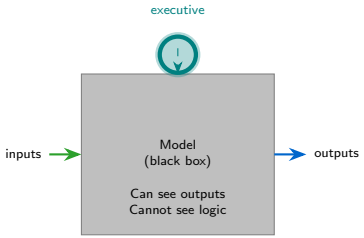
Why do institutions trust models with billions in decisions but struggle to govern them?

The governance paradox:

- Models drive capital allocation, loan approvals, trading decisions worth trillions
- But governance committees often lack the technical depth to challenge them
- Developers say the model works; validators must prove it does not
- Executives approve models they cannot fully understand

Why this happens:

- Models have become black boxes even to their builders
- Validation requires expertise that is scarce and expensive
- Pressure to deploy quickly conflicts with thorough review
- Failures are rare enough that governance seems optional – until disaster strikes

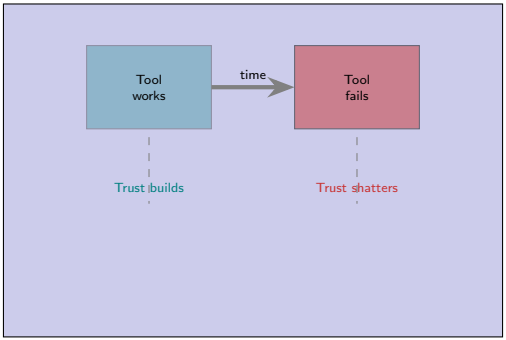


Key Insight

The gap between model complexity and governance capability is the root cause of model risk failures.

Institutions trust models because they have no choice. Governing them requires expertise, independence, and courage to say no.

Have you ever relied on a tool you did not fully understand – and it let you down?



Examples:

- Navigation app routes you into a closed road
- Spell-checker confidently suggests the wrong word
- Credit score drops without explanation
- Autopilot misreads a sensor and crashes

Reflection

Models fail at the edges of their training data. The question is whether governance catches failures before they reach production.

What are the components of a model risk management framework?

Three pillars of model risk management:

1. **Model development:** Sound design, documented assumptions, tested implementation
2. **Independent validation:** Challenge by experts who did not build the model
3. **Governance and use:** Oversight, inventory, ongoing monitoring, limits on use

Supporting infrastructure:

- Model inventory: complete registry of all models
- Model tiering: classify by risk to focus validation effort
- Validation cycle: annual for high-risk, less frequent for low-risk
- Escalation: model risk committee decides approval or rejection

Component	Owner
Development	Business unit
Validation	Independent team
Governance	Risk committee
Audit	Third line

Separation of duties:

- Builders cannot validate their own models
- Validators report to risk, not to the business
- Audit reviews the process, not the models

Key Insight

Model governance is not about bureaucracy. It is about ensuring that models work before they reach production.

The framework has three lines of defense: build, challenge, and assure. No single team controls the entire lifecycle.

How does a model validation process work from development through ongoing monitoring?

The validation lifecycle:

1. **Development:** Developer builds model, documents assumptions, performs initial testing
2. **Documentation:** Complete specification submitted for validation
3. **Independent validation:** Validator reviews theory, tests outcomes, benchmarks alternatives
4. **Validation report:** Approved, conditional, or rejected
5. **Deployment:** If approved, model enters production with monitoring
6. **Ongoing monitoring:** Performance tracked continuously against thresholds
7. **Periodic review:** Re-validation on schedule or if performance degrades
8. **Retirement:** Model decommissioned when replaced or obsolete

Validation tests three things:

- **Conceptual soundness:** Is the theory correct and appropriate?
- **Outcome analysis:** Do predictions match reality?
- **Benchmarking:** Could a simpler model work just as well?

Conditional approval:

- Model can operate but must fix findings within a deadline
- Used when issues are non-critical but need remediation
- Escalates if not resolved

Key Insight

Validation is not a one-time gate. Models must be monitored and re-validated as long as they remain in production.

Development builds the model. Validation challenges it. Monitoring ensures it stays valid. All three are mandatory.

How do centralized and federated model governance structures compare?

Centralized governance:

- Single validation team reviews all models across the institution
- Consistent standards and methodology
- Easier to audit and report
- Risk: bottleneck if validation demand exceeds capacity

Federated governance:

- Each business unit has its own validators
- Central team sets standards and performs oversight
- Scales better in large institutions
- Risk: inconsistent application of validation standards

Dimension	Better Fit
Small firm	Centralized
Large firm	Federated
Simple models	Centralized
Diverse models	Federated
Consistency priority	Centralized
Speed priority	Federated

Hybrid approach:

- Federated validators for routine models
- Central team for high-risk and cross-cutting models
- Central oversight of validation quality

Key Insight

Most large institutions use federated governance with central oversight to balance consistency and scalability.

Centralized governance ensures consistency. Federated governance ensures speed. The choice depends on size and complexity.

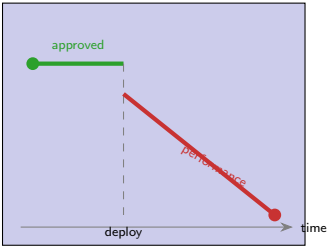
What happens when a model is approved by governance but fails in practice?

