Chartis

VALIDMIND™

AI Risk Summit

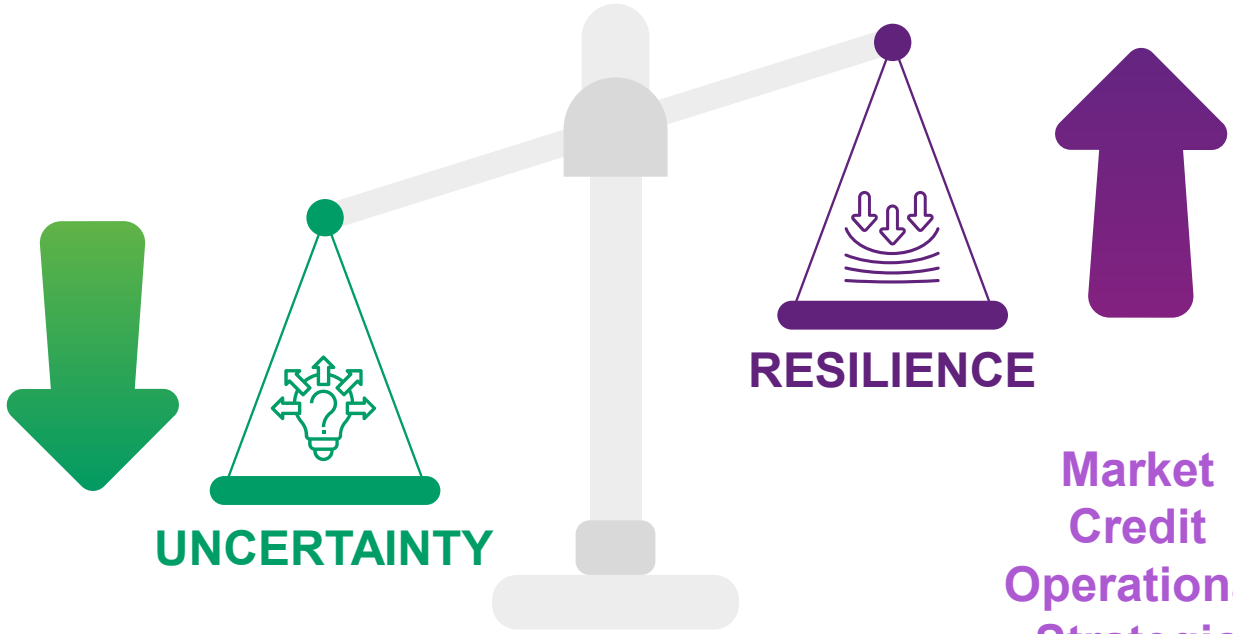
Michael Versace
Chartis Research
Michael.Versace@chartis-research.com

