AI Risk Management & Governance

The next lap in managing I&T risks

Thomas Kok, CISM CRISC

IBF Fellow (Risk Management)

Head of Group Technology, Information & Cyber Risk | OCBC Group

August 2020

Information sensitivity: Public / Unclassified
Purpose: Industry sharing at ISACA GTACS 2020

GTACS 2020
GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA Singapore Chapter

Agenda

Definitions

What could be AI risks?

Managing AI Risks

AI Risk Governance

Conclusion

Definitions

Unless we have grounded definitions, we bring more confusion into our conversations.

Artificial Intelligence

A set of technologies that seek to simulate human traits such as knowledge, reasoning, problem-solving, perceptions, learning and planning, and produces an output or decision[1].

Note 1: Such as recommendation, prediction, classification.

Model

A quantitative method that applies mathematical and domain-specific theories, techniques and assumptions to process input data into quantitative estimates.

An **AI Model** is a model which uses AI.

AI System

An application which uses one or more AI Models in the implementation of its requirements.

This could be an enterprise application, or an end-user computing (EUC) application.

What could be AI risks?

Bias model

Security issue

Accountability

Data privacy

Misuse of data

'Malicious' learning

System outage

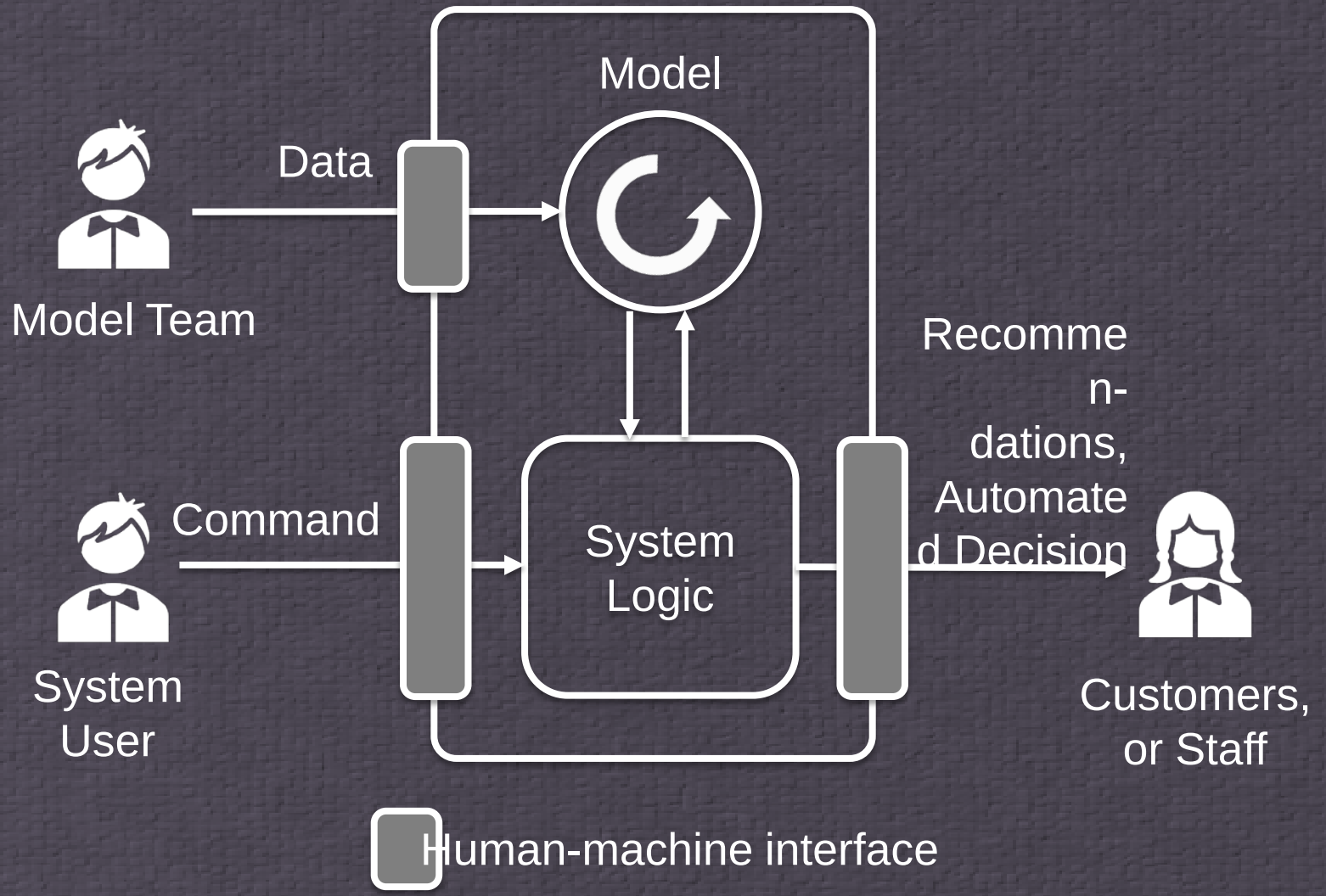
Transparency

Explainability

Not ethical recommendation

Cause harm

Simplified Anatomy of an AI System



Information Risk (i.e. data-related)

Information risk is the business risk relating to compromises of confidentiality, integrity and availability of information (in physical or digital form), possibly resulting in multi-faceted impact.

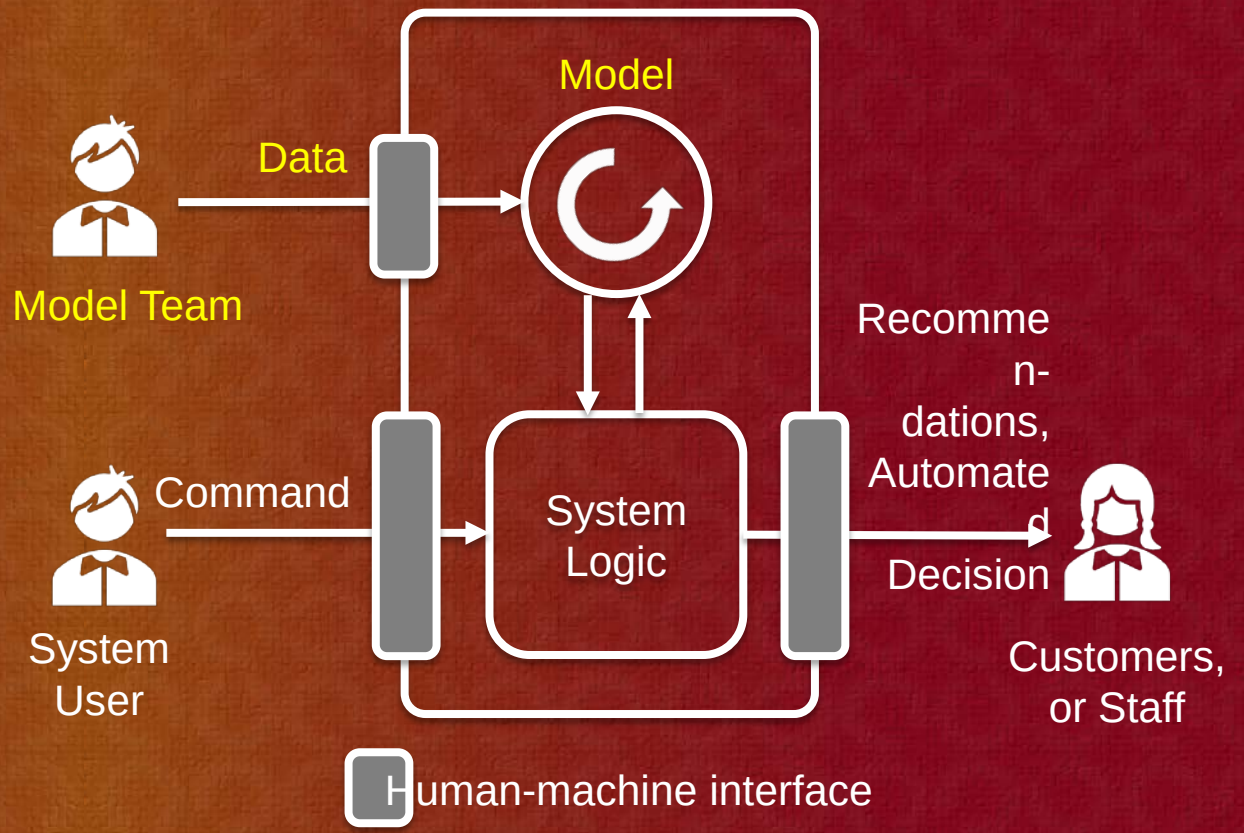
Data is an Asset

BUT …

Data is NOT enough, NOT complete, NOT clean.

