*HELPING ORGANISATION SURVIVE AND THRIVE……*

# Navigating the Unknown: A Webinar on 2024 Risk Landscape and Risk Management Strategies

May 2024

# About Us

**GRC Partners Asia Sdn Bhd**, incorporated in 2011, our office is strategically located at the bustling Amcorp Trade Centre in Petaling Jaya, Malaysia. As a trusted SAI360 Partner for over a decade, we have honed our expertise in critical domains such as Governance, Risk, and Compliance (GRC), Environmental Health and Safety (EHS), and Sustainability. Our team comprises 20 dedicated SAI360 Consultants, distributed across Malaysia (7), Singapore (3), and India (10). These seasoned professionals bring a wealth of experience in SAI360 project implementation and ongoing support.

Our commitment extends to serving Malaysia's prominent Government-Linked Companies (GLCs), including Tenaga Nasional Berhad (TNB), Permodalan Nasional Berhad (PNB), and the National Heart Institute (IJN). With a strong local presence, we foster close relationships with our valued clients, ensuring that their needs are met with precision and excellence.

**We are resellers/partner with SAI360** is an international SaaS/cloud-based platform that provides governance, risk and compliance (GRC) solutions for various industries and sectors, on a **rapid deployment** method.

It helps organisations to manage and broaden their risk horizon, adapt to changing business eco-system, improve transparency and accountability, improve their performance, and create a culture of ethics and integrity. This helps monitoring the different kinds of organisations to do things the right way, avoid problems, follow rules and do better.

# Panelist

Tanay Ghosal,

Head- GRC Solution,

GRCPA

Dr. Nurmazilah MAHZAN,

Independent Non-Executive Director,

TH Plantation Berhad

Alvin Shi Chee Chin,

Head – BCM ,

Time dotcom Berhad

# Webinar Overview

**Topics**:

- ❑ Emerging Risk and Stress Testing.
- ❑ Technology Risk Insights and Cybersecurity Insurance.
- ❑ GEN AI – Usage and its challenges.

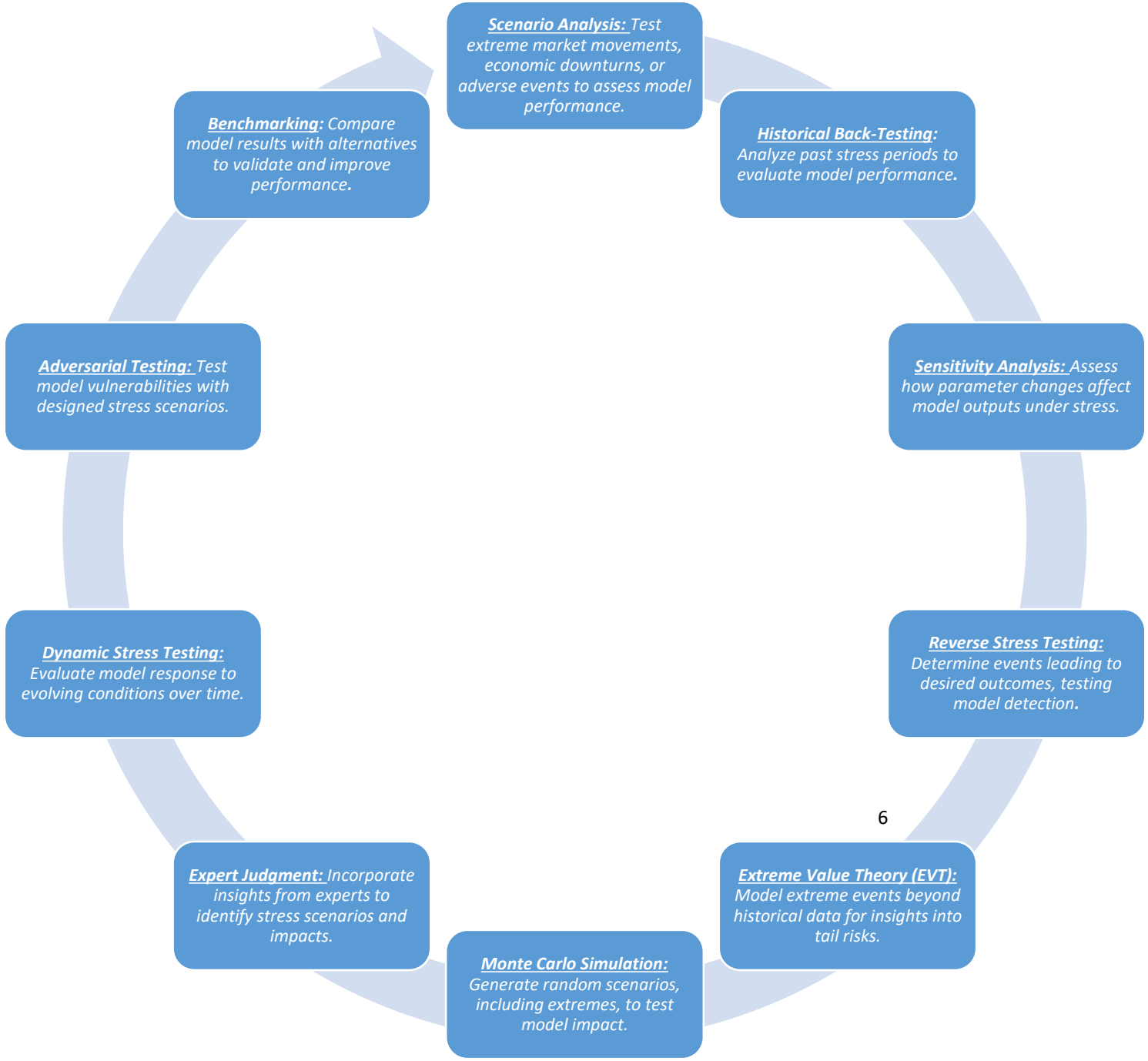
**Date**: May 17th, 2024
**Format**: Online
**Duration**: Panel discussion approximately 1.15 hour

