** dal caricamento dei dati sul portale ACN	**18 mesi dalla conferma di ACN**

sanzione amministrativa pecuniaria fino a 0.1% del fatturato annuo su scala mondiale

QUALI AZIENDE SONO INTERESSATE?

OPERATORI DI SERVIZI ESSENZIALI (I) E IMPORTANTI (II)

SETTORI AD ALTA CRITICITA' (I)	ALTRI SETTORI CRITICI (II)
ENERGIA: elettricità Gas, petrolio, Idrogeno	**SERVIZI POSTALI E CORRIERI**
SANITA' prest. sanitaria, laboratori, R&S, farmaceutica	**GESTIONE DEI RIFIUTI**
TRASPORTI	**CHIMICO:** fabbricazione, produzione distribuzione
BANCARIO E INFRASTRUTTURE FINANZIARIE	**FOOD**: Produzione, trasformazione e distribuzione Alimenti
ACQUA POTABILE E ACQUE REFLUE	**FABBRICAZIONE** disp. Medici, elettronica, macchinari, autoveicoli, rimorchi
INFRASTRUTTURE DIGITALI	Fornitori di **SERVIZI DIGITALI**
GESTIONE SERVIZI TIC	**R&D**
SPAZIO	

Medie/Grandi imprese

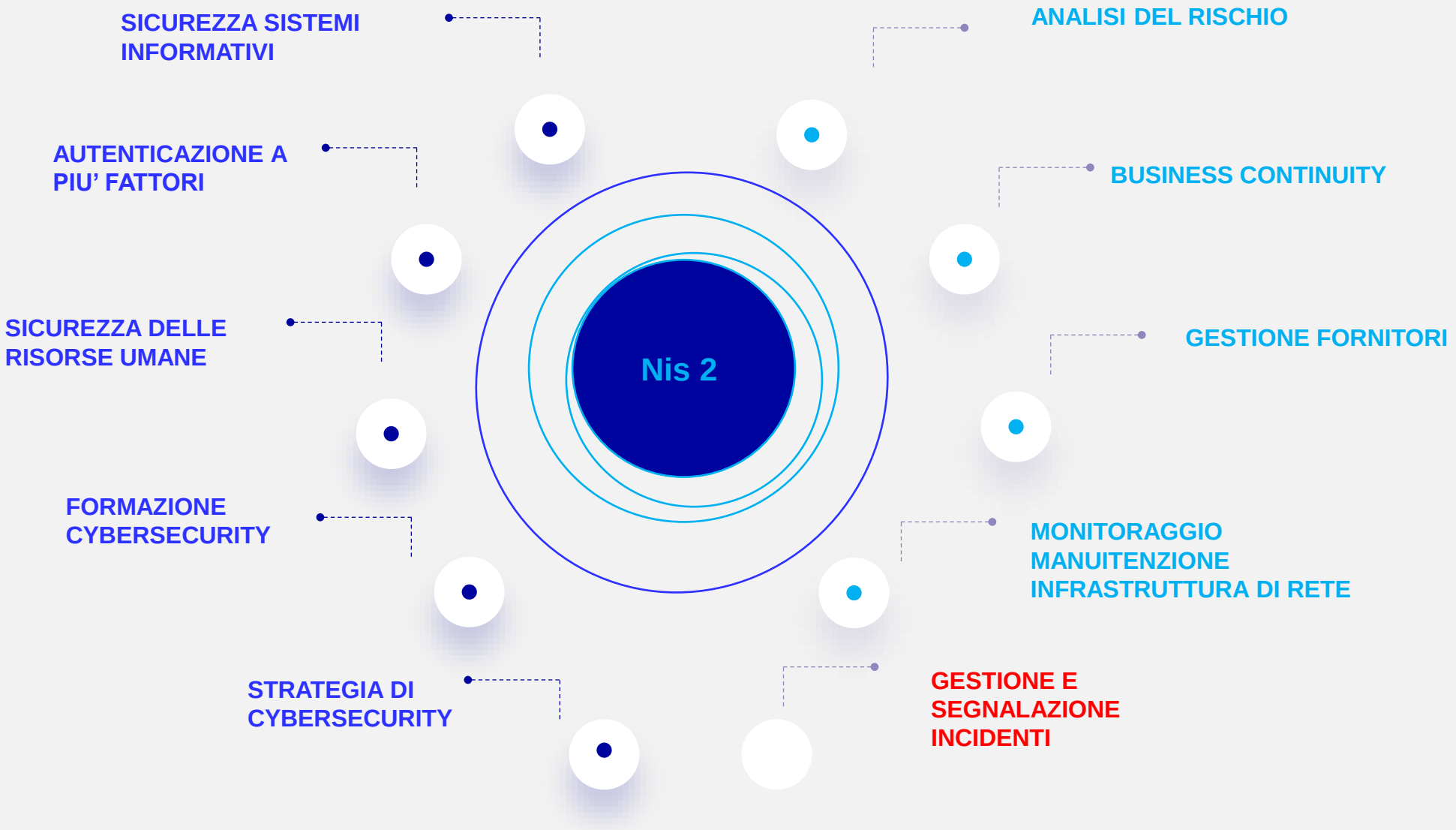
Dipendenti >50; fatt annuo tot >10 mln

SUPPLYCHAIN
Indipendentemente dalla dimensione

che rappresentino **un elemento sistemico nella catena di approvigionamento, anche digitale** dei settori in tabella

QUALI MISURE ADOTTARE

OBIETTIVI NIS 2



QUALI PRINCIPALI ELEMENTI DI PRESCRIZIONE

Governance	Vigilanza	Gestione del rischio	Supply chain	Segnalazione Incidenti
La **gestione della cyber sicurezza non è più un compito relegato esclusivamente alla funzione dei sistemi informativi**, ma diventa una **responsabilità diretta dell'organo di gestione aziendale**, come ad esempio il **Consiglio di Amministrazione.**	**Soggetti essenziali**: La normativa prevede un **regime di vigilianza completo** (ex ante- ex post) e sanzioni **fino a 10 mln di euro o pari al 2% del** fatt/anno/globale **Soggetti Importanti: regime di vigilanza leggero(ex post) e sanzioni fino a 7** mln di euro o pari al 