Compliance through Continuous Delivery

BY STEVE FENTON

How the financial service industry and other regulated organizations can manage compliance and innovation without compromise.

First edition

Octopus Deploy

Compliance through Continuous Delivery

How the financial service industry and other regulated organizations can manage compliance and innovation without compromise.

Ed.1.2025.2

Introduction

Organizations in the financial services industry feel the perceived trade-off between throughput and stability more keenly than those in unregulated sectors. There seems to be an unresolvable tension between slowing down the rate of software delivery to perform adequate validation of its fitness, and speeding up the rate of software delivery to respond quickly to security and compliance issues.

Traditionally, organizations have implemented a slow-by-default deployment pipeline dominated by manual checks and approvals, with an exceptional process to expedite changes when there's an urgent need. The problem with this approach is that the rarely-used expedited channel increases instability, because the usual checks were skipped to create a slimmed-down path to production. Most production issues and regressions result from an expedited change in this setup.

In Continuous Delivery (Addison-Wesley, 2010), Dave Farley and Jez Humble share that the best solution to this tension is to create a streamlined deployment pipeline for all changes that uses automation to reduce manual handling. When you implement a Continuous Delivery pipeline, you increase throughput and stability, breaking the trade-off.

A modern deployment pipeline doesn't skip past the checks the business needs. Instead, it reduces friction with automation and strong tooling so that organizations can have a fast and reliable path to production. This is now essential to regulated industries, as we strive to secure supply chains, reduce attack windows, and deliver safely and securely at all times.

This report looks at the relationship between different approaches to deployment pipelines in the context of regulated organizations. We offer a deep analysis of approval strategies, including the impact of approval chains and cross-organization interaction.

This report is based on data explicitly collected from organizations in the financial industry. The survey was conducted early in 2025 and had 50 respondents.

The impact of new regulations

While the **Digital Operational Resilience Act** is an EU initiative, it provides an opportunity to assess the impact of new regulations on technology teams. The legislation was enacted in 2023 with a compliance deadline of January 17, 2025. It provides a useful benchmark for the cost of adopting changes to comply with new regulations.

With the steady rise in cyberattacks, the act was developed to protect the financial sector. It applies to institutions offering financial services in the EU and their third-party suppliers of information and communication technology (ICT). It draws on existing frameworks such as **ISO:27001** and **NIST Cybersecurity Framework (CSF)** and covers topics like:

- Incident management, classification, and reporting
- Operational resilience testing
- Data sharing arrangements
- Managing third-party risks

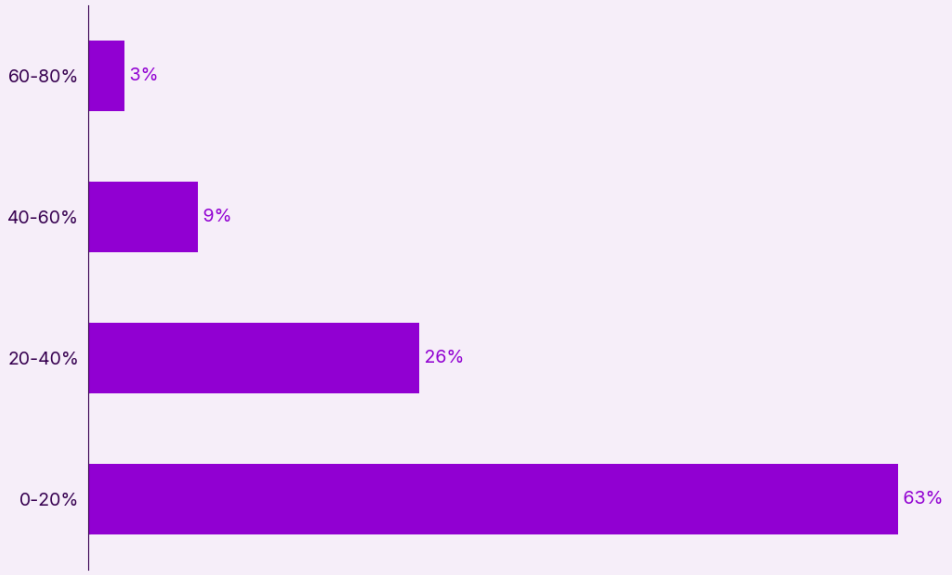
Penalties for non-compliance

Like similar regulations, non-compliance penalties include significant monetary fines, public reprimands, and legal action against senior executives.

In 2024, worldwide regulatory fines increased to a record-breaking **$19.3 billion**. In the US, regulators issued **$4.3 billion in financial penalties**.

In addition to financial and reputational damage, there is an increasing willingness to pursue criminal prosecution, which can mean jail time for executives. The maximum sentences vary by regulation, but are typically in the region of 5 to 20 years.

Impact on product delivery and feature development



The % of time software teams spend on compliance with new regulations.

We asked organizations to assess the impact of compliance with the new regulations in terms of the loss of focus on other software development work. Most organizations lose up to 20% of their roadmap to compliance activities, such as software changes, process changes, and tool adoption. 38% of organizations are losing more than 20% of their time, which highlights that the investment in compliance can be significant.

Many organizations with low compliance overheads operate solely in domestic markets outside of the EU. They have assessed the regulations and concluded they are not required to comply. These organizations often still apply standards such as ISO:27001 or NIST CSF.

Compliance with existing standards was also cited as a reason for organizations having a low overhead of adopting the Digital Operational Resilience Act. These organizations already had many mechanisms in place for compliance and could identify and close gaps more easily.

Where the Digital Operational Resilience Act was the organization's driver for adopting these practices, the investment required has been far higher. To attain compliance, these organizations must revise processes, introduce controls, and revise previous tool choices.

