AI GOVERNANCE

Stefania Lauciello, BSIDES, Dublin, May 24th, 2025

DISCLAIMER

The views and opinions expressed in these slides are those of the presenter and do not necessarily reflect the views of BSIDES or any other company or organisation.

http://linkedin.com/in/stefania-lauciello-b191921a

WHO AM I

- 20 years' experience in ICT Audit, Governance, Risk, Compliance
- CISA, CRISC, CISM certified
- Undertaking a Diploma in Advanced Banking Risk Management with the Institute of Banking
- Chair of nonprofit Intercultural Language School
- Director of Cyber for Schoolgirls
- Committee Member of Swimming Club
- Mother and wife
- I love travelling and swimming

AGENDA

- **Background** of NIST AI RMF
- **AI Risks**
- **NIST AI Risk Management Framework (RMF)**
- **Key Components of the** Framework
- **Case Study**

AI Generated Image

BACKGROUND

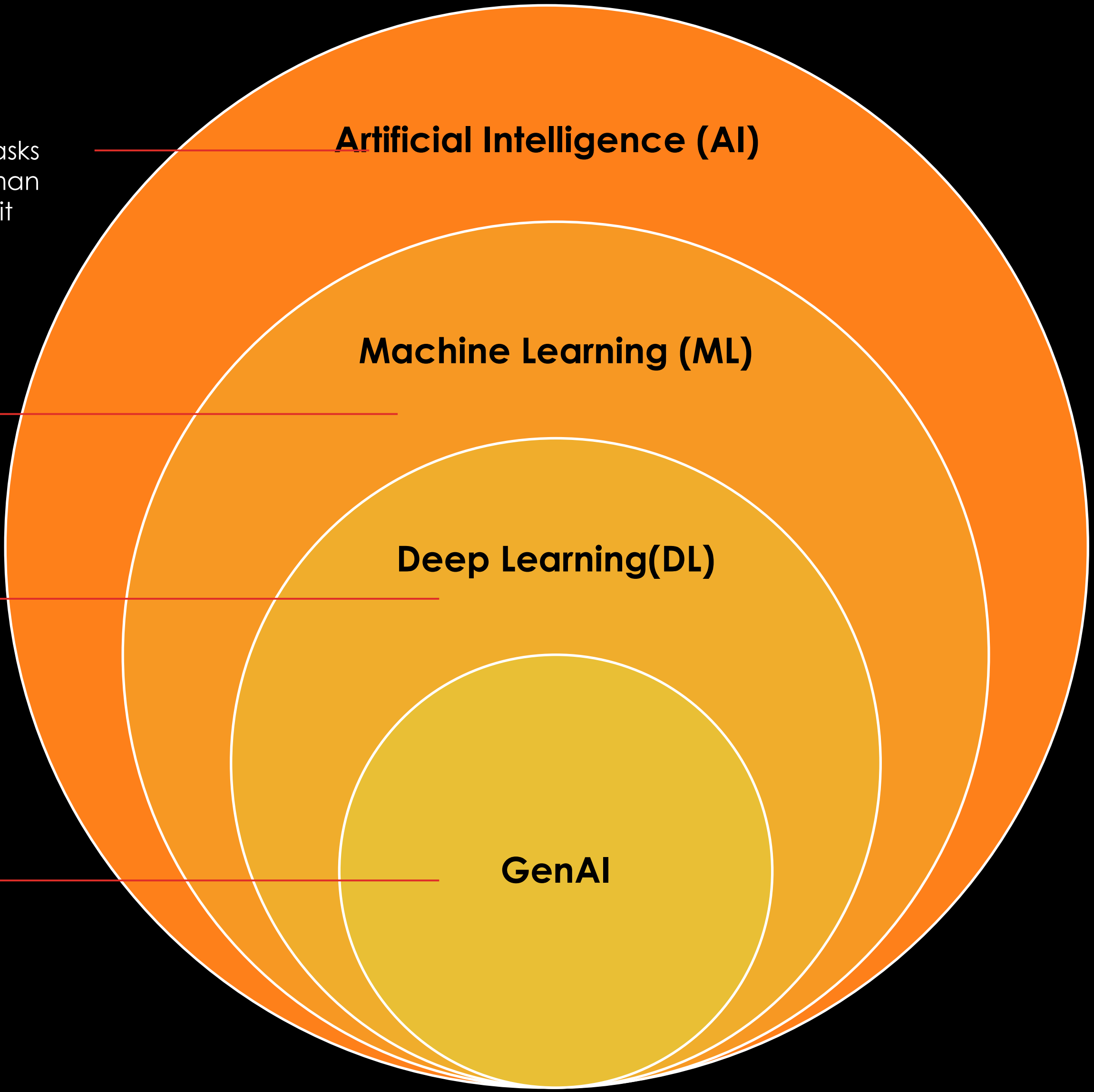
- NIST developed the AI RMF 1.0 in 2023
- It is the result of collaboration among private companies, government agencies, academia and non-profit organisations
- Increases TRUST in AI technology
- Helps to Mitigate AI risks

