Why do banks with entire risk departments still get surprised by crises?

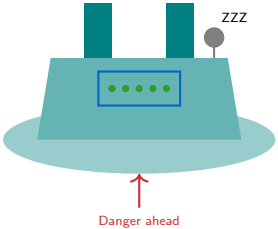
The paradox:

- Banks spend millions on risk management systems
- They hire teams of specialists, run stress tests, set limits
- Yet crises still happen – and risk managers are often blindsided

Why measurement is not enough:

- Risk can be identified but ignored by business lines
- Culture can prioritize short-term profit over long-term safety
- Organizational silos prevent information from reaching decision-makers

The institutional challenge:
Building a framework that balances risk-taking (essential for profit) with risk control (essential for survival).



The ship has sophisticated instruments, but the lookout is asleep.

Insight

Risk management is not just about tools and models – it is about whether the organization listens when risk warnings are raised.

The best risk models in the world are useless if the culture ignores their warnings.

Have you ever followed all the rules and still been caught off guard?

Think about a time when you:

- Checked all the boxes (studied, prepared, planned)
- But still encountered an unexpected problem
- Perhaps the rules did not cover the actual scenario
- Or the problem came from outside the system you were managing

That is the institutional risk dilemma:

- Institutions design frameworks to manage known risks
- But crises often come from unknown risks, or from failures in execution
- Rules create a false sense of security if culture and judgment are weak

What makes institutional risk different from individual risk:

- Scale: thousands of decisions across hundreds of people
- Complexity: risks interact in unpredictable ways
- Accountability: who is responsible when a distributed system fails?

Reflection

Institutional risk management is about building systems that work even when individuals make mistakes – and designing a culture that surfaces problems before they become crises.

The gap between policy and practice is where most risk management failures occur.

What are the three lines of defense in institutional risk management?

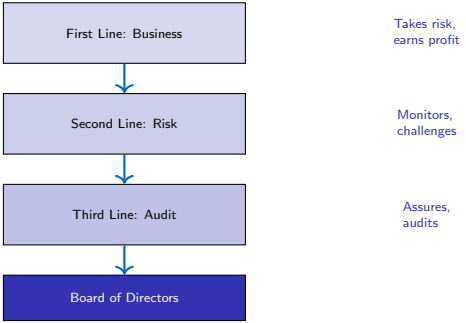
The standard model:

1. **First line (Business Units):**
   Business units own and manage risks in their daily operations. They are profit centers and risk takers.

2. **Second line (Risk and Compliance):**
   Risk management and compliance functions set policies, monitor limits, and challenge the first line. They are independent but advisory.

3. **Third line (Internal Audit):**
   Internal audit provides independent assurance that the first and second lines are functioning. They report to the board.

Why this structure:
Separation ensures that risk-takers do not also judge their own risk. Independence is the defense against conflicts of interest.



Insight

The three lines only work if the second and third lines have real independence and authority to escalate concerns to the board.

Independence is not about organizational charts – it is about whether risk managers can say no.

How does a bank stress test work from scenario design to capital decision?

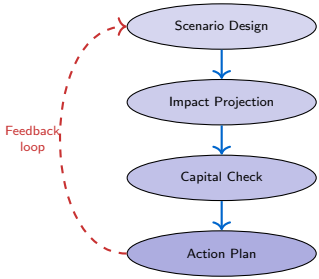
The stress testing cycle:

1. **Scenario design:**
   Regulators or the bank design adverse economic scenarios (recession, market crash, interest rate shock).

2. **Impact projection:**
   The bank models how its balance sheet, profit and loss, and capital would evolve under each scenario over a multi-year horizon.

3. **Capital adequacy check:**
   Does the bank maintain minimum capital ratios even in the stress scenario? If not, it must raise capital or reduce risk.

4. **Action plan:**
   If weaknesses are identified, the bank must submit a plan to strengthen capital, reduce exposures, or improve liquidity.



The cycle repeats annually, with scenarios evolving to reflect new risks.

Why stress tests matter:
They answer the forward-looking question: can the bank survive a severe but plausible crisis?

Insight

Stress tests shift risk management from backward-looking (what happened) to forward-looking (what could happen).

The stress test is a rehearsal for crisis – it reveals weaknesses before they become failures.

How are the risk management architectures of a bank and a fintech structured differently?

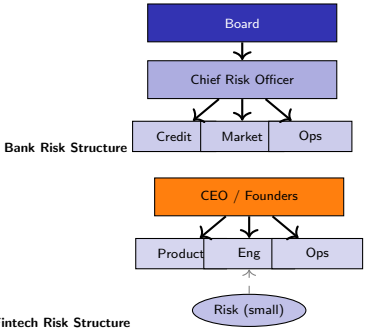
Traditional bank:

- Centralized risk function with direct reporting to the board
- Formal three lines of defense model
- Deep regulatory oversight (capital requirements, stress tests)
- Risk committees at board and management levels
- Established risk culture built over decades

Fintech startup:

- Risk management often embedded within product teams initially
- Lean structure with overlapping responsibilities
- Lighter regulation (depending on license) but growing fast
- Risk function scales as the company grows
- Culture focused on speed and innovation – risk can be an afterthought

The tension:
Fintechs move faster, but banks have stronger risk controls. The challenge is scaling risk management without killing agility.



Insight

Banks have risk infrastructure by regulation; fintechs must build it intentionally as they scale.

Risk architecture must match the institution's complexity and regulatory obligations.

What happens when risk management becomes a compliance exercise instead of genuine protection?

