

How Responsible AI Impacts Business Decisions



PEOPLE | ETHICS | BETTER DECISIONS



Responsible AI as a business decision discipline, not just compliance



Why now: enforcement, customer trust, board scrutiny, AI-driven operating models



The decision chain: data, model, product, deployment, monitoring, vendors



Ownership across executives, product, AI leads, risk, compliance, procurement



Core question: where does AI risk change go/no-go, pricing, risk appetite?



Why Responsible AI Is Now an Executive Priority



AI has shifted from experimentation to enterprise deployment



Governance is now an executive issue, not a technical detail



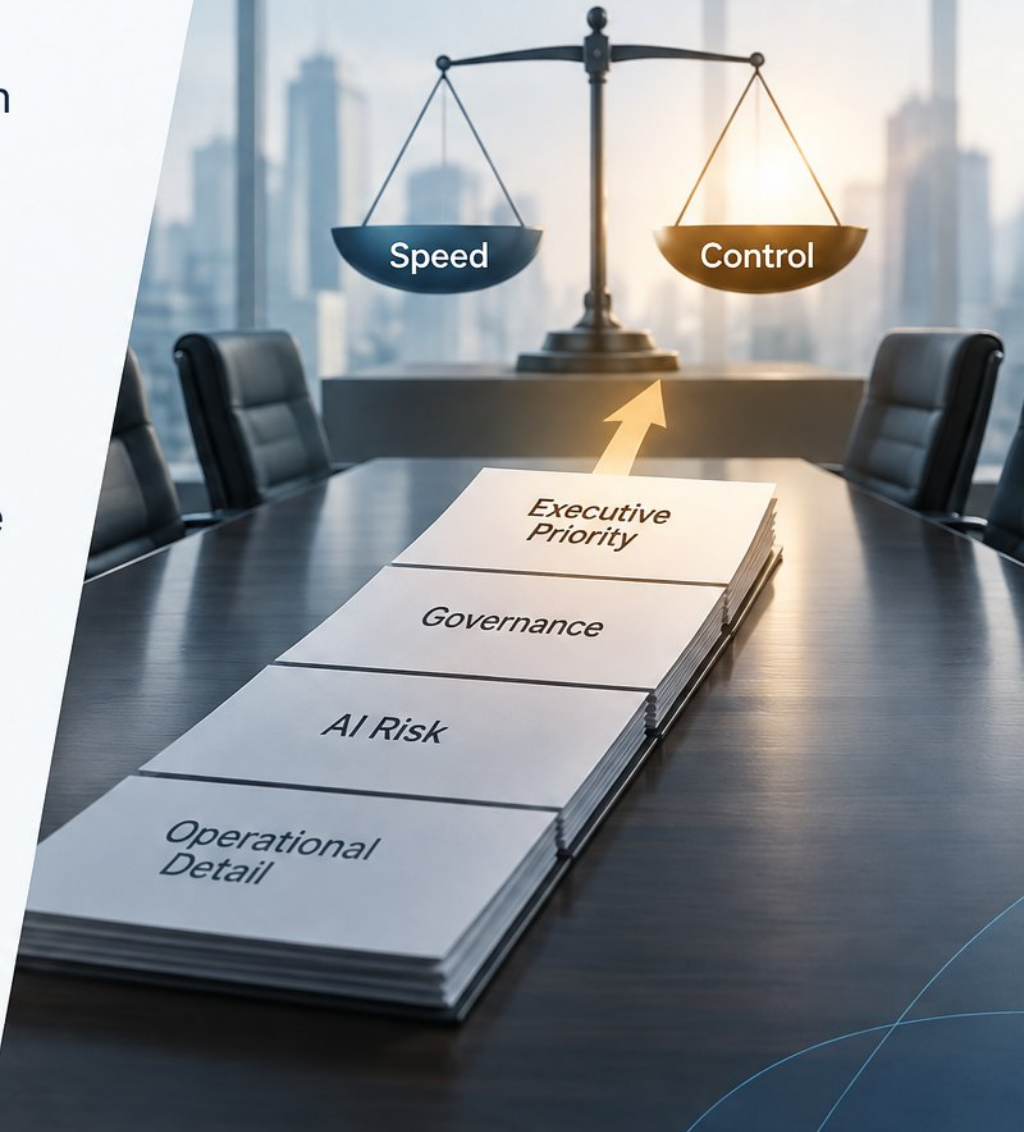
Regulators, boards, customers, and procurement teams expect evidence of controls



