3. AI IN RISK MANAGEMENT IMPACTS OF AI IN THE ERM FRAMEWORK

3.1. INTEGRATING RISKS GENERATED BY AI IN THE ERM FRAMEWORK

In order to manage AI risks in a secure, vigilant and resilient manner, organisations need to analyse their risk profile through the components of their risk management framework. The COSO 2017 ERM Framework gives the foundations for such an analysis.

The diagram below of the five components of the COSO ERM 2017 Framework illustrates specifically how to use a risk management framework to better capture and follow the new risks created by AI.

GOVERNANCE & CULTURE
Exercises Board Risk Oversight - Establishes Operating Structures - Defines Desired Culture - Demonstrates Commitment to Core Values - Attracts, Develops, and Retains Capable Individuals.

STRATEGY & OBJECTIVE-SETTING
Analyzes Business Context - Defines Risk Appetite - Evaluates Alternative Strategies - Formulates Business - Objectives.

PERFORMANCE
Identifies Risk - Assesses Severity of Risk - Prioritizes Risks - Implements Risk Responses - Develops Portfolio View.

REVIEW & REVISION
Assesses Substantial Change - Reviews Risk and Performance - Pursues Improvement in Enterprise Risk Management.

INFORMATION COMMUNICATION & REPORTING
Leverages Information and Technology - Communicates Risk Information - Reports on Risk, Culture, and Performance.

Source: COSO ERM 2017 - Integrating with Strategy and Performance Executive Summary, April 2017. Page 6.
Available at: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

1. GOVERNANCE AND CULTURE FOR AI-RELATED RISKS

- Map or define the organisation's mandatory or voluntary AI-related requirements.
- Consider opportunities for embedding AI in the organisation's culture and processes.
- Look for ways to increase board awareness of AI-related risks.
- Map the operating structures, risk owners for AI-related risks, reporting lines and ERM and strategic planning process to identify areas for improved oversight and collaboration.
- Create opportunities for collaboration throughout the organisation.
- Embed AI-related skills, capabilities and knowledge in hiring and talent management to promote integration.

2. STRATEGY AND OBJECTIVE-SETTING FOR AI-RELATED RISKS

- Examine the value creation process and business model to understand impacts and dependencies on all capital resources in short, medium and long term. To assist this process, conduct:
  - Megatrend analysis to understand the impact of disruptive new technologies and the linked emerging issues in the external environment
  - Strengths, weaknesses, opportunities and threats (SWOT) analysis
  - Impact and dependency mapping for all types of capital
  - An AI materiality assessment to describe significant AI usage issues
  - Engagement with internal and external stakeholders to understand AI emerging usage trends
  - Analysis of the impact of AI implementation on specific resources
- Throughout the risk management process, align with the organisation strategy, objectives and risk appetite.
- Consider the AI-related risks that will impact the organisation's strategy or objectives.

3. PERFORMANCE FOR AI-RELATED RISKS

3.A. IDENTIFY RISK

- Examine the organisation's risk inventory to determine which AI-related risks have or have not been identified.
- Involve AI risk owners and IT teams in the risk identification process to leverage subject-matter expertise.
- Convene meetings across the organisation with risk management, data scientists, AI users and IT teams to understand AI-related risks.
- Identify the AI-related risks that may impact the organisation's strategic and operational plans.
- Define the impact of AI-related risks on the organisation precisely.
- Use root cause analysis to understand drivers of the risks.

3.B. ASSESS AND PRIORITISE RISK

- Understand the required output of the risk assessment – what is the likely impact in terms of the strategy and business objectives.
- Understand the organisation's criteria for prioritising risks.
- Understand the metrics used by the organisation for expressing risk, qualitative and quantitative.
- Select appropriate assessment approaches to measure risk severity.
- Select and document data, parameters, assumptions, algorithms and open source library usage.
- Leverage subject-matter expertise to prioritise AI-related risks.
- Identify and challenge organisational bias against AI issues.

3.C. IMPLEMENT RISK RESPONSES

- Select an appropriate risk response based on organisation-specific factors such as costs, benefits and risk appetite.
- Develop the business case for the response and obtain buy-in.
- Implement the risk response to manage the risk.
- Evaluate risk responses at organisation level to understand the overall impacts to the risk profile.

4. REVIEW AND REVISION FOR AI-RELATED RISKS

- Identify and assess internal and external changes that could substantively affect the strategy or business objectives.
- Review ERM activities to identify changes to ERM processes and capabilities.
- Pursue improvements in how AI-related risks are managed by ERM.

5. INFORMATION, COMMUNICATION AND REPORTING FOR AI-RELATED RISKS

- Identify relevant channels for internal and external communication and reporting.
- Communicate and report relevant AI-related risk information internally for decision-making.
- Communicate and report relevant AI-related risk information externally to meet regulatory obligations and support stakeholder decision-making.
- Continuously identify opportunities for improving the quality of AI-related data reported internally and externally.
- Provide stakeholders with a communication channel to report any anomaly linked to the use of AI.

3.2. SCOPE OF AI-RELATED RISKS

AI-related risks will vary with the organisation, which may apply its own definitions. However, applying ERM processes to AI-related risks will support the whole organisation in reviewing and identifying extensively where such risks are present.

We have identified 14 themes and 26 key issues:

MACRO RISK CATEGORIES	THEMES AND PROCESSES	AI-RELATED RISK KEY ISSUES
STRATEGIC AND ENVIRONMENTAL RISKS	Governance	AI strategy execution and follow up.
		Organisation and responsibility for AI projects.
		Impacts on stakeholders/ data ecosystem.
		Do employees have the right qualifications and training?
	Data and infrastructure governance	Data quality management.
		Data acquisition: reliability and availability of external data in the long term.
		Infrastructure and security.
	Liability	Automated decision processes are likely to raise new situations where the final responsibility needs to be clarified.
	Environmental impact	High energy consumption.
	Data property/ sovereignty breach	Foreign legislation enabling governments to access cloud suppliers data in contradiction with the GDPR.

BUSINESS RISKS	Product conception	Ethical by design.
	Product production	Human-centric production processes.
	Product distribution	Client information/ freedom of decision/ access to a market open to competition (no monopoly).
	Market disruption	Systemic risk from the same decision processes/ unintended consequences for society.
OPERATIONAL RISK	IT risks: data and Information	Risk of data quality / data governance.
		Risk of unavailability data/ data ownership.
		Risk of data hacking / security.
		Risk of untraceable data/ compliance with the EU General Data Protection Regulation (GDPR).
		Algorithm divergence.
		Maintenance of open source algorithm, dependency on external providers, intellectual property interpretability, transparency and "explicability".
		Storage: cloud or local data lake.
	Organisation and project management	Line of reporting/ common rules.
	Human resources	Risk of losing human expertise.
		Risk for certain roles to become obsolete.
		Risk of lack of competencies.
	Externalisation	Dependency on external providers or specific skills. An alternative plan should always be ready.
	Continuity of activity / recovery plan	Contracts with external partners, especially new players, should ensure continuity of activity by enabling the organisation to run the algorithms and access the codes and data in case the partner stops its activity.