



MARSH

16 marzo 2026

AI Risk – Framework, strumenti di compliance e correlazione con la Data Protection

Carlo Drioli – Head of Business Resilience & Digital Risk,
Marsh Risk Consulting

Chi siamo

Offriamo servizi professionali sfruttando le più elevate competenze nella gestione del rischio, della strategia e del capitale umano.

MARSH

INTERMEDIAZIONE ASSICURATIVA E RIASSICURATIVA,
CONSULENZA SUI RISCHI

SERVIZI DI CONSULENZA SU
CAPITALE UMANO E STRATEGIA

MARSH

Leader globale nell'intermediazione assicurativa e nella consulenza sui rischi.

GUY CARPENTER A MARSH BUSINESS

Specialista nei servizi di intermediazione riassicurativa

MERCER A MARSH BUSINESS

Leader nella consulenza su capitale umano, servizi attuariali, previdenziali e investimenti

OLIVER WYMAN A MARSH BUSINESS

Leader nella consulenza manageriale strategica

Risk Consulting assiste i propri clienti nel disegno e nell'implementazione di soluzioni di risk management dedicate

NEL MONDO

2.000+ colleghi

130 uffici
HQ New York



IN ITALIA

100+ colleghi

2 uffici
Milano e Roma

MARSH



Quotata al NYSE ed è una Fortune 250



Uffici in oltre 130 paesi



90.000+ colleghi nel mondo



Fatturato annuo: \$ ~24.5 miliardi



Oltre 150 anni di leadership e innovazione

Lo speaker di oggi



Carlo Drioli

*Head of Business Resilience
& Digital Risk*

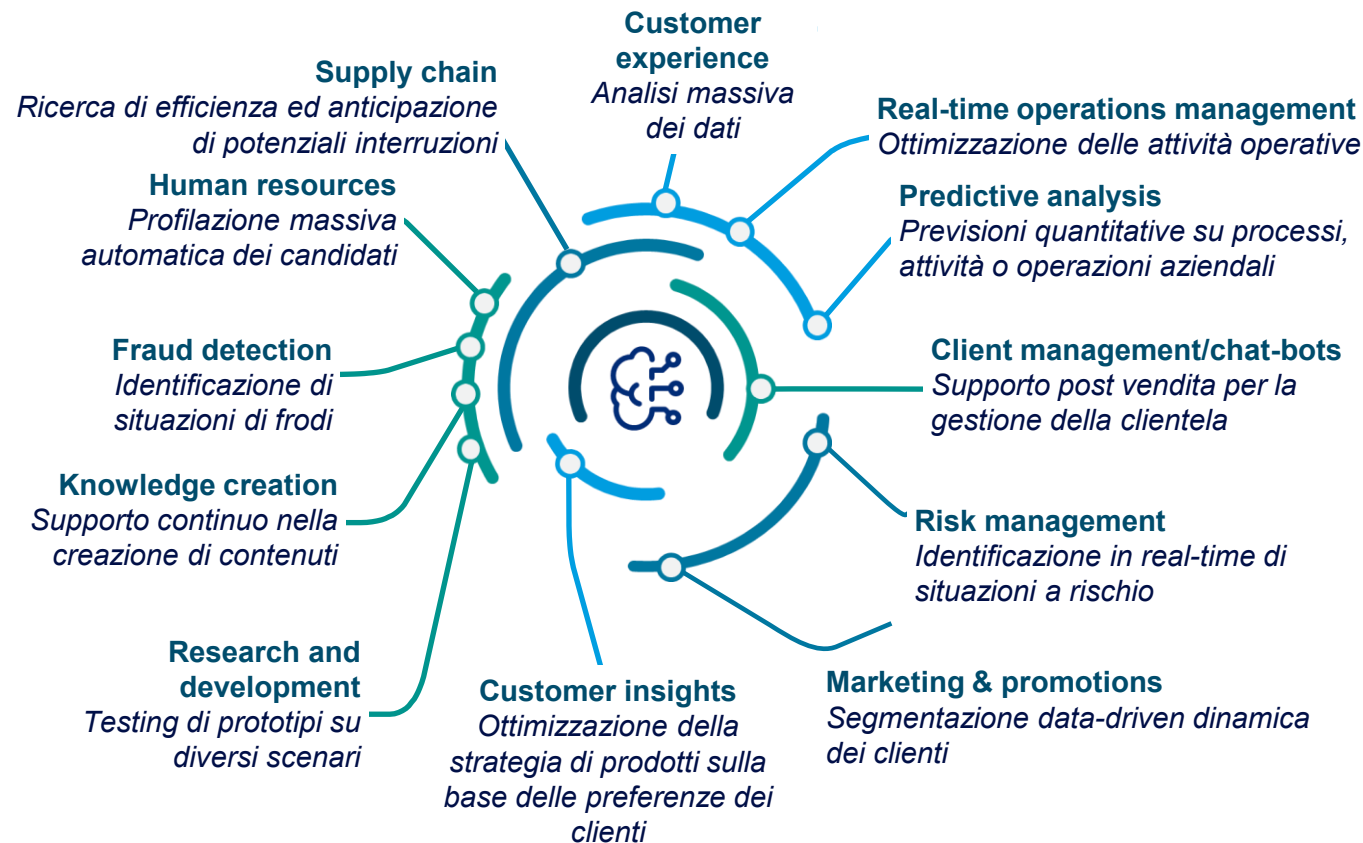
- **Responsabile della practice Business Resilience & Digital Risk** per Marsh Risk Consulting, con 18 anni di esperienza.
- Professionista esperto nelle tematiche di **Risk Management, Business Continuity Management, Cyber Risk, Data Protection**, oltre che di **IT Governance** e di **Program Management** di iniziative complesse di Digital Transformation.
- Implementazione di **Sistemi di Controllo ICT** in primari gruppi nazionali e internazionali.