Responsible AI links to revenue growth, cost savings, and trust



Unmanaged AI risk: bias, opacity, data exposure, vendor dependency



Core Concepts: From Principles to Decision Criteria



Responsible AI: maximize benefit, minimize risk across the AI lifecycle



Core principles become business tests you can measure and audit



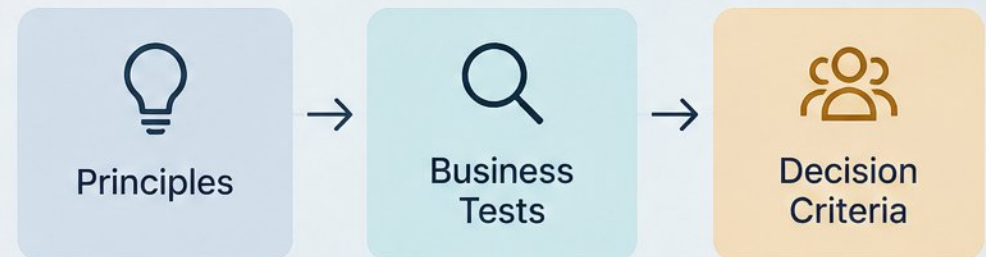
Aspiration vs. control: what is documented, reviewed, or escalated?



Watch for principle washing and stalled governance after policy launch



Decision screen: business value, risk tier, evidence, approval gates



Where AI Risk Enters the Business Decision Chain

From foundational inputs
to accountable outcomes



Regulatory and Compliance Landscape

Different approaches. A shared goal: trustworthy AI.



EU



Four regulatory models:
risk-based rules, transparency
duties, prohibitions, sector
oversight



EU AI Act:
general application and
Article 50 transparency
since 2 August 2026



Annex III high-risk duties
from 2 December 2027;
Annex I products from
2 August 2028



US



US: no federal AI law;
state patchwork on
transparency, employment,
health care



China



Regulation reshapes procurement, contracts, audit rights, and launch criteria.

Risk Assessment and Decision Frameworks

RESPONSIBLE AI
SAFER DECISIONS
STRONGER OUTCOMES



Eight-risk taxonomy: model, data, privacy, security, bias, operational, reputational, third-party



Prioritize risks using likelihood, severity, detectability, and reversibility



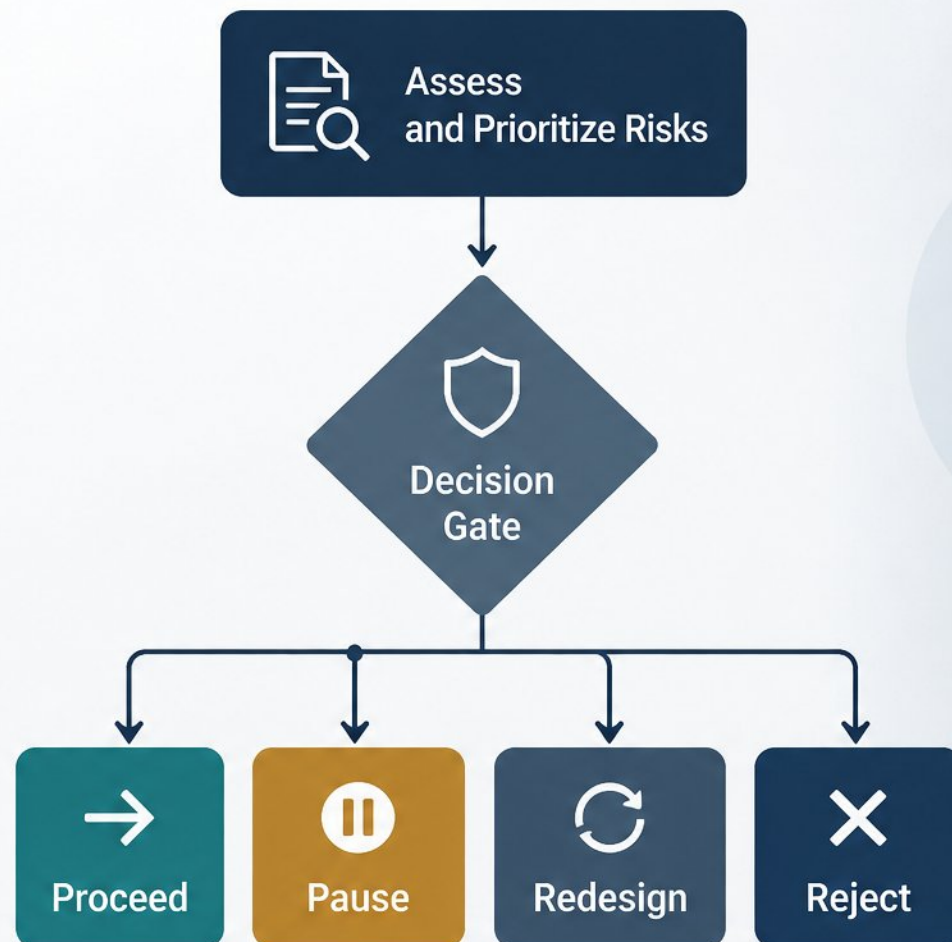
NIST AI RMF core: Govern, Map, Measure, Manage — iterative, not a checklist