1,4% del fatt/anno/globale	**«misure tecnico-organizzative "adeguate"»** per gestire i rischi per la sicurezza dei sistemi di rete e di informazione che i soggetti essenziali e importanti sono tenuti ad attuare	I soggetti identificati devono **garantire la cybersecurity lungo la supply chain** valutando il livello di maturità cyber dei fornitori	I soggetti identificati sono incaricati di inviare **un preallare entro 24 ore dell'incidente** e successiva **comunicazione entro 72 con aggiornamento delle informazion**i inviate precedentemente

- **SANZIONI AMMINISTRATIVE**
- **SOSPENSIONE MANAGEMENT**
- **ADDEBITO COSTI AUDITS**

RICAPITOLANDO....

SCADENZE

- Registrazione su portale di ACN
- Inserire ogni anno i dati sul portale di ACN
- Rispettare i tempi corretti di comunicazione incidenti cyber

OBBLIGHI CYBER

- Analisi del rischio
- Mantenimento continuità operativa
- Gestione Policy +documentazione a supporto in caso di verifica ACN
- Formazione Risorse Umane
- Procedure gestione Incidenti
- Mantenere monitoraggio sui fornitori

SANZIONI

- SOSPENSIONE MANAGEMENT
- SOSPENSIONE CERTIFICATI
- MULTEEE!!!!

VISIONE STRATEGICA

APPROCCIO MULTIDISCIPLINARE	Coinvolgimento diversi stakeholder aziendali (IT, OT, Operation, HR, C-Level)
TEMPISTICHE STRINGENTI	Le tempistiche richieste sono una grande prova per le aziende soprattutto per le PMI coinvolte che sono meno mature dal punto di vista Cyber
IMPLICAZIONI PER CYBER INDUSTRIALE (OT)	Una sfida importante quella della Cyber degli asset industriali dove ad oggi il livello di maturità e consapevolezza è ancora limitato
EFFORT RICHIESTO	Difficoltà nell'applicazione dei requisiti richiesti dalla normativa e nell'implementazione di azioni di mitigazione del rischio

—NIS2: LA UNI PDR CSF

COME DIMOSTRARE LA COMPLIANCE ALLA NIS2?