AI Generated Image

> “A BRANCH OF COMPUTER SCIENCE DEVOTED TO DEVELOPING DATA PROCESSING SYSTEMS THAT PERFORM FUNCTIONS NORMALLY ASSOCIATED TO HUMAN INTELLIGENCE, SUCH AS REASONING, LEARNING, AND SELF-IMPROVEMENT”

NIST Definition of AI

AI, ML, DL, GENAI



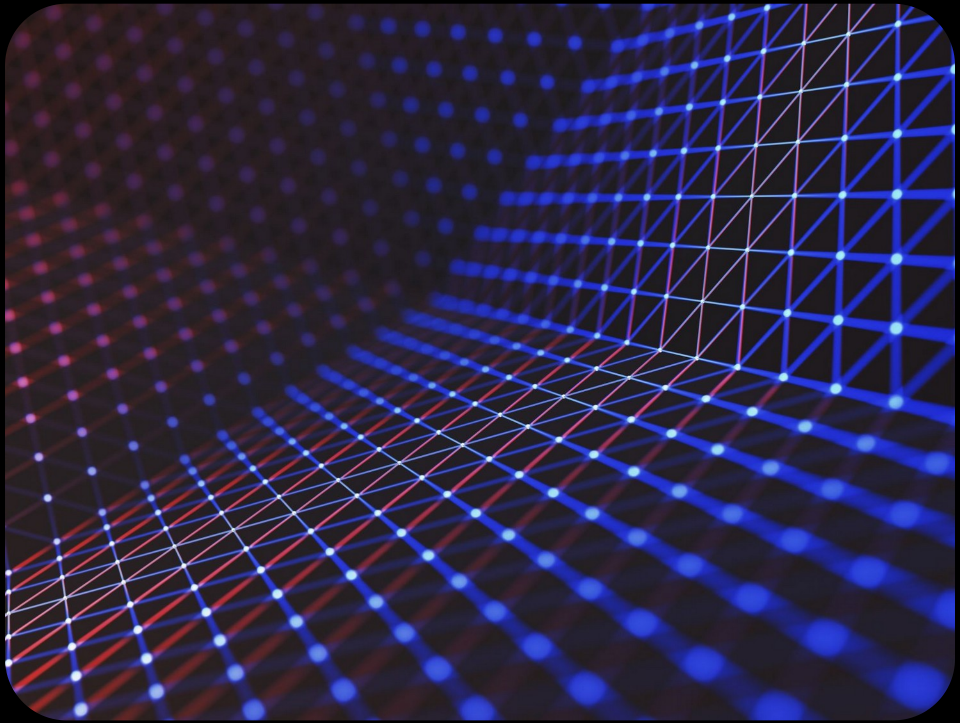
Data Processing System capable of performing tasks that typically require human intelligence, detect credit card frauds

Branch of AI that teaches computers to learn from data and automatically improves over time, like a child it learns based on what it sees/training data, e.g. credit scoring tool

Subset of ML that uses neural networks (multiple layer connections) complex algorithms to handle complex problems, e.g. face recognition tools