A small number of organizations were not aware of the legislation, and our survey has prompted them to investigate further, which suggests awareness is not universal. Many organizations may have yet to identify if they are subject to the act.

Specific focus areas

Organizations are managing the impact of the legislation through increased focus on resilience and security. Common changes being made were:

- Strengthened disaster recovery and business continuity planning
- Enhanced monitoring and alerting systems
- Improved incident management and classification processes
- More rigorous security testing and vulnerability management

A particular difficulty is the need to improve the practice of third-party suppliers and improving supply chain security.

Increased compliance overhead

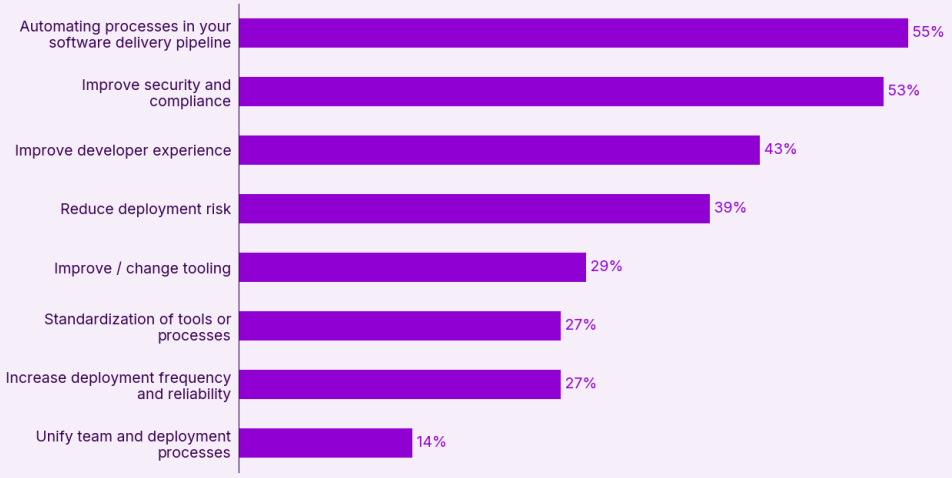
Multiple respondents note the administrative burden, including:

- More frequent security patching requires additional deployment cycles
- Enhanced documentation and audit trail requirements
- Increased internal audits and risk-related tasks
- More detailed incident reporting and classification

Organizations without automated deployment pipelines struggle to meet the demand for increased deployment frequency. Some organizations have needed to replace tools that present barriers to compliance.

Continuous Delivery and DevOps initiatives

In regulated industries, organizations are using Continuous Delivery and DevOps to achieve their compliance goals and increase their ability to ship working software. Alongside initiatives to increase security and compliance, organizations are looking at automation, improved tooling, and standardization to smooth the path to production, as this will help them meet demands for increased deployment frequency that legislation such as the Digital Operational Resilience Act require.



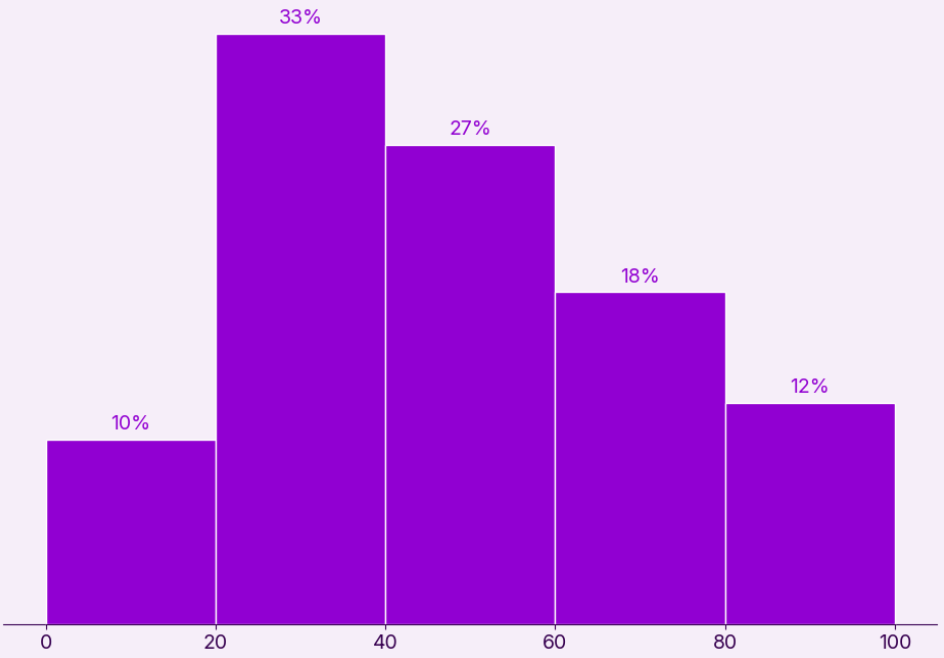
Top initiatives in the financial services industry by % of organizations. Multiple selections allowed.

More than half of organizations surveyed were looking at automating processes in their software delivery pipeline (55%) and improving security and compliance (53%).

Improving software delivery

A recurring theme in our research was the need for organizations to improve their deployment frequency and change lead time. The ability to deploy early and often is a competitive advantage as it provides more frequent feedback loops and increases agility. In the context of compliance, there's an additional need to update dependencies and third-party code to ensure vulnerabilities are removed quickly.

We used measures of deployment frequency and change lead times to calculate a normalized delivery score on a 100-point scale, with frequent deployments and low lead times scoring the highest and slow infrequent deployments scoring the lowest.



Distribution of delivery scores, which are based on deployment frequency and change lead times.

