SECURITY SUMMIT

Security Summit

Roma 23 giugno 2026

Clusit

ASTREA

Sessione

Cyber security e AI: a un anno dalla ISO/IEC 42001, cosa sta cambiando davvero

Ilaria Savini | Innovation & ICT BD, Strategy and Growth Lead DNV BA Italy & Adriatics,

11.30 -12.10 23 giugno 2026

Garibaldi Conte

Membro del Comitato Scientifico

Co – Fondatore e Managing Director – ATSEC Information Security Srl

Ilaria Savini

Innovation & ICT BD, Strategy and Growth Lead Lead

Piccoli aggiornamenti

- Primo certificato al mondo ISO/IEC 42001 (Cognizant) 16 dicembre 2024

  …poco più di un anno fa

cognizant Investor Home Financials News & Investor Events Governance ESG Investor Resources

ethical way

TEANECK, N.J., Dec. 16, 2024 /PRNewswire/ -- Cognizant (NASDAQ: CTSH) today announced it has received accredited ISO/IEC 42001:2023 certification for its artificial intelligence management system. Cognizant is the first global IT service company to receive this accredited certification, which underscores Cognizant's commitment to responsible AI development and deployment while strengthening its position as a trusted partner in digital transformation.

"We are honored to receive the first ISO/IEC 42001:2023 accredited certification in our industry," said Ravi Kumar S, CEO at Cognizant. "In today's market, businesses demand partners who not only drive innovation but also align with their values and sustainability goals. This certification solidifies our role as a trusted leader in enabling ethical and sustainable digital transformation worldwide."

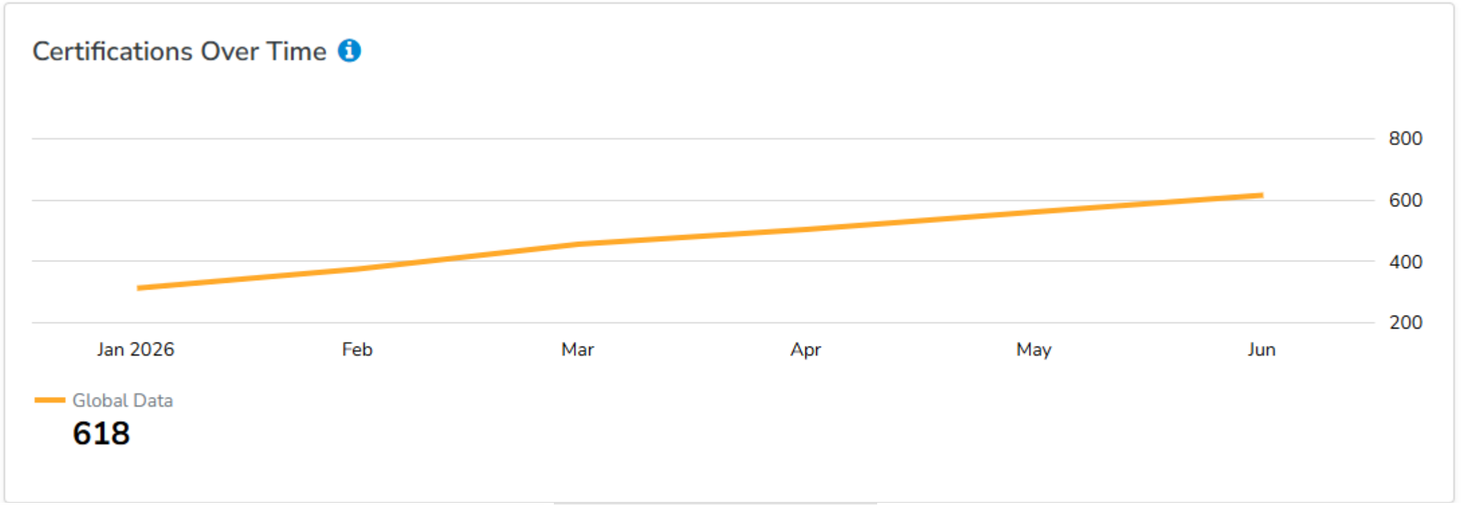
ISO/IEC 42001 is the world's first international standard for artificial intelligence management systems (AIMS). It provides organizations with a comprehensive framework to manage AI risks and opportunities throughout the AI system lifecycle, while ensuring responsible development and deployment of AI solutions. The certification was issued by DNV, a leading global provider of management systems certification and training.

