

The State of AI

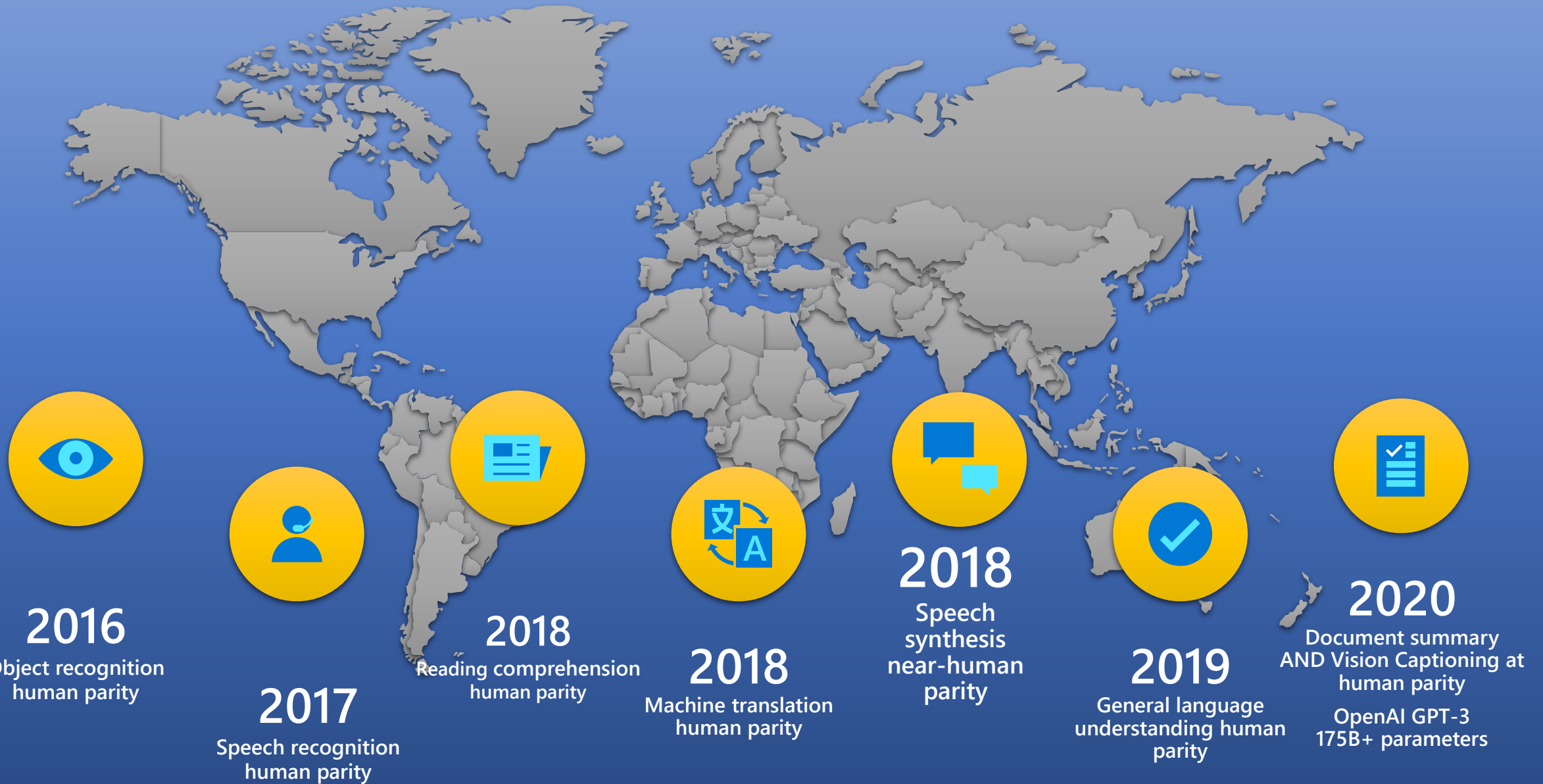
Insights & Considerations
BarnOwl
Aug 2023

[Click here for the recording of the session.](#)

