NULL/OWASP CHENNAI MEETUP, 2025

ROHIT KUMAR

GRC RISK ANALYST, LOGITECH

# AI in GRC
# Enhancing Governance and Governing AI

## A dual perspective on transforming GRC and overseeing AI responsibly

# Oveview

01 **What is GRC?**

Aligning IT and business with policies, risk management, and regulations

02 **Why AI+GRC?**

Data deluge and regulatory complexity require intelligent tools

03 **Part 1: AI for GRC**

Use cases (risk monitoring, compliance automation, etc.).

04 **Part 2: GRC for AI**

AI-specific risks, ethics, regulations (EU AI Act, NIST, etc.).


⚠️ Note: This is not a seminar, not a lecture - Let’s talk

# What is GRC?

**Governance**

**Policies, oversight, and structures to meet objectives.**

**Risk**

**Identifying, assessing, mitigating financial, security, legal risks.**

**Compliance**

**Ensuring operations follow laws, regulations, internal policies.**

## Integrated Approach

GRC combines these to reliably achieve objectives while addressing uncertainty and acting with integrity

## Benefits

Data-driven decisions, streamlined processes, reduced silos

# Why Combine AI and GRC?

## 01 Data Explosion

Organizations have more data and faster-changing regulations than ever.

## 02 Automation Potential

McKinsey notes up to 80% of an employee's time could be spent on AI-automatable tasks

## 03 Speed & Scale

AI can process vast logs, policies, and threat data continuously.

## 04 Industry Trend

Gartner predicts "by 2025, over 50% of major enterprises will use AI and ML to perform continuous regulatory compliance checks," up from <10% in 2021

# AI in Risk Monitoring and Reporting

## CONTINUOUS RISK MONITORING

AI ingests live feeds (logs, metrics, threat intel) for 24/7 vigilance.

## ANOMALY DETECTION

Models automatically flag unusual behavior or outliers in network, application, and user data.

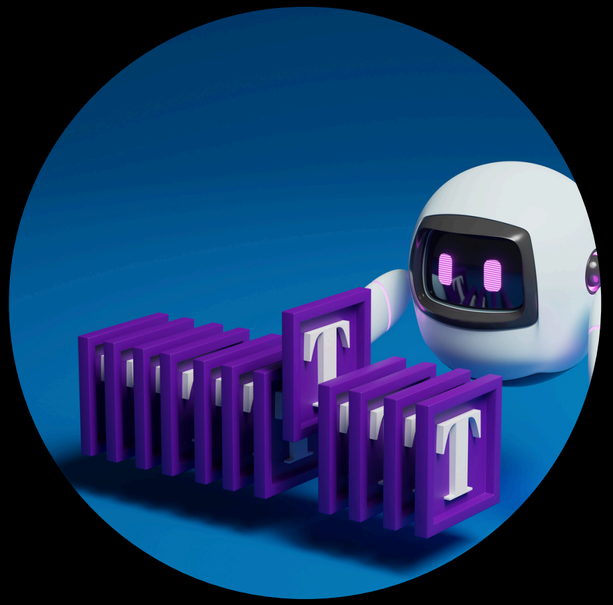
## IMMEDIATE ALERTS

Reduces lag in seeing new risks; risk teams are notified in real time.

## METRICSTREAM SURVEY

48.2% of organizations are actively piloting AI for risk monitoring

# AI for Compliance Automation



## Routine Task Automation

Controls testing, policy document review, regulatory change scans.

## Consistency & Speed

AI chatbots or generative tools answer policy questions instantly.

## Audit Streamlining

Populate audit docs, generate reports from raw data.

## MetricStream Survey

43.5% of GRC teams are automating compliance workflows with AI

# AI in Third-Party Risk Management

## 01 Continuous Vendor Monitoring

AI scans supplier data, news feeds, social media for risk indicators and even dark net to gather all the intel of a vendor

## 02 Automated Analysis

Extracts insights from vendor contracts, ESG reports, financials and security questionnaires.

