FEDERAL NEWS NETWORK

EXECUTIVE SURVEY SERIES

DevSecOps

Sponsored by ATLASSIAN

Been there.
Scaled that.

Change is hard, especially for government agencies. Atlassian is here to help ease the pain of shifting to DevOps. Transform your agency workflows and speed application deployment time with open, flexible software.

Work smarter and faster, together.

- Unified workflows, centralized dashboards
- Streamlined knowledge management
- Real-time, visual data, task-tracking, and messaging notifications
- Best-in-class security

Visit www.atlassian.com/government

ATLASSIAN

It's not quite time to declare the waterfall approach to technology development dead, but without a doubt, this long-time, and much maligned, approach that worked a half century ago is on life support.

Meanwhile the acceptance and understanding of development, security and operations across the federal government is growing, particularly among technology workers.

A new Federal News Network survey of federal employees showed how the deep roots of DevSecOps have anchored themselves in the soil of project and program management.

A majority of respondents who work in technology said their agency has had at least one successful project using DevSecOps. These respondents also recognized the value of using an approach that promotes continuous integration to speed up new capabilities for citizens and to automate redundant or time-consuming processes.

It's among non-IT workers, however, where the concept of DevSecOps needs some cultivating.

The survey showed almost 95% of self-identified respondents who do not work in technology were not familiar with DevSecOps. More than half said their business or mission area was rarely or not involved in developing project requirements.

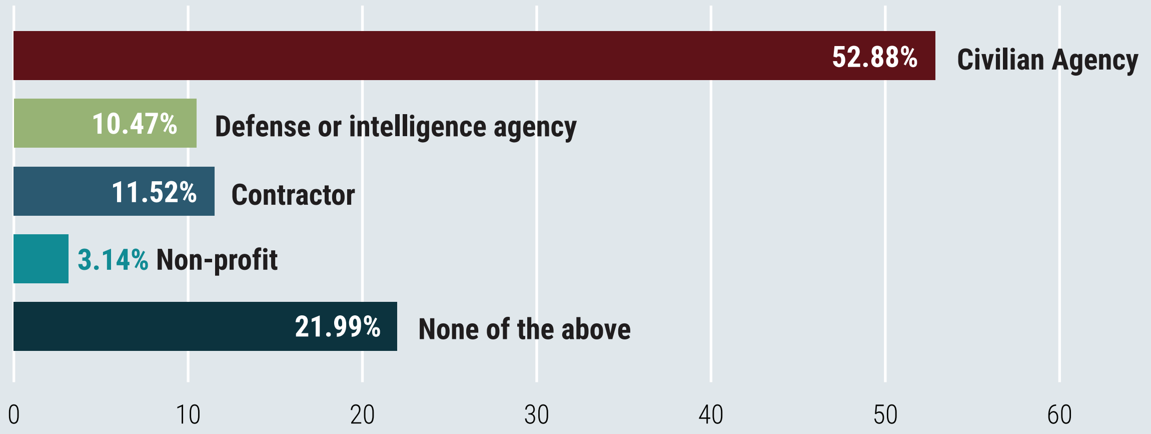
These non-IT employees said the biggest obstacles to moving toward a culture of continuous integration and improvement are training of employees, software tools and frustration with the federal budget process.

One thing is clear from the survey: While the ground is fertile, the DevSecOps approach needs plenty of water and sunshine to thrive in the coming years. The desire to change and to bring in modern, innovative approaches to technology development is real.

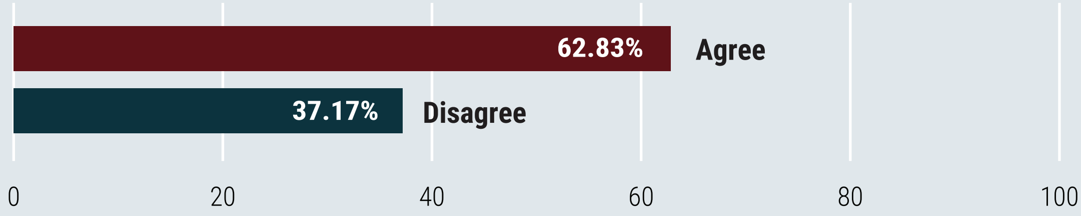
The survey leaves us with plenty of reasons to be optimistic. As one respondent said, "We have been doing this for a while now. It takes time to change the culture from waterfall to DevSecOps, but the culture has now shifted."