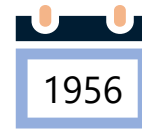
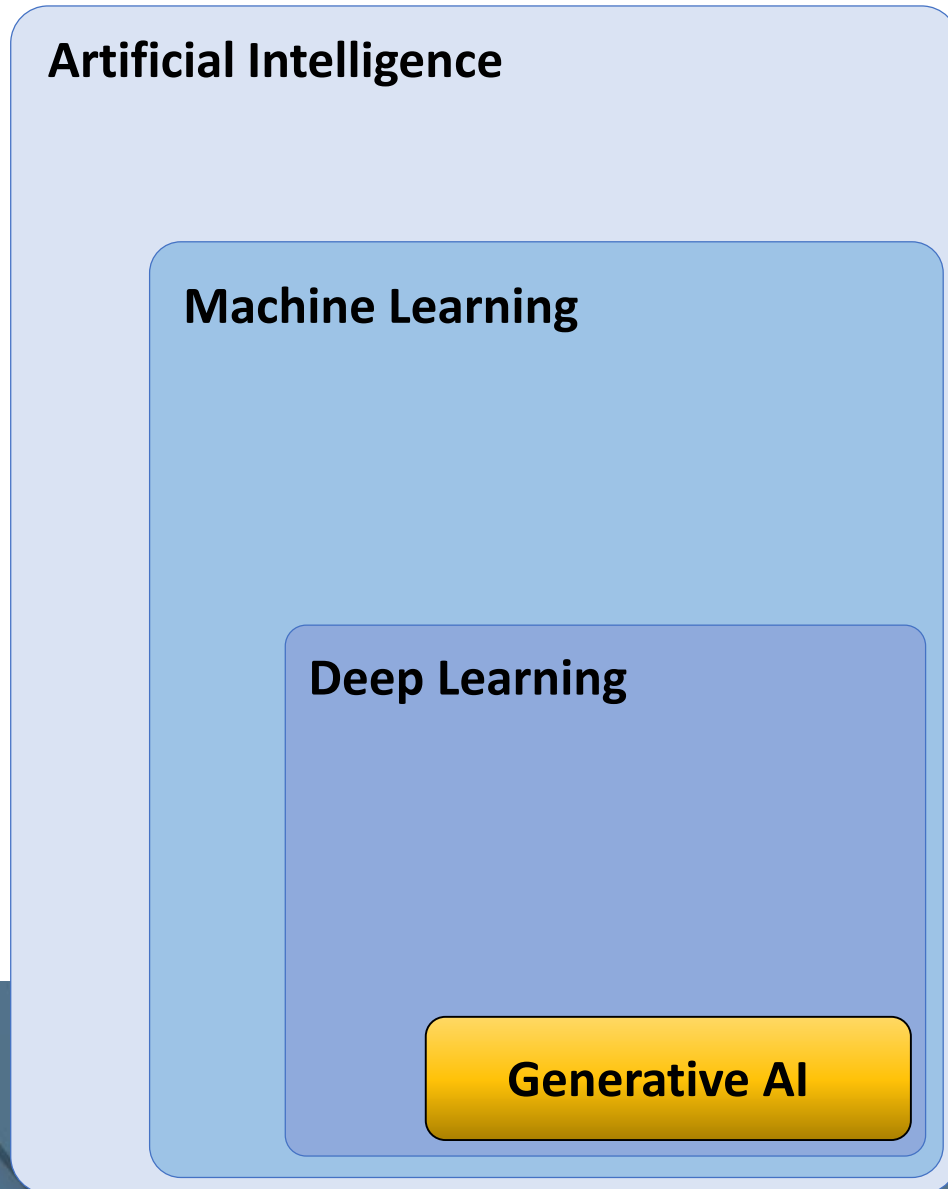
Lionel Moyal
Channel Partners Lead – Africa Region
Limoyal@microsoft.com



Breakthrough AI grounded in world-class research



AI Evolution



Artificial Intelligence

the field of computer science that seeks to create intelligent machines that can replicate or exceed human intelligence



Machine Learning

subset of AI that enables machines to learn from existing data and improve upon that data to make decisions or predictions



Deep Learning

a machine learning technique in which layers of neural networks are used to process data and make decisions



Generative AI

Create new written, visual, and auditory content given prompts or existing data.



2023 – The Era of Generative AI

GPT-3

Prompt:

Summarize this personal finance article in two sentences for my tax-filing customers:

<https://www.fidelity.com/learning-center/personal-finance/tax-pitfalls>

Response:

Tax pitfalls can be costly, so it's important to be aware of them. Some common tax pitfalls include failing to file or pay taxes on time, not reporting all income, claiming too many deductions, and not keeping accurate records.

Codex

Prompt:

Table customers, columns = [CustomerId, FirstName, LastName, Company, Address, City, State, Country, PostalCode]

Create a SQL query for all customers in Texas named Jane

query =

Response:

```
SELECT *  
FROM customers  
WHERE State = 'TX' AND  
FirstName = 'Jane'
```

DALL·E

Prompt:

A ball of fire with vibrant colors to show the speed of innovation at our media and entertainment company

Response:



ChatGPT

Prompt:

I'm having trouble getting my Xbox to turn on.

Response:

There are a few things you can try to troubleshoot this issue, First, Next, check the power cord ...

