ISRM

AI IN RISK MANAGEMENT
SPECIAL INTEREST GROUP

GLOSSARY: KEY AI TERMS FOR RISK PROFESSIONALS

June 2024

CONTENTS

FOREWORD

A MESSAGE FROM THE GROUP CHAIR

As Chair of the Institute of Strategic Risk Management's Special Interest Group for AI in Risk Management, I have had the pleasure of working with some very talented and experienced professionals, notably the lead author of this glossary, Pauline Norstrom. Pauline, CEO Anekanta AI and a Vice Chair of our group, brings her many years of commercial technology and AI experience to our subject matter, AI in risk management.

In fast-moving environments such as AI, there's a risk that, no sooner than a publication arrives, it's out of date. With that in mind, revisions are likely, and readers should subscribe for updates.

The aim of the AI in Risk Management Special Interest Group is to encourage debate on the use of AI in strategic risk and crisis management. I hope you find this glossary helpful.

Andrew Tollinton
Chair, Co-Founder, SIRV

INTRODUCTION

The deployment of new AI technologies and solutions is rapidly redefining best practice in 21st century strategic risk management. Driven by AI, a new wave of digitalisation across industries is not only revolutionising the efficiency of operational planning, threat detection and management of complex contextual change - it is also revolutionising strategic decision making and enterprise value creation from the ground up.

As at the time of publication, the advent of easily-accessible and scalable Gen AI technologies has already fundamentally shifted the use case for AI integration across business functions for many organisations from being a future-focussed activity to a new strategic imperative. And as demand surges for new and emerging AI-driven solutions to complex organisational problems, it is likewise now a strategic necessity for all those involved in proactively advising on, monitoring and managing strategic risk profiles to have an effective working knowledge of key concepts relating to AI systems.

This glossary is intended to serve as a valuable and practical resource for strategic risk professionals and business executives alike, providing a concise and easily digestible summary of essential concepts and considerations related to AI within the context of organisational decision making and strategic risk management. By ensuring they are equipped with a working knowledge of AI terminology, risk managers across all disciplines can better navigate the complexities and potential risks associated with the adoption and deployment of AI systems.

Ultimately, this glossary aims to serve as a reference guide, offering a digestible summary of key AI terms, use cases, and strategic considerations. As investments AI-driven solutions continues to evolve at a rapid pace, alongside ongoing changes in a global regulatory environment currently best characterised by its uncertainty, the Special Interest Group will continually review and update this publication in line with emerging trends and contextual changes.

This publication therefore represents a first step in the ongoing journey to support risk professionals with practical knowledge on AI integration in risk management, and the insights required to effectively engage with both the opportunities and risks AI technologies bring for their organisations.

SUMMARY: **KEY AI TERMS**

AI SYSTEM

An artificial intelligence system is a computer program designed to simulate human intelligence and perform tasks that typically require human cognitive abilities.

AUTOMATION

Automation refers to the use of technology to perform tasks that were previously done by humans.

AUTONOMOUS

Autonomous refers to the ability of a system to operate independently without human input.

CONTINUOUS LEARNING

Continuous learning refers to the ability of an AI system to improve its performance over time by learning from new data and experiences.

DATA ANNOTATION

Data annotation is the process of labelling data with relevant information to train AI systems. This can involve assigning labels to images, text, or other types of data.

DATA MINING

Data mining is the process of extracting knowledge and insights from large datasets. AI algorithms are often used for data mining tasks to identify patterns, trends, and relationships within the data.

INFERENCE

In AI, inference refers to the process of using a trained AI model to make predictions or classifications based on new data.

INTERNET OF THINGS (IOT)

The Internet of Things (IoT) refers to the network of physical devices embedded with sensors, software, and other technologies that collect and exchange data.

LIFE CYCLE

In AI, the life cycle refers to the different stages involved in developing, deploying, and managing an AI system. This includes stages like data collection, model training, deployment, monitoring, and maintenance.