Premessa

Vantaggi e rischi dell'utilizzo di strumenti di AI in azienda

Adozione dell'AI, vantaggi enormi...

...ma grandi rischi da gestire



AI Risk Taxonomy definita dal Massachusetts Institute of Technology

- 01 Discrimination and toxicity
- 02 Privacy and security
- 03 Misinformation
- 04 Malicious actors and misuse
- 05 Human-computer interaction
- 06 Socioeconomic and environmental harms
- 07 AI system safety, failures and limitations

Rischi dell'AI

Global risks ranked by severity

Near-term (2 years)

- 1 Misinformation and disinformation
- 2 Extreme weather events
- 3 State-based armed conflict
- 4 Societal Polarization
- 5 Cyber espionage and warfare
- 6 Pollution
- 7 Inequality
- 8 Involuntary migration or displacement
- 9 Geoeconomic confrontation
- 10 Erosion of human rights and /or civic freedoms

Longer-term (10 years)

- 1 Extreme weather events
- 2 Biodiversity loss and ecosystem collapse
- 3 Critical change to Earth systems
- 4 Natural resource shortages
- 5 Misinformation and disinformation
- 6 Adverse outcomes of AI technologies
- 7 Inequality
- 8 Societal polarization
- 9 Cyber espionage and warfare
- 10 Pollution (air, soil, water)

Risk categories

- Economic ● Environmental ● Geopolitical ● Societal ● Technological



Key insights

- I rischi specifici di un utilizzo improprio dell'AI sono riconosciuti nel lungo periodo.
- L'AI da un lato pone nuovi rischi, ma dall'altro soprattutto comporta e amplifica – già nel breve periodo – rischi preesistenti.
- Fare previsioni di lungo periodo è impossibile, data l'evoluzione esponenziale di queste tecnologie.

Rischi dell'AI

AI generativa come generatore di nuovi rischi e «amplificatore» di rischi preesistenti

01 Discrimination and toxicity

Unfair discrimination and misrepresentation; exposure to toxic content; unequal performance amongst groups

02 Privacy and security

Compromise of privacy by obtaining; leaking or correctly inferring sensitive information; AI system security vulnerabilities and attacks

03 Misinformation

False or misleading information; pollution of information ecosystem and loss of consensus reality

04 Malicious actors and misuse

Disinformation, surveillance and influence at scale; cyberattacks, weapon development or use, and mass harm

05 Human-computer interaction

Overreliance and unsafe use; loss of human agency and autonomy

06 Socioeconomic and environmental harms

Power centralization and unfair distribution of benefits; increased inequality and decline in employment quality; Economic and cultural devaluation of human effort; competitive dynamics; governance failure; environmental harm

07 AI system safety, failures and limitations

AI pursuing its own goals in conflict with human goals or values; AI possessing dangerous capabilities that could cause mass harm; lack of capability or robustness; lack of transparency or interpretability; AI welfare and rights

L'AI Act si fonda su un approccio risk-based

The AI Act classifies AI systems into four categories. The criteria for classification include the system's intended purpose and potential impact on health, safety or fundamental rights.



Unacceptable risk

Applies to AI systems that **pose risk to safety and fundamental rights**, including applications that manipulate cognitive behavior, biometric identification by law enforcement, biometric categorization (e.g., race, sexual orientation, religious views), emotion recognition in the workplace or educational settings, and scraping for facial images.