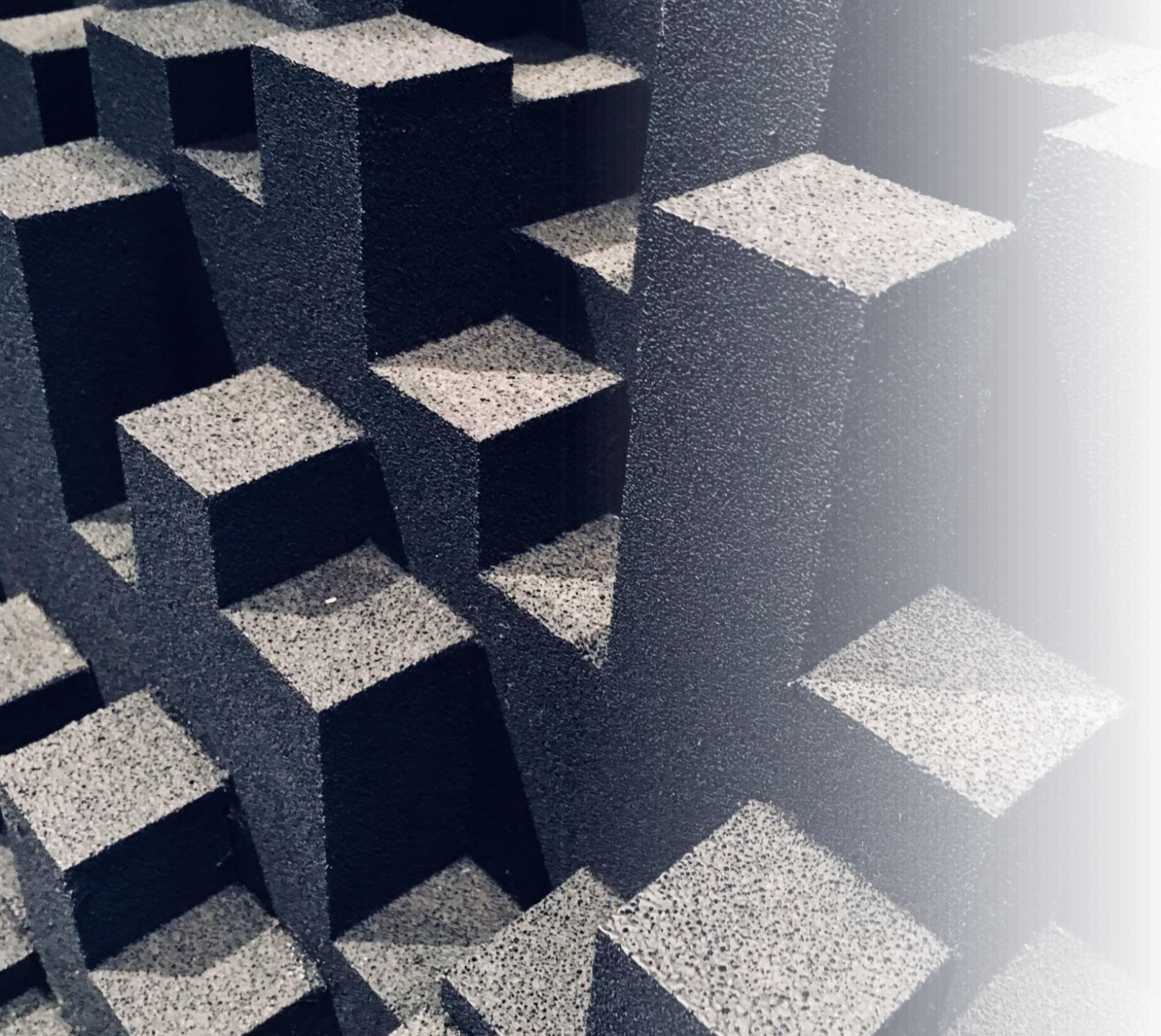
Prompt:

Thanks! That worked. What games do you recommend for my 14-year-old?

Response:

Here are a few games that you might consider:

(bulleted list) ...



Some Real Life Examples...

ChatGPT: Forensic Analysis

Me:

Please read the 3 PFMA audit reports provided from the Auditor General and tell me about any noteworthy trends related to medical negligence

ChatGPT Response:

Based on the information extracted from the three reports, here are some noteworthy trends:

- **Increasing Estimated Settlement Value of Claims:** *There has been a significant increase in the estimated settlement value of claims against departments, particularly provincial health departments. This value rose from an unspecified amount in the 2020 report to R124.15 billion in the 2021 report and further to R153.64 billion in the 2022 report.*
- **Increasing Outstanding Claims:** *The value of outstanding claims has also increased over the years. In the 2020 report, the outstanding medical negligence claims against the provincial department of health amounted to R5.5 billion. This amount increased to R124.15 billion in the 2021 report and R103.64 billion in the 2022 report.*
- **Increasing Paid Out Amounts:** *The amount paid out in medical negligence claims has also increased over the years. In the 2020 report, the Gauteng Department of Health paid out claims of **R501 million**. This amount **increased to R1.76 billion** in the 2021 report and **R856 million in the 2022 report**.*
- **Impact on Service Delivery:** *The reports highlight that these claims have a significant impact on service delivery in the health sector. The funds used to pay out these claims are often taken from budgets meant for other strategic priorities, including service delivery.*
- **Concerns about Management of Claims:** *The reports express concerns about the management of these claims. The measures implemented by departments to manage and defend medico-legal claims are often flawed, leading to successful claims being paid from funds earmarked for service delivery.*
- **Efforts to Address Medico-Legal Claims:** *Despite the increasing trend of claims, there have been efforts to address this issue. In 2015, the health minister approved a strategy to address the increasing medico-legal claims. However, there were shortcomings in the measures implemented by management for medico-legal claims.*

Me:

Give me more details about these medical negligence claims?