ROBOT

A robot is a programmable machine that can perform tasks autonomously or with human assistance.

ARTIFICIAL GENERAL INTELLIGENCE

A hypothetical type of artificial intelligence with human-level or surpassing cognitive abilities. An AGI would be capable of learning, adapting, and applying its knowledge across various domains, similar to a human.

NARROW AI

Narrow AI refers to the current state of AI technology, which is focused on performing specific tasks exceptionally well. These tasks are typically well-defined and require specialized knowledge.

EXPERT SYSTEM

An expert system is a computer program that simulates the knowledge and reasoning abilities of a human expert in a specific domain.

BIAS

Bias in AI refers to the tendency of AI systems to favour certain outcomes or make discriminatory decisions based on the data they are trained on, or the algorithms used.

DEEPFAKE

A deepfake is a synthetic media (image, video, or audio) that is manipulated using deep learning techniques to appear authentic. Deepfakes can be used to create realistic portrayals of people doing or saying things they never did.

GLOSSARY: **KEY AI TERMS FOR RISK PROFESSIONALS**

1 AI SYSTEM

Definition: An artificial intelligence system is a computer program designed to simulate human intelligence and perform tasks that typically require human cognitive abilities.

Legal Definition: "An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment."

This the definition of an AI system utilised within the OECD AI Principles framework adopted in May 2019. The definition has since been written into law in the EU AI Act as the only legal definition of AI in the world.

It is important to understand that an AI system may comprise a number of AI techniques used together to achieve the purpose for example, it may be a software platform which utilises Generative AI and machine learning techniques together in order to fulfil a goal.

Use case: AI systems are used in various applications, including fraud detection, medical diagnosis, facial recognition, and self-driving cars.

Strategic Opportunity: AI systems can automate tasks, improve decision-making, and generate new insights from data.

Key Risk Considerations:

Strategic	Over-reliance on AI, lack of transparency in decision-making, and job displacement.
Financial	Investment costs, maintenance, and potential for misuse leading to financial losses.
Reputation	Bias in AI systems can damage an organisation's reputation.
Operational	System failures, security breaches, and lack of control over AI behavior.
Legal/Regulatory	Compliance with data privacy laws, AI regulations, and potential liability for AI actions.

2 AUTOMATION

Definition: Automation refers to the use of technology to perform tasks that were previously done by humans.

Use case: Automation is used in manufacturing, customer service, data processing, and other industries.

Strategic Opportunity: Increased efficiency, reduced costs, and improved accuracy.

Key Risk Considerations:

Strategic	Job displacement, skills gap, and potential for human error in designing and implementing automation.
Financial	Investment costs, maintenance, and potential for downtime.
Reputation	Concerns about job losses and lack of human interaction can damage reputation.
Operational	System failures, technical glitches, and the need for human oversight.
Legal/Regulatory	Compliance with employment laws and regulations related to workplace automation.

3 AUTONOMOUS

Definition: Autonomous refers to the ability of a system to operate independently without human input.

Use case: Autonomous robots, self-driving cars, and intelligent drones.

Strategic Opportunity: Increased efficiency, ability to operate in hazardous environments, and potential for new applications.

Key Risk Considerations:

Strategic	Safety concerns, lack of control over autonomous systems, and ethical considerations.
Financial	Liability for accidents or damages caused by autonomous systems.
Reputation	Public perception of autonomous systems and potential for misuse.
Operational	System malfunctions, security vulnerabilities, and the need for robust safety measures.
Legal/Regulatory	Developing legal frameworks to govern the use of autonomous systems.

4 CONTINUOUS LEARNING

Definition: Continuous learning refers to the ability of an AI system to improve its performance over time by learning from new data and experiences.

Use case: This allows AI systems to adapt to changing environments and improve their accuracy in tasks like fraud detection or medical diagnosis.