As the name implies, these AI systems **will be prohibited in the EU**.



High-risk

Applies to AI systems with the potential to have **adverse impacts on safety or fundamental rights**. This category includes AI systems that manage or operate critical infrastructure, medical devices, or vehicles; assess eligibility for employment, benefits, or creditworthiness; provide risk assessments for law enforcement; and assist in judicial decision making.



Transparency risk

AI systems with a **clear risk of manipulation** (e.g., chatbots) will require various disclosures to inform users they are interacting with a machine.

Examples include chatbots and deepfakes.



Minimal risk

All other **AI system risks**, minimal or low-risk AI systems must comply with existing legislation.

Examples include spam filters and video games.

AI Risk, Gov & Compliance

Strumenti per la compliance con l'AI Act

- La Commissione Europea ha lanciato recentemente l'[AI Act Single Information Platform | AI Act Service Desk](#)



AI Act Explorer

The AI Act Explorer is an online tool designed to help users to browse through different chapters, annexes and recitals of the AI Act in an intuitive way.



Compliance Checker

The AI Act compliance checker is a tool that assists in evaluating whether AI systems and general-purpose AI models meet the requirements set by the AI Act.



AI Act Service Desk

Contact the AI Act Service Desk team whenever you need further assistance — including in your own language. The Service Desk enables stakeholders to submit questions about the AI Act and receive answers from a team of experts working in close cooperation with the EU AI Office.



Check an AI system or an AI model

Do you want to check an AI model or an AI system?

Question information

AI model [More info](#)

AI system [More info](#)

General-purpose AI models

Does your AI model qualify as a general-purpose AI model?

Question information

Yes

No

Models presenting systemic risk

Which of the following statements apply to your AI model?

Question information

The model has high-impact capabilities

The Commission designated the model as a model presenting systemic risk

None of the above

Results

Your role

According to the AI Act, you are considered a provider of a general-purpose AI model under [Article 3 \(3\)](#).

Risk level assessment

Your AI model likely qualifies as a general-purpose AI model with systemic risk.

Your obligations

Your AI model likely qualifies as a general-purpose AI model. In that case, you must comply with the obligations under [Articles 53 and 54 AI Act](#), which means:

- draw up and maintain technical documentation about the model, including details of the development process, to provide to the AI Office upon request. National competent authorities can also ask the AI Office to request information on their behalf when this information is needed for their supervisory tasks (see further [Article 53 \(1\)\(a\)](#), [Annex XI AI Act](#));
- provide information and documentation to downstream AI system providers to help them understand the model's capabilities and limitations and comply with their own obligations (see further [Article 53 \(1\)\(b\)](#), [Annex XII AI Act](#));
- put in place a policy to comply with Union law on copyright and related rights, and in particular identify and comply with, including through state-of-the-art technologies, a reservation of rights expressed pursuant to [Article 4 \(3\)](#) of Directive (EU) 2019/790 (see further [Article 53 \(1\)\(c\)](#) AI Act);
- draw up and publish a sufficiently detailed summary of the content used for training the model (see further [Article 53 \(1\)\(d\)](#) AI Act), according to the [template for general-purpose AI model providers to summarise their training content](#) ;
- cooperate as necessary with the Commission and the national competent authorities in the exercise of their competences and powers (see further [Article 53 \(3\)](#) AI Act);
- if established outside the EU, appoint an authorised representative in the Union before placing their model on the market (see further [Article 54 AI Act](#)).

Your general-purpose AI model is also likely to present systemic risk. In that case, you must comply with the additional obligations under [Article 55 AI Act](#), namely:

Analisi preliminare rispetto alla FRIA (Fundamental Rights Impact Assessment) stabilita dall'art. 27

AI Risk, Gov & Compliance

Framework e standard di riferimento



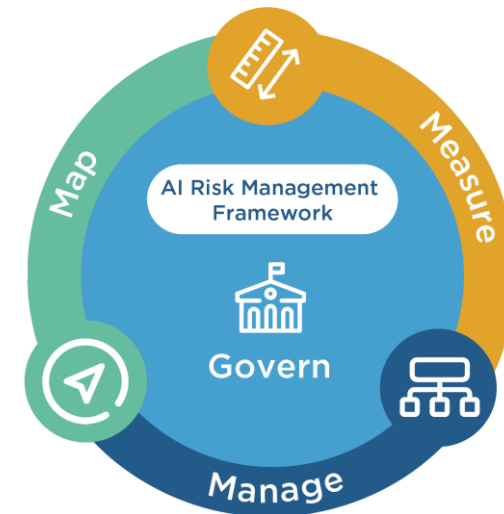
ISO/IEC 42001:2023 - AI management systems