ChatGPT Response:

The 2022 report provides a detailed discussion on medical negligence claims against departments, particularly provincial health departments. Here are some key points:

- Claims are made against departments through litigation for compensation as a result of a loss caused by the department. The most common type of claim is medico-legal claims (medical negligence and malpractice claims) against provincial health departments. Departments do not normally budget for such claims; and those that do, often do not budget enough. The measures implemented by departments to manage and defend medico-legal claims are also flawed. As a result, all successful claims will be paid from funds earmarked for service delivery, further eroding departments' ability to be financially sustainable and to deliver on their service delivery commitments (Page 54).*
- In 2021-22, the **estimated settlement value of claims against departments totalled R153.64 billion**. This amount represents claims that have not yet been settled (by court order or mutually between the parties). The provincial health departments accounted for the largest portion of this amount (67%) (Page 54).*
- **Sixty departments (40%) had claims against them with an estimated settlement value that exceeded 10% of their budget for the following year. If paid out in 2022-23, these claims would use up more than 10% of these departments' budgets meant for other strategic priorities, including service delivery (Page 54).***
- The financial health of the health sector has been under immense pressure for years because of limited budget and poor financial management. This situation is made worse by medical negligence and malpractice claims, with the sector having paid R855.66 million in claims in 2021-22. Total claims against the sector currently stand at R103.64 billion (Page 54).*
- In 2015, the health minister approved a strategy to address the increasing medico-legal claims. However, there were shortcomings in the measures implemented by management for medico-legal claims (Page 54).*

Example: Forensic Analysis

Me:

Create a table comparing the values of paid out amounts, outstanding claims and estimated settlement values of claims across the 3 audited years.

ChatGPT Response:

Year	Paid Out Amounts	Outstanding Claims	Estimated Settlement Value of Claims
2020	R501m	R5,5bn	Not Available
2021	R1,76bn	R124,15bn	R124,15bn
2022	R856m	R103,64bn	R153,64bn

Please note that these figures are approximate and based on the information available in the reports. The estimated settlement value for the year 2020 was not mentioned in the report.

Me:

Do the reports mention anything about who the legal firms are that are making claims against the departments?

ChatGPT Response:

The reports do not provide specific information about the legal firms making claims against the departments. The documents mainly focus on the financial aspects, audit outcomes, and the impact of these claims, but they do not mention the names or details of the legal firms involved.

Example: Forensic Analysis

Me:

Give me some insights about the findings related to IT.

ChatGPT Response:

- **IT Security:**

Information security measures are critical to prevent cyberattacks and unauthorized internal activities.

Last year, government departments and entities experienced a drastic increase in cyberattacks, impacting 164 auditees (81%) out of 201 with ineffective security controls.

Hackers were successful in exploiting the security weaknesses at some of the auditees, resulting in some key government services not being available for a prolonged period and, in some cases, hackers using ransomware for financial gain.

The root cause was identified as inadequate information security governance.

- **IT Projects:**

20 out of 36 IT implementation or system acquisition projects reviewed did not meet time, cost, quality, or business expectations.

Poorly managed projects resulted in auditees incurring avoidable costs. R1,7 billion had been spent on system implementation projects that did not meet business expectations.

The root cause was identified as poor IT governance, where accounting officers and authorities did not fulfill their responsibilities.

- **IT Governance:**

128 auditees (63%) out of 202 had ineffective IT governance processes.

Ineffective IT governance processes have led to control environments that are vulnerable to abuse or misuse, IT expenditure that cannot be justified, and/or runaway IT projects.

The root cause was identified as accounting officers and authorities not fulfilling their responsibilities to ensure effective IT governance processes and oversight.

Metric	2020 Report	2021 Report	2022 Report
IT Governance	63% of auditees with ineffective IT governance processes	63% of auditees with ineffective IT governance processes	64% of auditees with ineffective IT governance processes
IT Security	81% of auditees with ineffective security controls	81% of auditees with ineffective security controls	82% of auditees with ineffective security controls
IT Projects	R1.261 billion spent on system implementation projects	R1.7 billion spent on system implementation projects that did not meet business expectations	R1.8 billion spent on system implementation projects that did not meet business expectations



Some Real Life Examples...