Generates new contents using AI, analyses huge amount of date to produce a new content, e.g. ChatGPT

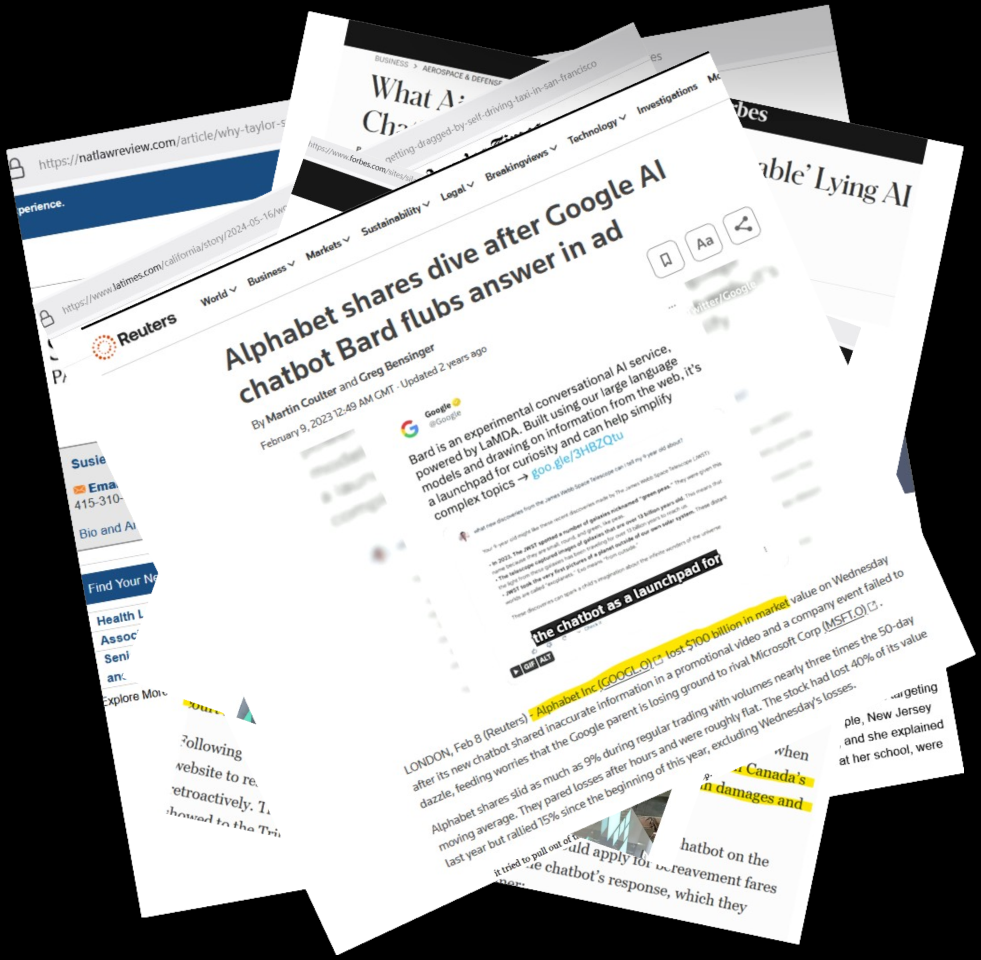
IMPORTANCE OF AI



- Impacting every sector
- Enhancing Risk Management, Fraud Detection
- Improving Cyber Security & Threat Detection
- Increasing Operational Efficiency & Automation
- Personalised and Automated Customer Support
- Increasing Demand for AI Risk Governance Skills

WHY AI RISK MANAGEMENT?