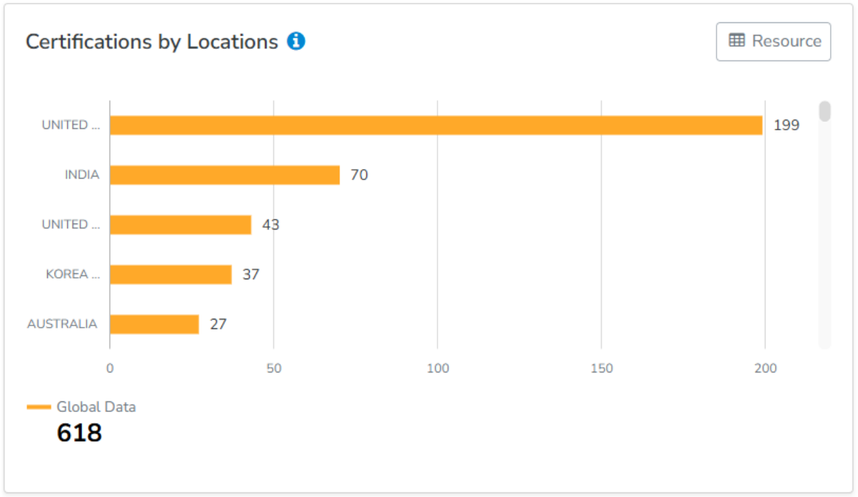
Certificati DNV in Italia e nel mondo

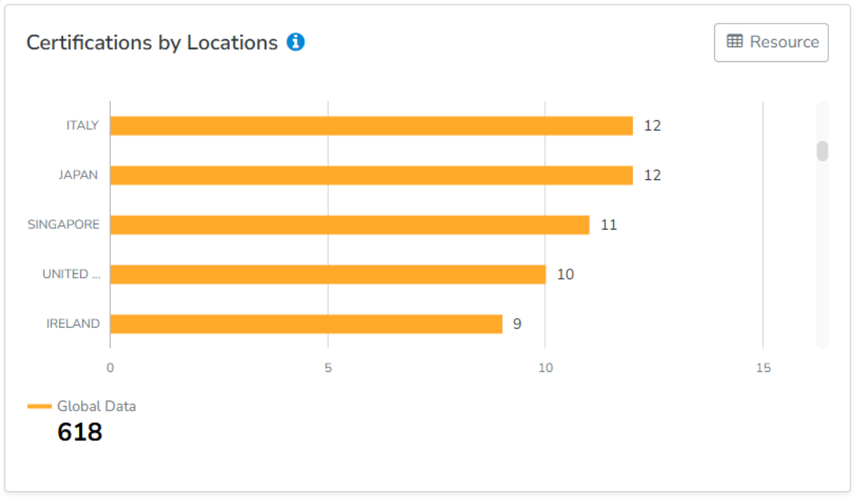
46 certificati nel mondo (al 23/6/2026)

6 certificati
(al 23/06/2026)