South Africa Risks 2023/24 Report
Institute of Risk Management of South Africa

Analysing Complex Content... Summarise the PDF I am looking at...

The image shows a side-by-side comparison of a PDF document and the Bing Chat interface. On the left, a PDF viewer displays the cover of the 'IRMSA RISK REPORT SOUTH AFRICA RISKS 2023/24 9TH EDITION'. The cover features a large, stylized red and orange graphic resembling a lightning bolt or a series of overlapping lines. The text on the cover is in a bold, sans-serif font. On the right, the Bing Chat interface is shown. It includes a navigation bar with 'Chat', 'Compose', and 'Insights' options. Below this, there's a 'Protected' status indicator. The main heading is 'Bing Chat Enterprise' with a shield icon, followed by the tagline 'AI-powered chat for work'. Three main action buttons are visible: 'Write' (Help me prepare and write a successful sales pitch), 'Compare' (Compare online and offline marketing strategies), and 'Analyze' (Create a SWOT analysis about environmental goals and impact). Below these are links for 'Terms' and 'Privacy', and a section for 'Choose a conversation style' with buttons for 'More Creative', 'More Balanced', and 'More Precise'. A dark blue button at the bottom right of the chat area says 'Summarize the PDF I am looking at'. The chat area also shows a green checkmark indicating 'Searching your page for information', a notification about permissions, and a status message: 'Your personal and company data are protected in this chat'. At the bottom, there's a search bar with the placeholder text 'Ask me anything...'.

File | C:/Users/lmoyal/Downloads/IRMSA-Risk-Report2023-Full.pdf

Ask Bing AI

1 of 56

Protected

Bing Chat Enterprise

AI-powered chat for work

Write
Help me prepare and write a successful sales pitch

Compare
Compare online and offline marketing strategies

Analyze
Create a SWOT analysis about environmental goals and impact

[Terms](#) | [Privacy](#)

Choose a conversation style

More Creative | More Balanced | **More Precise**

Summarize the PDF I am looking at

✓ Searching your page for information

Great! You can always review your permissions in Settings.

[Notification and App Settings](#)

Your personal and company data are protected in this chat

Ask me anything...

Analysing Complex Content... Summarise the PDF I am looking at...

The image shows a side-by-side comparison of a PDF document and its AI-generated summary. On the left, a PDF viewer displays the cover of the 'IRMSA RISK REPORT SOUTH AFRICA RISKS 2023/24 9TH EDITION'. A large, abstract red scribble is drawn over the top half of the cover. On the right, a chat window provides a structured summary of the report's content.

Protected

The report is divided into four sections:

- **Section 1: South Africa Risk Context.** This section provides an overview of the internal, transactional, and external environment in which South Africa operates, and the challenges and opportunities it faces ⁴. It also highlights the concept of a polycrisis, which refers to a situation in which multiple crises occur simultaneously or in quick succession, creating a complex and interconnected web of crises for governments, organisations and societies ⁵.
- **Section 2: South Africa Top Risks.** This section identifies and describes the top risks for South Africa, based on their impact and likelihood, as well as their interconnections and implications for the country's objectives and priorities ⁶. The top risks include economic collapse, political instability, systemic failure of public infrastructure, national grid failure, large-scale disruption of digitally enabled services, impact of climate change and climate action failure, proliferation of illicit economic activity, collapse of social security systems, and increasing unemployment and livelihood crisis.
- **Section 3: South Africa Scenarios ⁷.** This section presents three possible scenarios for South Africa's future, based on the drivers and outcomes of the top risks. The scenarios are: Perpetual Hangover, Fake it until we make it, and Owning our Future. The section also provides an analysis of the most likely scenario outcome for 2023/24, as well as suggested risk-response strategies to change the predicted scenario outcome.
- **Section 4: IRMSA's Call to Action ⁸.** This section provides a summary of the main findings and recommendations of the report, as well as a call to action for all stakeholders to work together to address the risks and opportunities facing South Africa. The section outlines 11 risk-response strategies that can help the country achieve inclusive growth, strengthen democratic institutions, protect the environment, and build a more resilient and prosperous future.

The report also includes a message from the IRMSA President, a preface, an executive summary, acknowledgements, references and abbreviations ⁹. The report is designed to be a valuable resource for policymakers, risk professionals, business leaders and decision-makers seeking to understand the threats and opportunities in South Africa and the South African market ³. The report is also intended to be a call to action for all citizens to lead from where they stand and to take bold action to prevent a polycrisis from turning into a failed or mafia state ¹⁰.

Learn more: [1. Page 2 - Line 3](#) [2. Page 13 - Line 23](#) [3. Page 9 - Line 3](#) [+7 more](#) 1 of 30 ●

[Answer from the web instead](#) [What is the IRMSA?](#) [How can I get a copy of this report?](#)

[Can you tell me more about the scenarios presented in Section 3?](#)

Your personal and company data are protected in this chat

Ask me anything...