# Emerging RISK

**Current Risk Scenarios**

| High Impact | Medium Impact | Low Impact |
| --- | --- | --- |
| • Cybersecurity threats.<br>• Social unrest and demographic shifts - Supply chain disruptions.<br>• Economic volatility.<br>• Climate change impacts | • Political instability.<br>• Technological disruption.<br>• Regulatory changes.<br>• Environnemental dégradation. | • Emerging infectious diseases<br>• ESG Disclosures.<br>• Labor and Migration |

# Stress Testing: Best ways



# TECHNOLOGY RISK MANAGEMENT

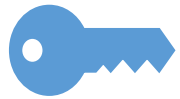
**SUBTOPICS**

***1. What is Technology Risk Management ?***

***2. What are the current risk landscapes and scenarios?***

***3. 2024 Technology Risk Focus in Malaysia***

***4. Cybersecurity Risk and its insurance (Key points to note before activating a cyber sec insurance)***



***5. Key Areas in Technology Risk areas that is often overlooked***

# *Understanding Technological Risk*

## Clearing up Confusion

People often misconstrue the scope of technology risk management, sometimes confusing it with only cybersecurity, while it encompasses a broader range of technological challenges

### Technology Risk = Cybersecurity Risk

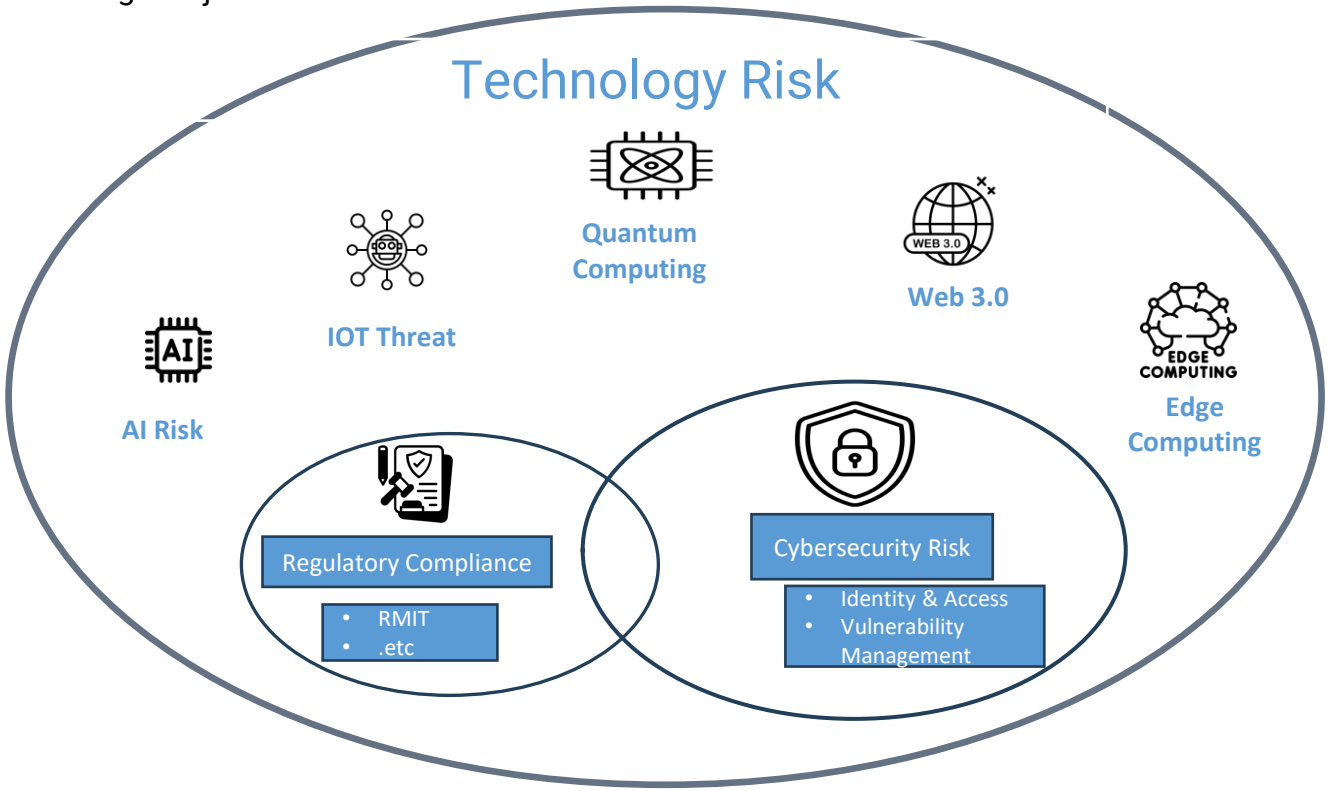
Many misunderstand that cyber-security risk represents entirely on technology risk , but it's just one facet in a complex landscape of technology risk

### Technology Risk = Regulatory Compliance

Meeting regulatory compliance alone doesn't necessarily mitigate all technology risk, it's a step but comprehensive Risk Management is essential

## What is Technology Risk

Technology Risk refers to potential threats, vulnerabilities or disruptions associated with the use of technology, which may impact an organization's operations, finances or strategic objectives



# 2024 Technology Risk Focus in Malaysia

## Rapid Digital Transformation

Malaysia’s aggressive expansion, supported by substantial RM 393.8 billion budget, risk accruing technology debts and challenges in ensuring nationwide tech readiness to sustainably manage and integrate new technology

