NOVA COOPERATIVE

The Top 5 Compliance Pitfalls Every Business Should Be Watching

Why today's biggest compliance failures often start as leadership and governance failures.

FEATURED GUIDE | EXECUTIVE RISK & GOVERNANCE

A practical guide for leaders

Five recurring organizational failures that create regulatory, financial, operational, cybersecurity and reputational exposure - and the questions leadership should be asking before those gaps become events.

THE EXECUTIVE VIEW

Compliance failures rarely begin with a deliberate decision to break a rule.

More often, they begin quietly: a responsibility nobody clearly owns; a vendor that bypasses review; a policy that has not kept pace with the business; an AI tool adopted before anyone considered the data; or a known risk that remains unresolved because everyone assumes someone else is handling it.

Individually, these decisions may seem small. Collectively, they can create significant regulatory, financial, operational, cybersecurity and reputational exposure.

The details of compliance vary by industry, but the underlying organizational failures are remarkably consistent. Across modern regulatory and risk-management expectations, leaders are increasingly expected to demonstrate that risk is understood, assigned, governed, resourced, monitored and working in practice - not merely documented.

The common thread is governance.

This guide highlights five pitfalls every organization should examine, regardless of size or industry, and provides practical questions leadership teams can use to identify gaps before someone else does.

How to use this guide

Use each section as a leadership discussion prompt. If the answer to a question is unclear, inconsistent across functions, or dependent on one individual, treat that uncertainty as a signal worth investigating.

01

Governance Without Clear Accountability

The Pitfall: Everyone is responsible - which often means no one really is.

One of the most common organizational failures is not the absence of policies or committees. It is the absence of clearly defined ownership. As businesses grow, responsibilities naturally cross departments. Without explicit authority, accountability and escalation, important issues can remain unresolved while everyone reasonably believes another function is addressing them.

What this can look like

- Technology owns the system while Operations owns the process.
- Legal interprets the requirement while Compliance monitors adherence.
- Cybersecurity sees the threat while Finance controls the budget.
- A risk remains open because each function reasonably assumes another function is responsible.

Questions leadership should ask

- Who has authority to accept significant risk?
- Who is accountable for remediation when a control or process fails?
- Are operational ownership and independent oversight clearly separated?
- Can significant issues reach executive leadership quickly?
- Does the board understand the organization's most significant risks?
- Can management demonstrate who made important risk decisions - and why?

THE NOVA PERSPECTIVE

Strong governance does not mean more committees. It means creating unmistakable lines between who owns the risk, who manages it, who challenges it, who accepts it and who needs to know about it.

02

Compliance That Exists on Paper but Not in Practice

The Pitfall: The policy says one thing. The business does another.

A beautifully written policy provides little protection if the organization cannot demonstrate that people actually follow it. Regulators, customers, auditors, insurers and boards increasingly care about evidence that controls operate effectively - not just whether a document says they should.

What this can look like

- A policy requires annual reviews, but nobody tracks completion.
- Vendor procedures require due diligence, but exceptions routinely bypass the process.
- Access reviews occur, but identified problems are not remediated.
- Training is completed, but nobody measures whether behavior changes.
- Risk assessments are performed, but their findings never influence priorities or budgets.

Questions leadership should ask

- Are controls actually performed at the frequency the policy requires?
- Is evidence retained in a way that can be produced when challenged?
- Are exceptions documented, time-bound and approved by the right authority?
- Are findings tracked through remediation and closure?
- Do policies reflect how the business actually operates today?
- Could the organization demonstrate control effectiveness tomorrow?

THE NOVA PERSPECTIVE

Documentation matters. Execution matters more. Strong compliance connects policy to process, ownership, controls, evidence, monitoring and continuous improvement.

03

Third Parties Become Your Risk Before They Become Your Vendor

The Pitfall: The business relationship moves faster than risk management.

Modern organizations rely on interconnected ecosystems of SaaS providers, cloud platforms, contractors, payment providers, data processors, AI services and outsourced operations. The problem is not outsourcing. The problem is believing accountability was outsourced with the work.

What this can look like

- A SaaS platform is purchased on a corporate card before Security or Legal sees it.
- A service provider gains access to sensitive data before contractual protections are finalized.
- A critical vendor passes onboarding but is never meaningfully reassessed.
- A fourth party creates a concentration or resilience dependency nobody mapped.

Questions leadership should ask

- Do vendors receive appropriate risk review before contracts, data exchange or system access?
- Do we know what company, employee and customer information they hold?
- Do contracts address security, privacy, incident notification, continuity and termination?
- Are critical providers monitored after onboarding?
- Do we understand material fourth-party dependencies?
- Can we quickly identify affected vendors during an incident?
- Is there a viable exit strategy if a critical provider fails?

THE NOVA PERSPECTIVE

Third-party risk management should not prevent the business from moving quickly. It should allow the business to move quickly with its eyes open.

04

Technology, Data and AI Are Moving Faster Than Governance

The Pitfall: Innovation happens first. Governance catches up later.

Employees can adopt cloud services, AI platforms, browser extensions and automation tools faster than traditional procurement, cybersecurity, privacy or compliance processes can evaluate them. The leadership challenge is no longer whether these technologies will be used, but whether the organization understands where, how, why and with what information.

What this can look like

- Employees adopt AI tools before approved-use standards exist.
- Sensitive information enters uncontrolled cloud or AI environments.
- Automated outputs influence decisions without defined human validation.
- Technology duplication grows because no one has enterprise visibility.
- Data ownership is unclear, making privacy, retention and access decisions harder.