Create a Table with the Top Risks from the report, their descriptions and Risk Treatment and Opportunities.

Top Risks	Description	Risk Treatment Options and Opportunities
Economic Collapse	<ul style="list-style-type: none"> Severe and prolonged contraction of the economy. Influenced by global and domestic factors. 	<ul style="list-style-type: none"> Implement structural reforms. Diversify the economy. Enhance fiscal discipline. Strengthen social protection. Leverage AfCFTA.
Political Instability	<ul style="list-style-type: none"> Social unrest, violence, or regime change. Influenced by corruption, governance failures, policy uncertainty, electoral disputes, or civil conflict. 	<ul style="list-style-type: none"> Promote transparency and accountability. Engage with stakeholders.-Develop a clear policy vision. Address root causes of conflict.-Enhance citizen participation.
Systemic Failure of Public Infrastructure	<ul style="list-style-type: none"> Widespread breakdown or deterioration of public infrastructure. Influenced by lack of investment, maintenance, and innovation; climate change; and governance challenges. 	<ul style="list-style-type: none"> Increase public spending on infrastructure. Promote private sector participation. Adopt smart technologies. Enhance infrastructure planning and coordination. Improve access to basic services.
National Grid Failure	<ul style="list-style-type: none"> Failure or disruption of the national electricity grid.- Influenced by ageing and unreliable power plants; insufficient and costly supply of coal; delays and cost overruns in renewable energy projects; and increasing demand for electricity. 	<ul style="list-style-type: none"> Invest in new and renewable energy sources. Improve energy efficiency and conservation measures. Enhance grid management and resilience. Promote regional energy cooperation and integration. Support research and innovation in energy technologies.
Large-Scale Disruption of Digitally Enabled Services	<ul style="list-style-type: none"> Loss or interruption of essential digital services due to cyberattacks, technical failures, or natural disasters. 	<ul style="list-style-type: none"> Implement robust cybersecurity measures. Develop a business continuity and disaster recovery plan. Educate staff and customers on cyber protection. Review cyber insurance coverage.-Foster international cooperation on cyber governance.
Impact of Climate Change and Climate Action Failure	<ul style="list-style-type: none"> Negative effects of global warming on the environment, society, and economy. Failure or delay in implementing effective measures to reduce emissions and adapt to climate change. 	<ul style="list-style-type: none"> Assess exposure and vulnerability to climate risks. Develop a climate risk strategy. Enhance risk modelling and pricing capabilities. Diversify product portfolio and offer innovative solutions. Support green initiatives and sustainable development.
Proliferation of Illicit Economic Activity	<ul style="list-style-type: none"> Growth of illegal or informal economic activities, such as smuggling, trafficking, counterfeiting, money laundering, or corruption 	<ul style="list-style-type: none"> Strengthen law enforcement and judicial systems. Enhance transparency and accountability measures

You are the Chief Risk Officer in an **insurance broking company**. Read this report and list the top 3 risks your company should be concerned about for the next year, and for each one suggest a set of mitigation actions. Show the results in a table, with the risk name, the risk description and why it is relevant to an insurance broking company

Risk Name	Risk Description	Relevance to Insurance Broking	Mitigation Actions
Large-scale disruption of digitally enabled services	Loss or interruption of essential digital services due to cyberattacks, technical failures, or natural disasters.	<ul style="list-style-type: none"> Affects availability and reliability of online platforms, systems, and data. Exposes company to cyber risks. 	<ul style="list-style-type: none"> Implement robust cybersecurity measures. Develop a business continuity and disaster recovery plan. Educate staff and customers on cyber protection. Review cyber insurance coverage.
Impact of climate change and climate action failure	Negative effects of global warming on the environment, society, and economy. Failure or delay in implementing effective measures to reduce emissions and adapt to climate change.	<ul style="list-style-type: none"> Increases frequency and severity of natural disasters and weather-related events. Affects demand and supply of insurance products and services. Increases regulatory and reputational pressures on the insurance industry. 	<ul style="list-style-type: none"> Assess exposure and vulnerability to climate risks. Develop a climate risk strategy. - Enhance risk modelling and pricing capabilities. Diversify product portfolio and offer innovative solutions. Support green initiatives and sustainable development.
Political instability	Social unrest, violence, or regime change due to corruption, governance failures, policy uncertainty, electoral disputes, or civil conflict.	<ul style="list-style-type: none"> Affects stability and security of the country, business environment, and investor confidence. Affects regulatory framework and policy direction of the insurance industry. Affects social cohesion and trust among stakeholders. 	<ul style="list-style-type: none"> Monitor political situation and developments in the country. Engage with relevant authorities and industry associations. Build strong relationships with customers and suppliers. Develop a crisis management plan.