Jason Miller
Executive Editor
Federal News Network

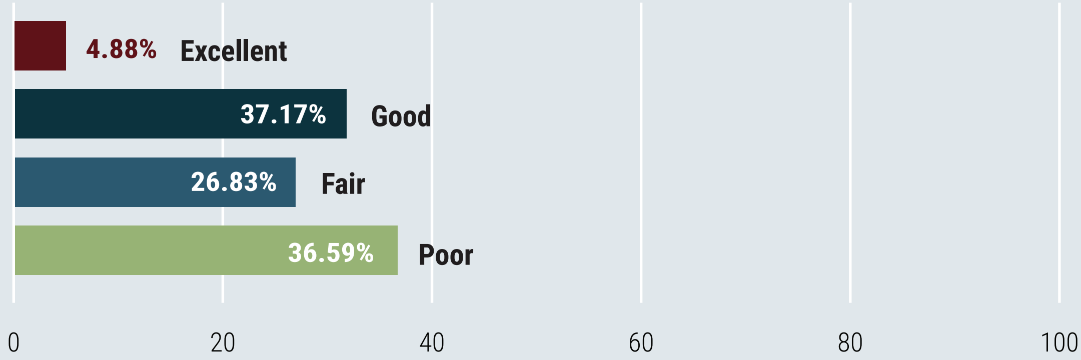
I work for a



A majority of the time, I work in the technology field, whether or not I'm in the 2210 occupation series.



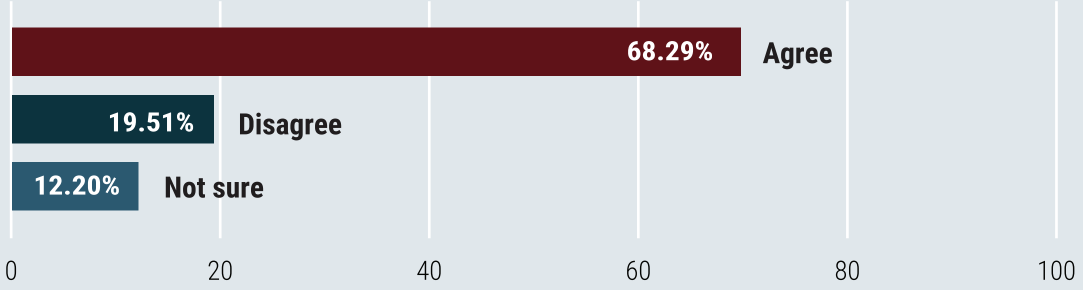
How would you rate the maturity of DevSecOps in your agency today?



COMMENTS:

- There are a few small pockets of success, but the strategy within the AF is still too fragmented (split between the Acquisitions and Communications communities), which leaves an incredible amount of risk to long-term improvements and sustainment of this new/emerging capability. It is possible to achieve, but is currently very reliant on a small, fragile leadership cadre.
- Implementation of SECOPS Consolidation Project in 1st Qtr FY20 did not contain a transition plan.
- My agency thinks that continuous integration (CI) is DevSecOps, and it's not. DevSecOps is incomplete in the USN.

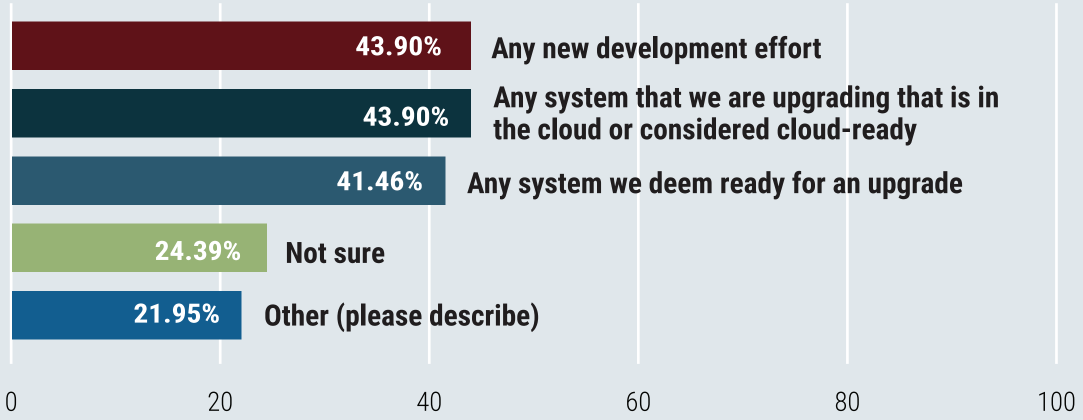
My agency has been successful at least once in using a DevSecOps approach instead of a waterfall approach to software or application development.



COMMENTS:

- The Dev with security in an automated pipeline is working but the Ops part is missing. also the continuous system of system test is missing. Also, there is only one program in PEO C4I that is "containerized".