Some example scores are shown below.

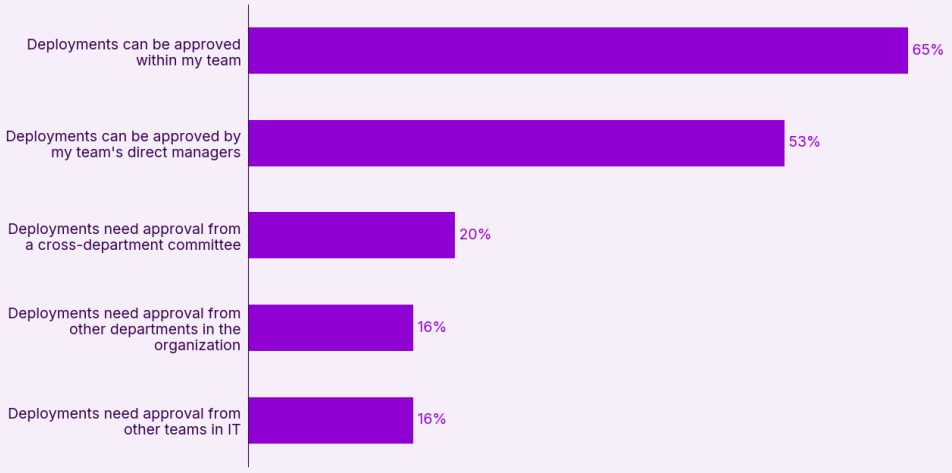
Deployment frequency	Change lead time	Delivery score
Many times a day	Less than an hour	100
Daily	Less than a day	75
Weekly	Less than a week	38

Lightweight change approvals

The **2019 State of DevOps report** found software delivery performance depended on **streamlined change approvals**, where approvals were performed using "peer review during the development process, supplemented by automation to detect, prevent, and correct bad changes early in the software delivery life cycle".

As regulated industries often have more burdensome compliance requirements, we wanted to review the impact of change approvals on change lead time and deployment frequency. We looked at who could approve a deployment, and at chains of approvals where multiple reviewers were required. We also looked at how approvals were captured.

Approvers and approval chains



Deployment approvals. Multiple selections allowed.

We expected short approval chains and local approvals (the team and their manager) to achieve the highest scores. While fewer manual approvals were generally associated with higher delivery scores, we also found approval chains outperformed single-point approvals in some specific cases.

The two highest performing approval chain setups were:

- Team → Direct Managers → Other Departments (median 68.8)
- Team → Direct Managers (median 56.2)

Including other departments in the approval chain did increase variability in the scores, so much of the success of this approach depends on the flow of information and the responsiveness of the approval process. However, the presence of the team responsible for the change and their direct manager had a powerful moderating effect on approvals requiring other IT teams or other departments.

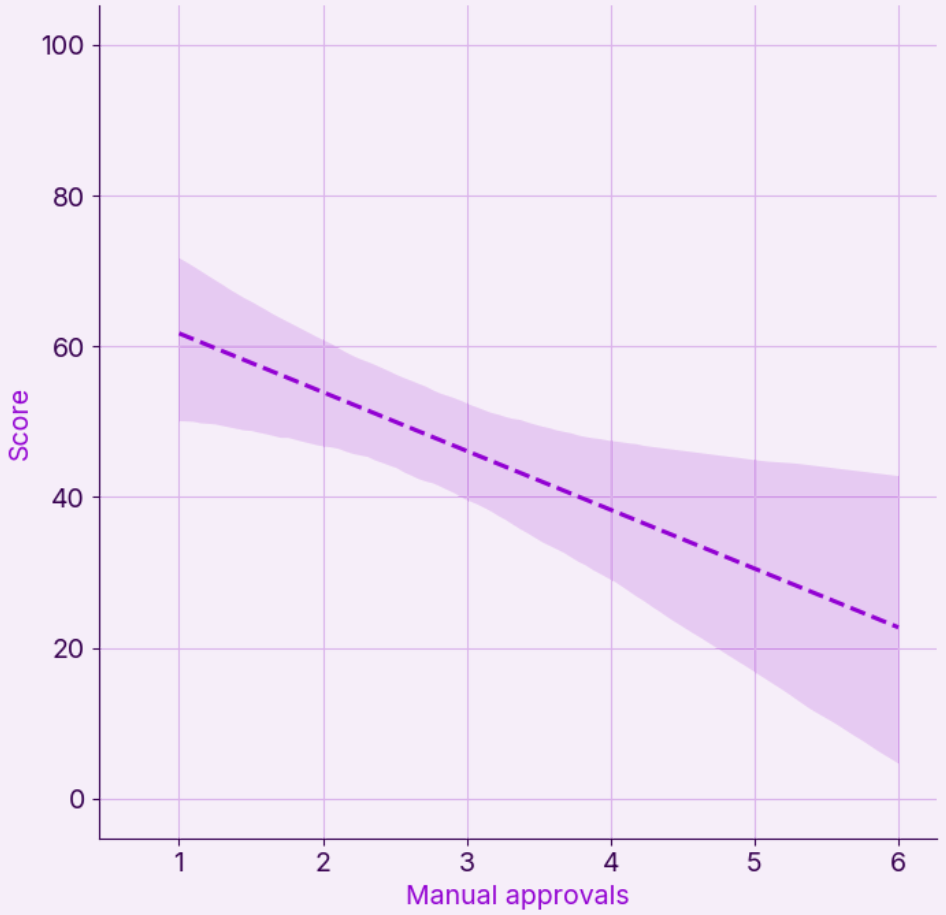
Reviews by the team, their direct managers, other IT teams, and other departments were all less effective when either the team's or the direct manager's approval was missing from the chain. This is true even where the approval chain was a single step (for example, just the team, just the manager, or just the other IT team). This was surprising, but perhaps reveals a positive dynamic where direct managers respond faster to reviews that the team has already checked, and other departments respond to these managers faster than they would react to the team.