You are an **auditor**, and your job is to audit the risk management policies of an organisation. **Create an audit checklist** that focuses on checking whether the organisation has put in place risk management measures and governance

Here is an audit checklist that focuses on checking whether the organization has implemented risk management measures for the top three risks identified earlier:

1. Large-scale disruption of digitally enabled services:

1. Does the organization have a cybersecurity policy in place that outlines its approach to managing cyber risks?
2. Has the organization implemented appropriate technical and organizational measures to protect its information systems, data, and networks from cyber threats?
3. Does the organization have a business continuity and disaster recovery plan in place that outlines how it will respond to and recover from a large-scale disruption of digitally enabled services?
4. Has the organization conducted regular training and awareness-raising activities for its staff and customers on how to protect their devices and data from cyber threats?
5. Has the organization reviewed its cyber insurance coverage to ensure that it meets its needs and expectations?

2. Impact of climate change and climate action failure:

1. Has the organization assessed its exposure and vulnerability to climate risks across its business activities, assets, and liabilities?
2. Does the organization have a climate risk strategy in place that aligns with its business objectives and stakeholder expectations?
3. Has the organization enhanced its risk modeling and pricing capabilities to reflect the changing risk landscape and customer needs?
4. Has the organization diversified its product portfolio and offered innovative solutions that address climate risks and opportunities?
5. Is the organization supporting green initiatives and sustainable development through its corporate social responsibility programs and partnerships?

3. Political instability:

1. Is the organization monitoring the political situation and developments in the country and assessing their implications for its business operations and strategy?
2. Is the organization engaging with relevant authorities and industry associations to advocate for a conducive regulatory environment and policy direction for its industry?
3. Has the organization built strong relationships with its customers and suppliers to ensure that it understands their needs and expectations in times of uncertainty or change?
4. Does the organization have a crisis management plan in place that outlines how it will respond to different scenarios of political instability that could affect its business continuity or reputation?



Foundation Models

General AI models such as Large Language Models, trained on vast amounts of data (GPT, LLAMA, etc..)

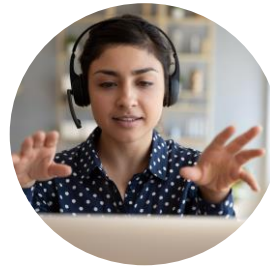


Copilots...