"Need to collect more, cleanse more"

Data may be Bias, Personal Identifiable or Confidential.



Information Risk (i.e. data-related)

Information risk is the business risk relating to compromises of confidentiality, integrity and availability of information (in physical or digital form), possibly resulting in multi-faceted impact.

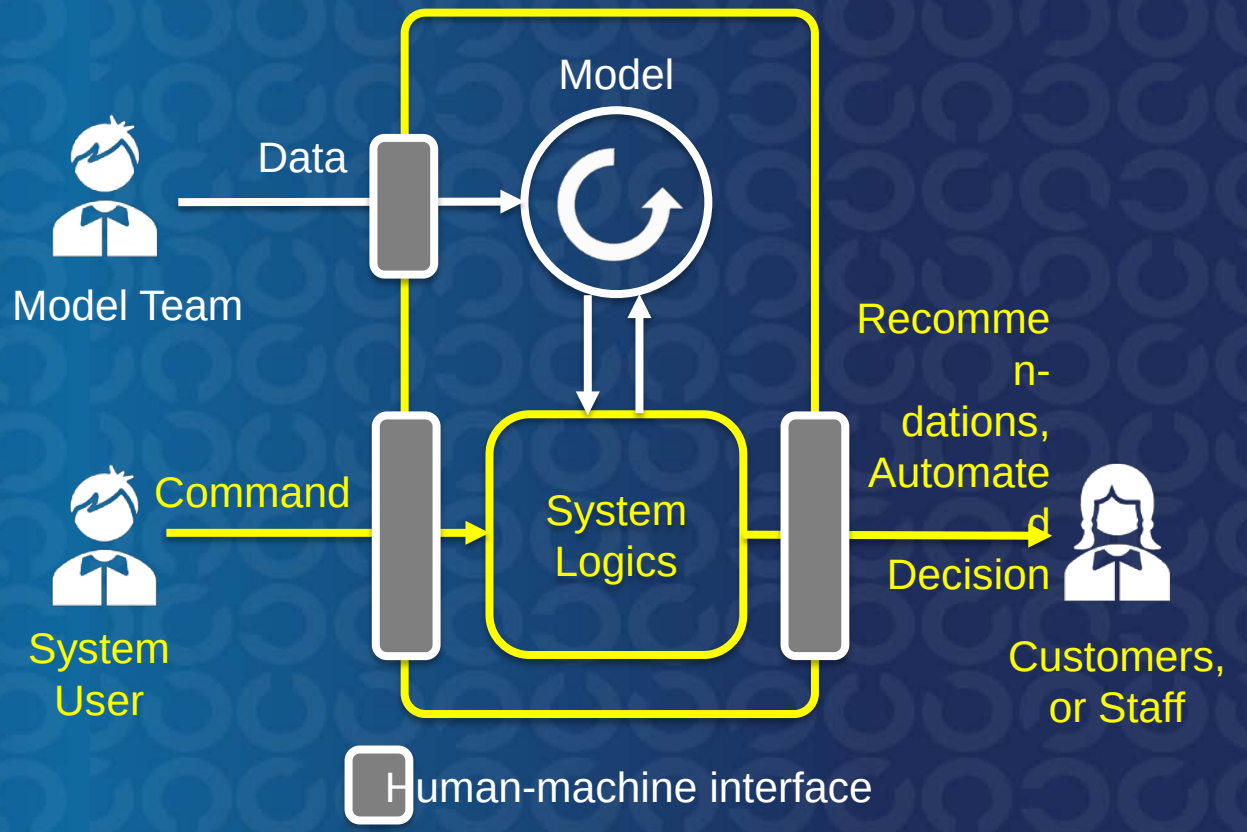
Data is an Asset	Data is a Liability	
BUT … Data is NOT enough, NOT complete, NOT clean. "Need to collect more, cleanse more" Data may be Bias, Personal Identifiable or Confidential.	Not handling data in accordance to sensitivity creates liability Concerns on information disclosure as a high volume of heterogeneous nature is needed	Data privacy issues, errors during cleansing, aggregation & manipulation issues Legal & regulatory breaches, fines, reputational impact

Technology Risk

Technology risk is the business risk relating to the disruption, failure and irregularity in essential services, arising from the use of information & communication technologies, possibly resulting in multi-faceted impact.