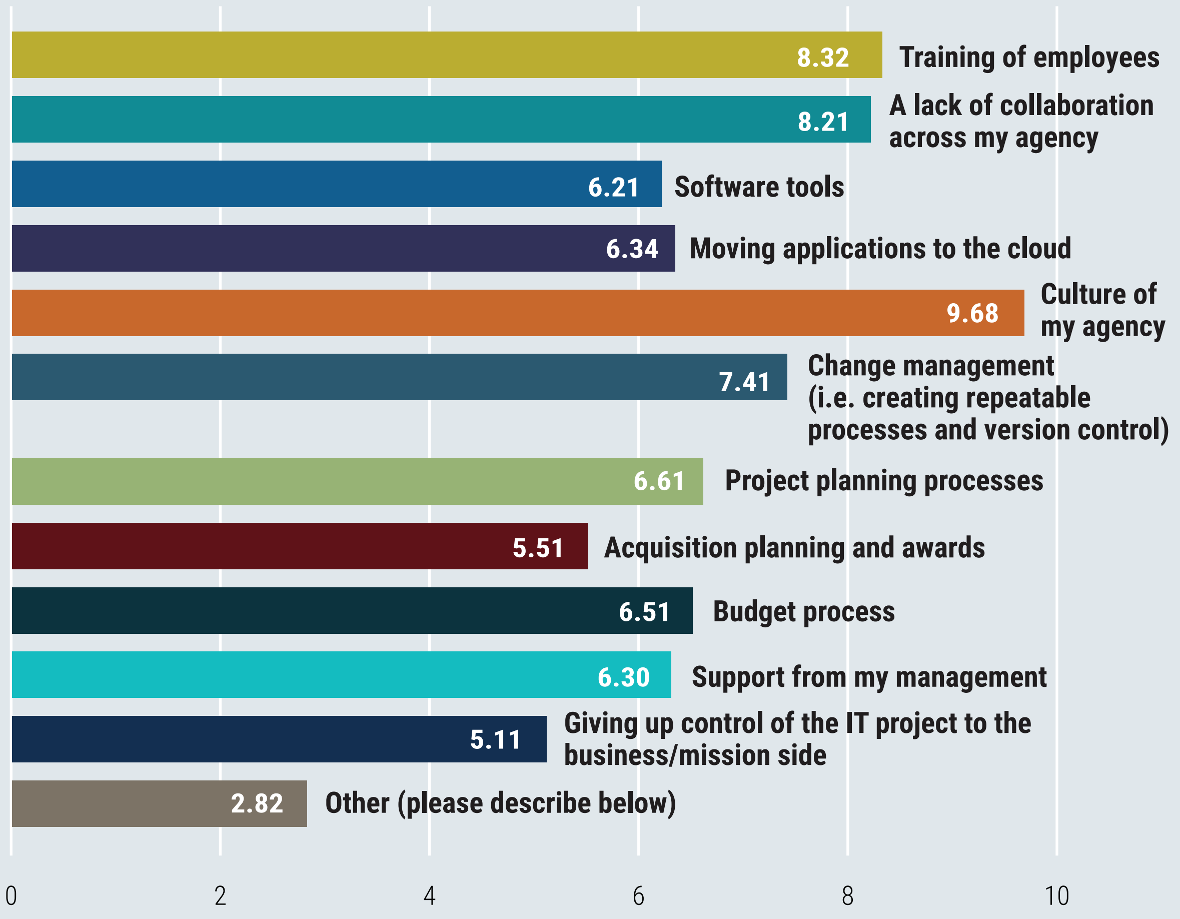
How do you decide which projects to use DevSecOps for? (Check all that apply)



OTHER (PLEASE DESCRIBE):

- Any effort that is web/cloud-based will benefit most from this strategy.
- It's mostly new development but the USN has a lot of legacy software that needs to be redesigned for modularity and containers and there isn't a plan in place. Programs are on their own to figure out their own legacy transformation.
- Right now it is based on if the project has a high enough priority/importance.
- Depends on the SOW in the development contract.