The strongest finding in the approval data was that **cross-department committees are universally bad for software delivery**. No approval chain could improve the scores achieved when a cross-department committee was involved in the approval process. This is likely caused by committee scheduling and poor information flow.

Delivery scores for common approval chains (medium and standard deviation).

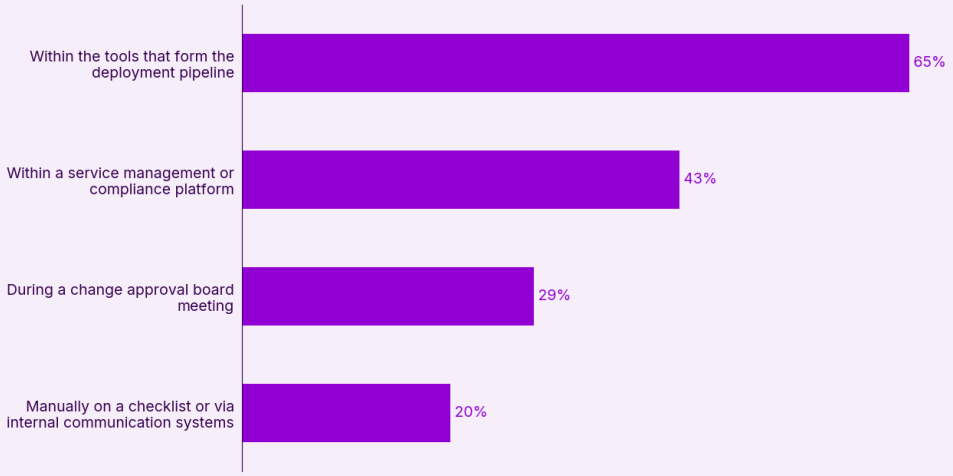
The special case of team and direct manager approval chains doesn't change the overall trend of increased manual approval steps reducing delivery performance. Organizations with a single approval had median scores 3x higher than those with 6 approvals.

Approval chains can be reduced by introducing automated checks and scans, and reviewing the approval process to check the validity of approval stages. Where a chain of approvals is needed, the healthy approval chain designs found in the data may reduce wait times and improve throughput.



Delivery scores by number of manual approvals.

Approval capture



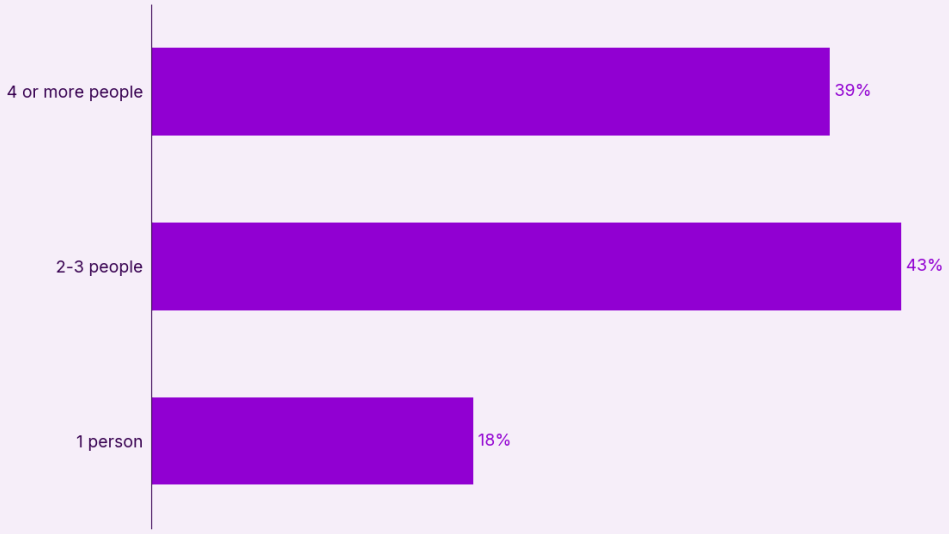
Where deployment approval is captured. Multiple selection allowed.

Unsurprisingly, capturing approvals within deployment pipeline and IT service management tools is more effective than collecting approvals in change approval board meetings or through communication tools and checklists.

Many organizations are being held back by multi-modal approval capture. This can happen when some approvers aren't willing to use the appropriate tools to approve the deployment, which means teams have to collect approvals from meetings or emails and progress the deployment when they arrive.

Not only do deployment and service management tools streamline the approval process, but they also improve the auditability of the approvals, as they can all be found in one place. When approvals depend on paper, emails, or other forms of electronic communication, it increases audit complexity. An organization may fail to meet audit requirements not because the process was not followed, but because the evidence cannot be found.

