riskonnect.



Walled-Off ERM and Compliance Functions? What That's Costing – and How to Fix It?

Enterprise risk management and compliance often operate independently, not because of a deliberate decision but because the structure around them was simply not built to connect the dots. This separation, however, can cause crippling blind spots that obscure problems and cost the company real money in delayed decisions, conflicting actions, lost productivity, and missed opportunities.

Risk and compliance have a common goal of protecting the organization. And both teams are usually well aware of impending regulatory change. The problem is in the execution of those changes – deciding what applies, who owns it, and how it gets done.

Here's how to find the gaps between knowing something is coming and making sure it gets done, close them, and work together to avoid costly mistakes.

One Goal, Two Perspectives

While ERM and compliance monitor the same regulators, the same requirements, and the same updates, they view those signals through different lenses. ERM looks at enterprise-level threats and opportunities in terms of the impact on long-term business goals. Compliance zeros in on the details to ensure strict adherence with the letter of the law.

Consider the two perspectives of the same event:

Compliance: Are we checking off every requirement to the letter?	ERM: What's the exposure if we get this wrong?
Focuses on rule-by-rule details.	Focuses on portfolio-level likelihood.
Considers enforcement precedent.	Considers business impact and control design.
Considers business impact and control design.	Measures residual risk and control effectiveness.
Can miss the broader risk impact of change.	Can miss regulatory technicalities.



The Cost of Disconnection

Both perspectives are genuinely legitimate and valuable – but are incomplete on their own. The one-sided view becomes a problem when interpretation, ownership, and follow-through are unclear. Isolated data silos, conflicting taxonomies, and separate reporting lines exacerbate confusion.

Two teams working in parallel cost the company in terms of:

Duplicated effort. Risk and compliance teams independently research, interpret, and act on the same regulatory development in parallel.

Inconsistent response. Similar changes get handled differently, depending on which team, region, or person happens to read the new rule or updated guidance first.

Slower cycle time. Every change triggers another ad hoc process to figure out what applies where and who is responsible.

The most damaging cost of fragmentation, however, comes from blind spots. What is slipping through the cracks because one team thought the other was handling it? Will regulatory change increase risk at the enterprise level – by how much? What wasn't prioritized because the two perspectives weren't connected to show the full impact?



Auditors are trained to find gaps between what has been tracked and what has been completed. The consequence is an audit finding with your organization's name on it.

Where the Breakdowns Happen

For every regulatory change, companies must see the signal, interpret the impact, and take appropriate action. The breakdown happens between the steps when deciding:

Does this apply to us?

The teams may see the regulatory signals but fail to sort out the meaning or prioritize actions because of the surrounding noise. Meantime, each team quietly pursues their own course of action with no resolution.

Whose job is this?

It's easy to assume others have it covered if ownership is implied by a job title instead of assigned to a specific person. Ownership is especially tricky to set when a regulatory change spans multiple business units, locations, or products.

Is it really done?

Tracked is not the same thing as done. A control, policy, or process marked "in progress" does not mean anything actually changed.

How to Close the Gaps

Structure, not goodwill, is what keeps teams in sync. Closing the gaps takes coordination mechanisms that work.

- **Joint triage forum.** Triage every item against applicability and impact using one consistent method that separates noise from what needs a decision. Decide if the change applies broadly or narrowly, and if it's high or low stakes for the organization. Agree on the timeline for actions and resolution based on priority tier.
- **Shared taxonomy.** Both teams need to speak the same language, e.g., what materiality means. Defining terms upfront stops misinterpretations down the road.
- **One system of record, not two.** Keep everything related to monitoring, assessment, ownership, and status in a single platform. Regulatory change is captured once, immediately tagged for relevance, and routed by business line, jurisdiction, or risk type.
- **Assigned owners for every actionable item.** Ownership – to a person not a department – must be named for every single change that requires action. This leaves no ambiguity.
- **Defined escalation paths.** Automatically route any stalled item upward for action instead of letting it languish in someone's inbox.
- **Track to closure.** Completion requires a genuine closing method – deadlines, escalation, and evidence of completion – not just a status report.
- **Committee-level reporting.** Include the stage of regulatory action items – not just vague "in progress" tracking – in risk committee and leadership reporting on a fixed cadence.





Build the Structure for Connection

Don't make the mistake of putting all your effort into monitoring regulatory change and assume the operational end will take care of itself. That rarely happens.

Without a shared, structured way to assess and reconcile applicability, determining the impact of every new regulatory change starts from scratch. Visibility is obscured by noise, applicability to the business is ambiguous, and ownership is unclear. That's where inconsistency creeps in.

To be sure, fixing the problems does not mean starting over. ERM and compliance do not need to become one function to work as one connected force. They need shared infrastructure that turns regulatory signals into coordinated action. A common platform gives both teams one place to capture change, assess applicability, assign ownership, route tasks, track evidence, escalate delays, and report status without friction.

That technology layer matters because handoffs are where regulatory response breaks down. Spreadsheets, email threads, and separate point solutions leave too much room for duplicated effort, missed ownership, and inconsistent reporting. A single system of record creates the connective tissue between ERM, compliance, and the business, centralizing the process while pushing accountability to the right owners across the organization.

The goal is not more meetings or another layer of oversight. It is disciplined execution at scale. When every regulatory change has a clear path, a named owner, built-in escalation, and evidence of completion, you can close the gap between knowing what is coming and proving that the right actions were taken.

Start anywhere. Expand everywhere.

Riskonnect is the leading provider of software that brings risk under one roof. The technology empowers organisations to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific.
To learn more, visit riskonnect.com.

INSURABLE RISK | GOVERNANCE, RISK & COMPLIANCE | BUSINESS CONTINUITY & RESILIENCE

CONNECT NOW

riskonnect

Copyright © 2026 Riskonnect, Inc.
All rights reserved.