Document with model cards, system cards, and regular impact assessments



Proceed, pause, redesign, or reject based on risk tolerance and board risk appetite



HIGHER STANDARDS
BRIGHTER POSSIBILITIES

Bias, Fairness, and Business Consequences

RESPONSIBLE AI
STRONGER OUTCOMES



Bias enters via data, labels, features, objectives, and feedback loops



Fallout: customer harm, discrimination, legal exposure, brand damage



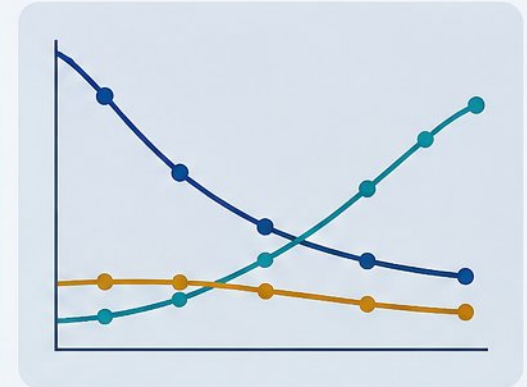
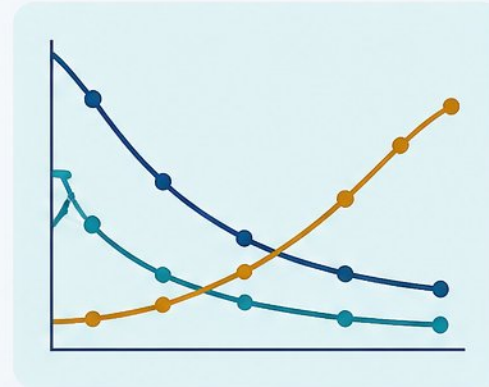
Fairness metrics conflict: demographic parity, equal opportunity, calibration



Impossibility results: not all fairness criteria can hold simultaneously



Decide when to adjust, constrain, or stop deployment



SPEED

CONTROL

Transparency, Explainability, and Customer Trust



Transparency means disclosing when AI is involved; **explainability** shows how decisions are made



Four explanation levels: system documentation, feature attribution, decision rationale, user disclosure



EU AI Act Article 50: AI interaction, synthetic content, emotion recognition, deepfake labelling



Poor or misleading explanations can undermine trust; use plain, user-friendly language



Balance proprietary protection with disclosure, human review, and appeal paths



Accountability, Governance, and Human Oversight



Governance structures: AI review boards, model risk committees, executive oversight



Three lines of defense: delivery, risk, and independent audit accountability



Human-in-the-loop, on-the-loop, or out-of-the-loop — matched to risk tier



Incident response, escalation, rollback, and remediation planning required



Documentation and audit trails that support defensible business decisions



Board expectations: strategic integration, named executive owner, risk appetite



Procurement and Third-Party AI Risk



Procurement is a control point: vendor models, data use, subcontractors, model updates



