AI Governance
Building the foundation of your AI Journey

PREPARED FOR:
CIO Forum

TRANSPARENT · HUMAN-CENTRIC · DATA-INFORMED

MINDOVER**MACHINES**.COM

Your Presenters

Steve Navarro
General Manager &
Chief Revenue Officer
Mind Over Machines

Alexandra Moylan, Esq.
CIPP/US, AIGP
AI Governance Attorney
Baker Donelson

AI Regulation
Crash course in what's going on

Artificial Intelligence is any technology that tries to replicate some broader aspect of human intelligence.

Federal Executive Order on AI

"a machine-based system that can, for a... human-defined objectives, make predicti... recommendations, or decisions influencin... virtual environments. Artificial i... machine- and human-b... virtual environm... models through... use model infere... information or acti..."

NIST

"AI refers to the ability of a machine to perform tasks ... would require ... recognizing patterns, ... conclusions, making..."

Colorado AI Regulation

"any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environment."

Ethics Wheel

The **AI Ethics Wheel** is a tool used by Mind Over Machines to map out the use case of an AI system to ensure ethical considerations are in place during the design of the system.
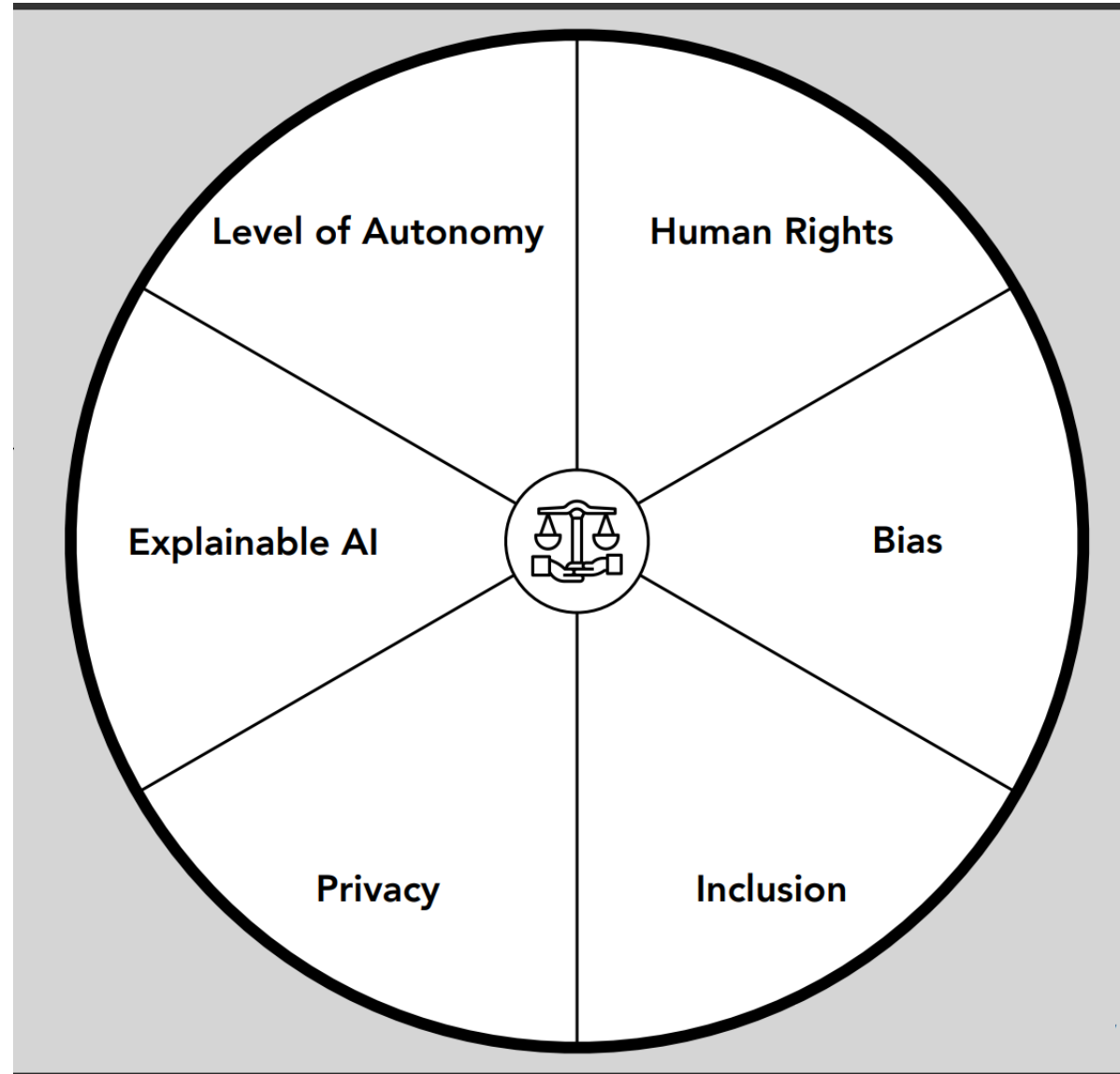
Ethics Wheel Items

