Why are the biggest risks facing finance today ones that did not exist a decade ago?

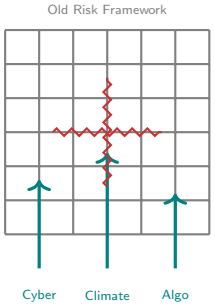
The shifting landscape:

- Traditional risk models were built for credit, market, and operational risk
- But technology has introduced entirely new risk categories
- Cyber attacks, algorithmic failures, climate shocks were not in the old frameworks

Why legacy models struggle:

- New risks have no historical data to calibrate models
- They are non-stationary – the threat evolves faster than models can adapt
- They are correlated in ways we do not yet understand
- They cross traditional boundaries between operational, strategic, and financial risk

The institutional challenge:
Risk frameworks must expand to cover threats that were unimaginable when the frameworks were designed.



New risks are breaking through the old framework like weeds through concrete.

Insight

The biggest risks are often the ones we have not yet learned to measure.

Risk management must evolve as fast as the risks themselves.

Has a technology failure ever affected your finances – even indirectly?

Think about a time when:

- An app or payment system went down and you could not complete a transaction
- A data breach exposed your personal information or required you to change passwords
- An algorithm made a decision about you (credit score, recommendation) that felt opaque
- A service you relied on disappeared because the company failed or was hacked

What this reveals about new risks:

- Technology creates dependencies – when it fails, the impact is immediate and widespread
- Digital systems are interconnected – a failure in one place cascades to others
- Users have little control or visibility into the systems they depend on
- Traditional insurance and regulation were not designed for these failure modes

Why financial institutions care:
If you as an individual experienced this, imagine the same failure modes at the scale of a bank serving millions of customers, processing billions in transactions daily.

Reflection

New risks affect everyone, but financial institutions face them at scale with systemic consequences.

Your personal experience with technology failure is a microcosm of institutional risk.

What new categories of risk has technology introduced to finance?

The new risk taxonomy:

1. **Cyber risk:**
   Attacks on digital infrastructure – data breaches, ransomware, distributed denial of service, insider threats.

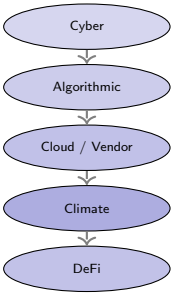
2. **Algorithmic risk:**
   Failures in automated decision systems – flash crashes, biased credit models, trading glitches.

3. **Third-party and cloud risk:**
   Dependence on external vendors – cloud outages, supply chain attacks, vendor failures.

4. **Climate risk:**
   Physical damage and transition costs – extreme weather, stranded assets, policy shocks.

5. **Decentralized finance risk:**
   Smart contract failures, oracle manipulation, governance attacks.

Common thread:
All are hard to quantify, have no historical benchmarks, and can materialize suddenly.



These risks do not exist in isolation – they amplify each other under stress.

Insight

New risks are characterized by deep uncertainty and the potential for rapid, correlated failures.

Traditional risk categories still exist, but new risks are growing faster.

How does a cyber attack propagate through interconnected financial systems?

The attack chain:

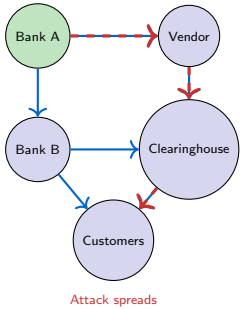
1. **Initial compromise:**
   Attacker gains access to one system through phishing, exploiting a vulnerability, or insider action.

2. **Lateral movement:**
   Once inside, the attacker moves to other systems using stolen credentials or exploiting trust relationships.

3. **Escalation:**
   Attacker gains higher privileges (admin access) to reach critical systems like payment processing or databases.

4. **Impact:**
   Data is stolen, encrypted (ransomware), or systems are disrupted. The attack spreads to connected institutions.

Why financial systems are vulnerable:
High interconnectivity means a breach at one institution can cascade to counterparties, vendors, and customers.



A breach at one institution propagates through trust and connectivity.

Insight

Cyber risk is systemic because financial systems are deeply interconnected.

The network that enables efficient finance also enables rapid attack propagation.

How do traditional and emerging risk frameworks differ in what they cover?

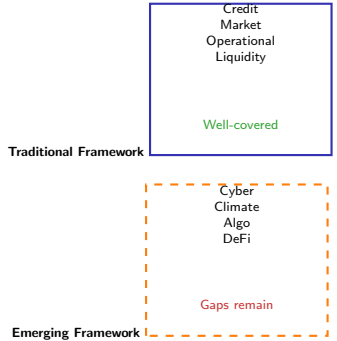
Traditional risk framework:

- Focus: credit, market, operational, liquidity
- Data: historical loss data, market prices
- Tools: value at risk, stress testing, capital ratios
- Regulation: well-established (Basel framework)
- Assumption: risks are stationary and measurable

Emerging risk framework:

- Focus: cyber, climate, algorithmic, decentralized finance
- Data: sparse, rapidly evolving, scenario-based
- Tools: red-team exercises, climate models, formal verification
- Regulation: developing (fragmented globally)
- Assumption: risks are non-stationary and adversarial

The gap:
Most institutions have mature frameworks for traditional risks, but emerging risks are bolted on rather than integrated.



Traditional frameworks are solid; emerging frameworks are still under construction.

Insight

The risk categories may be new, but the principles of identification, measurement, and mitigation still apply.

Emerging risks require new tools, but the risk management process is the same.

What happens when a risk that 'cannot be modeled' materializes anyway?