The governance-performance gap:

- Governance approves based on historical data and theoretical soundness
- Production exposes the model to conditions not seen in testing
- Data drift, regime changes, edge cases all emerge after deployment
- Models can pass validation and still fail in the real world

Common failure modes:

- Market conditions shift beyond training data range
- Input data quality degrades over time
- Users apply the model outside its intended scope
- Model interactions create unintended feedback loops

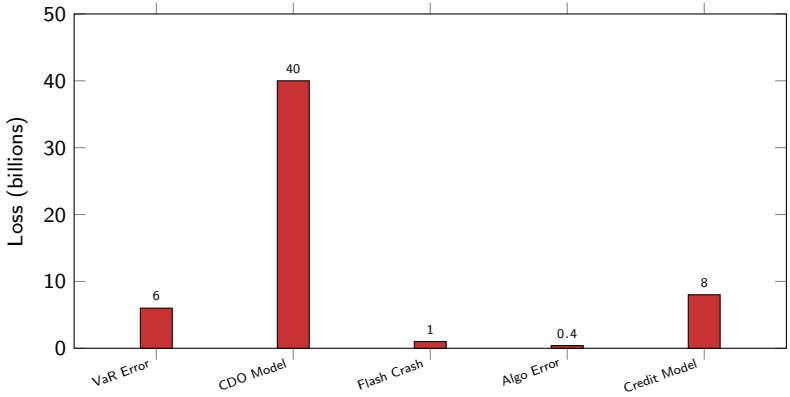


Key Insight

Approval is not a guarantee. Ongoing monitoring is the safety net that catches failures governance missed.

Governance reviews models in a lab. Production tests them in the wild. The gap between the two is where failures happen.

Where have model governance failures led to the largest financial losses?



- **VaR Error:** London Whale – flawed risk model masked exposure
- **CDO Model:** Financial crisis – models underestimated tail risk
- **Flash Crash:** Algo trading interaction caused market collapse
- **Algo Error:** Knight Capital deployment mistake
- **Credit Model:** Subprime models failed to predict defaults

Model governance failures are rare but catastrophic. Every major financial crisis since the turn of the century involved model risk.

Who is accountable when a model makes a harmful decision – the builder, the validator, or the executive?

Three perspectives on accountability:

1. **Builder:** Designed the model and is responsible for its correctness
2. **Validator:** Challenged the model and is responsible for catching flaws
3. **Executive:** Approved deployment and is responsible for the decision to use it

The reality:

- All three share accountability, but in different ways
- Builder is accountable for technical correctness
- Validator is accountable for independent challenge
- Executive is accountable for business judgment
- Regulators hold the institution accountable, not individuals – unless there is misconduct

When things go wrong:

- Builder blames validator for missing the flaw
- Validator blames executive for approving despite findings
- Executive blames builder for poor design
- All three point to incomplete data or unprecedented conditions

The governance fix:

- Clear roles and responsibilities
- Written approval decisions with rationale
- Escalation paths when parties disagree
- No single point of failure

Key Insight

Accountability requires clarity. Everyone must know what they are responsible for before the model fails, not after.

Model risk is a shared responsibility. Governance clarifies who owns what so that accountability is not diffused into invisibility.

Three questions to assess whether model governance is effective

The Model Governance Effectiveness Test:

Question 1: Can validators independently reproduce the model's results?

- If not, validation is theater, not substance
- Documentation must be sufficient for full reproduction
- Code, data, and methodology must all be accessible

Question 2: Are models re-validated when the world changes, not just on a schedule?

- Annual validation is not enough if markets shift mid-year
- Triggers: market stress, data drift, performance degradation
- Governance must be event-driven, not just calendar-driven

Question 3: Does the governance process have teeth – can it actually stop a model from deploying?

- If business pressure always wins, governance is symbolic
- Validators must have authority to reject, not just raise concerns

Application:

- Good governance: validator reproduces model, finds discrepancy, deployment pauses until resolved
- Pass on all three

Counter-example:

- Weak governance: validator flags concerns, business deploys anyway, validator is overruled by executive
- Fail on question three

Red flag:

- If no model has been rejected in years, governance is not working
- Effective governance says no to some models

Key Insight

Governance effectiveness is measured by its ability to stop bad models, not just approve good ones.

Your Challenge

Scenario:
You are a model validator reviewing a credit scoring model. The model developer claims excellent performance on historical data and provides a detailed technical specification. The business is eager to deploy because the model approves more loans than the current model.

Your task:
Design your validation plan. Answer the following:

1. What are the three most critical tests you would perform?
2. What evidence would convince you the model is safe to approve?
3. What findings would cause you to reject the model outright?
4. How would you handle pressure from the business to approve quickly?

Format:

- One page maximum
- Four sections corresponding to the four questions
- Use bullet points for clarity
- Assume you have full independence but limited time

Reflection

Validation is not about finding reasons to approve. It is about ensuring the model is safe before it reaches production.

This exercise mirrors the real work of model validators. Your job is to protect the institution from models that should not be deployed.