December 2, 2025

Uncertainty Demands Resilience

Governance
Risk
Compliance

~~Governance~~
Resilience
~~Compliance~~

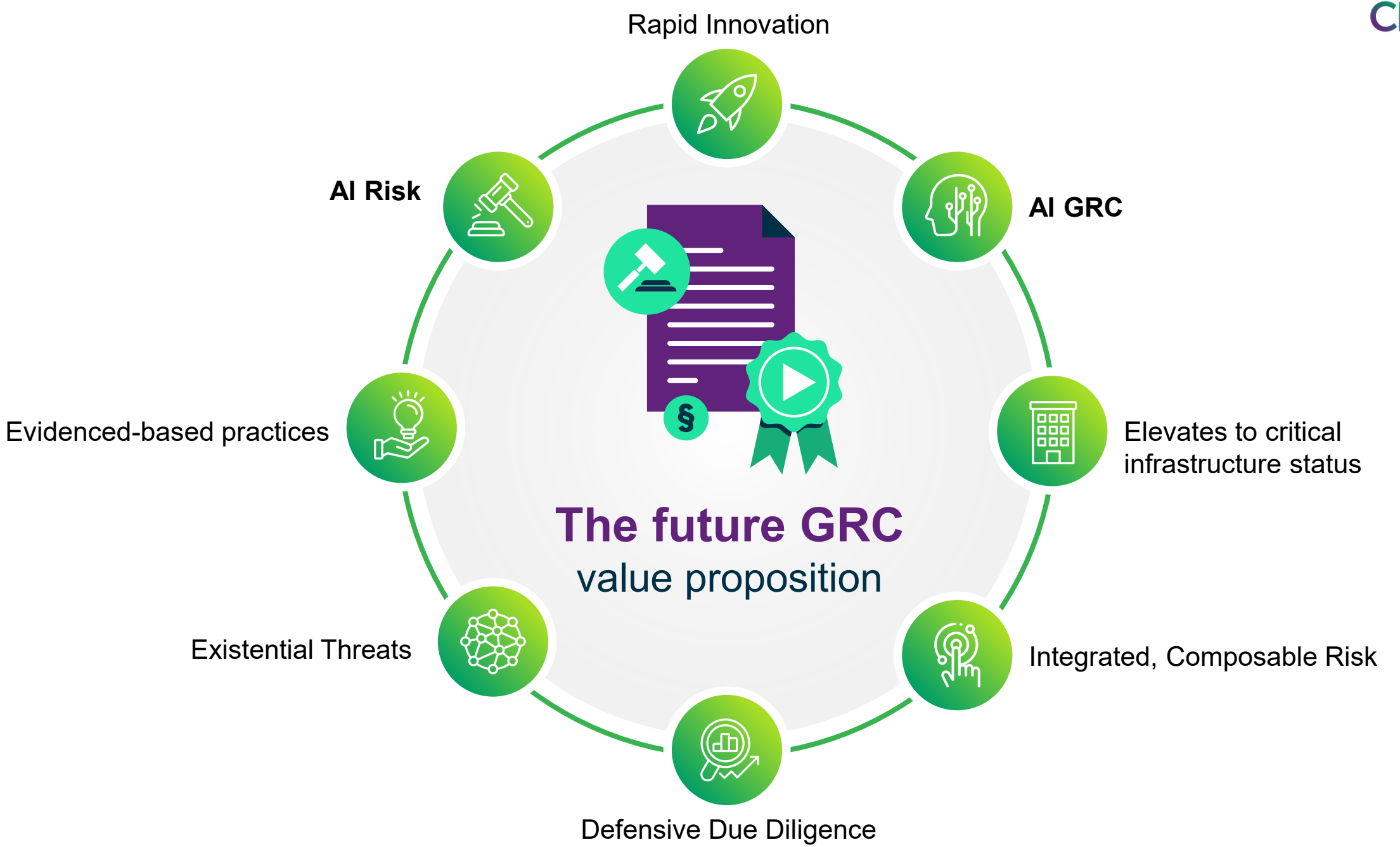


Geopolitics and leadership
Shifting supply chains
Rapid innovation, FOMO
Market structure, private credit, decentralized finance
Operational risk

Market
Credit
Operational
Strategic

Chartis Research | 2025
Copyright Infopro Digital Services Limited 2025. All rights reserved.

Chartis


Rapid Innovation
AI Risk
AI GRC
Evidenced-based practices
Elevates to critical infrastructure status
The future GRC
value proposition
Existential Threats
Integrated, Composable Risk
Defensive Due Diligence

Chartis

GDP – AI = 0.0

Michael Hsu

Former Acting US Comptroller of the Currency,
October 2025

AI Risk and Governance

Integration, automation, and industrialization

Chartis

Across the organization

Increased regulatory incidence

Regional context

Increased focus on tools

Consumer and enterprise models

Opportunities by institutional expansion

Integration of varied elements across the model cycle

Technology increasingly central

Traditional models still very important

Risks and confidence builders

- ✓ As firms mature in adoption, strategic clarity and leadership buy-in improve, but skills, resources, and regulatory clarity remain critical hurdles.
- ✓ While infrastructure and performance challenges are improving, data quality, integration, and trust remain the biggest obstacles to scaling AI effectively in compliance
- ✓ As internal alignment and strategic focus strengthen with AI maturity, external pressures grow as the defining hurdles for long-term adoption.
- ✓ Agentic AI is a double-edged sword: it promises efficiency but raises questions about control, accountability, and regulatory compliance.
- ✓ Unlike GenAI, Agentic AI is seen as challenging institutional governance and oversight