Strategic Opportunity: Improved performance and adaptability of AI systems.

Key Risk Considerations:

Strategic	Potential for AI systems to learn and adopt biases present in the data they are trained on.
Financial	Costs associated with ongoing data collection and training.
Reputation	Concerns about the 'unknowns' of continuously learning AI systems and potential for unintended consequences.
Operational	Ensuring data quality and security for ongoing learning processes.
Legal/Regulatory	Compliance with data privacy laws regarding data used for continuous learning.

5 DATA ANNOTATION

Definition: Data annotation is the process of labelling data with relevant information to train AI systems. This can involve assigning labels to images, text, or other types of data.

Use case: Data annotation is crucial for tasks like image recognition, sentiment analysis, and machine translation.

Strategic Opportunity: Improves the accuracy and effectiveness of AI systems.

Key Risk Considerations:

Strategic	Bias can be introduced into AI systems if the data used for annotation is biased.
Financial	Costs associated with hiring human annotators or using specialised annotation tools.
Reputation	Concerns about data privacy and potential misuse of data used for annotation.
Operational	Ensuring the quality and consistency of data annotations.
Legal/Regulatory	Compliance with data privacy laws regarding the collection and use of data for annotation.

6 DATA MINING

Definition: Data mining is the process of extracting knowledge and insights from large datasets. AI algorithms are often used for data mining tasks to identify patterns, trends, and relationships within the data.

Use case: Data mining is used in various applications, including:

1. Fraud detection: Analysing patterns in financial transactions to identify suspicious activity.
2. Customer segmentation: Grouping customers based on shared characteristics to personalise marketing campaigns.
3. Market research: Identifying trends and customer preferences to inform product development and marketing strategies.
4. Scientific discovery: Uncovering new knowledge from large datasets in fields like genomics and astronomy.

Strategic Opportunity: Uncovers hidden patterns and trends in data that can be used to:

1. Improve decision-making across the organisation.
2. Identify new opportunities for revenue generation or cost savings.
3. Gain a deeper understanding of customers, markets, and operations.

Key Risk Considerations:

Strategic	Focus on correlations over causations leading to misleading insights. For example, a correlation between ice cream sales and shark attacks doesn't imply a causal relationship. Overlooking the "human element" and relying solely on data-driven insights.
Financial	Costs associated with data storage, processing, and AI algorithms used for mining. Potential for wasted resources if data mining projects are not well-defined or don't yield valuable insights.
Reputation	Concerns about data privacy and potential misuse of information discovered through data mining. Transparency is crucial to building trust.
Operational	Ensuring data quality and security throughout the mining process. Dirty or inaccurate data can lead to flawed insights. The need for skilled data analysts and data scientists to interpret the results effectively.
Legal/Regulatory	Compliance with data privacy laws regarding the collection, storage, and analysis of data.

7 INFERENCE

Definition: In AI, inference refers to the process of using a trained AI model to make predictions or classifications based on new data.

Use case: Inference is used in various applications, like spam filtering, image recognition, and loan approvals.

Strategic Opportunity: Enables real-time decision-making and automation based on AI insights.

Key Risk Considerations:

Strategic	Bias in the training data can lead to biased inferences made by the AI model.
Financial	Costs associated with deploying and maintaining AI models for inference.
Reputation	Concerns about the fairness and transparency of AI-driven inferences, especially when used for high-stakes decisions.
Operational	Ensuring the accuracy, reliability, and 'explainability' of inferences made by the AI model.
Legal/Regulatory	Compliance with regulations related to fairness and non-discrimination in AI-powered decision-making.

8 INTERNET OF THINGS (IOT)

Definition: The Internet of Things (IoT) refers to the network of physical devices embedded with sensors, software, and other technologies that collect and exchange data.

Use case: IoT is used in various applications, including smart homes, industrial automation, and connected healthcare devices.