Real Life AI Incidents



https://natlawreview.com/article/why-taylor-s
https://www.latimes.com/california/story/2024-05-16/w
https://www.forbes.com/sites/
getting-dragged-by-self-driving-taxi-in-san-francisco
What A
Ch
rbes
able' Lying AI
Reuters
World
Business
Markets
Sustainability
Legal
Breakingviews
Technology
Investigations
Susie
Email
415-310-
Bio and A
Find Your Ne
Health L
Assoc
Seni
an
Explore More

Alphabet shares dive after Google AI chatbot Bard flubs answer in ad

By Martin Coulter and Greg Bensinger

February 9, 2023 12:49 AM GMT · Updated 2 years ago

Google @Google

Bard is an experimental conversational AI service, powered by LaMDA. Built using our large language models and drawing on information from the web, it's a launchpad for curiosity and can help simplify complex topics → goo.gle/3HBZQtu

the chatbot as a launchpad for

LONDON, Feb 8 (Reuters) - Alphabet Inc (GOOGL.O) lost $100 billion in market value on Wednesday after its new chatbot shared inaccurate information in a promotional video and a company event failed to dazzle, feeding worries that the Google parent is losing ground to rival Microsoft Corp (MSFT.O).

Alphabet shares slid as much as 9% during regular trading with volumes nearly three times the 50-day moving average. They pared losses after hours and were roughly flat. The stock had lost 40% of its value last year but rallied 15% since the beginning of this year, excluding Wednesday's losses.

Following
website to re
retroactively. T
showed to the Tri

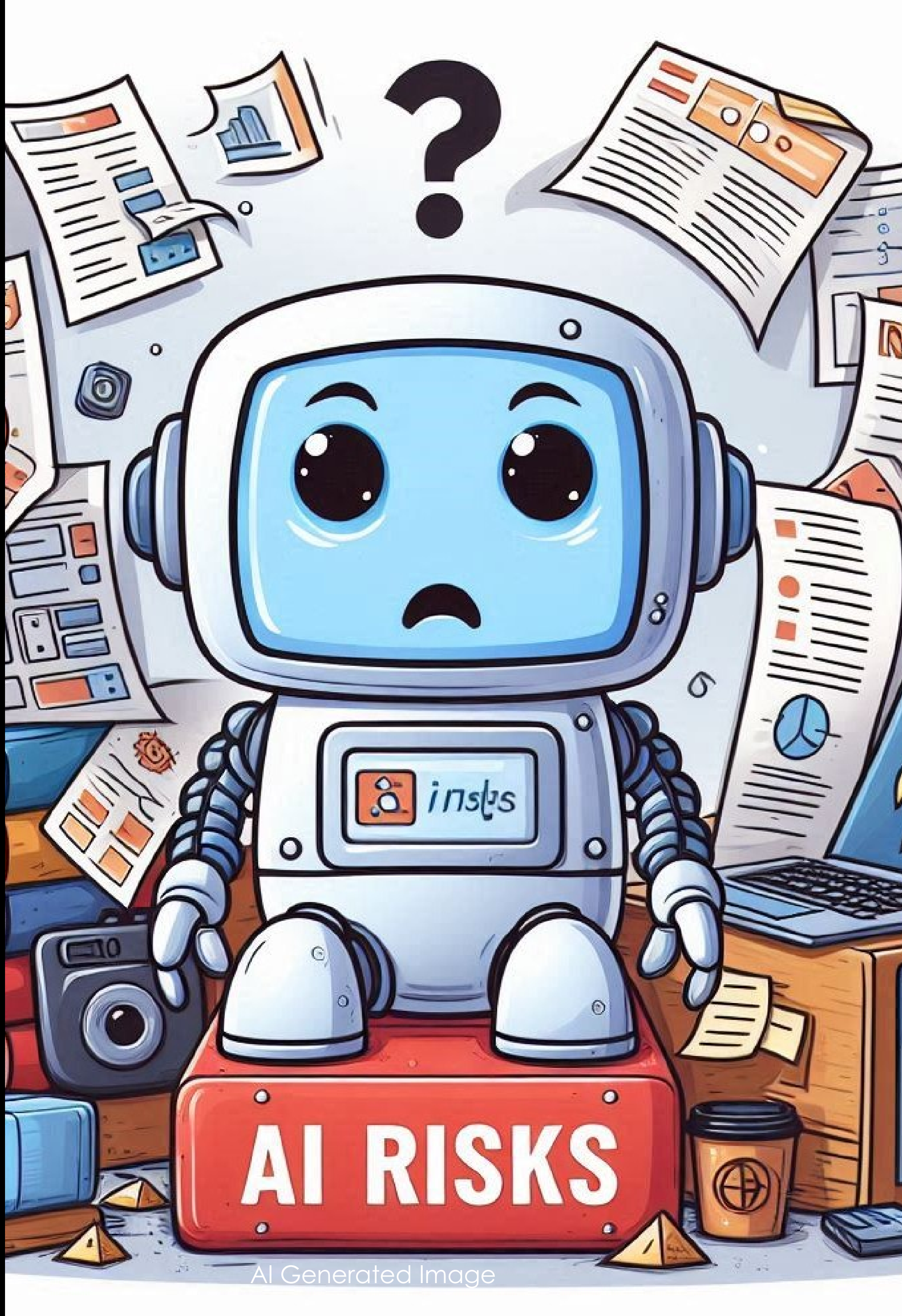
when
Canada's
in damages and
hatbot on the
uld apply for bereavement fares
e chatbot's response, which they
it tried to pull out of t