Per esperienza pregressa, Direttive e Regolementi non danno mai indicazioni su come e strumenti da utilizzare per dimostrare la compliance ai requisiti (poche eccezioni in perimetri ristretti e settori definiti); allo sttao attuale gli unici strumenti di attestazione e certificazione erano:

1. Certificazione ISO 27001;
2. Attestazione secondo le Linee Guida NIST-ENISA-Schema Nazionale;
3. Ceritificazione ISA 62443 (OT).

NOVITA’

UNI , su input ACN e con la collaborazione e supervisione di Accredia, ha costituito a fine 2024 un tavolo tecnico finalizzato alla definzione di una UNI PdR per la gestione delle compliance alla NIS 2. Da capire , ora che è stata presentata, se verrà presa in carico da Accredia e se verrà indicata da ACN come strumento di riferimento per la conformità alla NIS 2. La UNI PDR è aperta alle integrazioni alla ISO 27001 (sia per chi ne è già in possesso, sia per chi ha intenzione di farla).

COME DIMOSTRARE LA COMPLIANCE ALLA NIS2?

E’ in consultazione pubblica sul sito UNI la PdR (Prassi di Riferimento) “Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001 e al Framework NIST CSF 2.0 – Requisiti”. Al tavolo di lavoro con ACCREDIA, CINI (Consorzio Interuniversitario Nazionale Informatica) ed UNINFO ha partecipato attivamente ASSOTIC, rappresentata dal nostro Gabriele Vitali della Service Line Certificazione.

COME E' STRUTTURATA LA UNI/PDR XX:2024?

Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni armonizzato alla norma UNI CEI EN ISO/IEC 27001:2024 e al Framework NIST CSF 2.0 – Requisiti

- Adottata esclusivamente in ambito nazionale (se integrata con certificazione ISO 27001 puo' essere utile anche per le Organizzazioni che hanno attività internazionali). Chi è già in possesso della ISO 27001 potrà «attestare» il delta relativo ai requisiti NIST.

- Documento che introduce prescrizioni tecniche (elaborati dagli autori sotto la conduzione operativa di UNI)

- Basato su Annex SL della Direttiva ISO/IEC parte 1

- Contiene:

- Parte di Sistema (I requisiti della PdR sono scritti in forma "additiva")
- Appendice A (prospetto tabellare per indicare la relazione tra NIST CSF 2.0 con i Requisiti della 27001 e relativo Annex A (controlli)
- Appendice B (2 prospetti tabellari):
  - B.1 (Relazione tra Parte sistemica 27001 e NIST CSF 2.0
  - B.2 (Relazione tra Annex A 27001 e NIST CSF 2.0

UNI/PDR XX:2024

Esempio dell'Appendice A

Prospetto A – Relazione fra Punti e Controlli della norma UNI CEI EN ISO/IEC 27001:2024 e le Sottocategorie del Framework NIST CSF 2.0

Categorie e Sottocategorie NIST CSF 2.0	UNI CEI EN ISO/IEC 27001:2024		Attributi dei Controlli definiti dalla norma UNI CEI EN ISO/IEC 27002:2023						
	PUNTI PARTE SISTEMICA	CONTROLLI APPENDICE A	Capacità Operative	Domini di Sicurezza	Concetti di Cybersecurity				
			#Governance	#Governance_and_Ecosystem	#Identify	#Protect	#Detect	#Respond	#Recover
FUNZIONE GV									
GV.OC									
GV.OC-01	**4.1, 4.2, 4.3, 4.4, 5.2**	-							
GV.OC-02	**4.2, 4.3, 4.4**	-							
GV.OC-03	**4.1, 4.2, 4.3, 4.4**	5.31, 5.32, 5.33, 5.34		5.31, 5.32	5.31, 5.32, 5.33, 5.34	5.33, 5.34			
GV.OC-04	**4.2, 4.3, 4.4, 5.2, 7.4**	-							
GV.OC-05	**4.1, 4.2, 4.3, 4.4, 7.4, 8.1**	5.22		5.22	5.22				

UNI/PDR XX:2024

Esempio dell'Appendice B (B.1 + B.2)