## 03 Real-Time Alerts

Flags signs of vendor trouble (e.g. breach news, financial distress).

## 04 MetricStream Survey

21.2% of organizations leverage AI for third-party risk

# RegTech Case – KYC and AML

AI-driven solutions for compliance in finance and other regulated industries.

## KYC/AML AUTOMATION

AI models verify identities and detect fraud faster.

## ANTI-MONEY LAUNDERING

Pattern recognition across transaction data to catch unusual activity.

## COST SAVINGS

A Juniper Research report projects ~$1.2 billion in compliance cost savings by 2023 through AI-driven RegTech

## INSIGHT

AI finds complex fraud patterns and reduces false positives, improving audit outcomes.

# Benefits of AI in GRC

## Efficiency & Cost Reduction

Automates 80% of tasks: e.g. 65% lower breach costs with AI in security.

## Proactive Insights

Shifts GRC from reactive to predictive; leaders see risk “hotspots” in advance.

## Continuous Coverage

24/7 monitoring and compliance checks, no “off” hours.

## Better Reporting

AI-generated dashboards and summaries support data-driven decisions.

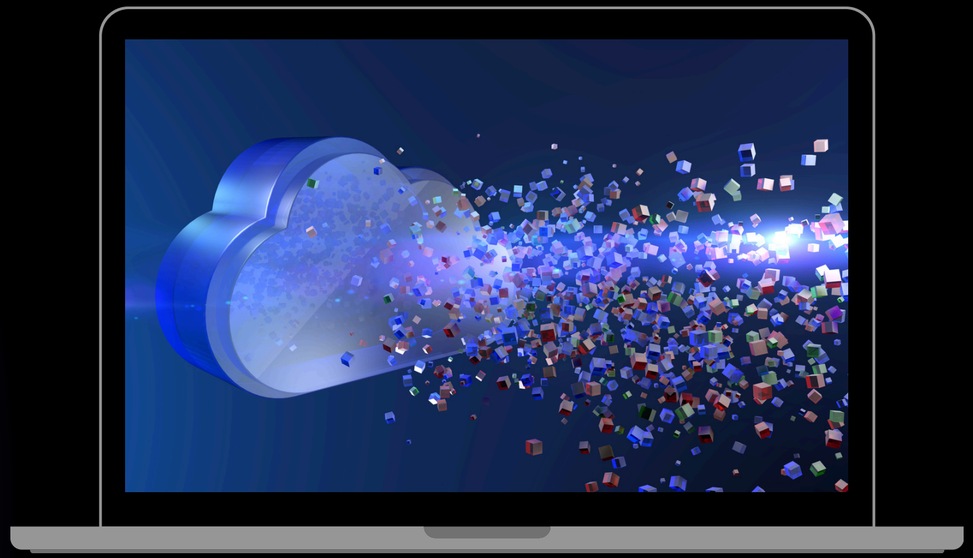
## Industry Voice

“AI will continue to reshape the GRC landscape…advancements in anomaly detection, predictive analytics, and automated reporting”

## Competitive Edge

Early AI adopters gain faster decision-making and stronger controls.

# L E T ’ s  h a v e  a  C h a t



# Why We Need GRC for AI

01 **New Category of Risk**

AI systems can introduce errors, biases, or unpredictable behaviors that impact compliance and safety.

02 **Regulatory Focus**

Governments are beginning to regulate AI (e.g. EU AI Act, US executive orders).

03 **Data Liability**

IBM reports only 29% of enterprises trust their data is ready for GenAI, highlighting data governance gaps

04 **Accountability Demand**

As Deputy AG Lisa Monaco noted, compliance reviews now consider “how well the program mitigates the company’s most significant risks … including … misusing AI.”

05 **Trust & Reputation**

Unchecked AI can cause scandals (e.g. biased decisions); GRC ensures responsible AI aligns with business values.

