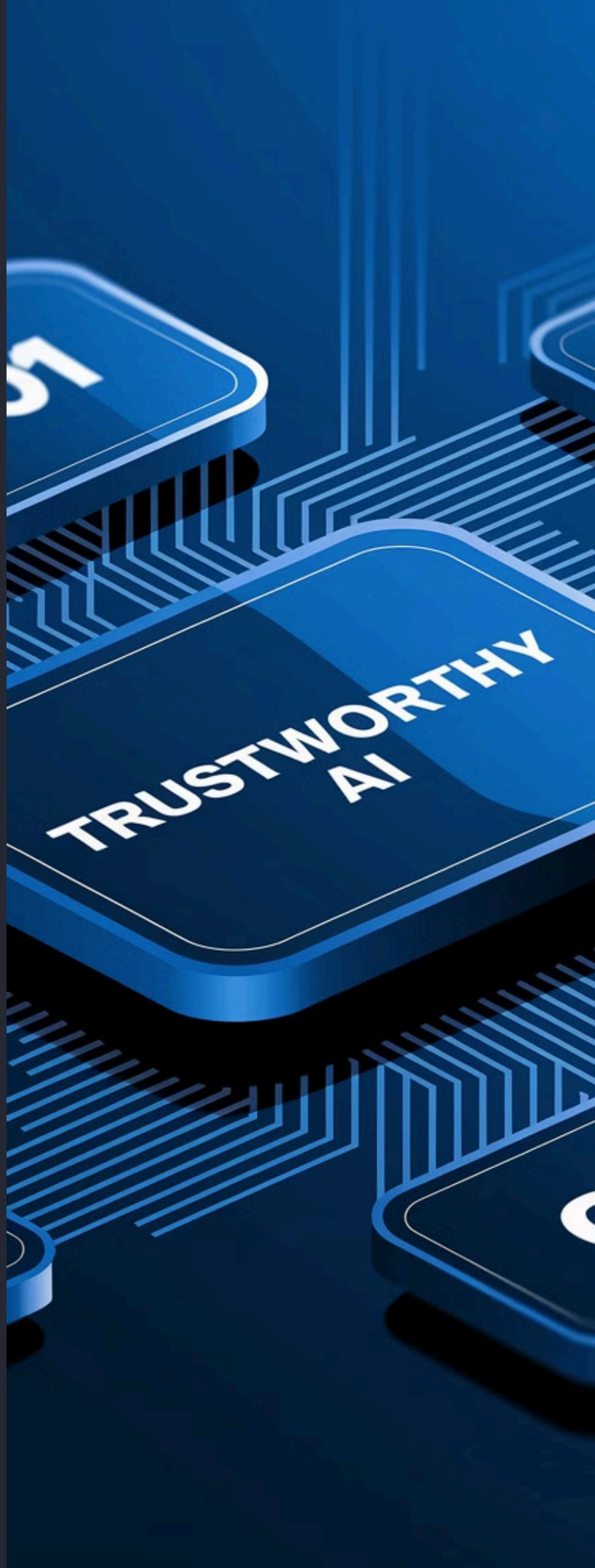
# The Trifecta of Trust: How ISO, NIST & GDPR Align on AI Risk

A comprehensive guide to navigating the overlapping frameworks that shape responsible AI governance in today's regulatory landscape.

@1davidclarke



# The Problem

### Rapid Innovation

AI technology is developing at unprecedented speed. New capabilities emerge weekly.

### Trust Gap

Public confidence struggles to keep pace. Concerns about ethics, bias and privacy persist.

### Regulatory Uncertainty

Organisations face a complex landscape of evolving standards and requirements.

# The Overlap Opportunity

## ISO 42001

Formalises AI management systems with clear governance requirements.

## NIST AI RMF

Provides flexible risk management approach across the AI lifecycle.

## GDPR

Establishes legal foundation for data protection and algorithmic processing.


# Accountability

### GDPR Demands

Controllers must demonstrate responsibility for automated processing. Documentation is essential.

### NIST Approach

Treats accountability as fundamental. Cross-cutting function that spans systems.

### ISO 42001 Structure

Formalises accountability through defined governance roles. Clarifies responsibilities.

# Transparency

### Explainability

GDPR requires that automated decisions be explainable to affected individuals.