Bias: Is the dataset accurately representative of the population?

Inclusion: Who is more proportionately advantaged through the AI? Is it user friendly?

Privacy: Does the AI collect people's data? What does it do with the data?

Explainable AI: Can the AI implementation be easily described? Can one justify AI-enabled decisioning?

Level of Autonomy: Does the AI prevent people from interfering with it? Does it require an overwrite to that end?

Human Rights: Does the AI discriminate against people? Does the AI deprive people of jobs?

Use Case:

Air Canada – Chatbot - Hallucination
Amazon – HR - Bias
OpenAI – Speech to Text - Accuracy
Samsung – Data leak - Privacy
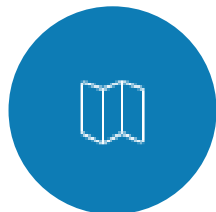Deep Fakes and Fraud

Beyond Intake

Holistic AI Governance
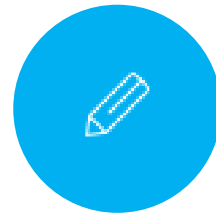
NIST AI Risk Management Framework

Govern

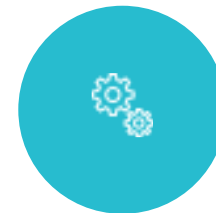How do we organize and oversee AI risk management?

Map

What are the AI risks and where do they exist?

Measure

How significant are our AI risks and how effective are our controls?

Manage

How do we respond to and control our AI risks?

