RESEARCH REPORT

capacitas®

DevSecOps: Bridging the gap or widening the Divide?

*A survey of IT leaders on the expectations and realities of adopting **DevSecOps** practices.*

Contents

Introduction..... 03
Key Findings 04
The Promise of DevSecOps 05
Opening up about the challenges of implementation..... 06
Making sense of the metrics..... 06
DevSecOps trade-offs: realities are far from expectations..... 07
Organisations are unprepared for changes in demand..... 08
Culture clashes over DevSecOps..... 08
Resistance to adaptation..... 09
The role of training..... 09
Are priorities achievable when security remains a problem?..... 10
Conclusion: DevSecOps can deliver, but approach is key..... 11
The Capacitas process will deliver..... 12

capacitas®

Introduction

DevOps is an approach to enterprise software development that aims to remove the barriers preventing organisations from delivering and updating systems at speed. It combines the processes, practices and tooling required to deliver speed without compromising quality.

The approach known as DevSecOps is a set of practices that takes this further, encouraging agile relationships between development and IT operations teams. Organisations, especially when working with a monolithic application can find a disconnect opens up between these teams which pass ownership between them, undermining efficiency and performance.

DevSecOps bridges this gap, combining the two functions, integrating ownership at each stage of the development cycle. It fully integrates security as a shared responsibility and encompasses culture, automation, and design. Amid unceasing demand for new applications and updates it helps organisations achieve faster development with higher quality and fewer incidents – and at reduced cost. It boosts efficiency and results in higher levels of governance.

But this evolving methodology requires expertise to handle the increased requirements and greater complexity of software as all organisations face a global shortage of developer skills. And with no one-size-fits-all solution to choose from when it comes to DevSecOps, every organisation is doing it differently, and few are getting what they want from it.

To get under the skin of DevSecOps maturity in the UK, Capacitas commissioned a survey of 200 IT decision makers at large UK businesses and public sector organisations that have either already adopted DevSecOps practices or are planning to in the near future.

By surveying decision makers on both sides of the DecSecOps journey, the following report is able to compare the expectations businesses have of the practice, against the reality of those that have already adopted them. Are organisations adequately prepared for the right challenges, are staff provided with enough training, and has DevSecOps delivered adequate return on investment? Capacitas wanted to know.

Key findings

Organisations are extremely positive about many aspects of DevSecOps across a range of indicators including **security, consistency, quality and cost.**

But three-quarters (**74%**) of organisations have seen an **increase in the most serious P1 incidents since implementing DevSecOps** – undermining the gains they have made in areas such as deployment frequency, lead time for changes, mean time to resolution, on-time delivery and change failure rate.

The pressure to **deliver software releases faster and to increase volume** is causing significant and unnecessary challenges.

The average time to fully adopt DevSecOps culture is **eight months**, but one-in-ten respondents said it has taken more than a year.

Organisations are moving fast and **are prepared to break things to achieve their objectives** but are settling for lower levels of performance and more problems than they need to.

The research found

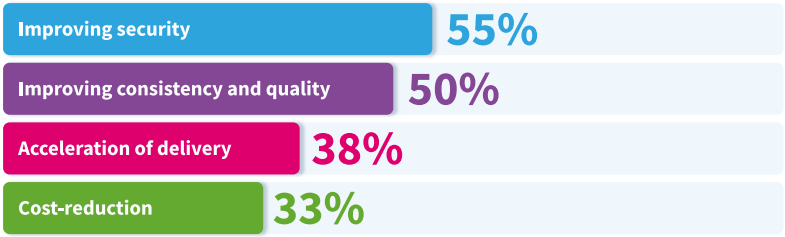
- Organisations are failing to use automation appropriately, leading to resourcing problems.
- Development teams have not fully embraced the methodology, leading to difficulties with implementation and optimisation of the practices that comprise DevSecOps.
- Organisations frequently focus too much on technology rather than the people and processes in combination. This is failing to achieve the buy-in that embeds the DecSecOps mindset of shared responsibility across all teams and throughout the IT lifecycle.
- **40%** of respondents say that within their DevSecOps set-up they still experience friction in security following implementation, indicating security teams are not satisfied with the output.

However, the research also showed that most respondents were seeing DevSecOps begin to improve quality, value and speed of delivery. What is critical is to have the right approach to adoption.

The promise of DevSecOps

When asked why they engage with DevSecOps, responses indicated the chief motivations are **to boost the quality of products delivered**, especially through improved security and consistency. Cost-reduction is a less important driver.

Drivers behind adoption of DevSecOps:



Respondents with DevSecOps can see the benefits

Almost all respondents say their organisation has seen improvements across a range of measures after implementing DevSecOps practices. The findings are more than encouraging:

> It is worth noting that almost all adopters (**97%**) are confident they can report back to their boards that DevSecOps is delivering return on investment. This is an even higher figure than the **74%** of those in the planning phase – proof of exceeded expectations when it comes to delivering ROI.

Opening up about the challenges of implementation

Organisations admit, however, that they face a wide variety of challenges to the implementation of DevSecOps, from limited security expertise (**30%**) to constraints around staffing, budget, and infrastructure (**14%**).