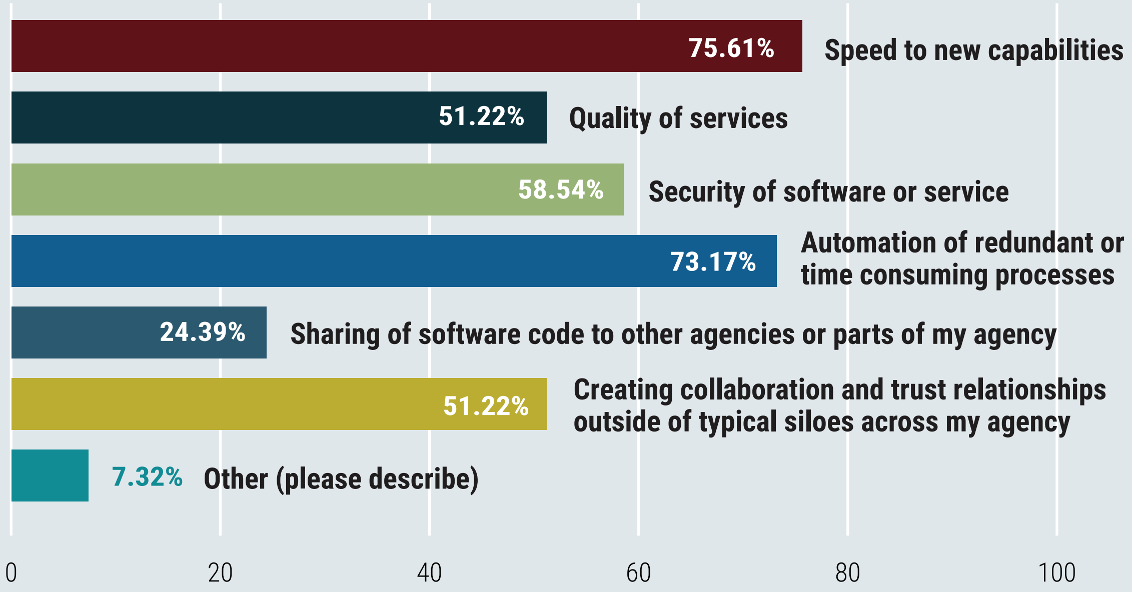
What are the biggest challenges in moving toward a DevSecOps approach to development? (Rate from biggest challenge to smallest challenge)



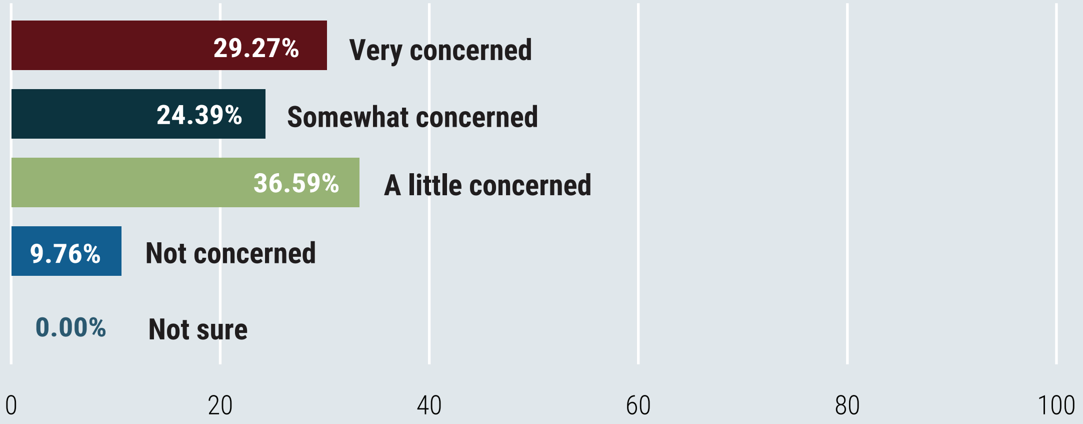
IF YOU SAID OTHER, PLEASE DESCRIBE:

- Identification of security requirements (lots of churn in establishing minimum controls).
- Knowledge on the process.
- Getting sufficient SME participation.
- Echelon I in the USN needs to mimic the Air Force (AF). The AF has a chief security officer and the AF has two fully functioning DevSecOps software factories with pipelines that are fully operational. The USN has NONE. The most famous USN DevSecOps pipeline is C2C24, and it's not fully operational because it needs support from OPNAV. DevSecOps can't be fully functional in the USN without a top down SECNAV/OPNAV/CIO plan. Those agencies are pretending that C2C24 works. Also, the USN needs to take all the training classes the AF offers!
- Ability to find and keep on board competent contractors to perform the work.
- Change Control Board stubbornly resists adopting streamlined processes.