Demand audit rights, data-use limits, training restrictions, incident notice, termination



Due diligence: security, privacy, bias testing, explainability, compliance posture



Manage lock-in, version drift, data leakage, and hidden subcontractors



AI-specific clauses: lawful-training warranty, AI bill of materials, model cards, indemnity



Use a procurement checklist and vendor risk scorecard

CONTRACT



Measuring Business Impact and ROI

BALANCING RISK, TRUST AND GROWTH

Costs and Investment



- Cost side: controls, testing, documentation, review, monitoring — and slower launches
- 99% of organizations report AI-related financial losses; average loss $\approx$ US\$4.4M



Benefits and Value



- Benefit side: fewer incidents, faster approvals, stronger enterprise sales, better retention
- Real-time monitoring: 34% more likely to grow revenue, 65% more likely to cut costs



Measure ROI holistically:
economic, reputational, and capability (real options) returns



Dashboards:
risk exposure, control coverage, incident trends, approval cycle time

Regulatory Deep Dive: EU AI Act and US State Laws

DIFFERENT JURISDICTIONS. SHARED GOAL: RESPONSIBLE AI.

PEOPLE
POLICY
PROGRESS

EU AI Act

2 August 2026

EU AI Act:
general application
since 2 August 2026;
Article 50 transparency live

2 December 2027

Annex III high-risk
obligations apply from
2 December 2027;
Annex I from 2 August 2028

2 August 2028



Providers

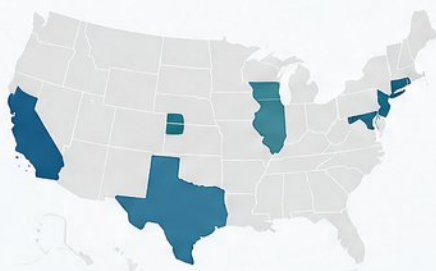
Providers own
AI literacy and
marking



Deployers

Deployers own
disclosures and
oversight

US State Laws



California
Colorado
Illinois
Texas
Connecticut
NYC

US state patchwork:
California, Colorado, Illinois,
Texas, Connecticut, NYC

Key Sectors



Employment



Health care



Lending



Housing



Consumer
protection

Sector rules bite in employment,
health care, lending, housing,
consumer protection

Compliance Approach



Complain to the strictest benchmark;
keep controls flexible; track preemption

CLEARER RULES. BRIGHTER OPPORTUNITIES.

Implementation Roadmap and Action Plan

90-day plan: inventory AI use cases, classify risk, assign owners



Build cross-functional operating model; train product, procurement, risk, compliance



Common pitfalls: skipping triage, gate theater, no named owner after Day 90

Decision Scenarios and Role-Based Applications

PEOPLE
PROCESS
RESPONSIBLE AI
BETTER DECISIONS



Scenario 1

AI hiring tool — go/no-go hinges on bias testing and human review



Scenario 2

Vendor model changes — demand audit rights and change notification



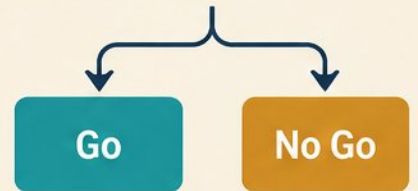
Scenario 3

Bias found in production — escalate, remediate, disclose, retest



Scenario 4

Pause high-value AI when compliance risk stays unresolved



Role checklists

executives, product, AI leads, risk, compliance, procurement



executives



product



AI leads



risk



compliance



procurement

Decision screen

business value, risk tier, evidence, approval gates



business value



risk tier



evidence



approval gates



CLEAR SCENARIOS.
ALIGNED ROLES.
RESPONSIBLE OUTCOMES.

Key Takeaways and Next Steps



Responsible AI is a business decision discipline shaping go/no-go, pricing, and risk appetite



Principles must become operational controls: risk tiers, evidence, gates, escalation



Regulation is a design input; compliance timelines are already in force



Bias, transparency, accountability, vendor risk are core business risks



Next steps: inventory AI, name owners, set risk appetite, launch the 90-day roadmap



PersonWise.

PersonWise • AI digital-human course platform



Scan the code or click anywhere to watch this course live, with voice Q&A

personwise.ai/t/0b449a92/public