Many underestimated the scale of some challenges. For example, only **18%** of those planning to implement DevSecOps expect to face difficulties because of their lack of security expertise, and **16%** foresee skills gaps and training needs, compared with **28%** of those who are already using the methodology.

The amount of time it takes to embed DevSecOps culture varies, but anything between three months and one year is most common, applying to 87% of those who have implemented the approach in their organisation.

> **“Only 18% of those planning to implement DevSecOps expect to face difficulties because of their lack of security expertise, and 16% foresee skills gaps and training needs, compared with 28% of those who are already using the methodology.”**

Making sense of the metrics

As with any investment, tracking the progress of DevSecOps and reporting back potential gains is an important consideration. This is why 93% of organisations are collecting metrics about their DevSecOps operations.

But this is where trouble starts for a significant percentage of organisations. Almost two-in-five respondents (**38%**) admitted they cannot extract any useful insights from the mass of metrics they collect .

> **“38% admitted they cannot extract any useful insights from the mass of metrics they collect.”**

For DevSecOps to succeed, team leaders need easy access to real insight. They need to extract the data that matters and view it in a dashboard, otherwise they cannot see the wood for the trees. This should include the performance of people and processes as well as the technology. For people, the level of collaboration and ownership in DevSecOps is vital, while processes must be transparent, allowing for rapid problem-solving and fast feedback. DevSecOps has to be data-driven so multi-disciplinary teams can continuously improve their delivery as well as their products.

DevSecOps trade-offs: realities are far from expectations

Although respondents are confident about the benefits of DevSecOps, some encounter major, potentially catastrophic, drawbacks, most of which can be eliminated with better implementation.

Most concerning is that almost three-quarters of organisations (74%) have seen an increase in P1 incidents.

These are incidents that inflict significant damage, leaving organisations stricken by hours of outage and unable to service customers or achieve performance targets. Worst of all – they cost money. Inadequate attention to processes and weak approaches to DevSecOps culture are likely to be major contributors to these very significant problems.

Three-in-five (**61%**) of those planning to implement the methodology but not yet operating it, said they anticipate **P1 incidents will increase after implementation**. This really is the "move fast, break things quickly and fix them even quicker" approach. Many of these organisations may be unaware of how much they are breaking unnecessarily.

> **"Almost three-quarters of organisations (74%) have seen an increase in P1 incidents."**

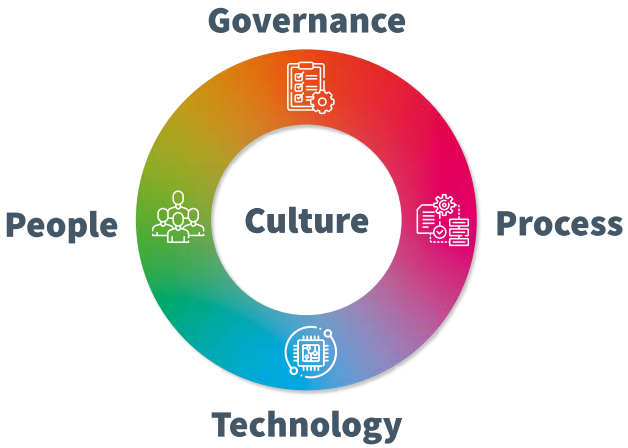
Organisations are unprepared for changes in demand

The research shows preparation is important. For example, **64%** of organisations using DevSecOps have seen demand for additional features increase within each new application release over the last year. This compares to less than half (**48%**) of organisations that are in the planning phase before they move to implementation.

But once organisations are operating DevSecOps, the research shows that for most the frequency of releases did not change significantly, on average moving from every ten days to once-a-week. With effective DevSecOps implementation this level of release frequency should be straightforward and trouble-free for almost any organisation.

Culture clashes over DevSecOps

DevSecOps is about more than technology – it requires a change of culture. Yet fewer than half of respondents (**47%**) say that their delivery teams have a high level of engagement and ownership of the application performance process and of implementing security practices. The need for deeper involvement in monitoring, logging and incident response practices may catch some organisations unawares – only **44%** of those planning to use DevSecOps anticipate teams will be extensively involved.



There are also widespread problems with the level of integration between the development, security and operations practices. Only **55%** of respondents who are working with DevSecOps practices say DevSecOps is fully integrated and working at the level they want, while **41%** say there is room for improvement, even though they have achieved full integration.

Resistance to adaptation

The research examined the **top three barriers to delivery teams** taking greater ownership of DevSecOps practices. Resistance to change was the most common issue (**51%**), followed by insufficient collaboration between teams (**47%**). These are significant factors that undo the benefits of any amount of new technology. **Unless attitudes change, practices will not.** The difficulty of resource constraints was also cited by **37%** of respondents. A lack of automation slows down processes and ties up teams in tasks from which they should be liberated.

Limited management support (**37%**) and lack of awareness and training (**33%**) were also cited as barriers.