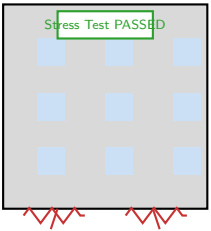
The warning signs:

- Risk reports are produced but not read by senior management
- Stress tests are passed by adjusting assumptions rather than fixing exposures
- Risk committees meet but do not challenge business decisions
- Compliance is measured by checklists, not by actual safety

Why this happens:

- Business pressure to meet growth targets overrides risk concerns
- Risk functions lack authority to stop profitable but risky activities
- Regulators focus on form (documentation) over substance (actual risk reduction)

The consequence:
The institution appears safe on paper, but underlying vulnerabilities remain unaddressed until a crisis exposes them.



Foundation failing

The certificate on the wall says the stress test passed, but the foundation is cracking.

Insight

Risk management that focuses on passing tests rather than preventing losses creates a dangerous illusion of safety.

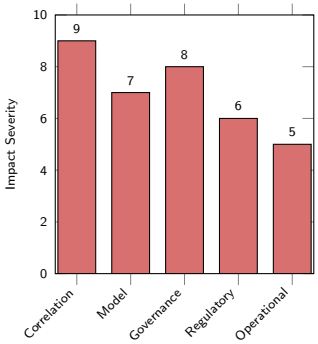
Box-ticking compliance is not protection – it is the appearance of protection.

Where have institutional risk failures caused the largest real-world damage?

Major failure categories:

- **Underestimated correlation:** Risks that appeared independent collapsed together (subprime crisis)
- **Model errors:** Models failed to capture tail risk or contagion (risk of default models pre-crisis)
- **Governance failures:** Risk warnings were ignored by senior management (rogue traders)
- **Regulatory gaps:** Shadow banking grew outside the regulated perimeter
- **Operational breakdowns:** Technology failures cascaded across systems

Common thread:
Most failures involved a combination of technical errors and organizational dysfunction – models failed, but also the culture failed to act on warning signs.



Correlation failures (systemic risk) caused the most damage historically.

Insight

The most dangerous failures are systemic – when multiple parts of the system fail simultaneously because they are interconnected.

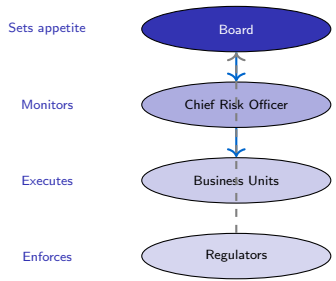
Individual risk failures are costly; systemic risk failures are catastrophic.

Who is accountable when risk management fails at an institution?

The accountability chain:

- **Board of Directors:** Ultimate responsibility for risk appetite and oversight. Can be held liable for negligence.
- **Chief Risk Officer:** Responsible for risk framework design, monitoring, and escalation. Must have authority to challenge business lines.
- **Business Line Heads:** Accountable for risks within their units. Compensation should reflect risk-adjusted performance.
- **Regulators:** Enforce minimum standards and can impose penalties, but cannot manage risk for the institution.
- **Shareholders and Creditors:** Bear the financial consequences of failure, but have limited operational control.

The challenge:
Accountability is distributed across many actors, which can create diffusion of responsibility – everyone is responsible, so no one feels responsible.



Accountability flows from the board down, but culture must support escalation upward.

Insight

Clear accountability requires not just organizational charts, but consequences for failures and rewards for preventing losses.

Accountability without consequences is theater.

Three questions to assess whether an institution's risk culture is real or performative

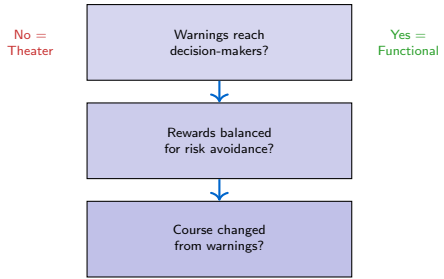
The Risk Culture Test:

1. **Do risk warnings reach decision-makers without filtering?**
   If risk reports must be sanitized before reaching the board, warnings will not be heard in time.

2. **Are risk-takers rewarded for avoiding losses as much as generating profits?**
   If compensation only reflects upside, risk-taking will be excessive. Balanced incentives matter.

3. **Has the institution ever changed course because of a risk warning?**
   If the answer is no, risk management is decorative, not functional.

Why this matters:
Culture is not what institutions say in their annual reports – it is what they do when profit and safety conflict.



A strong risk culture scores yes on all three questions.

Insight

Risk culture is revealed in decisions, not documentation.

The test is simple: does the institution listen to risk warnings, or just collect them?

Your Challenge

Scenario:
You are the chief risk officer for a day. A business unit wants to launch a new product with high expected returns but significant model uncertainty about tail risk. The business unit argues that competitors are already offering similar products and delay will cost market share. The stress test shows the product could be profitable in normal conditions but could breach capital requirements in a severe scenario.

Your task:
Use the risk culture test from slide 9 to structure your recommendation to the board:

1. Will your risk warning reach the board without being softened by the business unit?
2. Are you able to recommend rejection or delay without career consequences if the decision is unpopular?
3. Has the institution demonstrated willingness to prioritize long-term safety over short-term profit?

Deliverable:
Draft a short memo to the board explaining your recommendation (approve, approve with conditions, or reject) and the reasoning based on the three risk culture questions.

Learning goal

Practice translating technical risk analysis into strategic decisions that balance profit and safety.

The hardest part of risk management is not measurement – it is saying no when the answer is uncomfortable.