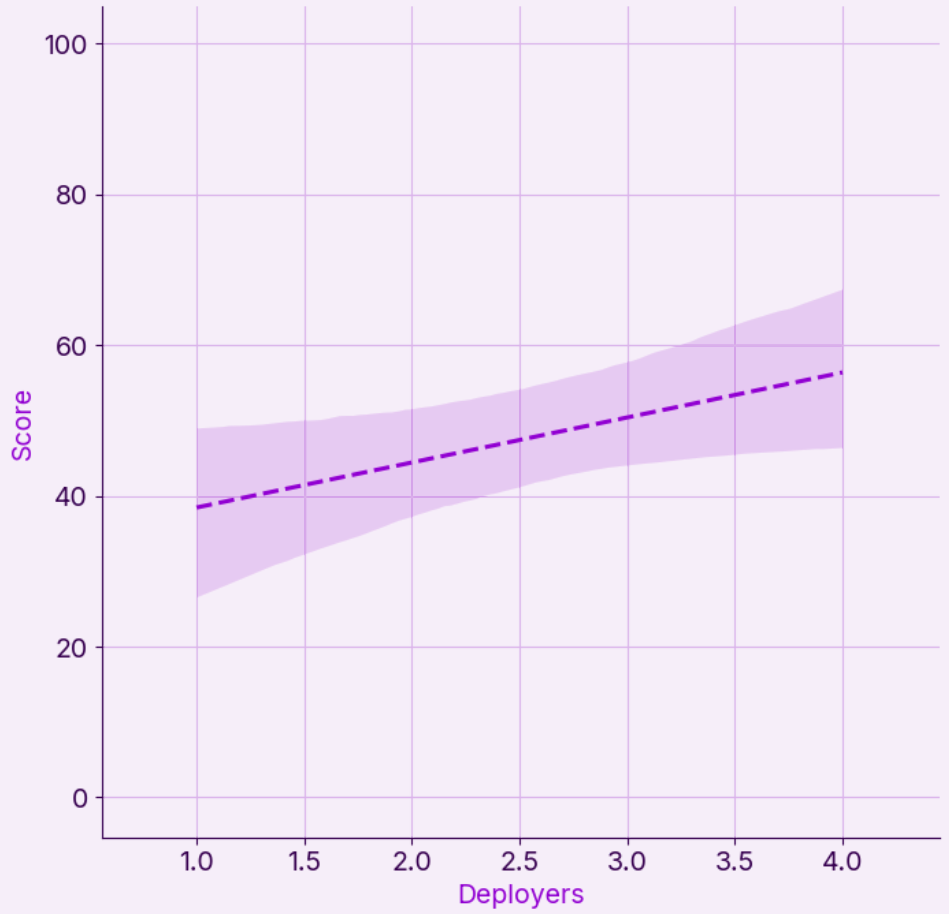
Triggering deployments



How many people can trigger a deployment.

Deployment gatekeepers reduce the speed and frequency of deployments by presenting a bottleneck that can be just as bad as an approval process. When fewer than 4 people can trigger a deployment, it introduces unnecessary delays. More than 60% of organizations surveyed had fewer than 4 deployers.

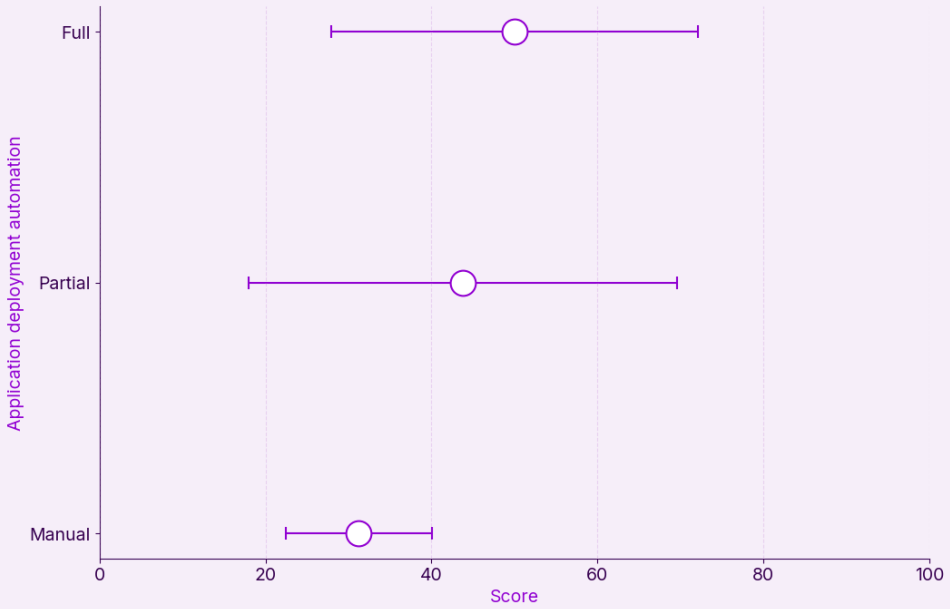
The median delivery score increases from 42 to 59 when the 4-deployer threshold is reached.



Delivery scores by number of deployers (people who can trigger a production deployment).

This echoes the finding of our **2023 deployment survey**, where having deployment gatekeepers prevented organizations from attaining the expected efficiency gains from deployment automation initiatives.