ISO/IEC 23894:2023 - AI — Guidance on risk management

ISO/IEC 38507:2022 — Governance of IT — Governance implications of the use of artificial intelligence by organizations

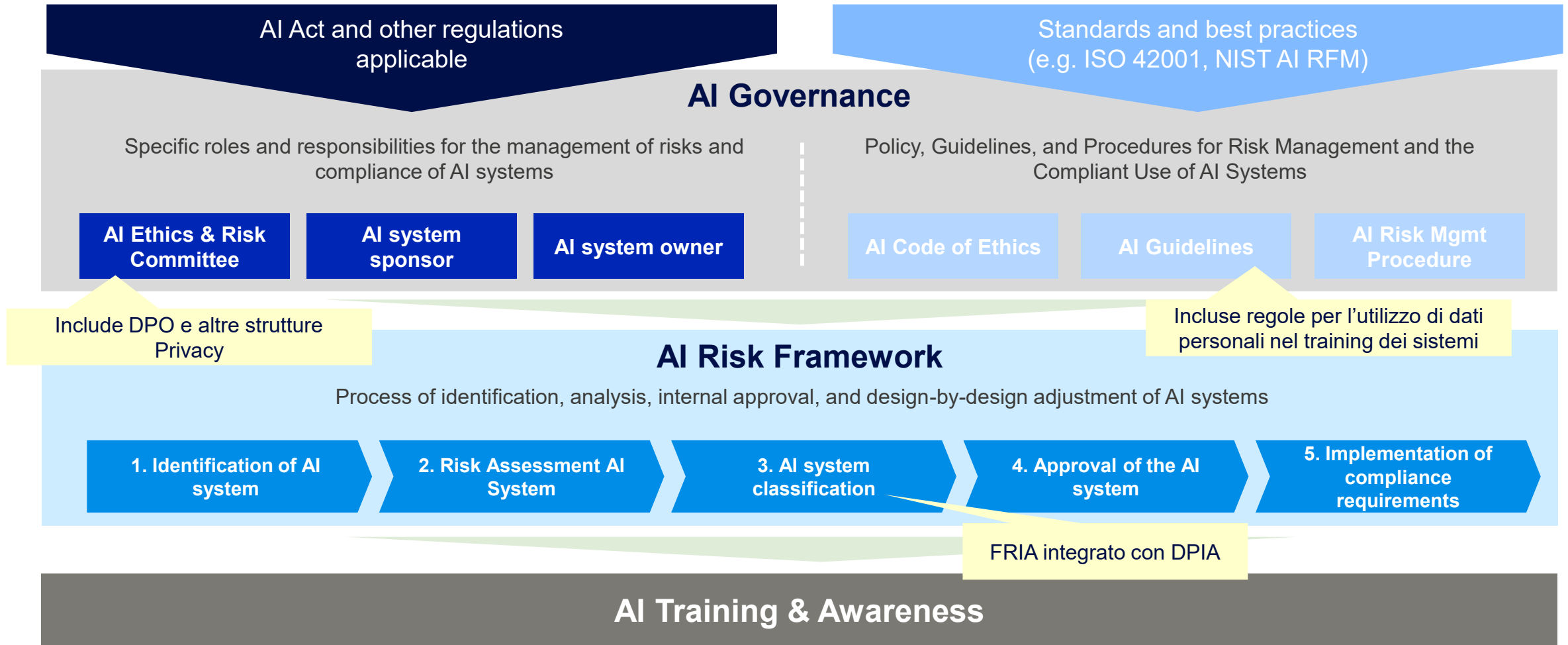


Integrazione con altre ISO, in particolare 27001 e 27701



AI Risk, Gov & Compliance

Esempio di un framework omnicomprensivo



MARSH

Marsh Advisory S.r.l. - Sede Legale: Viale Bodio, 33 - 20158 Milano - Tel. 02 48538 1 - www.marsh.it – marshadvisory@cert.marsh.it - Cap. Soc. Euro 10.400,00 i.v. - Reg. Imp. MI - N. Iscriz. e C.F.: 10027410157 - Partita IVA: 10027410157 - R.E.A. MI - N. 1338125

Società con socio unico soggetta al potere di direzione e coordinamento di Marsh S.p.A., ai sensi art. 2497 c.c.

We are leaders in risk, strategy and people. One company, with four global businesses, united by a shared purpose to build the confidence to thrive through the power of perspective.