AI System is either an enterprise IT system, or an end-user–computing (EUC) application.

- IT General Controls (Application, Infrastructure), EUC Controls
- Concerns with IT Availability, Resilience, Recoverability, Change, Incident, Problem, Patch Management
- Disruption of Services to customers and internal staff due to failure of AI Systems



Technology Risk

Technology risk is the business risk relating to the disruption, failure and irregularity in essential services, arising from the use of information & communication technologies, possibly resulting in multi-faceted impact.

AI System is either an enterprise IT system, or an end-user–computing (EUC) application.

- IT General Controls (Application, Infrastructure), EUC Controls
- Concerns with IT Availability, Resilience, Recoverability, Change, Incident, Problem, Patch Management
- Disruption of Services to customers and internal staff due to failure of AI Systems

Complexity ↑ ➡ Supportability ↓

➡ Incidents ↑

System Criticality ↑ ➡ Severity of impact ↑

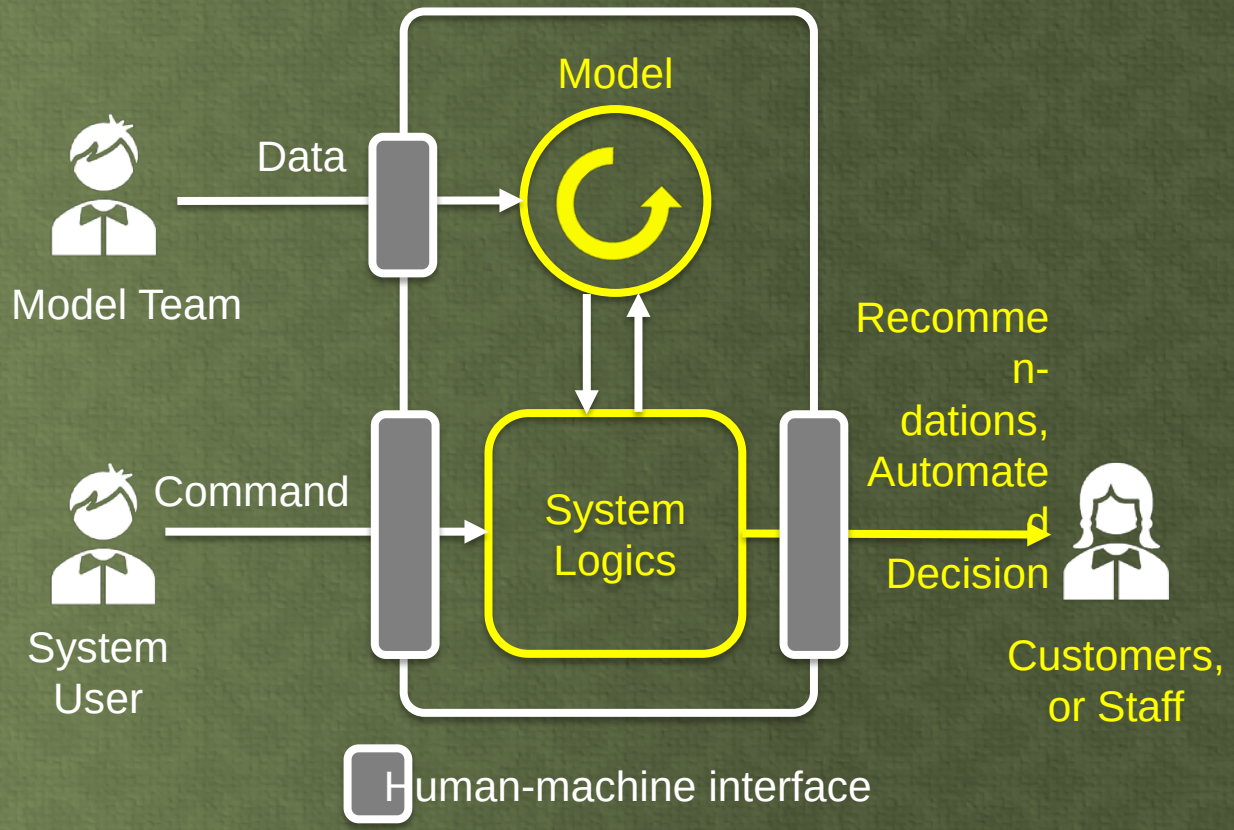
Model Risk

Model risk is the business risk relating to adverse consequences from decisions based on models that are incorrect or misused, where the consequences could be a multi-faceted impact.

Biased results ➡ Fairness of Model ↓

➡ Trust of System ↓
(Not fit for purpose)

"Why recruit her and not me?
Why promote him and not me?"



Model Risk

Model risk is the business risk relating to adverse consequences from decisions based on models that are incorrect or misused, where the consequences could be a multi-faceted impact.

Biased results ➡ Fairness of Model ↓

➡ Trust of System ↓
(Not fit for purpose)

"Why recruit her and not me?
Why promote him and not me?"

Unable to explain why ➡ Transparency ↓
Explain-ability ↓
Trust ↓

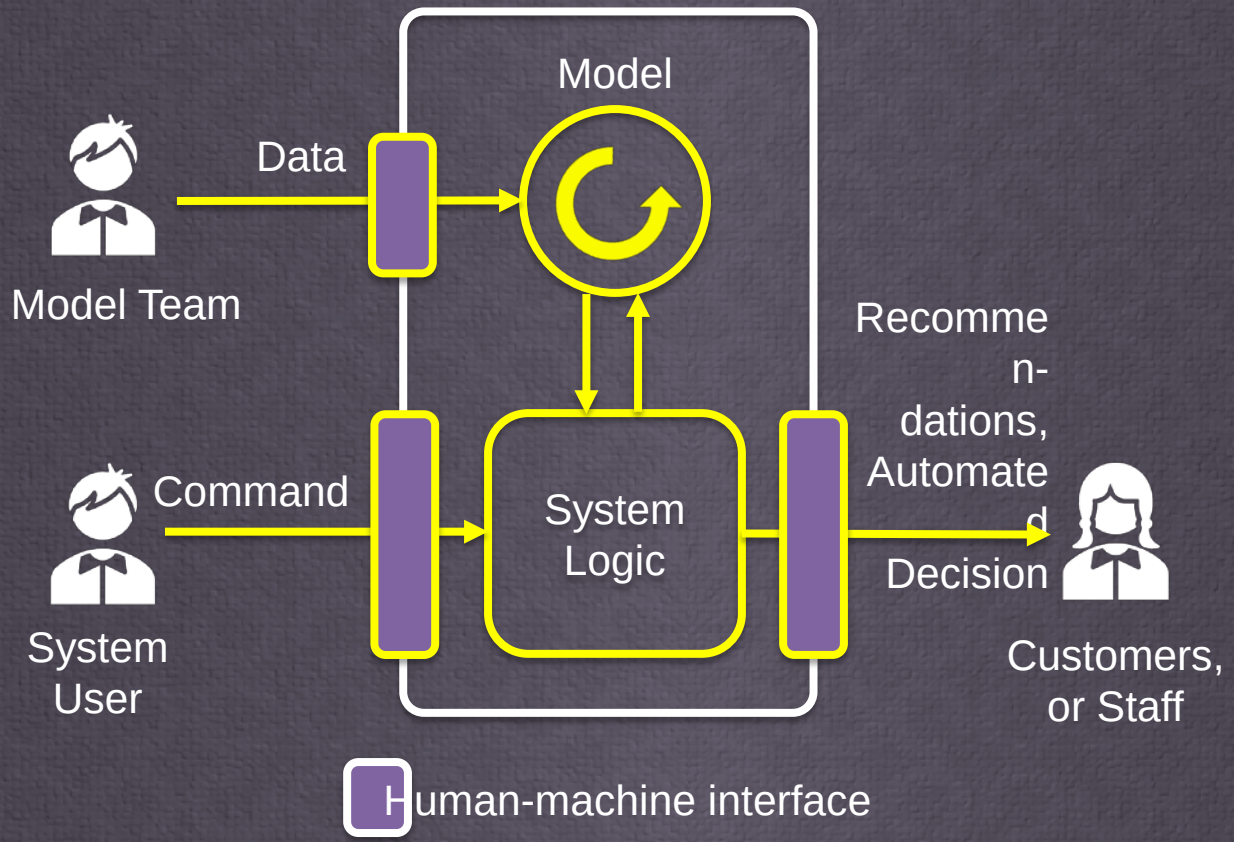
"Why are my attributes penalising me? Preventing me from getting this loan?"