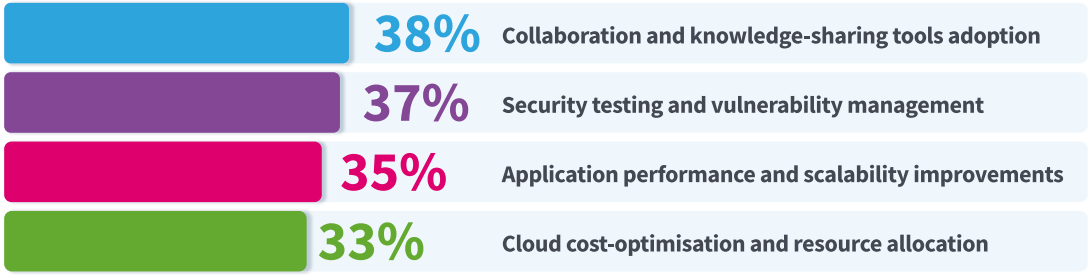
The role of training

Organisations are seeking to remedy these problems and support implementation of DevSecOps practices through training, both external and internal. Of those considering DevSecOps, only a quarter (**26%**) plan on providing internal training, compared with **42%** aiming to provide external support. However the reality after implementation is very different, when a shortage of skills becomes apparent. Of those operating with DevSecOps, **55%** provide external training and **52%** have provided internal training. The latter is a huge jump from the **26%** who are in the planning phase, highlighting how the internal challenges of implementing **DevSecOps are being underestimated.**

> **“52% have provided internal training. The latter is a huge jump from the 26% who are in the planning phase, highlighting how the internal challenges of implementing DevSecOps are being underestimated.”**

Are priorities achievable when security remains a problem?

All the organisations currently using DevSecOps have areas they plan to prioritise, such as:



But their ability to achieve these aims will be severely limited unless they tackle the significant problems, challenges and barriers outlined in this report.

Almost a quarter (**24%**) say their existing application architecture is not fit for purpose and therefore likely to cause friction. There is also a lack of adequate mandate and respondents admit problems among the broader DevSecOps environment are likely from their current DevOps support model.

Conclusion: DevSecOps can deliver, but approach is key

The evidence of this research is that organisations are **sacrificing quality for speed of delivery** when with the right approach to DevSecOps implementation and optimisation, they can achieve both.

Everyone is under pressure to achieve faster time-to-market as organisations seek greater business agility. Most that have implemented DevSecOps have certainly made gains and are reaping rewards in terms of faster product development and team efficiency, improved software quality, and cloud and tooling cost-reduction. But many continue to suffer significant drawbacks including **unacceptably high levels of P1 incidents**, failures of integration and poor adherence to true DevSecOps practices. These all erode the quality and performance and cost-effectiveness of the methodology.

Organisations face a reality check once they have embarked on DevSecOps, as this research shows. The hurdles and barriers to optimisation are often more complex than they expect. They should take every step possible to ensure that quality is paramount, but many clearly do not.

One organisation which has is UKHSA, which used automation to achieve significant efficiencies and reduced costs to support the scaling of healthcare systems that processed Covid-19 results. Automation captured four key DevSecOps metrics, pinpointing where bottlenecks were occurring, along with their root causes, allowing for adjustments of processes and pipelines across the delivery team.

Delivery speed was improved by 60% and production incidents reduced by a massive 89%, while saving £1m through optimisations.

Capacitas' own experience shows quality is the most worrying challenge for teams that are also under pressure to achieve speed and value. Organisations need to embed premium DevSecOps practice from the outset, employing engineering that improves product, quality and speed, while delivering value for money.

This is all achievable and founded on **a culture of ownership, continuous delivery, security, quality and extensive automation.** A four-stage discovery-realise-transform-protect model will fully optimise DevSecOps performance, locking in long-term gains and providing continuous benchmarking of teams.

Capacitas has a distinct and proven methodology that begins with an assessment across the core team to assess ten areas of DevSecOps maturity.

The Capacitas approach to DevSecOps

Detailed discovery workshops with teams identify the gaps and the opportunities for cost-reduction and where to increase speed and improve quality.

Building an implementation plan to address difficulties and deliver on opportunities.

DevSecOps toolchain definition. Define and support technical toolsets as required for adoption of toolchain and consolidation of tooling.

Further automation of testing and the consolidation of tools.

The automated collection of DORA metrics ensures engineering best practices are rigorously followed, highlighting pain points to delivery teams.

From a cultural perspective it is important to work with teams to deliver the implementation plan and roll out the new, tested, capability so DevSecOps becomes the ongoing engineering practice.

The Capacitas process will deliver:

- Faster product development
- Greater business agility
- Improved software quality
- Reduction of in-service incidents
- Cloud and tooling cost reduction
- Greater team efficiency

Why not **get in touch** to find out how we can help your organisation on its DevSecOps journey?


capacitas®
Only by adopting and embedding the very best DevSecOps practices can any organisation be sure it is fully optimising what is now an essential approach for heightened business agility in an ever faster and more competitive world.
www.capacitas.co.uk