How do you decide which projects to use DevSecOps for? (Check all that apply)

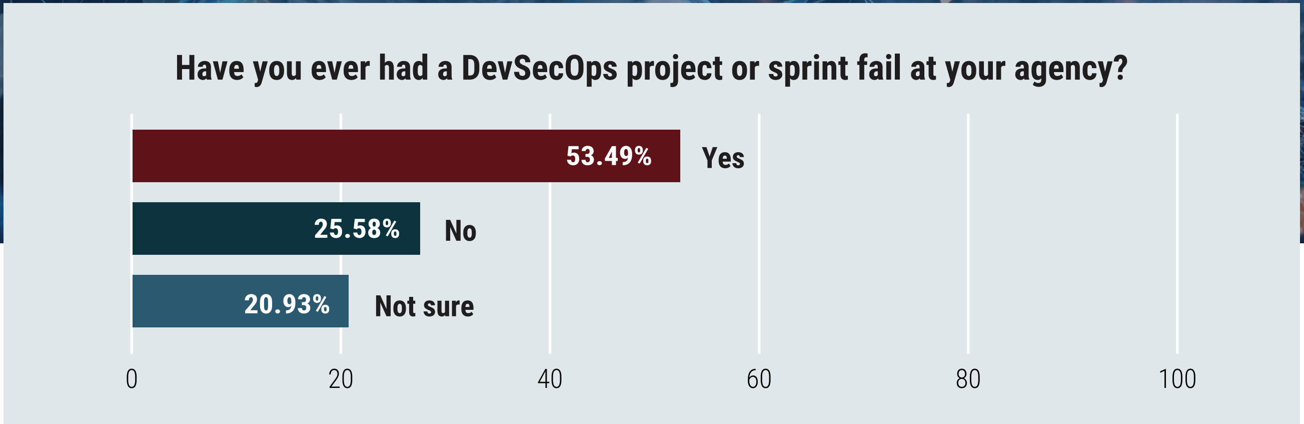


How concerned are you about DevSecOps project/sprint that will fail?



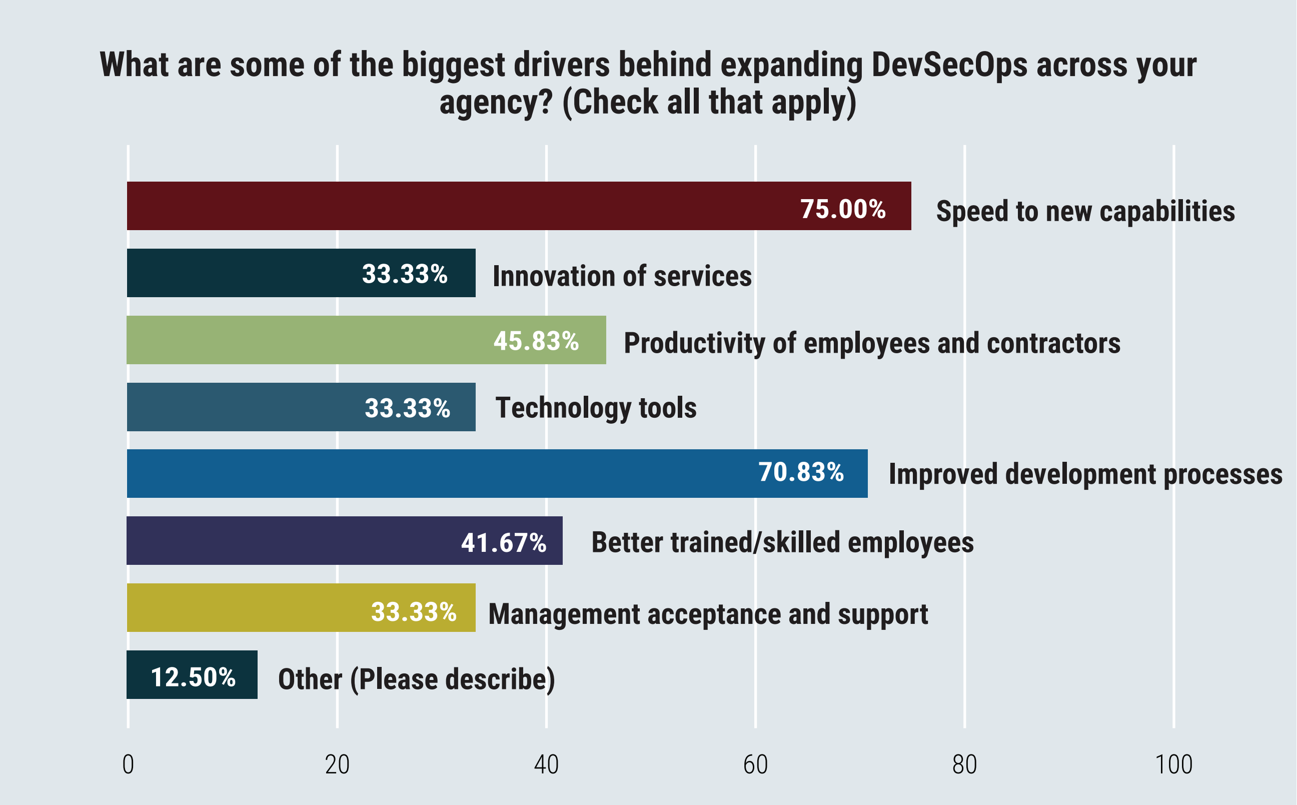
COMMENTS:

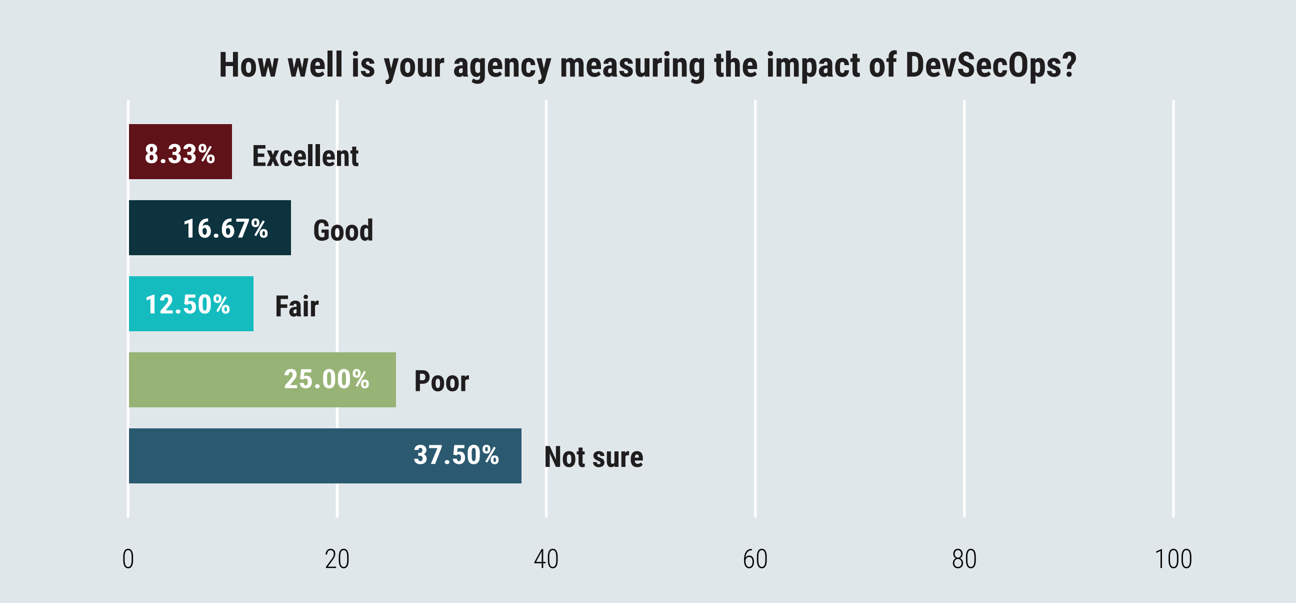
- Failure is expected. Agile is about constant improvement. Without failure, there is nothing to improve on.
- If the USN doesn't have a fully functional DevSecOps pipeline then the USN can't field software at the speed of relevance.
- Our IT goals are NEVER met in a timely fashion. We suffer 'brain drain' on a regular basis, losing competent developer contractors to higher bidders.
- IT problems do slow production down considerably.