Strategic Opportunity: Improves efficiency, automates tasks, and generates valuable data for further analysis.

Key Risk Considerations:

Strategic	Safety concerns, lack of control over autonomous systems, and ethical considerations.
Financial	Liability for accidents or damages caused by autonomous systems.
Reputation	Public perception of autonomous systems and potential for misuse.
Operational	System malfunctions, security vulnerabilities, and the need for robust safety measures.
Legal/Regulatory	Developing legal frameworks to govern the use of autonomous systems.

9 LIFE CYCLE

Definition: In AI, the life cycle refers to the different stages involved in developing, deploying, and managing an AI system. This includes stages like data collection, model training, deployment, monitoring, and maintenance.

Use case: Understanding the life cycle helps ensure a successful and responsible implementation of AI.

Strategic Opportunity: Provides a framework for managing AI systems effectively and mitigating risks.

Key Risk Considerations:

Strategic	Neglecting certain stages of the life cycle can lead to issues like bias or security vulnerabilities.
Financial	Costs associated with each stage of the AI life cycle, from development to ongoing maintenance.
Reputation	Poor management of the AI life cycle can damage an organisation's reputation.
Operational	Ensuring smooth transitions between stages of the life cycle and addressing potential issues throughout.
Legal/Regulatory	Compliance with regulations that may apply to different stages of the AI life cycle (e.g., data privacy during development).

10 ROBOT

Definition: A robot is a programmable machine that can perform tasks autonomously or with human assistance.

Use case: Robots are used in various applications, including manufacturing, logistics, surgery, and exploration.

Strategic Opportunity: Increases efficiency, productivity, and safety in various tasks.

Key Risk Considerations:

Strategic	Job displacement due to automation, and potential for misuse of robots.
Financial	Costs associated with purchasing, maintaining, and programming robots.
Reputation	Safety concerns about robots and potential for negative public perception.
Operational	Ensuring the safe and reliable operation of robots.
Legal/Regulatory	Compliance with regulations related to workplace safety and potential liability for robot actions.

11 ARTIFICIAL GENERAL INTELLIGENCE (AGI)

Definition: A hypothetical type of artificial intelligence with human-level or surpassing cognitive abilities. An AGI would be capable of learning, adapting, and applying its knowledge across various domains, similar to a human.

Use case: AGI has the potential to revolutionise numerous fields, from scientific discovery and complex problem-solving to automating various tasks currently requiring human expertise.

Strategic Opportunity:

Strategic	AGI could significantly enhance decision-making, leading to strategic advantages and increased efficiency.
Financial	Automating complex financial tasks, improving accuracy, and generating insightful reports.
Operational	Streamlining operations across various departments and optimizing resource allocation.

Key Risk Considerations:

Strategic	Over-reliance on AGI for decision-making could lead to unforeseen risks and reduced human oversight.
Financial	Potential job displacement due to automation, necessitating workforce retraining.
Reputation	Ethical concerns and potential misuse of AGI could damage public trust and brand reputation.
Operational	Malfunctioning or biased AGI could disrupt operations and lead to costly errors.
Legal/Regulatory	Uncertain legal frameworks around liability and responsibility for actions taken by AGIs.

12 NARROW AI (Artificial Narrow Intelligence)

Definition: Narrow AI refers to the current state of AI technology, which is focused on performing specific tasks exceptionally well. These tasks are typically well-defined and require specialised knowledge.

Use case: Narrow AI is used in various applications like facial recognition, spam filtering, and self-driving cars (limited to specific environments).

Strategic Opportunity: Improves efficiency, accuracy and automation in various domains.

Key Risk Considerations:

Strategic	Over-reliance on narrow AI and neglecting the broader implications of AI development.
Financial	Costs associated with developing, deploying, and maintaining narrow AI systems.
Reputation	Concerns about bias in narrow AI systems and potential misuse.
Operational	Ensuring the reliability and 'explainability' of narrow AI outputs.
Legal/Regulatory	Compliance with regulations that may apply to specific narrow AI applications (e.g., facial recognition).