targeting
ple, New Jersey
, and she explained
at her school, were

AI Generated Image

AI RISKS

- Ethical Risk (Bias & Discrimination)
- Governance Risk (Lack of Transparency & Accountability)
- Concentration Risk
- Operational Risks (Model inaccuracy, automation failures)
- Regulatory & Legal Risk
- Credit Risk
- Strategic Risk (Misguided Strategies & Risk Assessments)
- Cybersecurity Risks
- Reputation Risk
- Environmental Risk

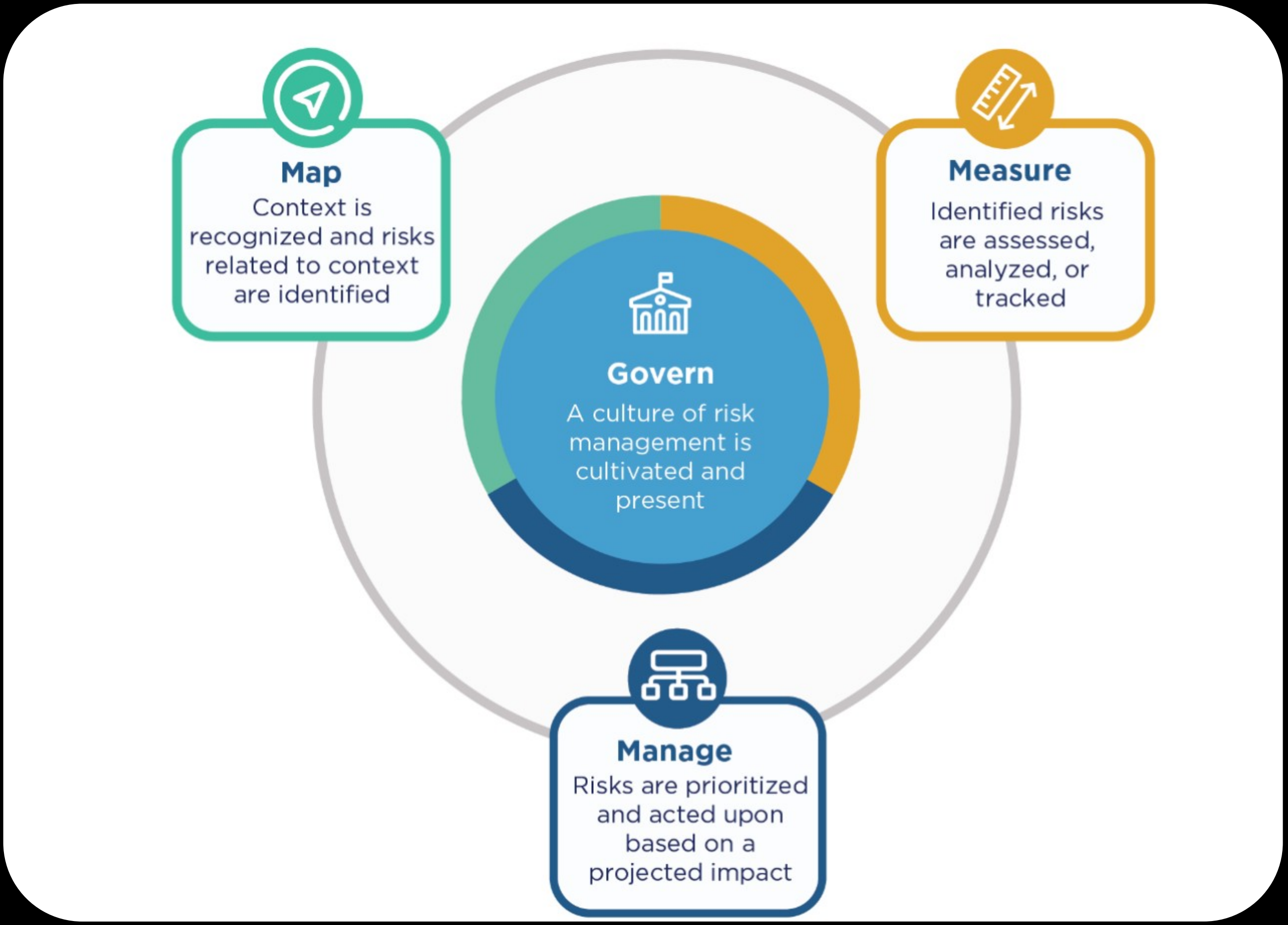


AI Generated Image

NIST AI RMF CORE

Technology Agnostic

Vendor Agnostic



Map
Context is recognized and risks related to context are identified

Measure
Identified risks are assessed, analyzed, or tracked

Govern
A culture of risk management is cultivated and present

Manage
Risks are prioritized and acted upon based on a projected impact

Data source: NIST AI RMF

GOVERN AI

1. Include the AI in the ICT RMF
2. Document an AI strategy, policy, standards and procedures
3. Raise awareness with AI customised training
4. Define roles and responsibilities
5. Document a governance structure

AI Generated Image

MAPPING

INVENTORY OF AI SYSTEMS AND TOOLS

DOCUMENT THE WHY, WHAT, WHEN, WHERE AND WHO

IDENTIFY THE BENEFITS OF EACH AI SYSTEM/TOOL

MEASURE AI RISKS

1. Determine a Risk Assessment Methodology
2. Risk Assess each AI system/tool
3. Define and Measure KRIs and KPIs
4. Continuous Monitoring of risk exposures
5. Review and Update your methodology and results when needed

AI Generated Image

MANAGING AI RISKS

1. Document Risk Mitigation Plans for risks exceeding the risk appetite