Deployment automation



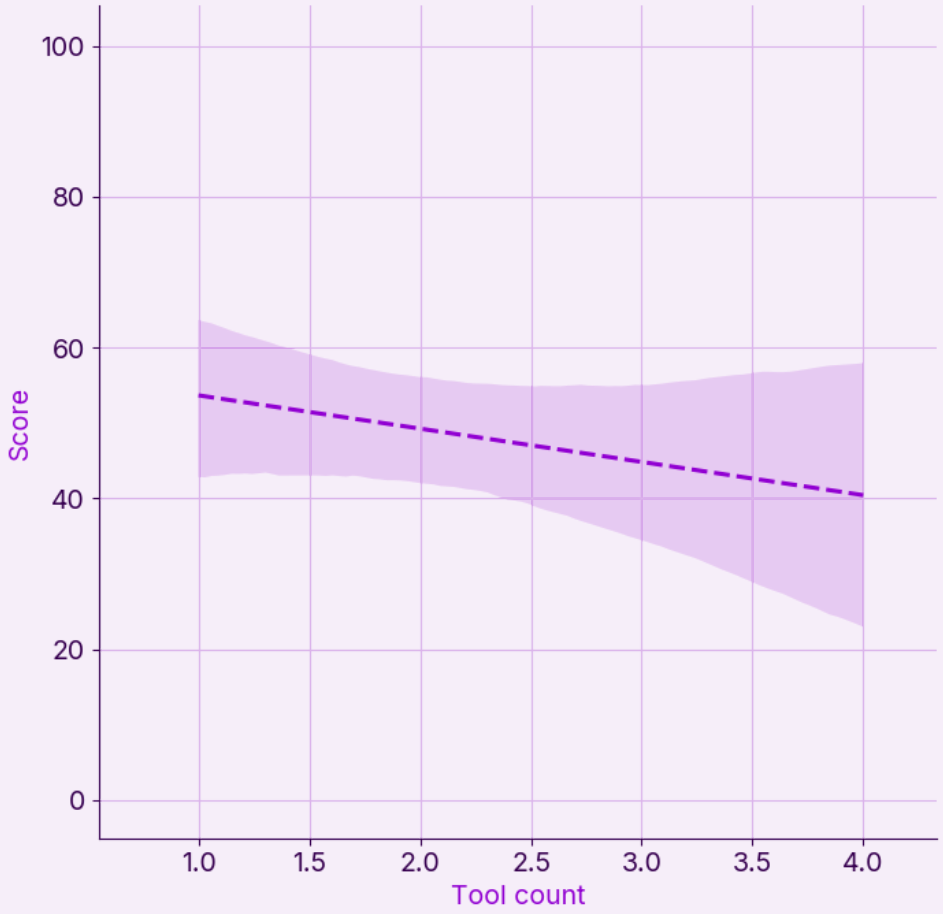
Impact of automation on delivery scores.

Automation is crucial to increasing deployment frequency and reducing change lead time. It also improves reliability outcomes as it lowers change failure rates and speeds up recovery times that require a code change. Automation removes a fundamental constraint for software delivery, moving the bottleneck into the approval and deployment triggering process.

Both application and database deployments benefit from automation. Once deployments are automated, this should be the only route for changes to be made. This prevents drift, encourages changes in version control, ensures all changes are tested in pre-production environments, and prevents unauthorized changes to the system as fewer people need production access.

Organizations must reduce wait times in the process to benefit the most from deployment automation. That means measuring and improving the queue times and elapsed times for change approvals (such as pull requests), deployment approvals, and triggering production deployments once approved.

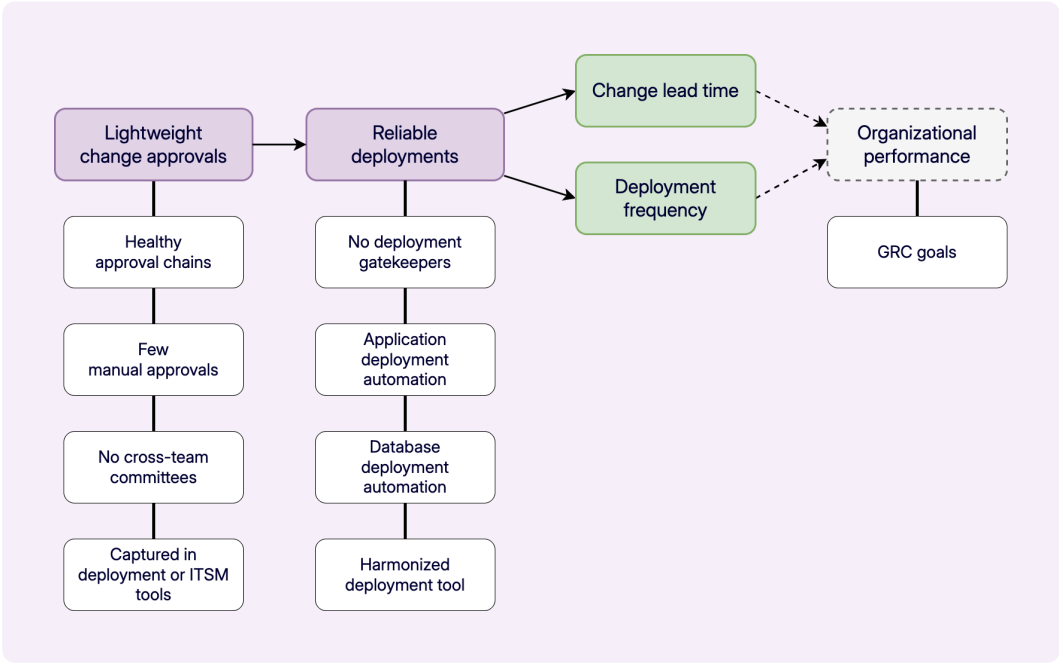
Standardizing software teams around a standard deployment tool can also increase delivery performance. Choosing a tool that offers deployment approval capture, or integrates with IT service management tools for approval capture, means approvers don't need to use different tools to process approvals for different teams. Organizations using Platform Engineering will likely be harmonizing tool choice through this initiative.



Delivery score by number of deployment tools.

Starting the improvement initiative

All the insights in the data point to the need for lightweight change approvals and reliable deployments. Working to improve these two components on your software delivery process will increase your ability to keep pace with supply chain security, implement and evidence compliance, and reduce deployment risks.



The qualities of lightweight change approvals are:

- **Healthy approval chains**: Where an approval chain is in place, having the team as the first stage and their direct manager as the second stage reduces approval delays.
- **Few manual approvals**: Reducing the number of manual approvals significantly reduces unnecessary delays, which are often caused by work waiting in a queue.
- **No cross-team committees**: The need for a cross-team committee approval is a universal source of friction.
- **Captured in deployment pipeline tools or ITSM tools**: Don't manage approvals manually, through email, or on a clipboard of wet signatures. Instead, features in deployment and ITSM tools can be used to streamline approvals and improve auditability.