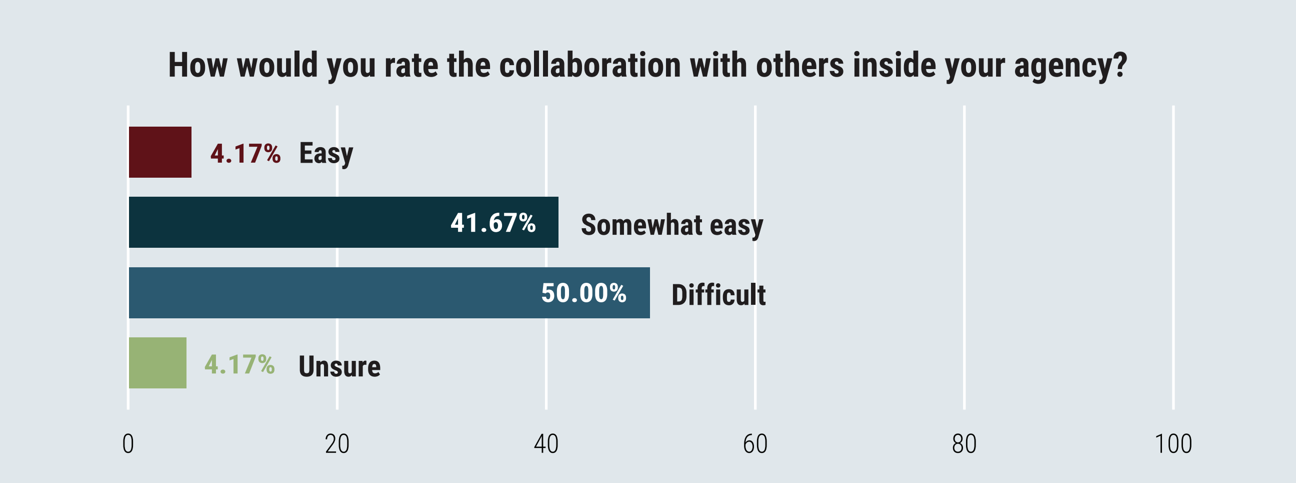


IF YES, WHY DID IT FAIL AND HOW HAVE YOU CORRECTED YOUR PROCESSES SO YOU DIDN'T HAVE FAILURES AGAIN?

- It failed due to lack of buy-in from a customer. The project was mandated, but not funded.
- From what I could see, we just deny it was a failure. Instead, we say that we stopped the project in order to save money and thereby call it a "win".
- Sharing information.
- Communication issues that have been resolved
- Loss of competent developers. Failure to adequately train new ones. We use Jira religiously (maintained by the product owners) but tickets are largely ignored by developers.
- Failed to produce a working product.
- We had to reassign people to various tasks.







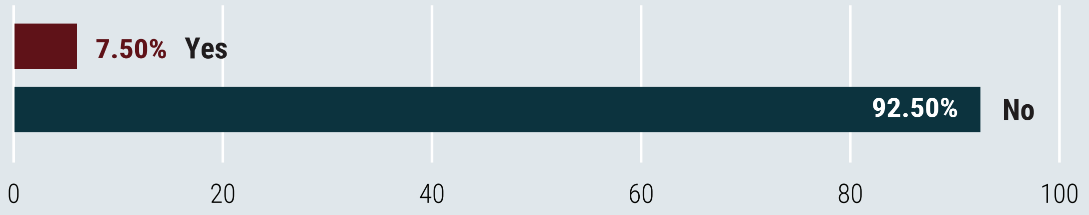
COMMENTS:

- Large agencies find collaboration difficult.
- Pay-as-you-go model of cloud consumption with DevSecOps is more painful than more static legacy capitalized purchases that are not often chargeback.
- Groups are unwilling to share information.

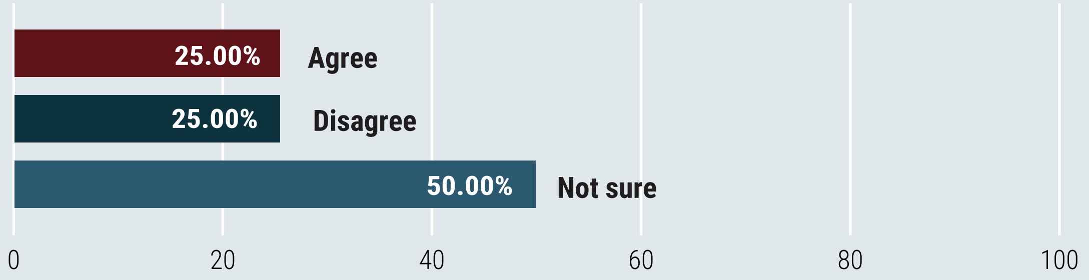
PLEASE OFFER ANY OTHER COMMENTS ON YOUR AGENCY'S MOVE TO DevSecOps:

- We are reliant on DOD which has done some good work in the standards arena for DevSecOps.
- We have been doing this for a while now. It takes time to change the culture from waterfall to DevSecOps. But the culture has now shifted.
- The agency needs a team specifically devoted to DevSecOps and continuous testing and development. Not sure we have the funding for this HR/skill need.
- We continue to have extremely low success on deployment of software upgrades because test fail obscure security requirements set at the Department level, requirements that are (understandably) ever-changing. I'm highly dissatisfied with the whole system and do not see a solution in sight.
- We're converting projects as their contracts change over.