Conversational, expert helpers scoped to assist with specific complex tasks



Sales & Marketing



Productivity



Customer Service



Competitive Intelligence



Legal

Introducing

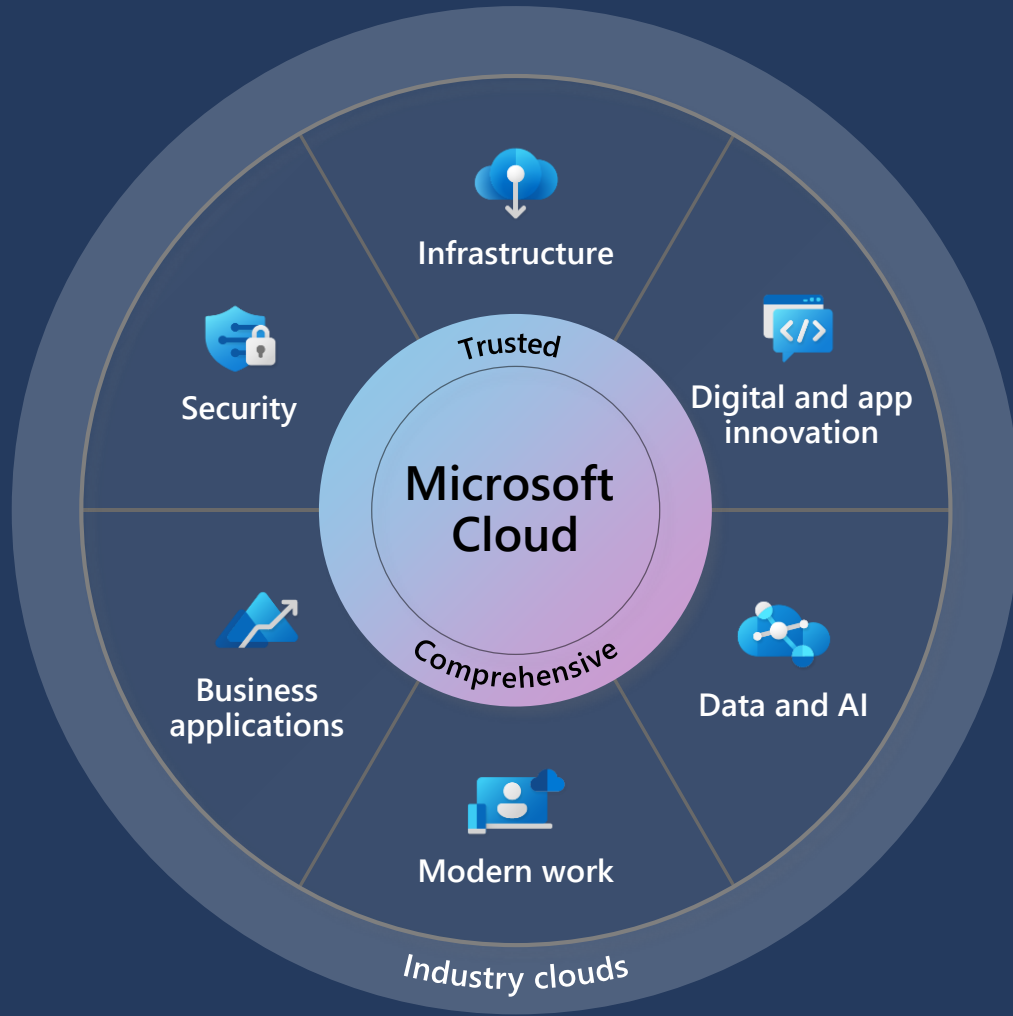


Microsoft 365 Copilot

 Microsoft 365



The next
revolution in
computing



Microsoft Cloud

Radically accelerate your organization's productivity with built-in AI

Differentiate from the competition with intelligent apps using AI

Microsoft Cloud
Runs on trust

Microsoft Cloud
Runs on trust

Your data is your data

Your data from any fine-tuning is not used to train the foundation AI models

Your data is protected by the most comprehensive enterprise compliance and security controls

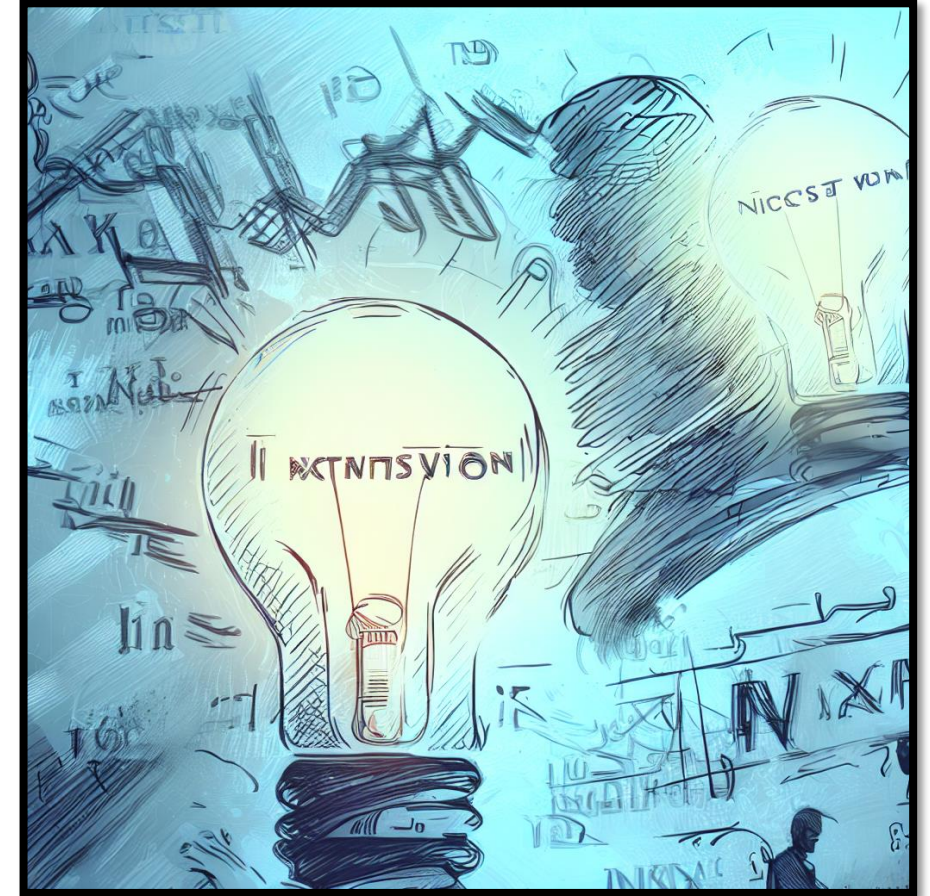
Next Steps?

- Understand your **data assets**
- The playing field has changed -> **Re-imagine and don't think incrementally!**
- **Responsible AI** -> Fairness, Reliability & Safety, Privacy & Security, Inclusivity, Transparency, Accountability

Key learnings & words of caution...

- AI Models are more than just an extremely rich knowledge base. **They demonstrate an ability to interpret and reason!** Used correctly, they are an incredibly powerful **assistant** to enhance productivity.
- However they are not infallible and may 'hallucinate' and make statements that are not in fact true.
- They are limited to the context you provide, and therefore can **amplify bias**. Ask for arguments & counter-arguments.

....



"A sketch depicting a tax incentive for investors in companies that drive innovation, futuristic, atmospheric"

Generated by Microsoft Designer (22 July 2023)