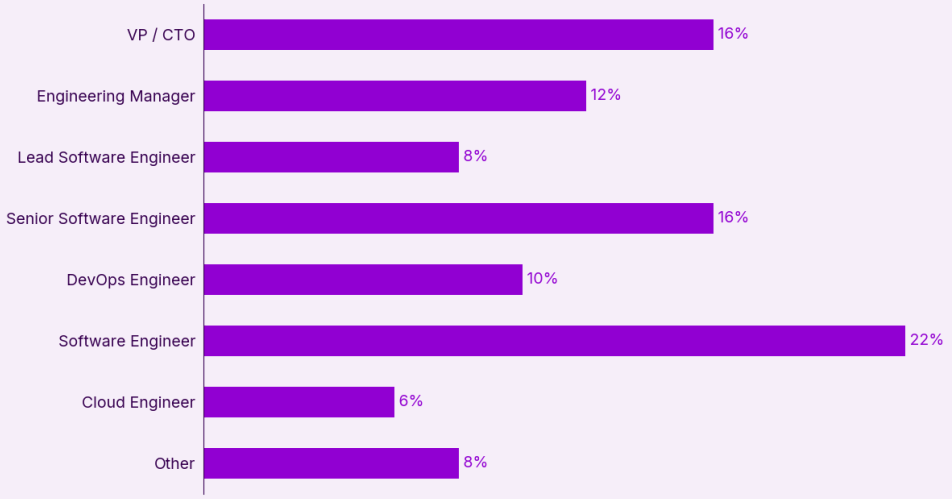
The qualities of reliable deployments are:

- **No deployment gatekeepers**: Having 4 or more people able to trigger production deployments reduces blocked deployments.
- **Application deployment automation**: Application deployments should be automated to all environments, with deployment tools managing environment progression.
- **Database deployment automation**: Database deployments should be automated just like application deployments. All database schema changes should be made through the automated route to prevent schema drift.
- **Harmonized deployment tools**: Standardizing on deployment tools reduces friction for development teams and those who work across many teams in leadership, compliance, security, and audit roles. It also increases observability of deployments across the organization.

Who completed the survey

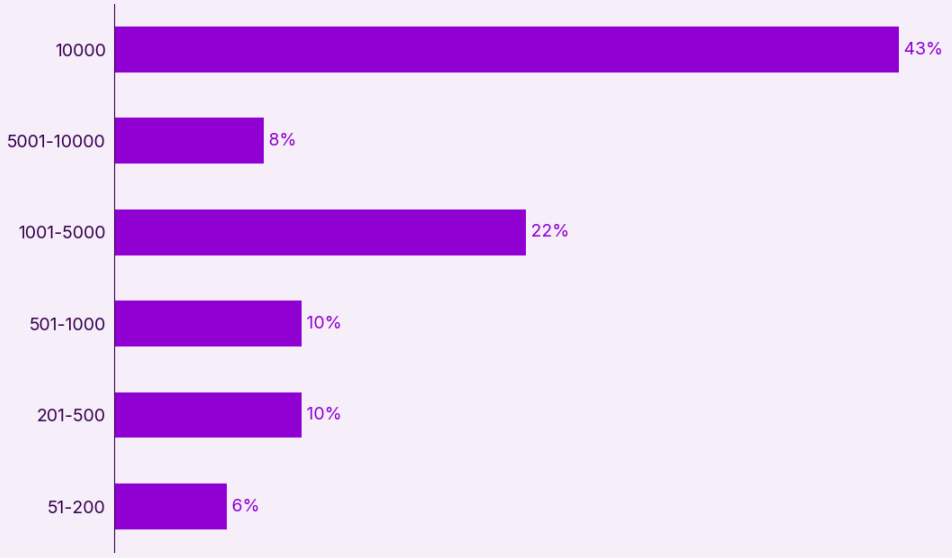
Responses were received from organizations in financial services, banking, fintech, investment banking and management, and insurance. From the specific industry categories, banking (33%) and fintech (31%) were the most common.

Responses were received from executive-level leadership (16%), engineering managers (12%), and from a number of engineering roles. These are shown below, organized to show management/executive roles first, developer roles by seniority, and other roles.



Responses by role.