## Geopolitical Risk

The interplay of geopolitical factors with Malaysia's tech advancements may introduce risk related to international trade tensions & political instability, affecting technology imports, investment and collaboration

## Regulatory Compliance

The upcoming cybersecurity bill by NACSA, to be tabled in early 2024, and the strengthening of the Personal Data Protection act highlight the legislative efforts to mitigate risk related to cyber threats and data breaches in an increasingly digital society

# *Key Areas in Technology Risk areas that is often overlooked*

## Risk Mitigation priorities for the next 12 months (top five)

- Digital and Technology Risk
- Macroeconomic volatility
- Inflation
- Geopolitical risk
- Cyber risks

❖ Risk Mitigation Strategy

Adapt a unified strategy in tech risk mitigation to align spending with value creation and integrate solutions with overreaching business goals

❖ Technology Risk Management

Transition from reactive to proactive risk management by enabling technology and industry collaboration

❖ Third Party Risk

Establish a comprehensive third-party management framework that encompasses not only security but also operational, financial, and other risk for holistic overview

❖ Awareness Program

Revamp cyber awareness program to include diverse, role specific training beyond phishing, tailored to modern threats and learning styles

❖ Cyber Insurance

Clarify Cyber Insurance coverage and its role ; it's a financial safeguard , not a complete risk mitigation strategy and does not restore reputation post incident

# A Deep Dive into the latest Cyber Attack Landscape

**8**
**Most breached country in Q3 2023**

**50 %**
**Increase in Cyber Attack**

**15**
**Reported cases a week (data breaches)**

**494 K**
**Leaked Accounts**

**144 %**
**Higher breach rate in Q3 2023 as compared to Q2 2022**

**50 %**
**Increase in Online Crime**

## Nation-State Cyber Warfare

Cyber operations by nation-states are expected to increase, particularly targeting crucial sectors such as critical infrastructure potentially resulting in both online and offline impacts.