# AI-Specific Risks to Govern

## Bias & Fairness

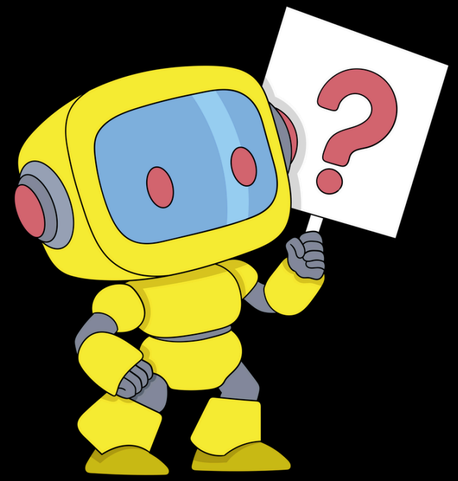
AI trained on biased data can discriminate (e.g. in hiring, lending). IEEE and regulators emphasize bias audits.

## Data Privacy

AI often requires huge datasets. Personal data in training can conflict with GDPR/CCPA if not handled properly.

## Security Threats

AI systems face adversarial attacks, model theft, or data poisoning that corrupt outcomes.




## Operational Risk

Unintended behaviors, system failures, or unethical recommendations from AI.

## Compliance Violations

Rogue or misconfigured AI might output advice that breaches regulations (fraudulent loan approvals, etc.).

## Transparency & Explainability

Many AI models (especially deep learning) are “black boxes.” Lack of explainability impedes compliance (e.g. GDPR “right to explanation”).

## Survey Findings

93% of orgs acknowledge GenAI risks, but only 9% feel prepared

# Regulatory Landscape


## EU AI Act (2024/2025)

Risk-based categories (unacceptable, high, limited, minimal) with mandatory controls for high-risk AI (risk assessments, transparency, data quality)

## US Regulations

State: NYC Local Law 144 (bias audits for hiring AI); CCPA/CPRA (automated decision profile consent).

Federal: FTC Act (no unfair/deceptive AI practices); Biden EO on AI (setting federal standards, NIST leadership).

## Other Jurisdictions

China’s AI guidelines, India’s draft AI policy – watch global trends.

Note: Even non-AI-specific laws (GDPR, anti-discrimination laws) apply to AI.

## Implication

AI projects must map to both technology standards (like NIST AI RMF) and legal requirements (like EU AI Act).

# AI Governance Frameworks

## NIST AI Risk Management Framework (RMF 1.0, 2023)

Four core functions – Govern, Map, Measure, Manage – for trustworthy AI

## ISO/IEC 42001:2023

The first AI management system standard; specifies requirements for an AI governance system.

## IEEE 7000 Series

A family of standards (e.g. IEEE 7001 for transparency, 7003 for bias) focused on ethical design.

## OECD AI Principles

(2019, updated 2024) Widely-endorsed guidelines emphasizing human rights, fairness, accountability

## Company Controls

Many firms are developing internal AI policies/councils or adopting frameworks like COBIT or their own “AI boards.”

**Takeaway:** Multiple frameworks exist; choose or align those fitting your organization (ISO 42001 + NIST RMF is a strong combo).

# Key Challenges Integrating AI into GRC


### Legacy Systems & Data Silos

Existing platforms often lack APIs or integration points. Bridging old systems to new AI tools requires effort.

### Skill Gaps

Shortage of professionals with both deep AI and GRC expertise

### Data Quality

AI is only as good as the data it's trained on. Incomplete or biased data undermines models.