Sample Workflow

Getting started with a sample governance workflow

Governance Foundations

- You need an intake form that must be very easy to promote participation
- You need an intake team who can sift through the submitted forms
  - Normally a very small team leading your AI efforts (your AI champions)
- You need a **Governance Board** comprised of a cross-functional team
  - Normally represented by Executive, IT, Legal, HR, & Ops
- You need a Risk Management Framework to operationalize safeguards
- You need supporting use case documents such as a **CBA**, detailed use case form, **adoption plan**
- You need an AI Security Review team who will review the risk assessment from a tech/social/business perspective
- **Stage gates** in the development process to review what has been built
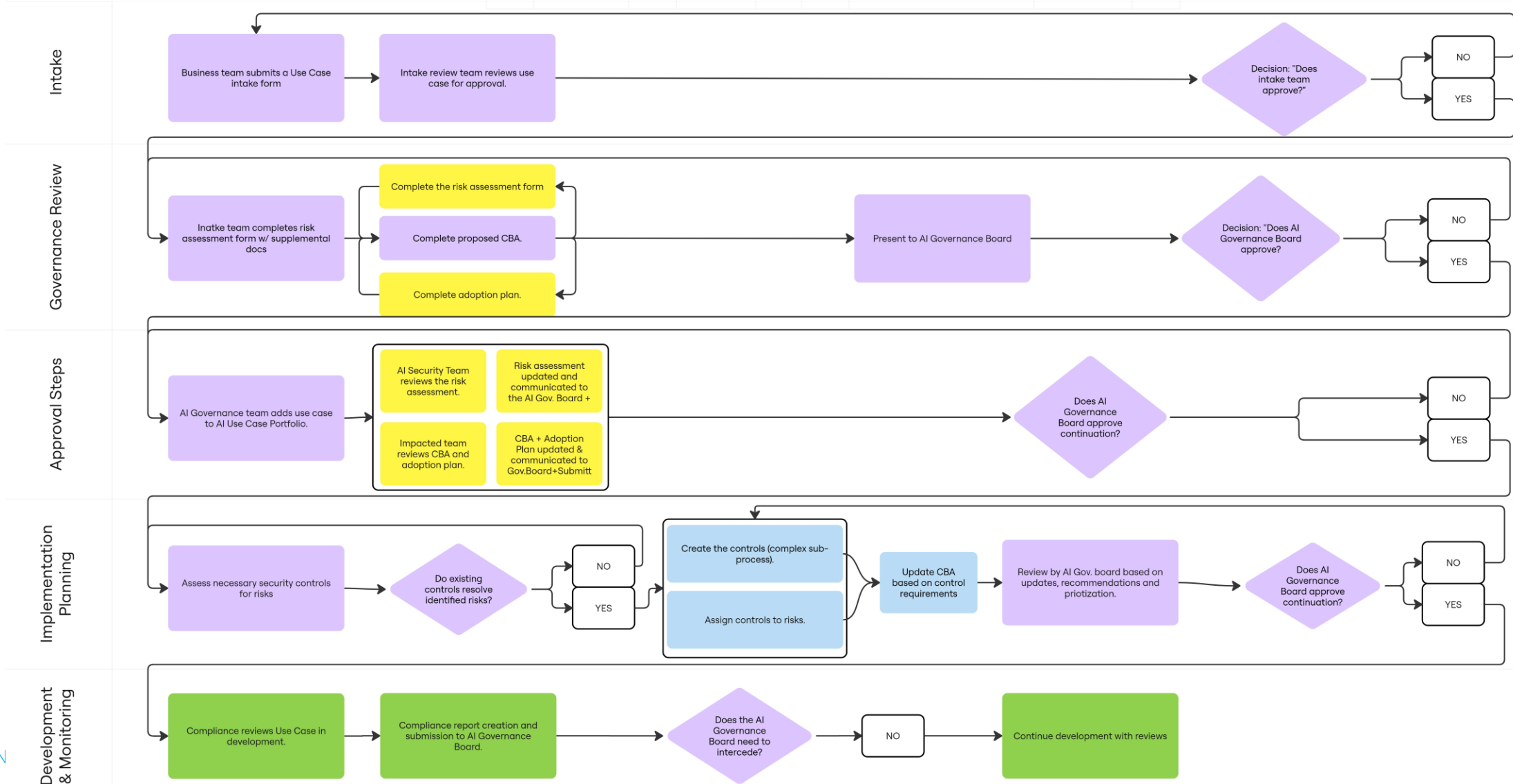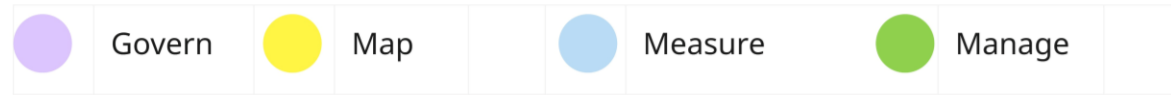
5 Most Common AI Ethics Principles

AI ethics principles

- Human-centric and socially beneficial
- Fair
- Explainable and transparent
- Secure and safe
- Accountable

Gartner.