13 EXPERT SYSTEM

Definition: An expert system is a computer program that simulates the knowledge and reasoning abilities of a human expert in a specific domain.

Use case: Expert systems are used in various applications, including medical diagnosis, financial planning, and legal reasoning.

Strategic Opportunity: Provides access to expert knowledge and facilitates decision-making in complex situations.

Key Risk Considerations:

Strategic	Limited scope and inability to adapt to new situations compared to general AI.
Financial	Costs associated with developing and maintaining expert systems.
Reputation	Reliance on expert systems can lead to overconfidence and neglecting human expertise.
Operational	Ensuring the accuracy and 'up-to-dateness' of knowledge within the expert system.
Legal/Regulatory	Compliance with regulations that may apply to the specific domain of the expert system (e.g., medical diagnosis).

14 BIAS

Definition: Bias in AI refers to the tendency of AI systems to favour certain outcomes or make discriminatory decisions based on the data they are trained on, or the algorithms used.

Use case: Bias can manifest in various ways, from biased facial recognition algorithms to loan approval systems.

Strategic Opportunity: There's an opportunity to develop fairer and more unbiased AI systems through careful data selection, algorithm design, and ongoing monitoring.

Key Risk Considerations:

Strategic	Biased AI systems can perpetuate societal inequalities and lead to discriminatory outcomes.
Financial	Costs associated with mitigating bias and potential legal repercussions.
Reputation	Public backlash and loss of trust if AI systems are perceived as biased.
Operational	Ensuring the fairness and transparency of AI decision-making processes.
Legal/Regulatory	Compliance with anti-discrimination laws and regulations that may apply to AI development and deployment.

15 DEEPFAKE

Definition: A deepfake is a synthetic media (image, video, or audio) that is manipulated using deep learning techniques to appear authentic. Deepfakes can be used to create realistic portrayals of people doing or saying things they never did.

Use case: Deepfakes have potential applications in entertainment and education but can also be used for malicious purposes like disinformation campaigns.

Strategic Opportunity: Deepfakes can be used for creative storytelling and educational purposes.

Key Risk Considerations:

Strategic	Potential for deepfakes to be used to spread misinformation and manipulate public opinion.
Financial	Costs associated with creating and detecting deepfakes.
Reputation	Damage to reputations of individuals targeted by deepfakes.
Operational	Challenges in detecting and mitigating the spread of deepfakes.
Legal/Regulatory	Developing legal frameworks to address the misuse of deepfakes.

ABOUT US

ISRM AI IN RISK MANAGEMENT SPECIAL INTEREST GROUP

Andrew Tollinton
Group Chair

Co-Founder, SIRV
London, United Kingdom

Pauline Norstrom
Co-Chair

CEO, Anekanta AI
London, United Kingdom

Hart Brown
Co-Chair

CEO, Future Point of View
Oklahoma City, United States

Mads Paerregaard
Committee Member

CEO, Human Risks
Aalborg, Denmark

Piotr Senkus
Committee Member

Professor, University of Warsaw,
Warsaw, Poland

Douglas Gray
Committee Member

Strategic Risk Consultant
Paris, France

ISRM ABOUT THE INSTITUTE OF STRATEGIC RISK MANAGEMENT (ISRM)

The Institute of Strategic Risk Management (ISRM) is a leading global centre for the promotion and sharing of best-practice strategic risk and crisis management capabilities and thought leadership amongst practitioners, academics, and policy makers.

Across the Institute's global chapter network, our members and fellows help progress and promote the underlying understanding and capabilities associated with strategic risk and crisis management, alongside developing their own personal and professional networks.

The ISRM provides best-practice training, hosts leading events across its global and local networks, and provides strategic advice to support organisations' management of complex risks.

ISRM

www.isrm.org