



AI Risk Management Framework

Executing an effective
playbook



Anil Cheriyan
Founder, Phase IV Ventures
Board Member / Former CIO

Effective Risk Playbook = Trust

AI Risk Management Framework

Effectiveness Mindset

GenAI Opportunity

Amazing opportunity with several POCs launched and scaling rapidly in all aspects of business....

...expanding with increased sophistication as autonomous and physical integration technologies evolve



Operational Efficiencies



Customer Interactions



Productivity / Knowledge Management



New Business Models



Autonomous Agents

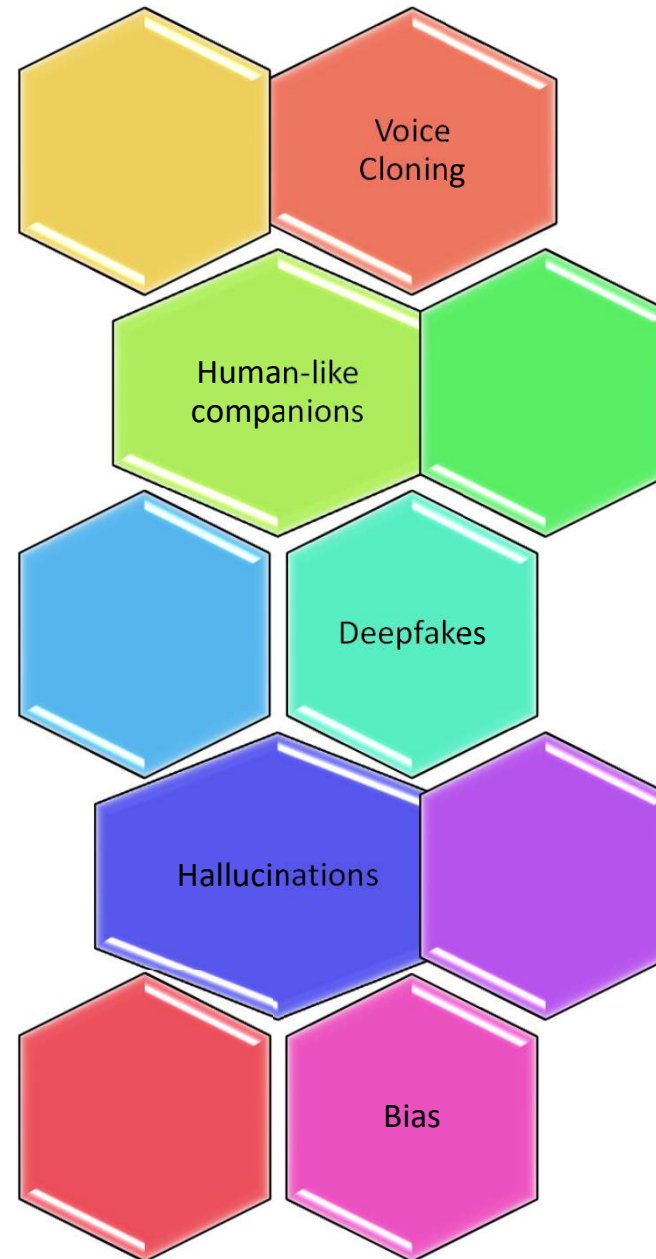


Humanoid Robots

Horror stories abound

*As the quest for
Artificial General
Intelligence
continues....*

*...we have already seen
several examples of
misuse and abuse of AI*



Horror stories abound

*As the quest for
Artificial General
Intelligence
continues....*

*...we have already seen
several examples of
misuse and abuse of AI*



Unclear Regulatory Environment

*Waiting for a unified
and comprehensive
regulatory
environment is futile*



US Federal – Executive
Order



US States – Fragmented /
Disjointed



EU – Risk based



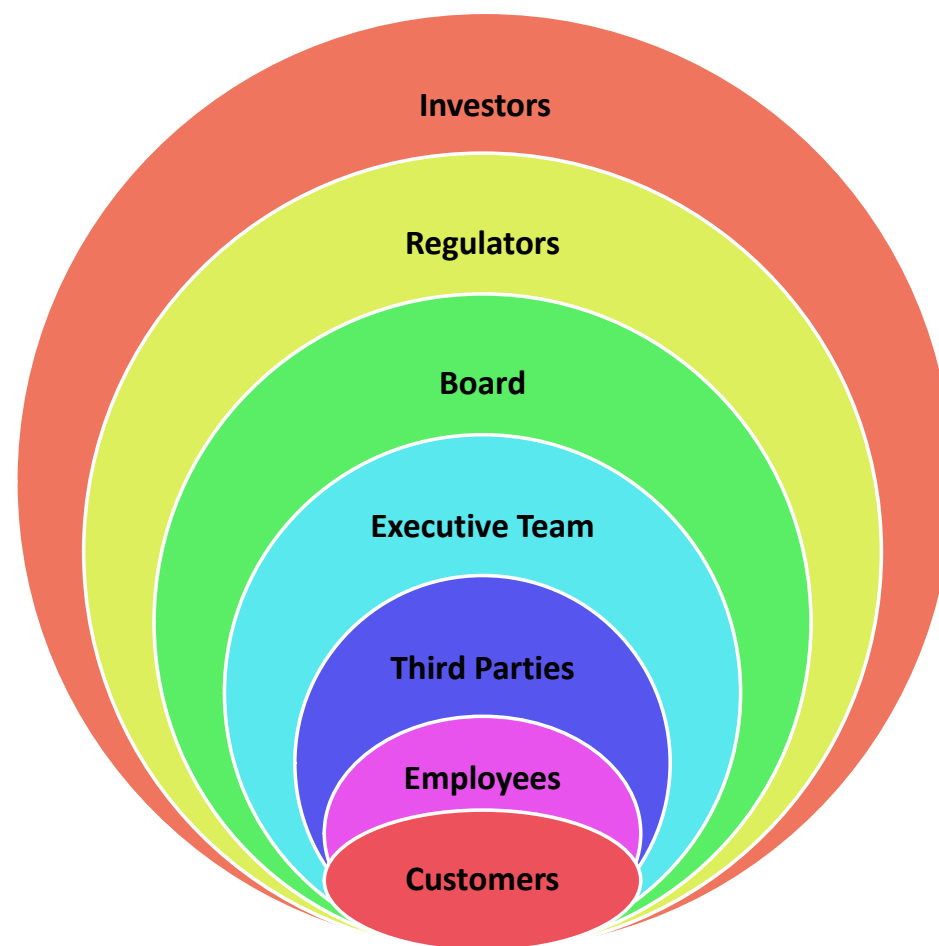
China - Algorithm
Management

Managing Risk = Trust

It is imperative that companies proactively execute an effective AI Risk Management Playbook.....

...to build Trust with all their stakeholders

STAKEHOLDERS



*5-layer Framework
with hierarchy of
interdependencies
from the top-down*

*Most current
“responsible AI”
frameworks are lists
with little guidance on
relative importance*



1

Inherent Risk

Identify inherent risks that naturally exist before risk mitigation measures are applied

Human AI Interface

Bias

Hallucinations

Model Drift

Cybersecurity

Privacy

Technology Maturity

Third Party Risk

2

Risk Mitigation

Establish risk mitigation routines to identify, assess and execute steps to reduce the impact or likelihood of risk occurrence

AI Literacy

Risk Awareness / Education

Talent Management

Key Risk Indicators

- e.g., Bias fairness scores, Hallucination rates, Data leakage, Unauthorized use

Reinforced Learning

“Shift Left” AI Lifecycle

3

Governance

*Define processes, rules
and structures to
oversee risk
management*

Cross-functional Engagement

Role Clarity & Accountability

”Guard Rails” Risk Tolerance / Acceptance

Transparency (Good, Bad & Ugly)