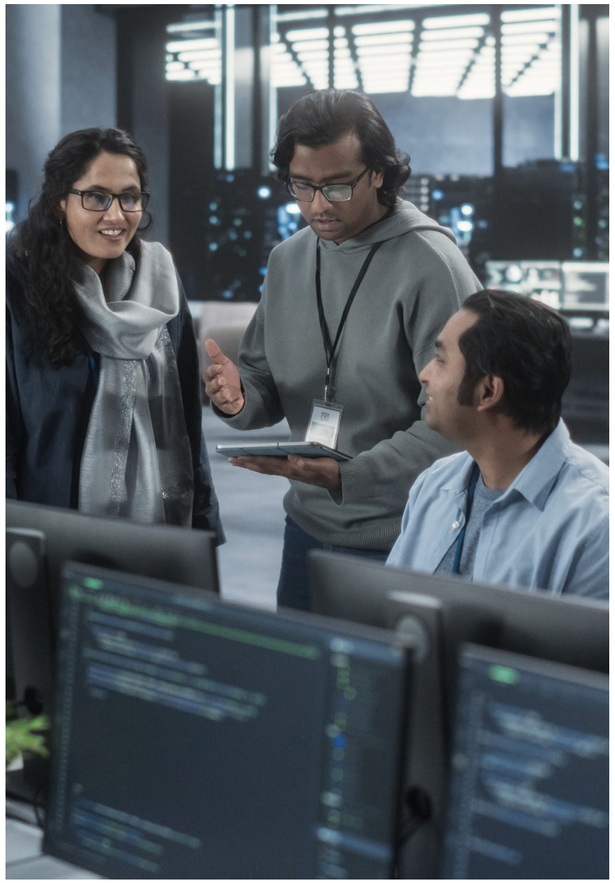
Certificati nel mondo







Considerazioni sul SG



1. Sistema AI è un prodotto/servizio ma la certificazione ISO/IEC 42001 **non certifica il prodotto/servizio**
2. Ruoli specifici (**manager designato**), regole specifiche (**alcuni controlli obbligatori**)
3. Impatto culturale, **necessità di un cambiamento (nostro e delle aziende)**
4. **Multidisciplinarietà** dei team di progettazione, di sviluppo e di audit
5. Terminologia e requisiti spesso **diversi da altri standard o impiegati in modo diverso**
6. **Allegati (2 normativi)** gestiti in modo diverso da 27K, di conseguenza anche i controlli
7. Controlli obbligatori, controlli in nota e controlli aggiuntivi (incidono su audit time)
8. **AI** diverse e cicli di vita diversi:
   - **statiche** (nate per un compito specifico, spente una volta terminato il compito)
   - **dinamiche** (nate per continuare a svolgere un compito a tempo non determinato)
   - **incrementali** (nate per un compito specifico e capaci di migliorare nel tempo)

Macroaree di attenzione

1. Sviluppo, fornitura e/o uso di un Sistema AI – **in che ruoli gioca l'organizzazione?** La scelta cambia tutto, soprattutto i tempi di audit
2. Non è una certificazione come le altre, **l'oggetto principale non è il Sistema di Gestione ma i Sistemi AI gestiti all'interno del Sistema di Gestione**
3. La **complessità** è calcolata con parametri specifici, non paragonabili ad altri standard, la ISO/IEC 42006 è importantissima per noi, un LA potrebbe vedere cose non emerse nelle fasi contrattuali (succede spesso)
4. La ISO/IEC 42001 **non è strutturata per «proteggere» l'organizzazione che la utilizza ma per proteggere chi utilizzerà le AI** (progettazione responsabile, fornitura responsabile, uso responsabile) ✯ individui, gruppi di individui, società
5. **Ciclo di vita (software) e qualità dei dati sono aspetti critici**

2025

6. **Consapevolezza del ruolo**
7. **Analisi rischi** verticale sui processi di sviluppo
8. Difficoltà a definire le modalità di applicazione dei **controlli specifici sui set di dati** (acquisizione, qualità, provenienza, preparazione) per le varie fasi di progetto (addestramento, verifica, validazione ecc.) – Annex A 10 domains, 10 Control objectives, 38 Controls
9. **Valutazione di impatto solo** su aspetti legati a diritti umani e svincolate dal Risk Management