Prospetto B.1 – Relazione fra i Punti della norma UNI CEI EN ISO/IEC 27001:2024 e le Sottocategorie del Framework NIST CSF 2.0

Norma UNI CEI EN ISO/IEC 27001:2024		Sottocategorie NIST CSF 2.0
Numero Punto	Titolo Punto	
4.1	Comprendere l'Organizzazione e il suo Contesto	GV.OC-01, GV.OC-03, GV.OC-05
4.2	Comprendere le Esigenze e le Aspettative delle Parti Interessate	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.SC-04, GV.SC-05
4.3	Determinare il Campo di Applicazione del Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05
4.4	Sistema di Gestione per la Cybersicurezza e la Sicurezza delle Informazioni	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07

Prospetto B.2 – Relazione fra i Controlli dell'Appendice A della norma UNI CEI EN ISO/IEC 27001:2024 e le Sottocategorie del Framework NIST CSF 2.0

Controlli in Appendice A della norma UNI CEI EN ISO/IEC 27001:2024	Attributi dei Controlli definiti dalla norma UNI CEI EN ISO/IEC 27002 :2023			Sottocategorie NIST CSF 2.0
	Capacità Operative Valore '#Governance'	Domini di Sicurezza Valore '#Governance_and_Ecosystem'	Concetti di Cybersecurity Valori '#Identify', '#Protect', '#Detect', '#Respond', '#Recover'	
5 Controlli Organizzativi				
5.1	#Governance	#Governance_and_Ecosystem	#Identify	GV.PO-01, GV.PO-02
5.2	#Governance	#Governance_and_Ecosystem	#Identify	GV.RR-02, GV.SC-02
5.3	#Governance	#Governance_and_Ecosystem	#Protect	GV.RR-02, PR.AA-05
5.4	#Governance	#Governance_and_Ecosystem	#Identify	PR.AT-01, PR.AT-02
5.5	#Governance		#Identify #Protect #Respond #Recover	RS.CO-03, RS.CO-02, RC.CO-03

GRAZIE PER L'ATTENZIONE

MAURIZIO GENNA
ICT Product Manager

maurizio.genna@bureauveritas.com

BUREAU VERITAS ITALIA

VALENTINA MUSSI
National Market Leader Cyber & Digital

valentina.mussi@bureauveritas.com

BUREAU VERITAS ITALIA

BUREAU
VERITAS

Shaping a World of Trust

Grazie per l'attenzione!

Approved by

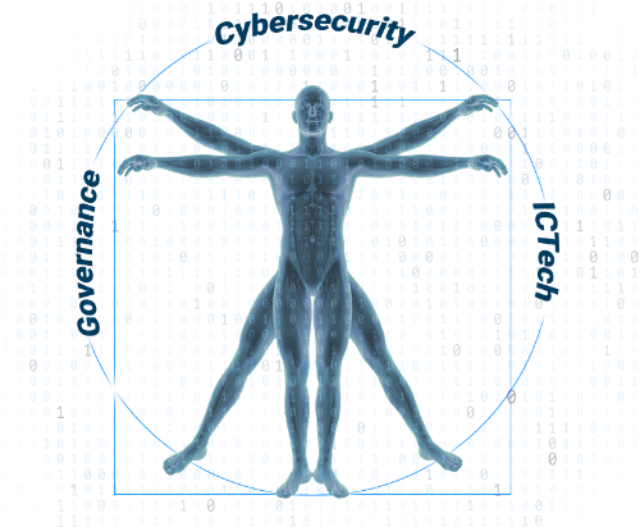
QUESTIONARIO

- ❑ Gradimento
- ❑ Newsletter

Scrivere a eventi@ithum.it per:

- ✓ Attestato di partecipazione
- ✓ Slide proiettate
- ✓ Informazioni varie
- ✓ Registrazione

ITHUM
it's for human



Fields of interest:
Training & **Certifications**
Specialized **Consultancy**

Founded in **2005**
by ICT professionals

HQ located **in Rome**
Active in Italy & Europe

Collaborative & strategic approach
to build Value

Cyber Security

- IT Security
  - Attacks & Warfare
  - Defence & Analysis
  - Secure Coding
  - Operation Technology Security
- Governance & Management
- Intelligence & Social
- Investigation & Forensic
- Regulatory Compliance
- Artificial Intelligence