Three Lines of Defense

Legal / Regulatory Compliance

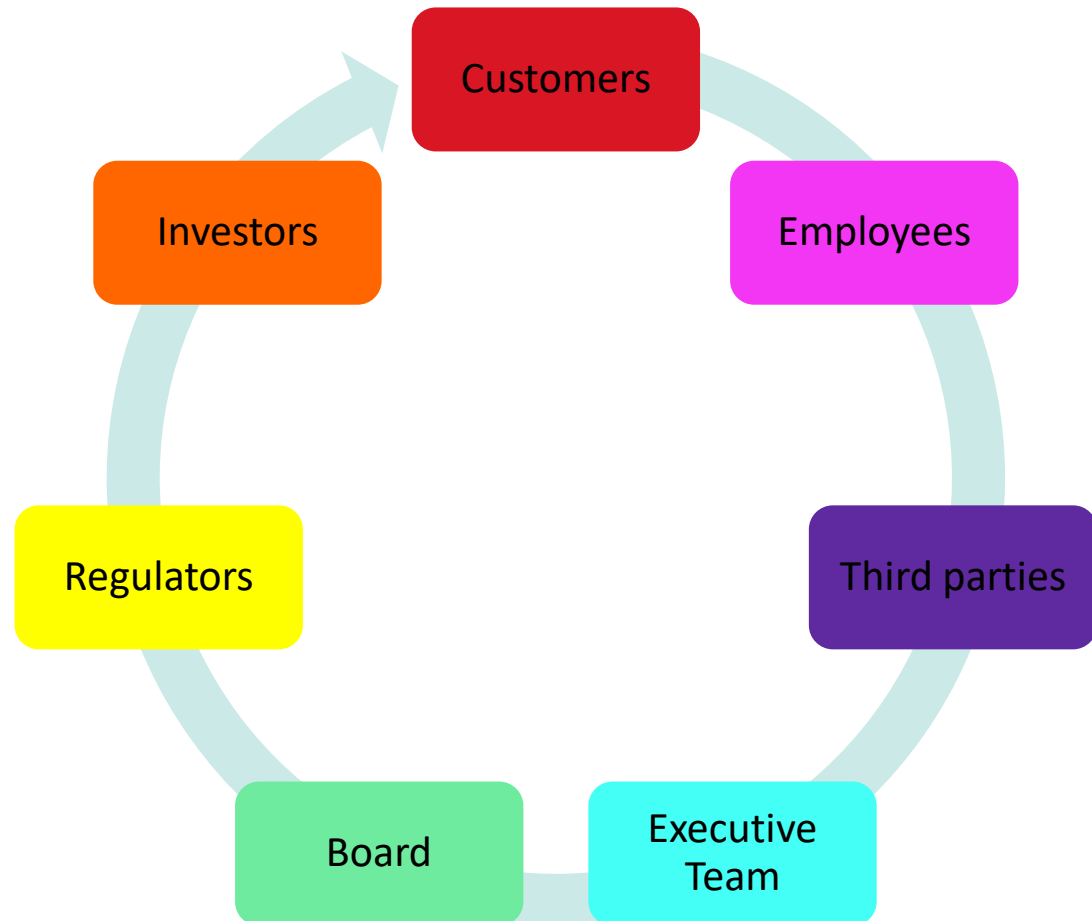
Crisis Management Plan

4 Communications

Establish communications protocols that ensure timely, accurate and transparent communications to stakeholders of risk events and their mitigation

Define hierarchy of communications based on risk event severity

Validate and practice using Crisis Management exercises



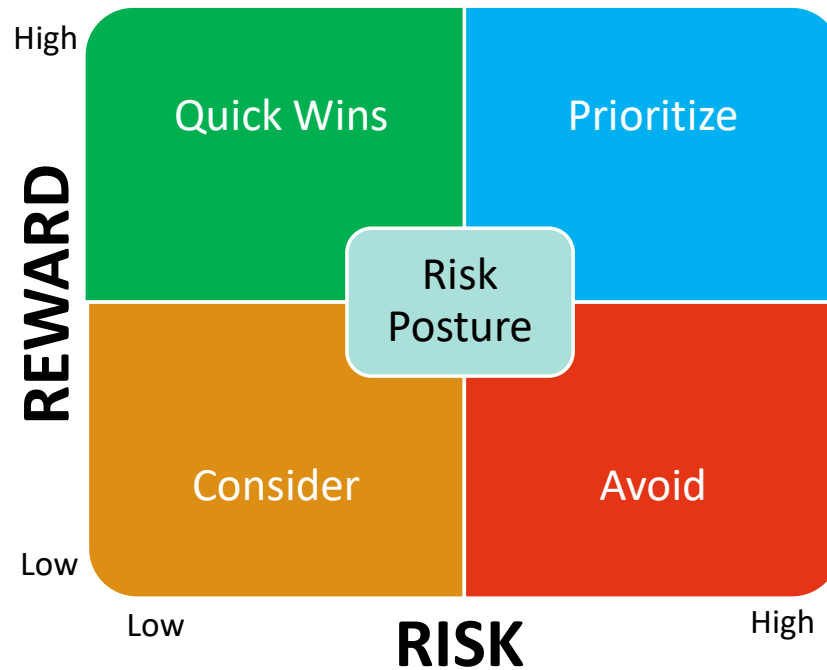
5 Appetite

Work with Board to establish Risk Appetite based on assessment of company's overall ecosystem

Highly regulated institutions tend to be conservative or risk averse

Assess each AI opportunity against the Risk Reward matrix

Risk Appetite sets tone for rest of the Risk Framework



Effectiveness Mindset

FROM

- Anecdotal
- Fearful
- Reactive
- Silos
- Group think
- Obscurantist
- Bottoms up



TO

- Data Driven
- Risk Aware
- Proactive
- Cross Functional
- Accountability
- Transparent
- Tone at the Top



Executing Risk Playbook is key to building Trust

Appetite

Communications

Governance

Risk Mitigation

Inherent Risks

Leveraging the right AI Risk Management Framework



With an Effectiveness Cultural Mindset



- **Anil Cheriyan**
- **Email:**
acheriyan1@gmail.com
- **LinkedIn:**
[linkedin.com/in/anil-cheriyan-7779955](https://www.linkedin.com/in/anil-cheriyan-7779955)