

GRC Chaos

The High Price of Audits and Non-Compliance

Rising regulatory complexity overwhelms security teams relying on fragmented tools, manual workflows, and limited automation—putting organizations at greater risk of errors, inefficiencies, and costly penalties due to outdated processes and poor GRC collaboration. Swimlane surveyed 500 IT and cybersecurity decision-makers in the US and UK to highlight the urgent need for unified workflows and intelligent automation to streamline evidence collection, reduce risk and restore confidence in audit readiness.

The Compliance Burden is Getting Heavier



96%

96% of organizations struggle to keep up with evolving regulations.



29%

Only 29% of organizations consistently meet compliance standards.



51%

51% of organizations have faced or fear fines due to noncompliance.

Fragmented Tools, Fractured Processes



92%

92% use 3+ tools to gather audit evidence.



39%

Just 39% of evidence collection is automated.



54%

Top manual tasks: verifying configs (54%), tracking tasks (54%), and cross-referencing data (50%).

Manual Work is Costing Time — and Accuracy



54%

54% spend over 5 hours/week on manual compliance tasks.



62%

62% report errors in audit evidence gathering.

GRC and Security Don't Speak the Same Language



90%

90% of organizations worry about poor collaboration between security and GRC teams.



36%

Key issues: misaligned priorities (36%), poor communication (34%), unclear requirements (33%).

What's at Stake When Compliance Fails

39%



The top three risks organizations associate with poor compliance management are: Financial penalties (39%), increased vulnerability to breaches (36%), and reputational damage (36%).



Bring Order to Compliance Chaos

Siloed tools, teams, and manual work turn audit readiness into a burden. With growing regulatory pressure, it's time to shift from reacting to transforming. This research shows the need for a unified and automated approach.

[Download Report](#)