Scalable AI Governance Framework

Legend: Govern (purple) · Map (yellow) · Measure (blue) · Manage (green)

Intake
- Business team submits a Use Case intake form
- Intake review team reviews use case for approval.
- Decision: "Does intake team approve?" → NO / YES

Governance Review
- Inatke team completes risk assessment form w/ supplemental docs
  - Complete the risk assessment form
  - Complete proposed CBA.
  - Complete adoption plan.
- Present to AI Governance Board
- Decision: "Does AI Governance Board approve?" → NO / YES

Approval Steps
- AI Governance team adds use case to AI Use Case Portfolio.
  - AI Security Team reviews the risk assessment.
  - Risk assessment updated and communicated to the AI Gov. Board +
  - Impacted team reviews CBA and adoption plan.
  - CBA + Adoption Plan updated & communicated to Gov.Board+Submitt
- Does AI Governance Board approve continuation? → NO / YES

Implementation Planning
- Assess necessary security controls for risks
- Do existing controls resolve identified risks? → NO / YES
  - Create the controls (complex sub-process).
  - Assign controls to risks.
- Update CBA based on control requirements
- Review by AI Gov. board based on updates, recommendations and priotization.
- Does AI Governance Board approve continuation? → NO / YES

Development & Monitoring
- Compliance reviews Use Case in development.
- Compliance report creation and submission to AI Governance Board.
- Does the AI Governance Board need to intercede? → NO → Continue development with reviews

Legend: Govern • Map • Measure • Manage

Intake

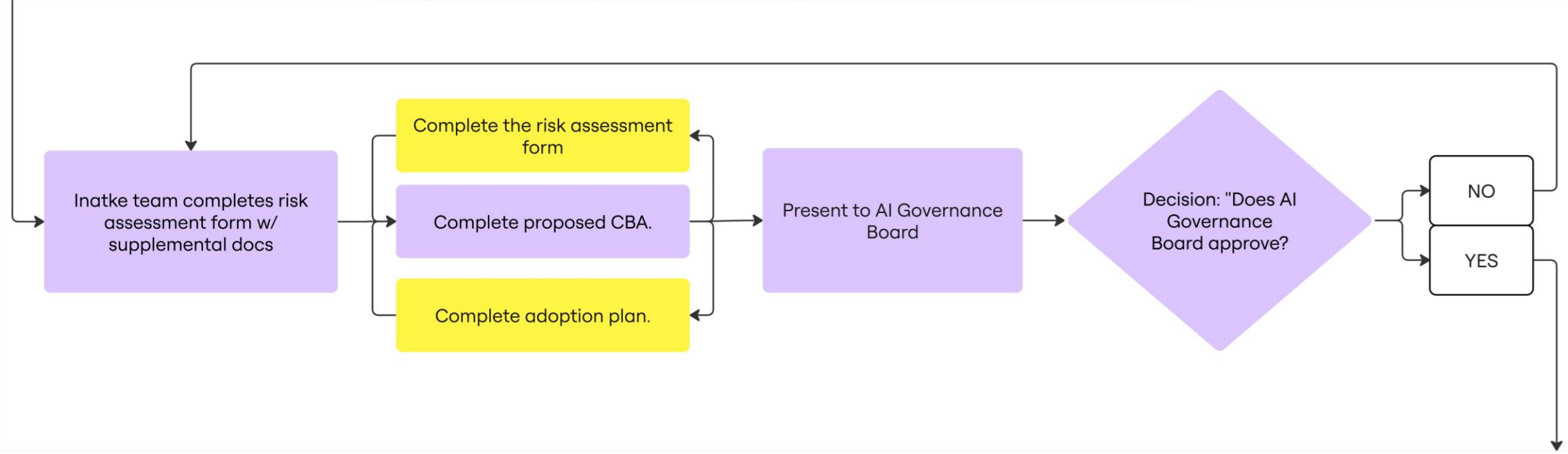Business team submits a Use Case intake form → Intake review team reviews use case for approval. → Decision: "Does intake team approve?" → NO / YES

Set yourself up for success with thorough documentation before getting started.