### Regulatory Uncertainty

Evolving guidelines on AI transparency, ethics, and liability

### Security of AI

Models and pipelines themselves can be attacked (e.g. data poisoning, model theft)

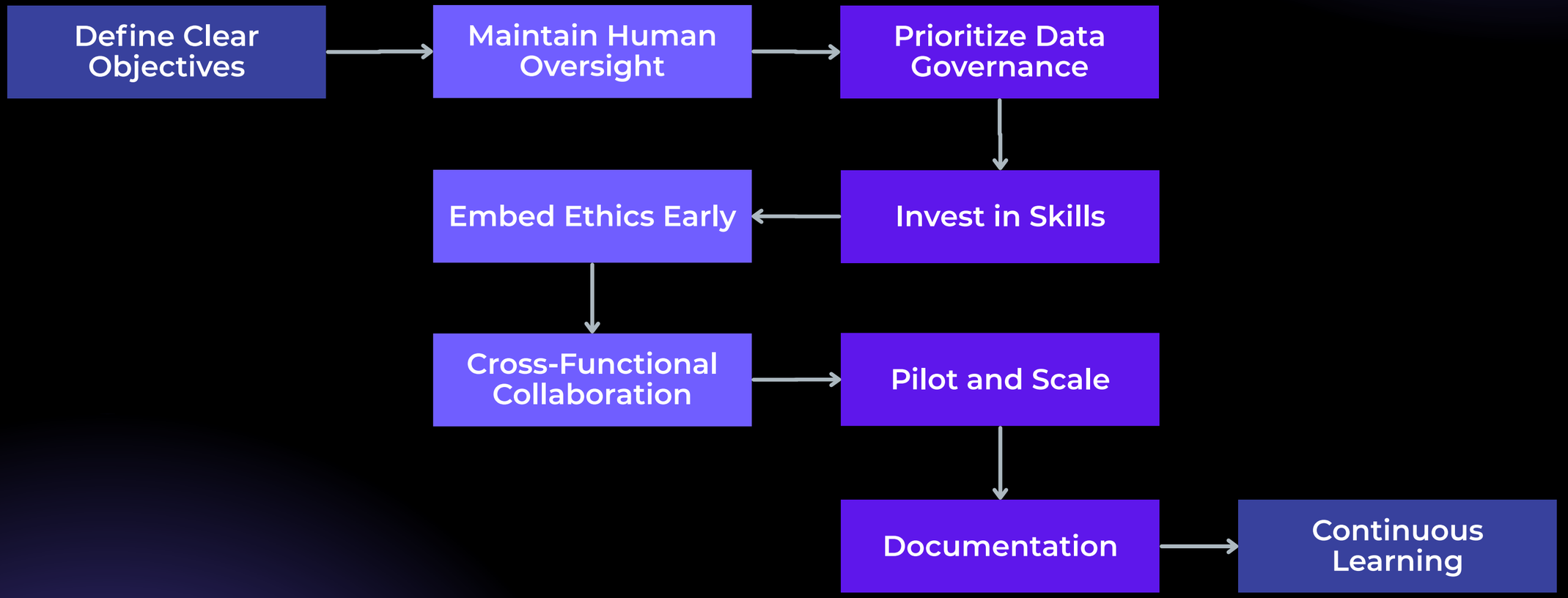
### Ethics & Bias

Risk of AI outputs conflicting with inclusion goals

### Organizational Resistance

Change management – getting stakeholders to trust and adopt AI tools.

# Best Practices & Recommendations



# Conclusion and Key Takeaways

- **AI is a Game-Changer for GRC:** Empowers 24/7 risk monitoring, smarter compliance, cost savings
- **GRC is Essential for AI:** We must govern AI to ensure fairness, safety, and legal compliance
- **Strategic Imperative:** As one expert puts it, a strong AI governance program “is no longer optional but a strategic imperative”
- **Action Items:** Start small, align AI projects with your GRC framework, upskill your team, and establish clear AI policies.

The organizations that proactively embrace AI in GRC – with the right controls – will gain a competitive edge and build greater stakeholder trust.

**AI will continue to reshape the GRC landscape...with advancements in anomaly detection, predictive analytics, and automated regulatory reporting.**

# Thank You

Scan for Resources

Scan for Contact