Governance

- National & International Standards
  - Information Security
  - Artificial Intelligence
  - Business Continuity
  - Quality
  - IT Services
  - Anti-Bribery
  - Environment Social Government
  - Privacy GDPR
  - Professional Profiles UNI/EN (ICT & HR)
- Project Management & Framework
- Job Safety & Security
- Management & Soft skills

ICTech

- IT & Operative Systems
- Networking & DevNet
- Cloud & Virtualization
- Containers
  - Docker
  - Kubernetes
- Blockchain
- Development & Programming
- Industry 4.0 (IoT, Big Data, AR)
- Artificial Intelligence, Deep & Machine Learning

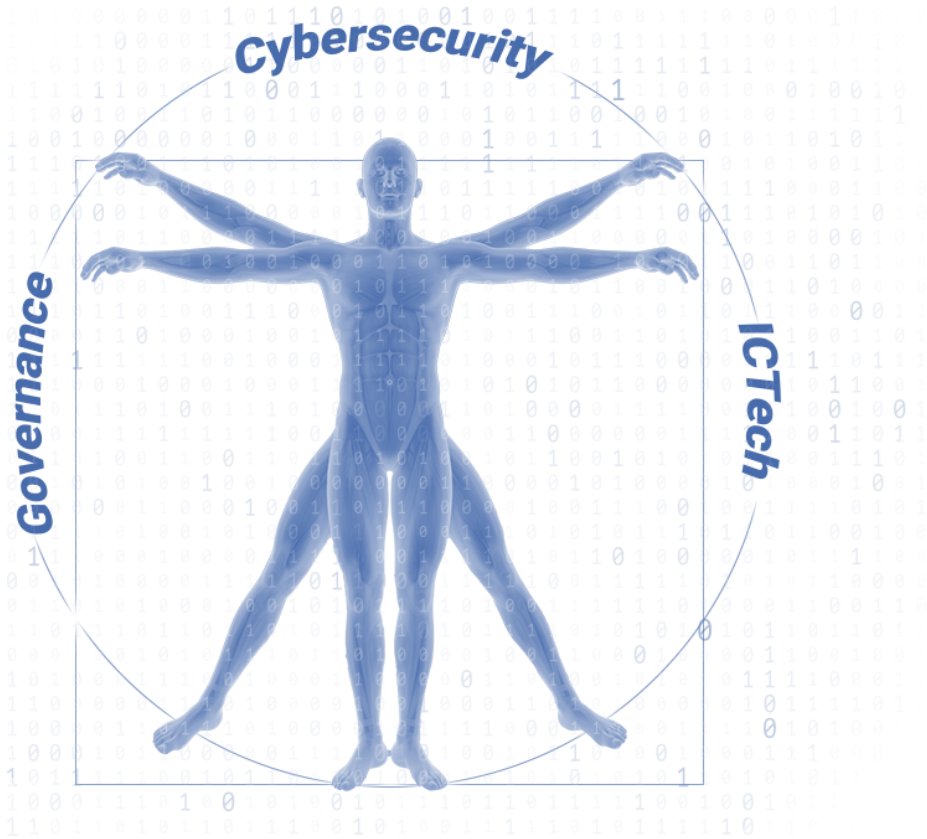
ITHUM
it's for human

(+39) 06 2158915
(+39) 06 86726329

Via Cristoforo Colombo, 149
00147 Roma (RM) Italy

informazioni@ithum.it

www.ithum.it



Corsi correlati

Auditor/Lead Auditor ISO/IEC 42001

Inizio corso: 8 maggio 2025

NIS 2

Inizio corso: 21 marzo 2025

Compliance Normativa

Inizio corso: 31 marzo 2025

DAILY AI Generativa: per il lavoro di tutti i giorni

In collaborazione con **Talents Venture**

Inizio corso: 25 marzo 2025

I nostri Webinar

Evento precedente

12 dicembre 2024

Prossimo evento

18 marzo 2025 – ore 17:00

Informazioni, materiali e registrazione:
www.ithum.it/natale-con-la-nis2

Q&A