Human-Machine Interaction Risk

HMI risk is a business risk unique to AI systems as in some use cases, the model learns from interactions with humans, while in others, the automated decision from the model could harm humans.

'Poisoning AI' - Manipulate data resulting in 'wrong' learning & wrong decisions or recommendations.

Human interaction with AI System could cause Model to learn the wrong responses.

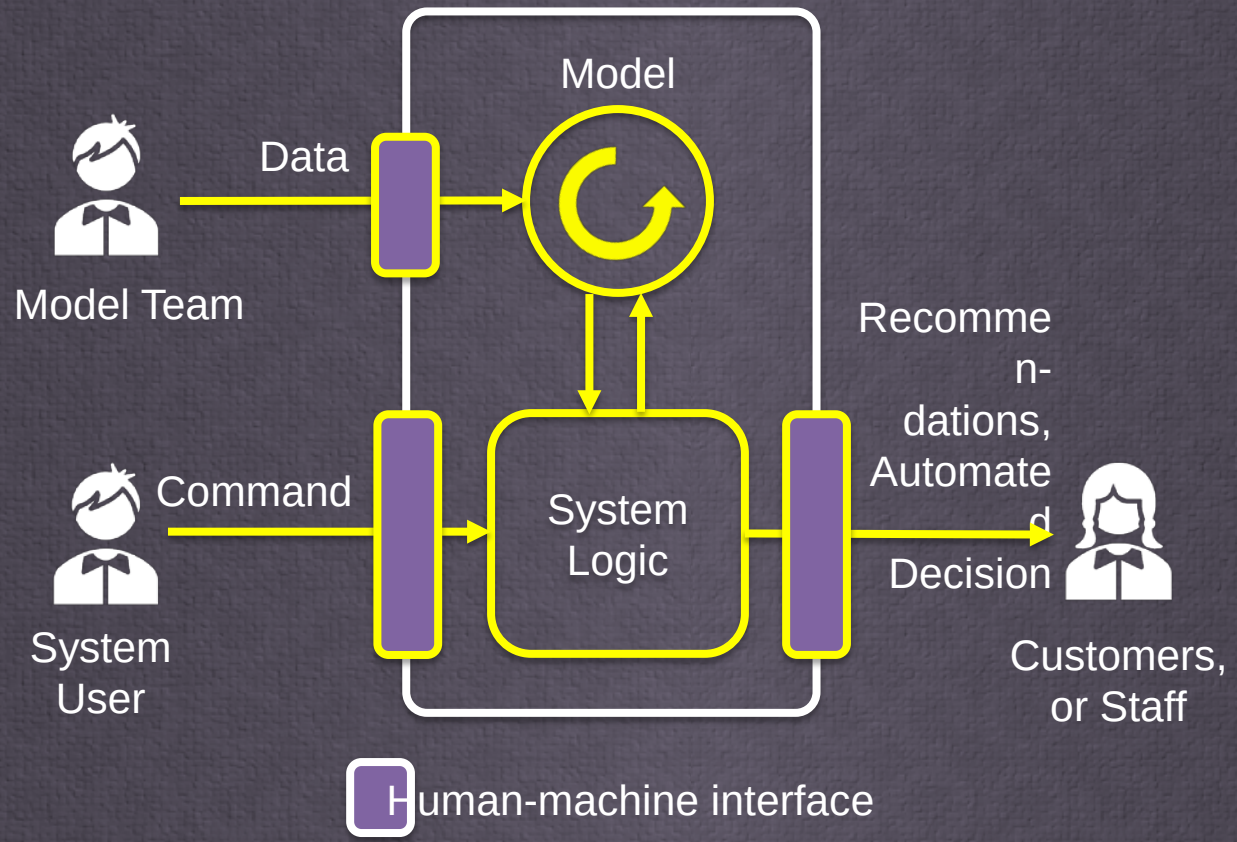


Human-Machine Interaction Risk

HMI risk is a business risk unique to AI systems as in some use cases, the model learns from interactions with humans, while in others, the automated decision from the model could harm humans.