La struttura dello standard

1 Scope

2 Norm

3 Terms and definition

4 Organizational context

5 Leadership

6 Planning

7 Support

8 Operation

9 Performance evaluation

10 Improvement

Annex A
Control objectives and control measures

Annex B
Implementation guidance for AI controls

Annex C
Organization objectives and sources of risks

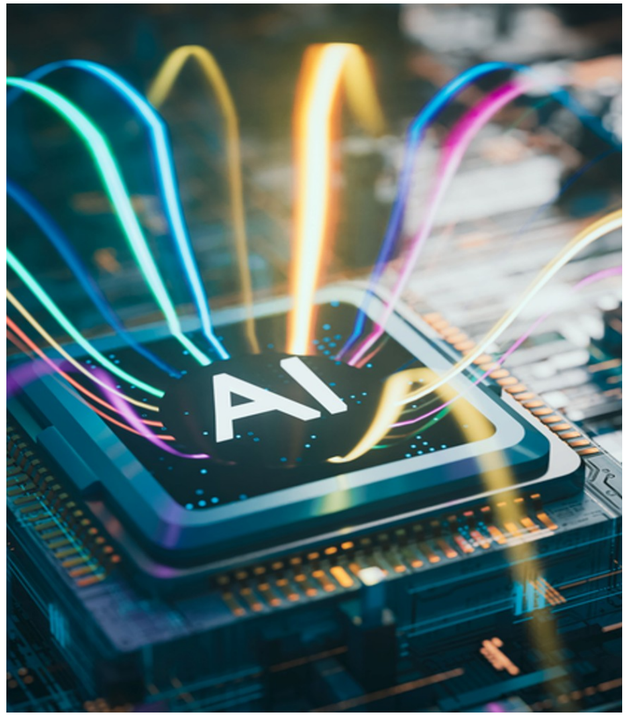
Annex D
Cross industry application of AI management systems

DNV

Non solo ISO 42001 e 42006 …Standard per gli audit

12 standard necessari per entrare nel cuore della ISO/IEC 42001 di cui 6 funzionali alla certificazione (indicati dalla ISO/IEC 42006):

1. **ISO/IEC 22989:2022** - Information technology - Artificial intelligence - Artificial intelligence concepts and terminology (**è fondamentale** per comprendere e applicare la ISO/IEC 42001 – gratuita sul sito ISO)
2. **ISO/IEC 5338:2023** - Information technology - Artificial intelligence - AI system life cycle processes
3. **ISO/IEC 42005:2025** - Information technology — Artificial intelligence — AI system impact assessment



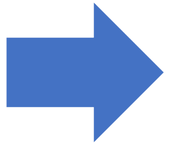
4. **ISO/IEC 23894:2023 -** Information technology - Artificial intelligence - Guidance on risk management
5. **ISO/IEC 5259-3** Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines
6. **ISO/IEC TR 24027:2021** - Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making

Cyber security & AI

- Gli **attacchi** possono essere classificati come attacchi **durante lo sviluppo e l'addestramento dei sistemi di AI o durante l'inferenza o il funzionamento dei sistemi di IA, o entrambi**. I sistemi di IA sono suscettibili di attacchi considerati convenzionali per tutti i tipi di sistemi informativi.
- **Gli attacchi di sicurezza convenzionali ai sistemi di elaborazione delle informazioni possono ancora colpire i sistemi di AI** e pertanto devono essere implementati controlli di sicurezza delle informazioni, come quelli descritti nella norma ISO/IEC 27002.
- I **sistemi di AI devono essere considerati come componenti software** che di solito sono integrati in un altro sistema, applicazioni o file di dati, **piuttosto che come un modello di AI o ML indipendente**. Pertanto, **le misure di sicurezza applicate al software e alle applicazioni si applicano anche ai sistemi di AI in tutte le fasi del ciclo di vita**, come la progettazione, l'implementazione o l'utilizzo di un sistema di AI in funzione.