## AI and Machine Learning Poisoning

Cyberattacks that compromise AI and machine learning systems through tactics like data tampering and steaking algorithms could weaken trustworthiness of AI-dependent security and decision-making processes.

## Ransomware Evolution

Ransomware continues to be a significant danger, evolving in sophistication and complexity. Cybercriminals are using advanced social engineering methods that are tougher to identify and defend against. There is a shift towards the formation of more structured ransomware groups that work together to increase the effectiveness of their attacks.

## Mobile Device Vulnerability

The growing reliance on mobile device in daily life is likely to draw more attention from cybercriminals, resulting in a rise of malware and attacks tailored to mobile technology

## Zero Click Exploits

The growing reliance on mobile device in daily life is likely to draw more attention from cybercriminals, resulting in a rise of malware and attacks tailored to mobile technology

# Navigating the Cyber Insurance Maze

## Benefits of Cyber Insurances

Financial Protection

Business Continuity

Expert Support

## Concern on Cyber Insurances

Not Comprehensive

False Security

Reputation Damage

## Coverage Areas

### First Party Coverage

Direct Losses to the organization including data losses, extortion and theft

### Third Party Coverage

Claims by others against the organization, such as privacy lawsuits and regulatory fines

## Areas to Take Note

Understand the Exclusion

Assess the coverage limits

Incident Response Time

Invest in Preventive Measures

## Call to Action

Review Cyber Risk Profile

Consult with Insurance Experts

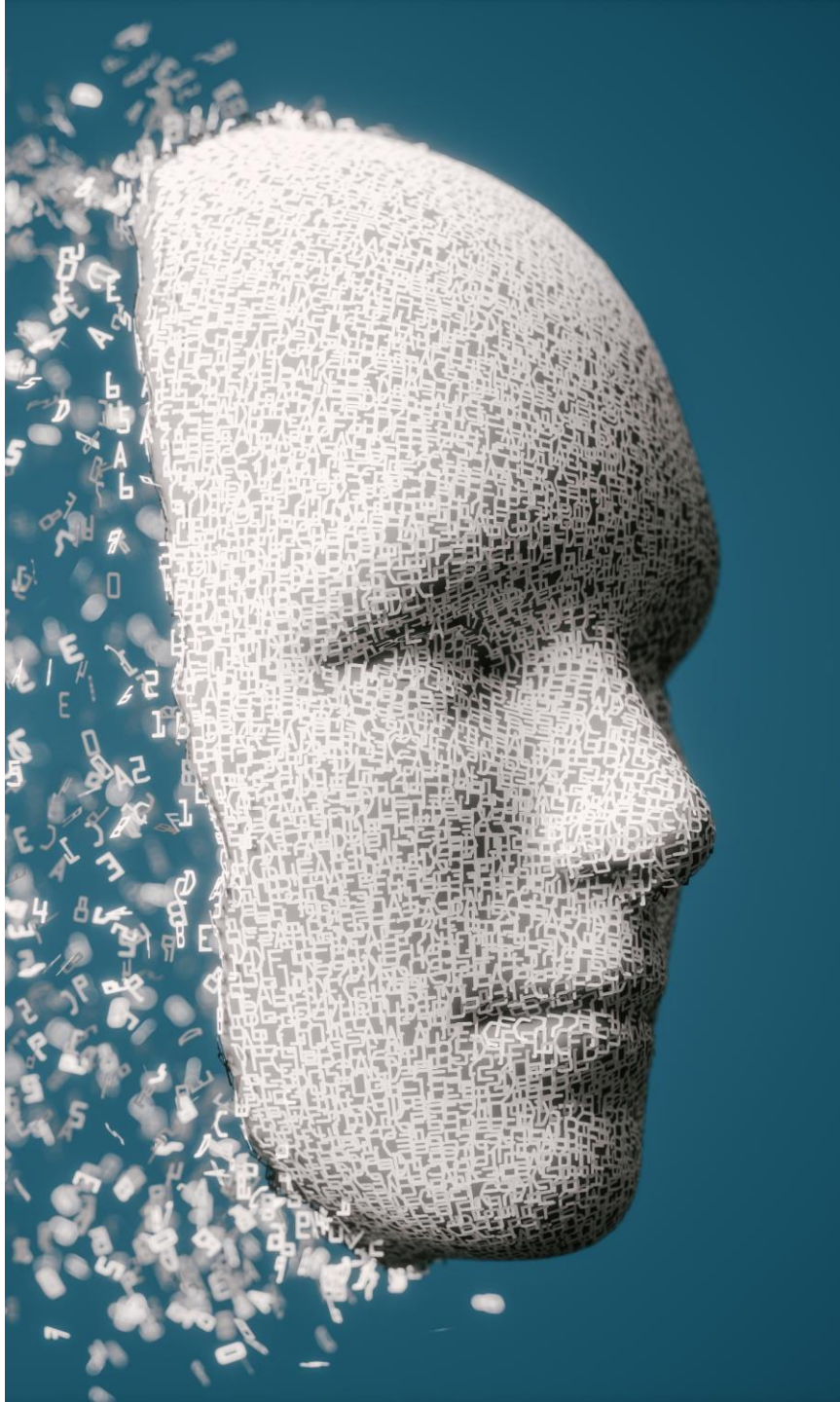
Integration with overall Risk Mitigation Plan