Cost Benefit Analysis is key. AI is evergreen.
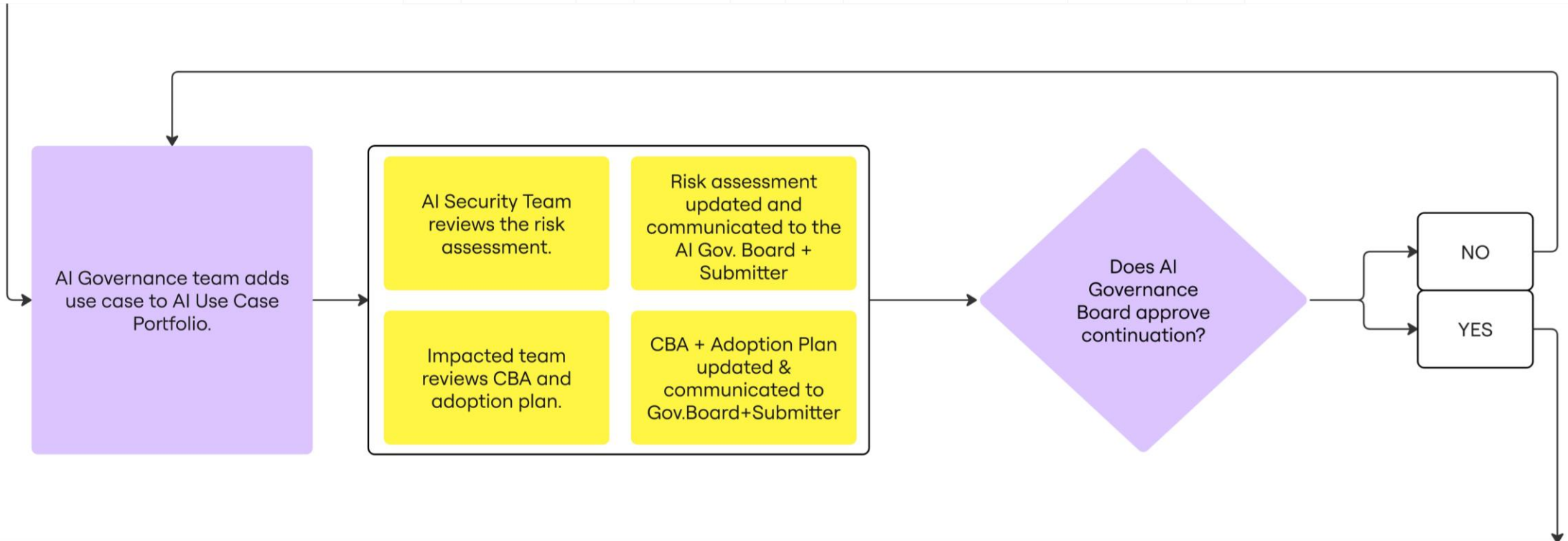
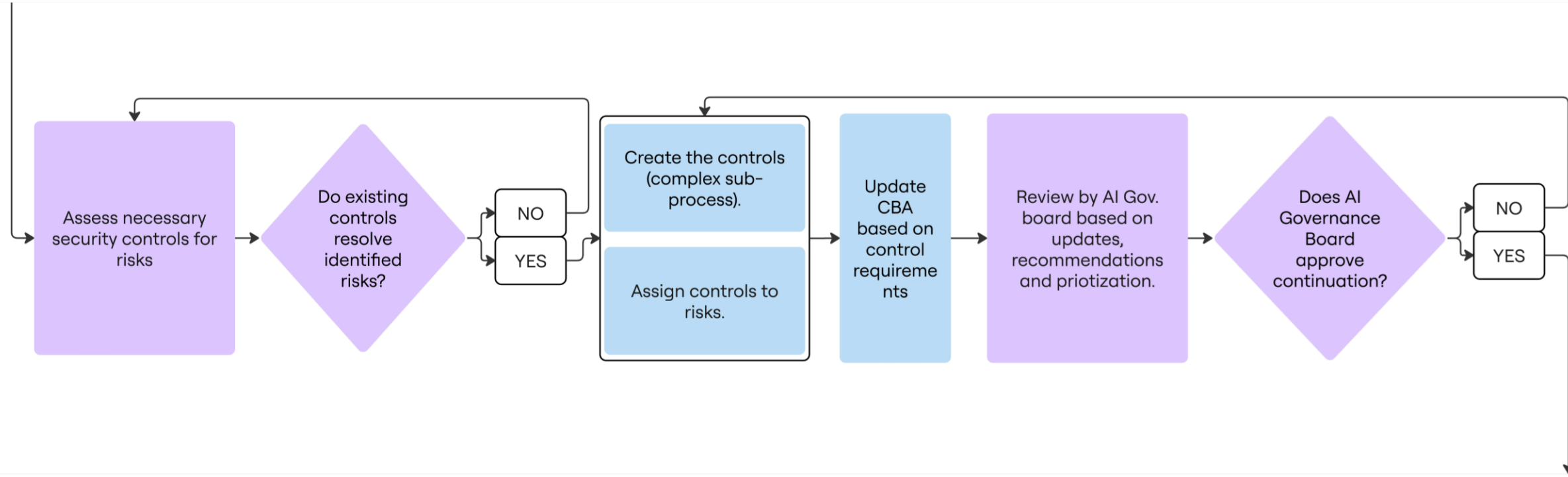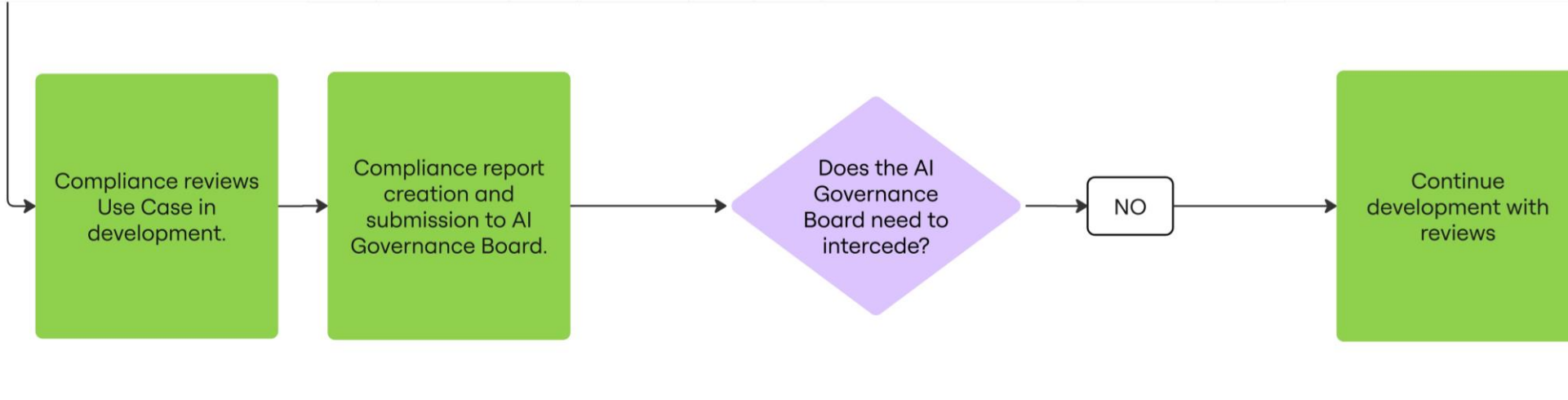*Don't overlook your adoption plan.*

Revisit security controls throughout the lifecycle.

Govern   Map   Measure   Manage

Development & Monitoring

Compliance reviews Use Case in development. → Compliance report creation and submission to AI Governance Board. → Does the AI Governance Board need to intercede? → NO → Continue development with reviews

Governance doesn't stop at development.

Align risk mitigation with your Red Team.

Thank You!

Every human has untapped potential.
We discover and nurture that potential.

in /mind-over-machines

✉ mindovermachines.com