La Governance ed I ruoli aziendali

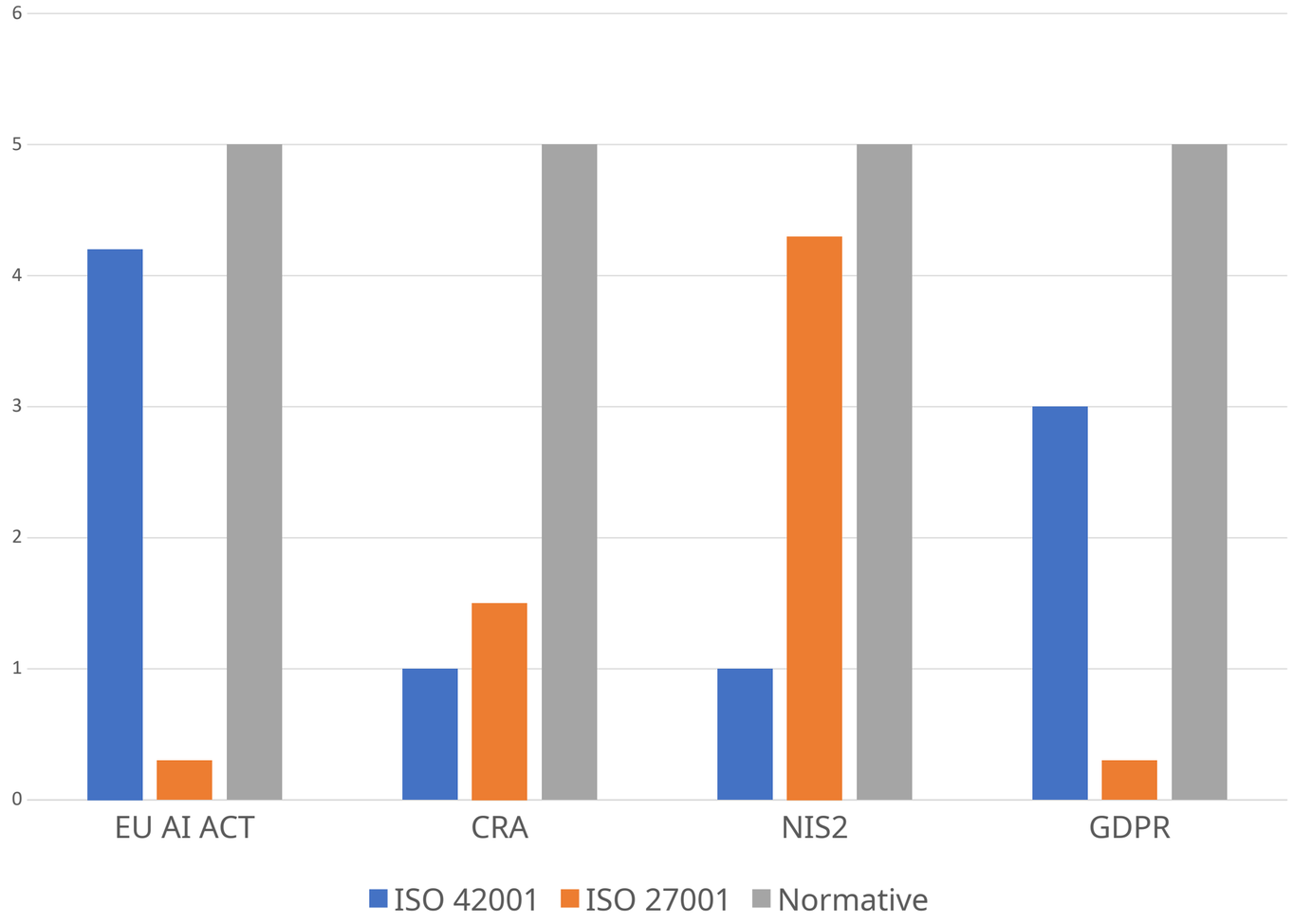
- **Nello stage 1** i problemi più comuni sono:
  - aver pensato ai **rischi** come nella 27001 (informazioni/asset invece che obiettivi AI)
  - non aver sviluppato i **processi** di valutazione di impatto, valutazione dei rischi e trattamento dei rischi garantendo quanto chiede la norma.
- **Nello stage 2** i problemi più comuni sono:
  - il **collegamento di impatti/rischi al ciclo di vita** (inclusa variabilità in funzione del ciclo e degli obiettivi per ciascuna AI)
  - le **metriche per la validazione** (la ISO/IEC 24027 è molto utile).



Cooperazione fra CISO, CIO, Head of AI, CAIO, R&D, Head of Digital Transformation, Resp. sistemi di gestione

In ultima analisi

1. AI Act (mandatorio – regola la IA) ma SGAI (v**olontario, contrattuale – regola il SG che produce l'IA**)
2. Gli impatti si misurano per **individui, gruppi di individui, società** (inteso come aspetto sociale), tenendo conto di **usi attesi e abusi**, considerando **aspetti tecnici, sociali e giuridici** – cambiando i parametri cambia tutto



Contatti:

Venite a trovarci al nostro Stand

ilaria.savini@dnv.com

www.dnv.it
https://www.linkedin.com/showcase/dnv-assurance/