# *Generative AI*

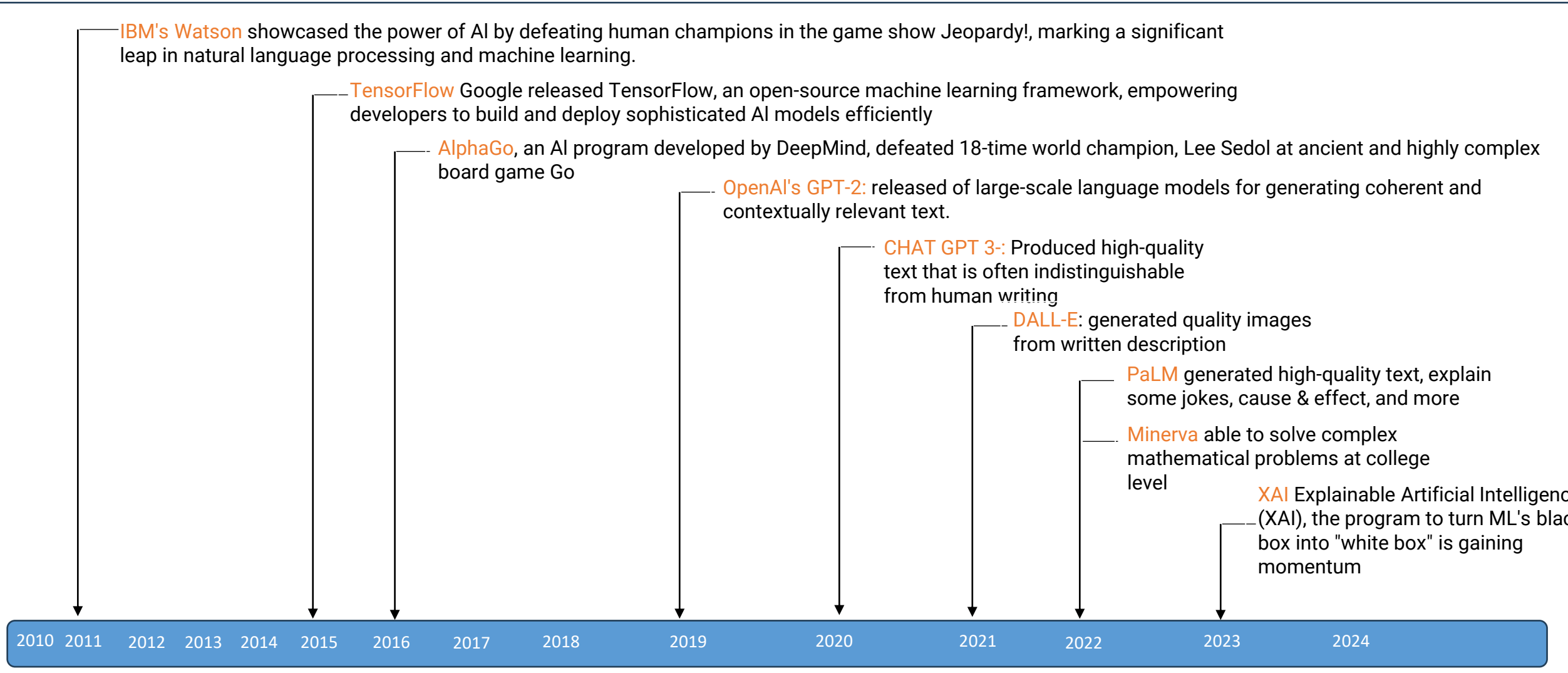
- In today's rapidly evolving world of artificial intelligence, one significant technology is taking the world by storm: Generative Al.