### Interpretability

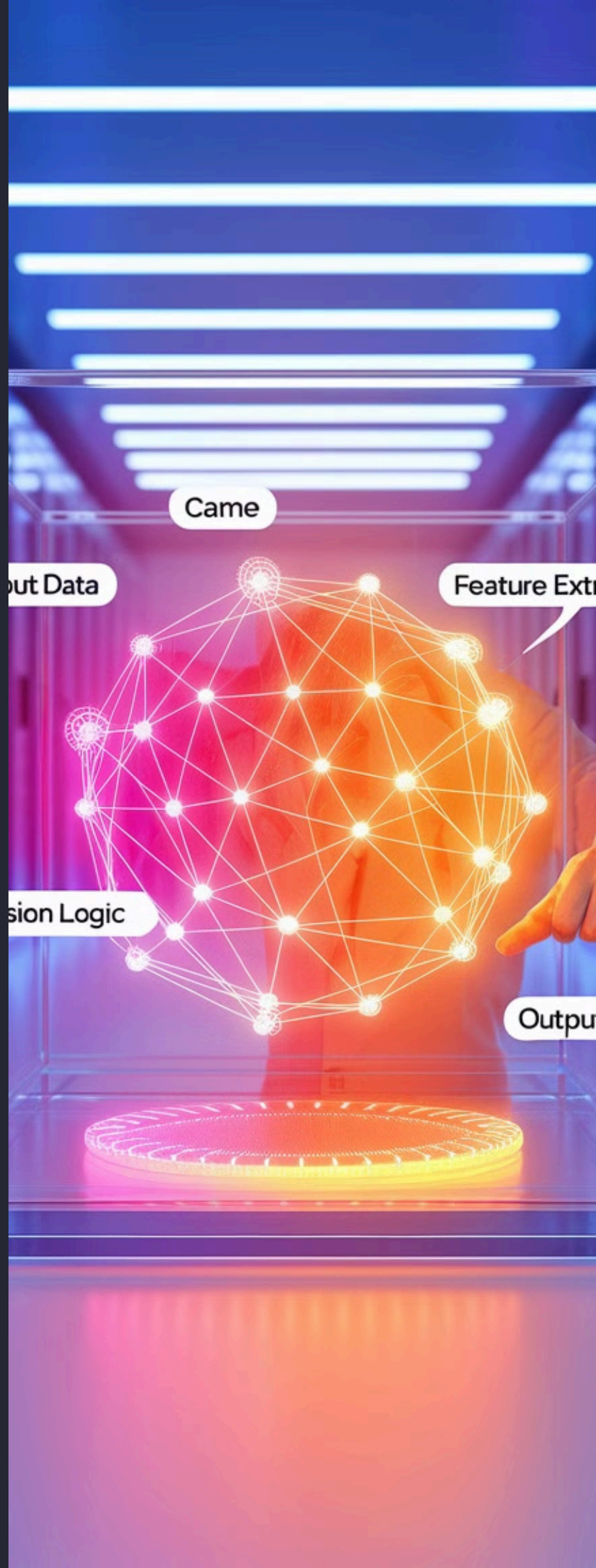
NIST emphasises understanding how AI systems make decisions. No black boxes.

### Documentation

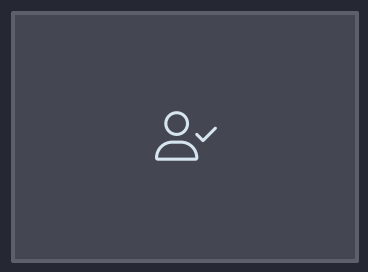
ISO 42001 mandates thorough records throughout the AI lifecycle.

### Trust Building

All frameworks agree: Transparent AI earns stakeholder confidence.

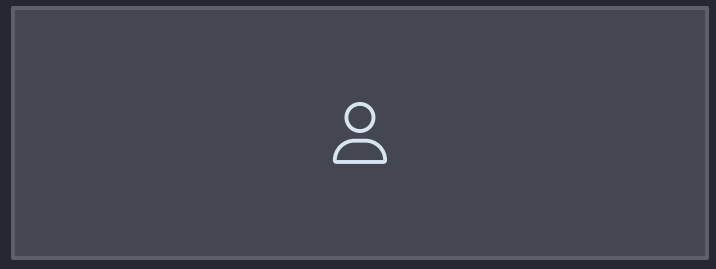


# Human Oversight



## Human Review Rights

GDPR guarantees affected individuals can request human intervention.