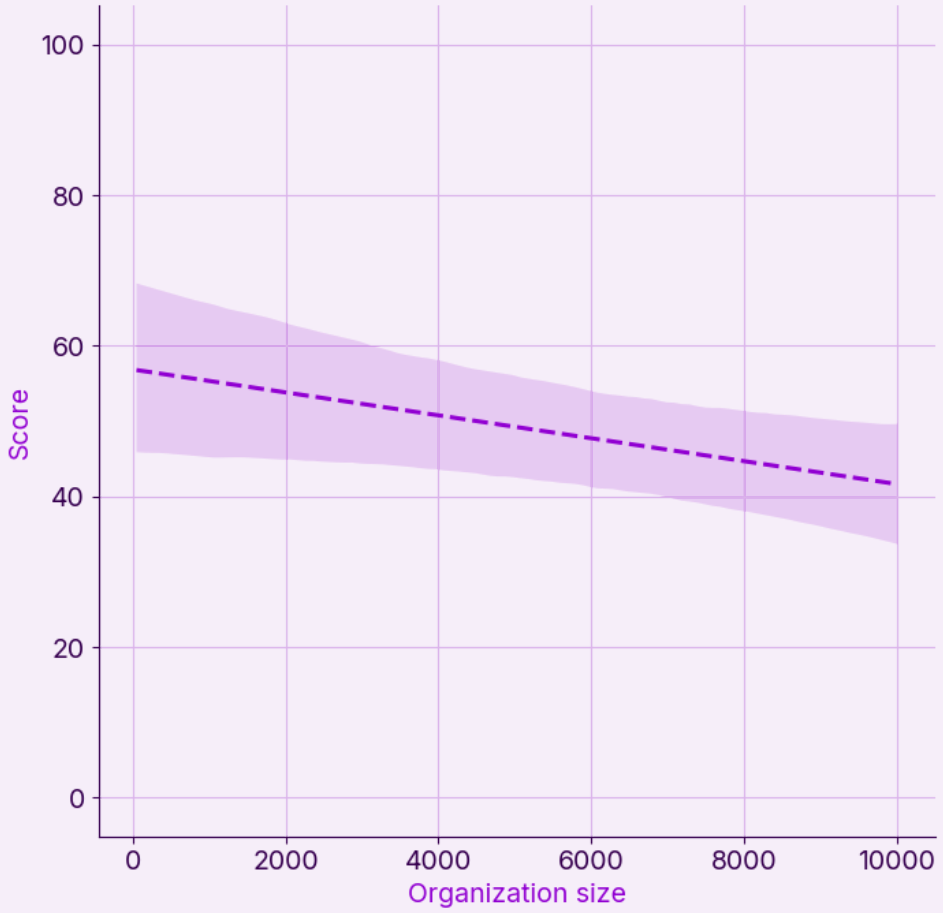
The majority of responses came from large organizations and Enterprises. The compliance costs for regulated industries make it more difficult for smaller organizations to operate profitably. However, some are managing to compete despite having fewer resources to help them navigate complex regulatory requirements.



Responses by organization size.

The size of organizations did affect delivery performance. This may be a signal that smaller organizations who default to lean product management and agile working can outpace larger organizations with more calcified processes. Large organizations and enterprises must view this as a competitive threat as small competitors are able to fit many more feedback cycles into their product roadmap, validating their feature ideas and changing direction rapidly to find their market niche.

On a positive note, the difference by organization size is less dramatic than differences by other dimensions. A large organization with lightweight change approvals and reliable deployments can still outmaneuver a smaller competitor.



Scores by organization size.

What organizations told us

Here are some of the scenarios described by respondents, arranged by category.

Organizations outside the EU:

> It has not impacted our DevOps processes because my company only operates in the US markets so this does not directly apply.

> Our Fintech company is US based and has strict rules for data interaction outside CONUS. However, it is an additional guideline we are now aware of and strive to achieve/exceed compliance of.

Legislation having low impact:

> We are fortunate in that we haven't had to change much based on the Digital Operational Resilience Act. Because we are already in the banking industry, we have already taken many of these things into account.

> It required confirmation that we were already following best practices, with a few enhancements in financial areas. Minimal changes required.

Legislation having a greater impact:

> We are giving a lot of importance to disaster recovery and SOC compliance work over feature work.

> We've had to dedicate time to ensuring we don't have any gaps. Addressing those gaps has taken time too (like updating logging requirements and monitoring requirements).

> The Digital Operational Resilience Act processes have an impact and as part of adopting them, some tools which were not compliant and had vulnerabilities (e.g., [...]) have been replaced by [...] and [...] and static and dynamic code checkers like [...] have been added to our pipelines.
>
> (Tool names redacted.)

> It has driven the deployment of more controls and monitoring. It has also affected the way we think about Business continuity and disaster recovery processes.

> It has increased internal audits, which has increased the amount of risk-related tasks the team has to focus on.

Organizations not aware of the requirements:

> I have never heard of the Digital Operational Resilience Act, so at the present moment it's not impacting our processes.

> I'm not familiar with the Digital Operational Resilience Act. I will be looking into it, once this survey is complete.

Continuous Delivery improves compliance

The financial services industry faces a critical juncture in 2025, driven by the increasing demands of regulatory compliance, particularly the Digital Operational Resilience Act, and the persistent need for rapid, secure software delivery.

This report has demonstrated that the perceived trade-off between throughput and stability is not insurmountable. Instead, organizations that embrace modern software engineering practices, focusing on lightweight change approvals and reliable deployments, are better equipped to navigate these challenges and gain a competitive edge.

Our findings highlight that automation, particularly in application and database deployment pipelines, is fundamental to increasing deployment frequency, reducing change lead times, and improving reliability.

Furthermore, the way organizations manage approvals significantly impacts their delivery performance. The data shows that minimizing manual approvals, avoiding cross-departmental committees, and capturing approvals within deployment or ITSM tools lead to superior outcomes. Critically, ensuring at least four individuals can trigger a production deployment eliminates a common bottleneck and boosts delivery scores.

While larger organizations may face more entrenched processes, the report shows that the principles of lightweight change approvals and reliable deployments can enable them to keep pace with smaller competitors.

By prioritizing these improvement initiatives, financial institutions can not only meet stringent compliance requirements but also foster innovation, enhance security, and deliver value to their customers at an accelerated pace.

The future of financial services lies in a strategic embrace of these principles, transforming regulatory burdens into opportunities for operational excellence and market leadership.

Further reading

- Continuous Delivery. Farley & Humble. Addison Wesley. 2010.
- **DORA: The State of DevOps Report**.
- **Octopus: Deployment survey report**.
- **Octopus: An overview of DevOps metrics**.

Find out how automated Continuous Delivery pipelines can simultaneously increase throughput and stability, resolving the speed-versus-safety trade-off and helping organizations meet increasingly demanding turn-around times for cybersecurity resolutions.