- Generative Al, or Generative Adversarial Networks (GANs), is an advanced subset of artificial intelligence designed to generate new, realistic data based on patterns learned from existing information

- GenAl programs can not only predict but also make, invent, and solve complex problems in many fields. Its impact varies from revitalizing art and music to revolutionizing finance, healthcare, gaming, and more



# Evaluation of Data Analytics with Deep Learning



# Use Cases of GEN AI in Risk Management

## Threats Analysis and Management

Machine learning engines can analyze large amounts of data from various sources. This information generates real-time prediction models that allow risk managers and security teams to address risks quickly. The models are fundamental to develop early warning systems that assure the uninterrupted operation of the organization and the protection of its stakeholders.

## Risk Reduction

AI also provides the ability to evaluate unstructured data about risky behaviors or activities in the organization's operations. AI algorithms can identify patterns of behavior related to past incidents and transpose them as risk predictors.

## Fraud Detection

Fraud detection traditionally requires intense analysis processes for financial institutions and insurers. AI systems can substantially decrease the workload of these processes and reduce fraud threats by using machine learning models that focus on text mining, social media analysis, and database searches.

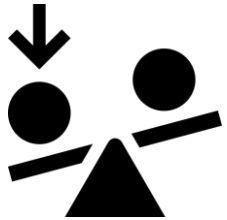
## Data Classification

AI tools can also process and classify all available information according to previously defined patterns and categories and monitor access to these data sets.

# Embracing the Future: Areas where GEN AI can Take Charge

1. Predictive Analytics for Risk Management: Leveraging advanced algorithms to forecast potential risks and mitigate them proactively.
2. Cybersecurity: Enhancing threat detection, vulnerability assessment, and incident response through AI-powered systems.
3. Compliance and Regulatory Compliance: Streamlining compliance processes, ensuring adherence to regulations, and automating compliance monitoring tasks.
4. Financial Risk Assessment: Analyzing market trends, assessing credit risks, and optimizing investment strategies using AI-driven models.
5. Supply Chain Management: Optimizing supply chain resilience, identifying disruptions, and implementing predictive maintenance strategies.
6. Fraud Detection and Prevention: Detecting fraudulent activities in real-time, minimizing financial losses, and safeguarding organizational assets.
7. Reputation Management: Monitoring online sentiment, managing brand reputation, and responding swiftly to potential reputation risks.
8. Environmental Risk Assessment: Analyzing environmental data, predicting environmental impacts, and developing strategies for sustainable risk management.

# GENERATIVE AI CHALLENGES



## 1. Biased Output and Fairness

Generative Al models can inadvertently perpetuate biases present in the training data. If the data used to train the model contains biases, the generated content may reflect and amplify those biases, resulting in biased decision-making processes, such as loan approvals or credit assessments

## 2. Data Quality and Generalization

Performance of generative Al models heavily relies on the quality and diversity of the training data. If the training data is not representative or lacks diversity, the generated outputs may not generalize well to real-world scenarios In organisations such as banks where accurate risk assessment is paramount, generative Al models must be trained on comprehensive and high-quality datasets to ensure that the synthetic data accurately reflects the complexities of the financial landscape.

## 3. Security and Privacy Risks

Generating realistic synthetic data may pose security and privacy risks if not handled with caution. Banks deal with sensitive customer information, and the use of generative Al could inadvertently create synthetic data that resembles real customer data. If this synthetic data is not properly secured, it may become a target for malicious actors. Serious considerations must be given if an organization wishes to use a third-party platform

# GENERATIVE AI CHALLENGES

## 4. Unintended Use and Manipulation

Generative AI can be misused for malicious purposes, such as creating realistic deepfakes or synthetic identities
Organizations need to be aware of the potential for such technologies to be used in fraudulent activities, including impersonation and identity theft

## 5. Explainability and Transparency

Generative AI models are often considered "black boxes" due to their complexity. Understanding how these models generate specific outputs can be challenging, leading to concerns about explainability and transparency.
Striking a balance between model complexity and interpretability is a key challenge.
Implementing safeguards to detect and prevent the malicious use of generative AI is essential to protect both customers and the integrity of any organizations

# Question & Answers

**Topic 1**

**Topic 2**

**Topic 3**

# Key Take Aways

*THANK YOU*


# Thank You