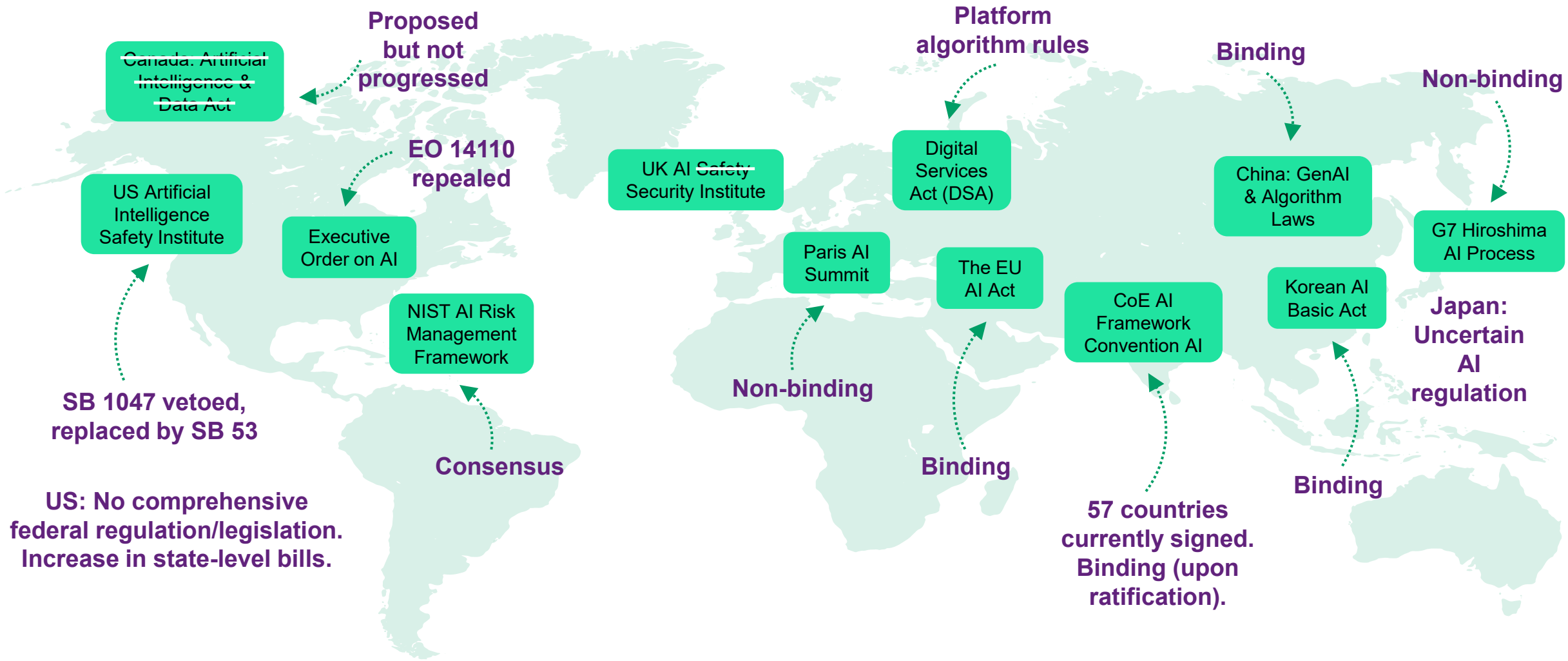
Chartis

Business Risks	Technical Risks	Data Risks	Agentic/Agent Risks
• Insufficient expertise/resource. • Resources to support AI systems post-deployment. • Persistent uncertainty over compliance expectations. • Knowledge gaps at executive levels Note: Business confidence improving in: • Clarifying strategy • Business case justification • Organizational alignment	• Poor-quality training data, foundational data availability and integrity overall • Integration & difficulty embedding AI into legacy infrastructures. • Judging model performance and operational trust • Scalability and post-deployment model upkeep less critical	• Regulatory clarity • Data privacy • Unclear data strategies • Insufficient data expertise Note improvement in: • Learnings from disappointing past experiences	• Inability to meet auditability and accountability requirements\ • Job displacement and over-reliance on automation • Unease about losing human expertise or oversight as AI becomes more independent. • Diminished accuracy and performance visibility • Data privacy or information security risks and cyber risk frameworks • With GenAI risks skew toward data quality and explainability,

Chartis Research | 2025
Copyright Infopro Digital Services Limited 2025. All rights reserved.