'Poisoning AI' - Manipulate data resulting in 'wrong' learning & wrong decisions or recommendations.

Human interaction with AI System could cause Model to learn the wrong responses.



Recommendations which have a material impact to customers and staff should be reviewed.

This includes automated decision which leads to physical machinery actions which could cause harm.

Managing AI risks

AI risk is managed in accordance to an AI risk management framework which covers risk governance, communications, monitoring, assessment, mitigation and acceptance.

The framework is supported by a set of policies, standards, control processes and risk mitigation initiatives.

How to manage AI risks?

How to manage AI risks?

Comprehensive risk identification & assessment

Robust controls as risk response

Upskill staff to be aware & competent with AI Systems

- Establish a multi-disciplinary team of SMEs to perform risk management: Business, IT, Risk (I&T risk, model, ops risk), Security, Legal, Compliance, …
- Formulate risk scenarios, think beyond traditional impact of IT systems
- Consider the 'powers' we have bestowed on the AI systems

How to manage AI risks?

Comprehensive risk identification & assessment

Robust controls as risk response

Upskill staff to be aware & competent with AI Systems

Human-centric AI:

- Controls to be in place to ensure no harm to humans – preventive, detective and corrective

Human-oversight:

- Based on inherent risk, automated decision-making to establish: Human-in-the-Loop, Human-over-the-Loop, Human-out-of-the-Loop

Model performance monitoring, escalation and rapid responses.

Model complexity – consider a simpler learning algorithm/network to trade-off to enhance transparency

How to manage AI risks?

Comprehensive risk identification & assessment

Robust controls as risk response

Upskill staff to be aware & competent with AI Systems

Understand:

- Applicable AI techniques and implications to design, development, testing, operating, overriding, monitoring of AI Models and the overall AI Systems.
- AI Model Risk and principles of responsible or trustworthy AI, e.g. Human Agency, Fairness, Ethics, Transparency.
- How to perform independent assurance of AI systems and form an opinion on responsible or trustworthy AI ?
- Evolving legal and regulatory expectations.

AI Risk Governance

Integrate into the Enterprise Risk Governance Structure

Clear roles and responsibilities enabling the objectives to direct, monitor & evaluate risk management