2. Monitor and Report on the progress of the RMP
3. Regular Review and Adjustment of Risks
4. Update existing policy and methodology based on lessons learned

AI Generated Image

CASE STUDY

Company Infinity decides to implement the NIST AI RMF to enhance their risk management around AI.

1. Infinity organises workshops and **training** around the NIST AI RMF
2. A **sponsor** from senior management is identified, e.g. CEO
3. The **ICT RMF** is updated to include AI and **AI strategy, policy, standards** and **procedures** are **documented**
4. **An organisational structure for AI is defined,** roles and responsibilities
5. The risk or IA function organise corroborative interviews with developers and representative of all departments to **map all existing AI systems and tools – AI inventory**
6. The risk function defines a methodology for AI risk assessment and **start documenting risks for each AI systems/tools** in the AI inventory
7. The risk function together with the AI system owners and/or risk owner develop **KRIs**. The AI system owners develop **KPIs**. Metrics are **reported** to the relevant committees/stakeholders.
8. **Risk Mitigation Plans** are documented and reported for risks exceeding Infinity's risk appetite.
9. The process and documentation are enhanced based on lessons learned.

OUTCOMES FOR THE FIRM

INCREASED TRUST

IMPROVED RISK MANAGEMENT

COMPLIANCE

STRATEGIC USE OF AI

INCREASED OPERATIONAL RESILIENCE

AI Generated Image

THANK YOU

http://linkedin.com/in/stefania-lauciello-b191921a