AI regulation

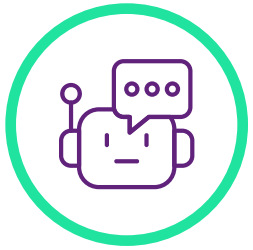
Diverse, but sufficient to assess AI model risk, acquire tooling, and design GRC coverage



What degree of assurance is actually possible

Insurers staging a retreat – a “systemic, correlated, aggregated risk”

AIG, Great American and WR Berkley seek permission in the US to limit liabilities from AI models, agents, chatbots.



Industry leaders look to offer policies excluding liabilities tied to businesses deploying **AI tools including chatbots and agents.**

Claims could be excluded if related to “any actual or alleged use” of AI, including any **product or service sold by a company “incorporating” the technology.**

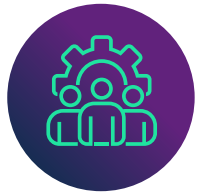
- Too much of black box
- Claims are likely to increase over time
- Who’s liable with things go wrong

AI risk potentially involves many different parties, including developers, model builders and end users.

Does AI need an enterprise *“Code of Conduct”*

Data governance

- High-quality datasets
- Assess potential distortions and biases
- Privacy and copyright controls
- Relevant, error-free, and secure data



Human Oversight

- HITL
- Preventing health and safety risks
- Ability to decide not to use, question the system in any situation

Monitoring and remediation

- Continuous risk identification and analysis
- Dispute resolution
- Mitigation plans definition

Transparency and provision

- Ensure sufficiently transparent operation so that results can be interpreted, reproduced, judged