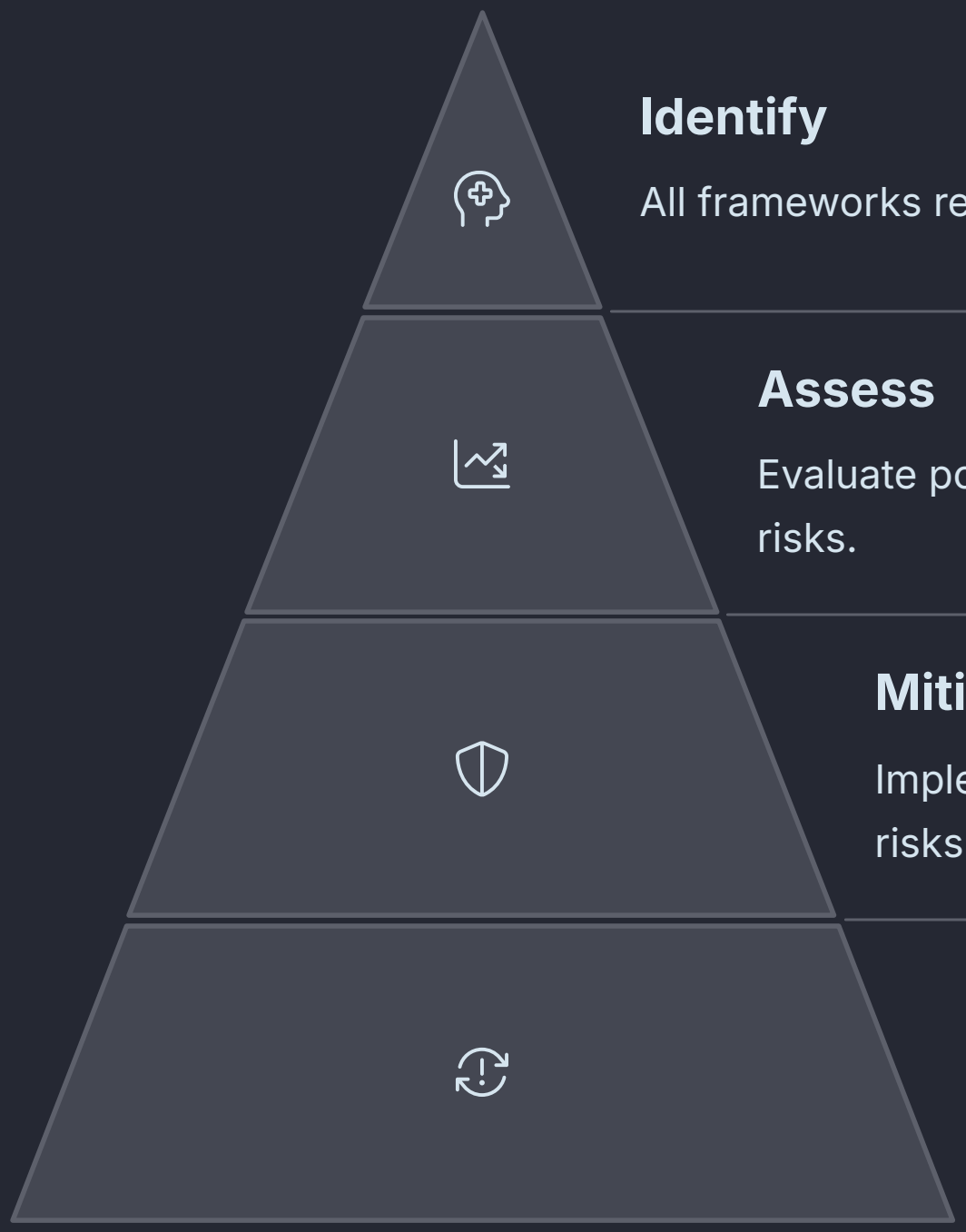
## Configurable Teams

NIST encourages flexible human-AI collaboration models.

## Lifecycle Supervision

ISO 42001 embeds human oversight from design to decommissioning.

# Risk Management



## Identify

All frameworks require systematic discovery of potential risks.

## Assess

Evaluate potential impacts and likelihood of identified risks.

## Mitigate

Implement controls to reduce or eliminate priority risks.

## Monitor

Continuously track effectiveness through documented audit trails.


# Implementation Strategy

### Map Your Framework Overlaps

Identify where ISO 42001, NIST AI RMF and GDPR requirements converge. Focus on these areas first.

### Consolidate Documentation

Create unified records that satisfy all three frameworks. Avoid maintaining separate compliance systems.

### Implement Shared Controls

Deploy governance mechanisms that address multiple requirements simultaneously. Leverage the synergies.

### Continuous Improvement

Regularly review your integrated approach. Adapt to evolving interpretations of all frameworks.