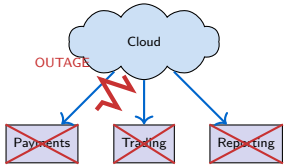
The warning signs:

- Risk teams declare certain events too rare or complex to model
- Institutions assume that unmodeled risks will not happen in their planning horizon
- Resources are allocated only to measurable risks
- Board oversight focuses on regulatory capital, not emerging threats

What happens when the unmodeled risk hits:

- No contingency plan exists because the scenario was not rehearsed
- Capital reserves are insufficient because the risk was not in the calculation
- Response is reactive and chaotic rather than planned
- Regulators and stakeholders ask why the institution was unprepared

The lesson:
Just because a risk is hard to model does not mean it is safe to ignore.



All systems down simultaneously

One cloud outage takes down payments, trading, and reporting all at once.

Insight

Unmodeled risks are still risks – scenario analysis and contingency planning matter even when quantification is impossible.

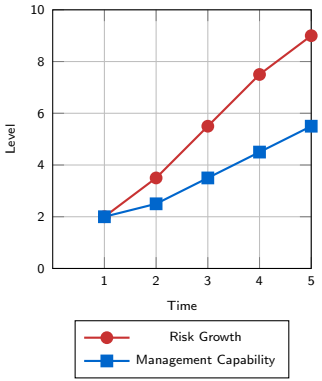
The absence of a model is not the absence of risk.

Where are emerging risks growing fastest relative to institutions' ability to manage them?

Risk growth vs management capability:

- **Cyber:** Attack sophistication is growing faster than defenses. Institutions are reactive, not proactive.
- **Cloud concentration:** Dependence on a few large cloud providers creates systemic risk that regulators are only beginning to address.
- **Climate physical risk:** Frequency and severity of extreme weather are outpacing insurance and infrastructure adaptation.
- **Algorithmic complexity:** Machine learning models are deployed faster than validation and governance frameworks can scale.
- **Decentralized finance:** Protocol innovation is outpacing regulatory and risk management development.

The gap:
The speed of risk evolution is exceeding the speed of institutional adaptation.



The gap between risk growth and management capability is widening.

Insight

Institutions must accelerate their adaptation or accept that they are falling behind the risk curve.

The risk management gap is a strategic vulnerability.

Who bears the cost when a new type of risk is not covered by existing regulation?

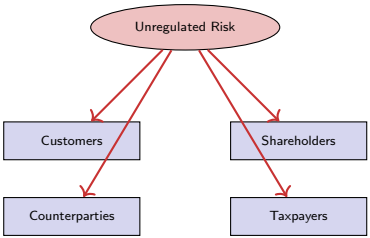
The regulatory lag:

- Regulation typically follows innovation with a delay of years
- During the gap, institutions operate without clear rules or capital requirements
- When a new risk materializes, it is unclear who is liable

Who pays:

- **Customers:** Lost funds, service disruptions, privacy breaches
- **Shareholders:** Equity value loss if the institution fails
- **Counterparties:** Losses if the institution cannot meet obligations
- **Taxpayers:** Bailouts if the institution is systemically important
- **The institution itself:** Reputational damage, legal costs, fines

The challenge:
Without clear regulation, accountability is ambiguous, and losses are distributed unpredictably.



When regulation lags, everyone bears some of the cost.

Insight

Regulatory gaps mean that risk costs are socialized rather than internalized by the institutions that create them.

The cost of unregulated risk is borne by those least able to anticipate or control it.

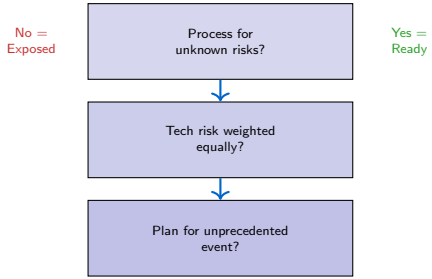
Three questions to evaluate an institution's readiness for emerging risks

The Emerging Risk Readiness Test:

1. **Does the institution have a process for identifying risks that are not yet in the model?**
   If risk management only tracks known risks, new threats will be invisible until they materialize.

2. **Are technology and operational risks given equal weight to financial risks?**
   If board attention focuses only on credit and market risk, cyber and algorithmic risks will be undermanaged.

3. **Is there a plan for a risk that has never happened before?**
   Scenario analysis and contingency planning should cover tail events, even if they seem improbable.



Strong readiness requires yes on all three questions.

Why this matters:
Readiness is not about predicting the future – it is about building systems that can adapt when the unexpected happens.

Insight

Readiness is about process and culture, not just technical capability.

The test reveals whether the institution is prepared to learn and adapt.

Your Challenge

Scenario:
Identify a new risk that affects finance today but did not exist a decade ago. Examples might include:

- Cloud concentration risk (dependence on a few large cloud providers)
- Algorithmic bias in lending decisions
- Ransomware targeting financial infrastructure
- Climate-related asset repricing
- Smart contract vulnerabilities in decentralized finance

Your task:
For your chosen risk, propose a measurement approach using the readiness test from slide 9:

1. How would you identify this risk before it is widely recognized? What early warning indicators exist?
2. How would you ensure this risk receives board-level attention alongside traditional financial risks?
3. What contingency plan would you design for a scenario where this risk materializes in an extreme form?

Deliverable:
Draft a short risk briefing for senior management explaining the risk, your proposed measurement approach, and your recommended contingency plan.

Learning goal

Practice building frameworks for risks that have no historical data or established models.

Emerging risks require creativity and scenario thinking, not just data analysis.