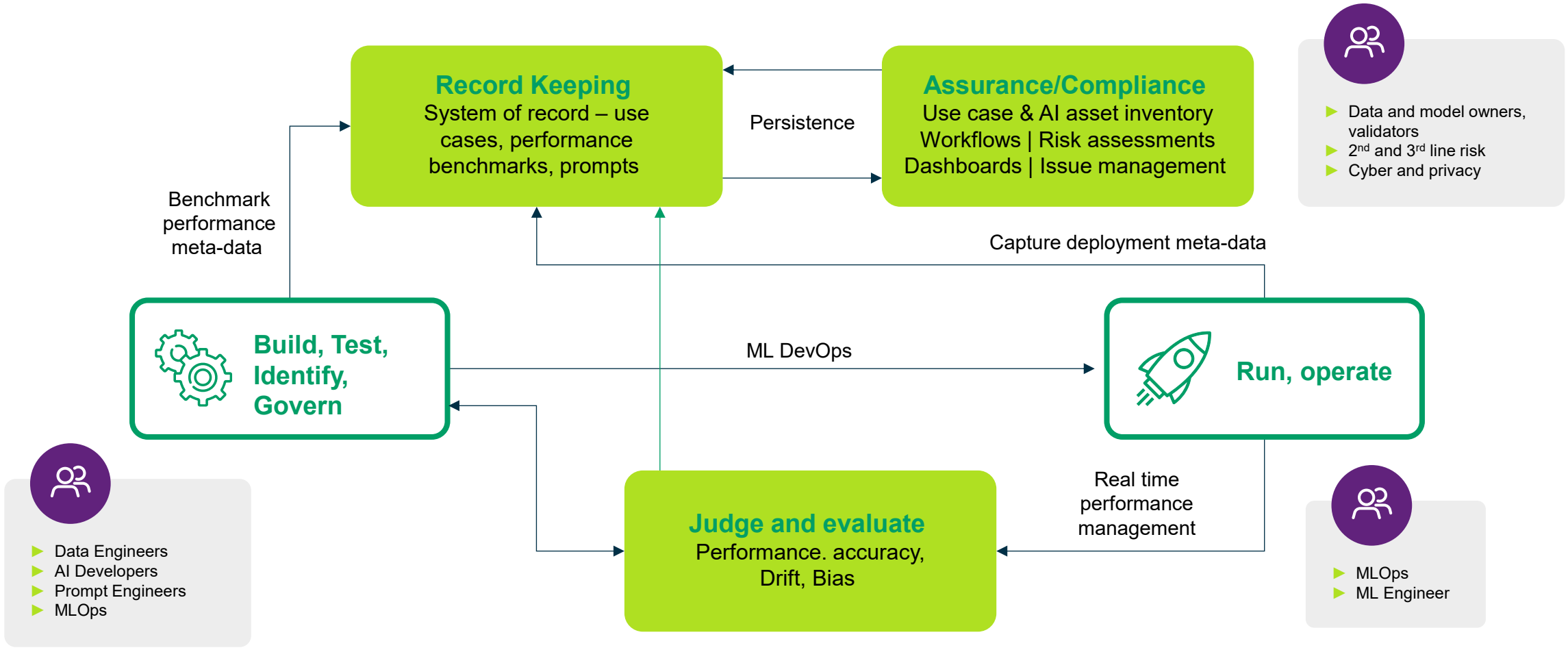
Technical persistence

- Detailed documentation about system monitoring, operation, and control
- Event logging and traceability

Identity, access, resilience

- Identity and access control
- Systems resistant to errors, failures, and inconsistencies
- Resistant to unauthorized attempts to alter use and operation

The CoC spans a lifecycle of AI models and LODs



Chartis

Unified GRC, MLOps, Model Risk Management, and Cybersecurity

A unified approach for managing model assets, evidence, performance attributes, and documentation from pre to post deployment, across the enterprise.

GRC Integration

Embedding AI into Governance, Risk, and Compliance content and workflows

- Policy and internal control associated with regulatory frameworks and compliance obligations.
- Real-time risk intelligence dashboards offering forward-looking views for boards and executives, not just rear-facing compliance reports.
- Continuous controls monitoring, proactive stakeholder engagement, and structured documentation (with clear ownership and audit trails) through unified platforms rather than disparate systems.

MRM & MLOps Integration

The intersection with MLOps provides:

- Testing, validation, automated version control and tracking of model changes, supporting audit and lifecycle management.
- Performance monitoring to detect drift, bias, and other issues, feeding governance processes for oversight and feedback loops.
- Ethical data usage guidance embedded in deployment pipelines, leading to dynamic and explainable AI across the ML lifecycle.

MRM Integration

The intersection with MRM provides:

- Secure data validation, authentication, and robust access controls to reduce bias and prevent adversarial exploits.
- New, model-specific security metrics and incident response protocols tailored for the rapid cascade effects if models are compromised.
- Continuous threat modeling specific to AI pipelines (including unique attack surfaces) and secure data integrity assurance.

Chartis

AI Risk

Robust AI model governance builds on some practices from GRC and financial model risk management and creates new automation

Ongoing monitoring post-deployment to detect performance issues, drift, and changing risk exposures.

Maintaining detailed documentation and validation records to meet regulatory and audit demands.

Structured identification, mitigation, and clear accountability assignment to manage risks effectively.

Cybersecurity Alignment

Cybersecurity is a foundational pillar for AI model governance, ensuring:

Secure data validation, authentication, and robust access controls to reduce bias and prevent adversarial exploits.

Continuous threat modeling specific to AI pipelines (including unique attack surfaces) and secure data integrity assurance.

New, model-specific security metrics and incident response protocols tailored for the rapid cascade effects if models are compromised.

Capability	GRC	MLOps	Model Risk Management	Cybersecurity
Compliance Mapping	Automated, multi-framework mapping	Policy updates via pipelines	Validation & audit records	Secure regulatory adoption
Risk Intelligence	Predictive dashboards	Bias & drift monitoring	Ongoing model reviews	Threat modeling & incident response
Monitoring & Audit	Real-time controls, unified platform	Version & performance tracking	Cross-functional documentation	Secure validation & monitoring
Ethical AI Practices	Board-level AI ethics, explainability	Data usage guidelines, explainable operations	Transparency & stakeholder feedback	Foundational security for ethical compliance

What to Watch

AI Governance becomes the platform for adoption, growth, and new phase of GRC innovation

1. Confidence builds, risks persist, solutions proliferate, standards drive regulator clarity, first line data and model engineering resources increase, success rates rise.
2. GRC principles, MRM and DevOps practices become embedded and expand with new tooling in AI system development, deployments
3. AI governance tooling creates confidence in the first line of defense and creates new pathways for compliance automation/benchmarking and independent audit
4. Potential insurance carve-outs drive more third-party AI transparency and accountability
5. Enterprise AI Codes of Conduct begin to emerge for agentic and agent-centric systems, built from consensus standards, as stakeholder responsibilities become clearer