Questions leadership should ask

- Do we know which AI and technology platforms employees are using?
- What company, employee or customer information enters those systems?
- Who approves new technology and material changes to existing technology?
- Are cybersecurity, privacy, legal and compliance involved early enough?
- Who validates AI-generated outputs used in important decisions?
- Do we understand intellectual-property, confidentiality, retention and model-risk implications?
- Can leadership explain the organization’s AI governance model today?

THE NOVA PERSPECTIVE

Good governance should not stop innovation. It creates the guardrails that allow organizations to innovate safely and at speed.

05

Waiting for a Crisis to Discover the Organization Isn’t Ready

The Pitfall: Having an incident response plan is not the same as being prepared to respond.

Cyber incidents, fraud, data breaches, vendor failures, regulatory inquiries, litigation and business interruptions differ in cause but often expose the same organizational weakness: many teams suddenly need to act together with incomplete information, competing priorities and little time.

What this can look like

- Technology, executives, counsel, insurers and communications teams operate on different timelines.
- Nobody is certain who can authorize notifications, expenditures or public statements.
- The technical response consumes leadership attention while ordinary operations still need to run.
- Critical decisions are made but not documented.
- The organization learns during the event that its contact lists, escalation paths or recovery assumptions are outdated.

Questions leadership should ask

- Is our response plan current, practical and known to the people who will use it?
- Have executives practiced their roles under realistic pressure?
- Are legal, insurance and external response relationships established before an event?

- Are decision rights and communication authorities predetermined?
- Can the business operate if a critical technology or provider becomes unavailable?
- Have we conducted a realistic tabletop exercise?
- Who manages the administrative and executive response while technical teams investigate and remediate?

THE NOVA PERSPECTIVE

Organizations should not discover their response structure during the incident. Preparation creates the space for good decisions when time, information and attention are in short supply.

THE COMMON THREAD

Governance turns compliance from a document into an operating discipline.

These five pitfalls may look different, but underneath them is the same fundamental question:

Does your organization know who is responsible for what - and can you demonstrate that it is actually happening?

Compliance can no longer live exclusively inside a compliance department. Cybersecurity, privacy, artificial intelligence, vendors, data, operational resilience and regulatory obligations increasingly intersect across the enterprise.

That makes effective compliance fundamentally a leadership and governance responsibility. The organizations best positioned for what comes next will not necessarily be those with the most policies. They will be the organizations that understand their risks, assign accountability, establish appropriate controls, test whether those controls work, identify change early and respond decisively when something goes wrong.

A useful leadership principle

If a risk is important enough to report, it is important enough to assign. If a control is important enough to require, it is important enough to test.

LEADERSHIP SELF-ASSESSMENT

Five questions to take back to your leadership team

These questions are intentionally simple. The value is in whether the answers are consistent, evidenced and understood across the organization.

01

What are the five risks most capable of materially disrupting our business today?

02

Can we name the executive accountable for each one?

03

Can we demonstrate that the controls protecting us are actually working?

04

What has changed in our business, technology, vendors, data or regulatory environment that our governance has not caught up with yet?

05

If something significant happened tomorrow morning, would everyone know exactly what to do?

If any answer is unclear, that is not necessarily a compliance failure. It is an opportunity to find the gap before someone else does.

ABOUT NOVA

National expertise. Boutique partnership. Built for complexity.

NOVA Cooperative Group is a national strategic advisory firm helping organizations navigate risk, resilience, transformation and the moments when getting it right matters most.

Our leadership team brings **more than 75 years of combined experience** spanning executive leadership, cybersecurity, technology, enterprise risk, governance, regulatory compliance, operations, incident response and organizational transformation.

Our cooperative model combines NOVA's core expertise with a curated network of specialized partners and trusted professionals. That allows us to build the right team around each challenge - with the reach and capability expected from a national firm and the accessibility, agility and personal attention of a boutique partner.

We don't simply identify problems, deliver a report and walk away.
We work beside you to solve them.

Core advisory areas
- Strategic risk, governance and regulatory readiness
- Cybersecurity and technology risk
- Third-party risk and operational resilience
- Data governance, privacy and AI governance

- M&A and transformation risk
- Strategic incident response support and executive coordination

NOVA Cooperative Group is proud to be a **woman-owned and veteran-owned business.** Those distinctions reflect values embedded in how we operate: service, accountability, integrity, discipline, collaboration and the willingness to step forward when the situation is difficult.

National capability. Boutique attention. One cooperative approach to solving what matters.

SELECTED REFERENCES

Built on current risk and compliance expectations

This guide is designed as practical executive guidance, not legal advice. Its themes align with widely used regulatory and risk-management expectations emphasizing risk assessment, governance, accountability, control effectiveness, third-party oversight, cybersecurity preparedness and responsible technology use.

U.S. Department of Justice
Evaluation of Corporate Compliance Programs - framework for assessing whether a compliance program is well designed, adequately resourced and empowered, and working in practice.
justice.gov/criminal/criminal-fraud/page/file/937501/dl

National Institute of Standards and Technology (NIST)
AI Risk Management Framework - governance and risk-management guidance for trustworthy and responsible use of artificial intelligence.
nist.gov/itl/ai-risk-management-framework

National Institute of Standards and Technology (NIST)
Cybersecurity Framework 2.0 - enterprise cybersecurity risk management framework with Governance as a core function.
nist.gov/cyberframework

Federal Trade Commission
Privacy and Data Security enforcement and business guidance - recurring expectations around reasonable security, data governance and representations to customers.
ftc.gov/business-guidance/privacy-security

NOVA Cooperative Group
Strategic advisory for risk, resilience and transformation.