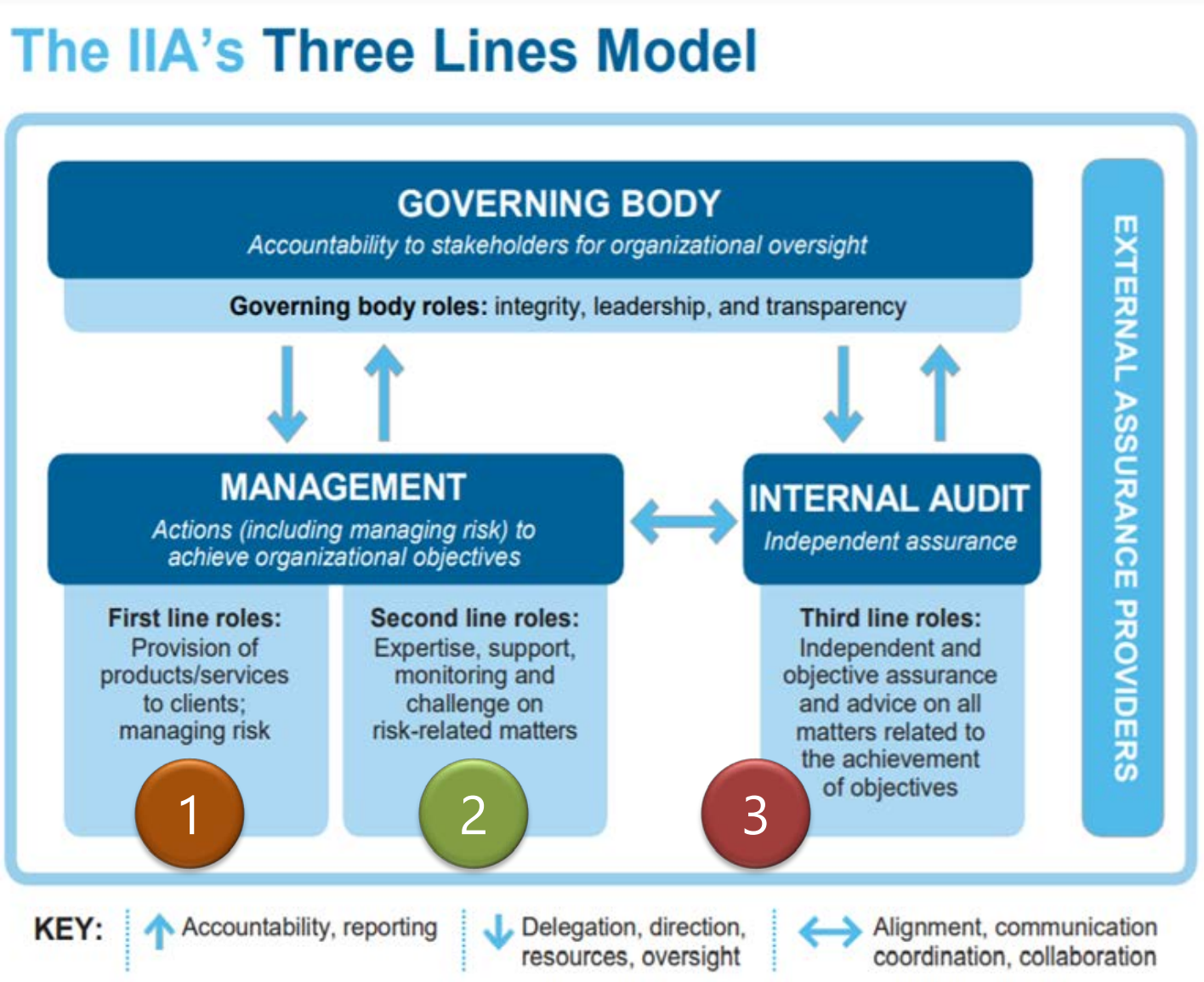
Integrate into Enterprise Risk Governance

- Integrate into 3 Lines of Defense
- Leverage existing enterprise risk appetite and tolerance

1
- Business Sponsors & Users
- IT & IS Teams
- DS & AI Teams

2
- Risk (I&T, Model, Operational)
- Legal & Compliance

3
- Internal Audit



Source: https://www.complianceweek.com/risk-management/iias-three-lines-of-defense-updated-to-stress-collaboration/29212.article

Clear roles and responsibilities enabling the objectives to direct, monitor & evaluate risk management

1

Business Sponsors & Users

IT & IS Teams

DS & AI Teams

- Business Sponsor is the **Risk Owner**
- Requirements include those relating to AI Models
- Designer & Developer (to align to Security-by-Design)
- Tester (including Model Validation)
- Change Board, System and Model Performance Monitoring
- Day-to-day management of AI risks

2

Risk (I&T, Model, Operational)

Legal & Compliance

- Risk Appetite, Oversight, Monitoring, Advisory & Challenge
- AI Risk Management Framework, Policies and Standards
- Risk Management Committees (with AI Risk as an additional agenda, and include AI-aware members)
- Risk Reporting to CRO, CEO and Board
- Enterprise-wide AI Risk Mitigation Initiatives
- Legal and Regulatory Compliance Advisory on AI expectations

3

Internal Audit

- Independent assurance of AI system and model controls
- Audit Reporting to CEO and Board

Conclusion

AI risk is the next lap for I&T risk, and it is necessary to engage a multi-disciplinary team of subject-matter experts to help identify risks beyond the traditional risks relating to Information and Technology, and to ensure robust controls are in place.

Above all, AI Risk Governance has to be established -- integrated into the Enterprise Risk Governance, and with clear roles and responsibilities.

Be ready for the future.

GTACS 2020

GOVERNANCE · TECHNOLOGY AUDIT · CONTROL · SECURITY

ISACA®

Singapore Chapter