Thank you

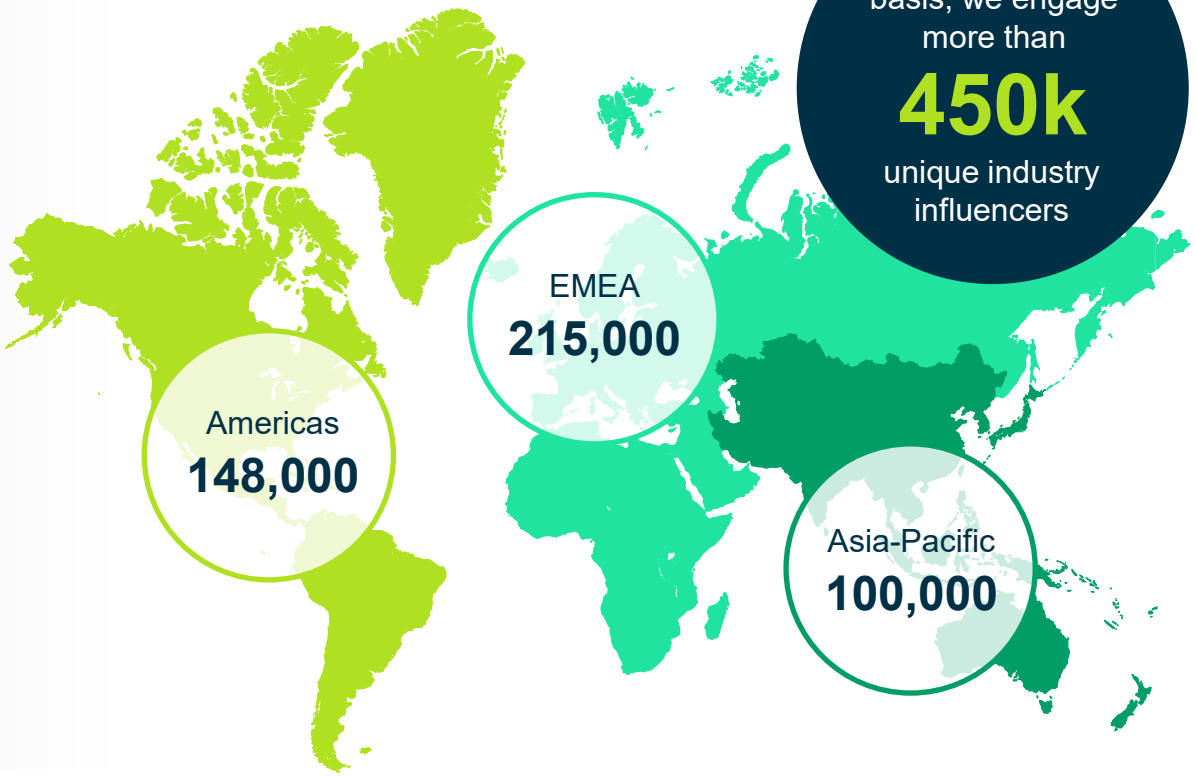
Who we are

Chartis Research is a global advisory and research firm with a decade of experience dedicated to risk technology and needs of vendors, end-users, and investors in the financial markets.

For risk technology vendors, clients engage with Chartis to add credibility to narratives and claims, for decision support in marketing, product and strategy, and to leverage targeted insights for successful pursuit of new or existing markets and customers.

We understand that purpose driven intention of our clients and bring it to life through our well-known benchmark reports, our thought leadership work, highly customized research and advisory services and the excellence of our experienced analysts.

Our global reach



Supporting Data

Disclaimer

The contents of this document are strictly private and confidential. No part of this document may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of Chartis Research.

The facts of this document are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Chartis Research delivers will be based on information gathered in good faith, whose accuracy we cannot guarantee. Chartis Research accepts no liability whatever for actions taken based on any information that may subsequently prove to be incorrect or errors in our analysis.

Terms and Conditions:

https://www.Infopro-digital.com/terms-conditions/research-and-marketing-services/?lang=en