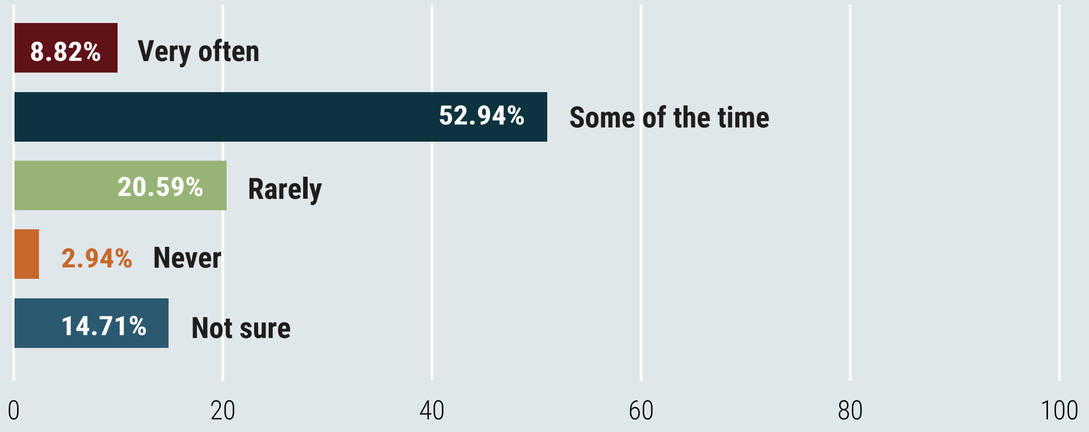
Are you familiar with the concept called DevSecOps for software development?



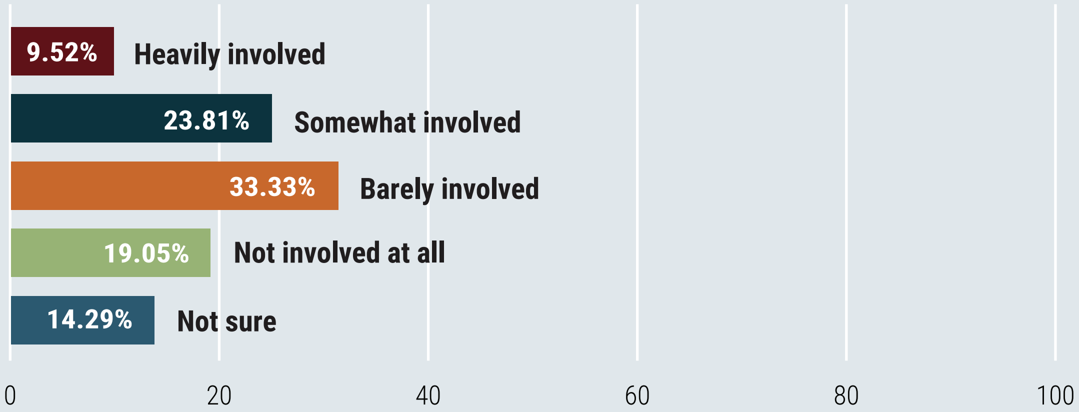
If yes, my agency is using an approach to software or project development called DevSecOps.



If no, my agency adopts new or innovative technology processes:



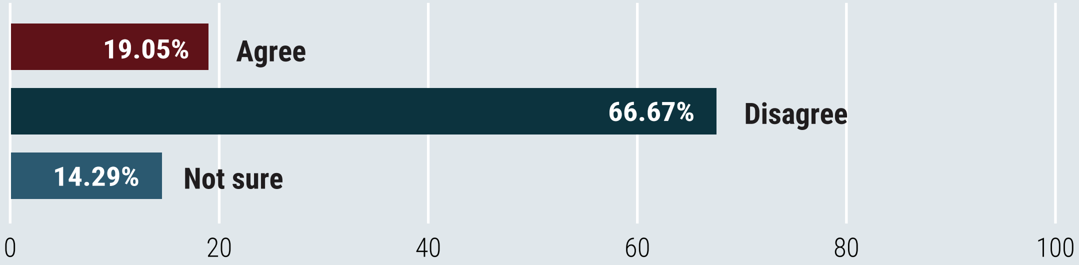
When it comes to developing project requirements and plans for internal or external technology services, my business/mission area is:



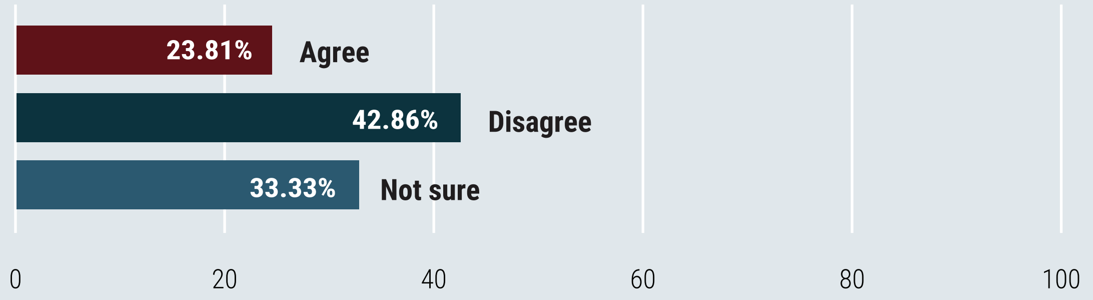
COMMENTS:

- Field managers are rarely asked what they need for major IT projects these days.

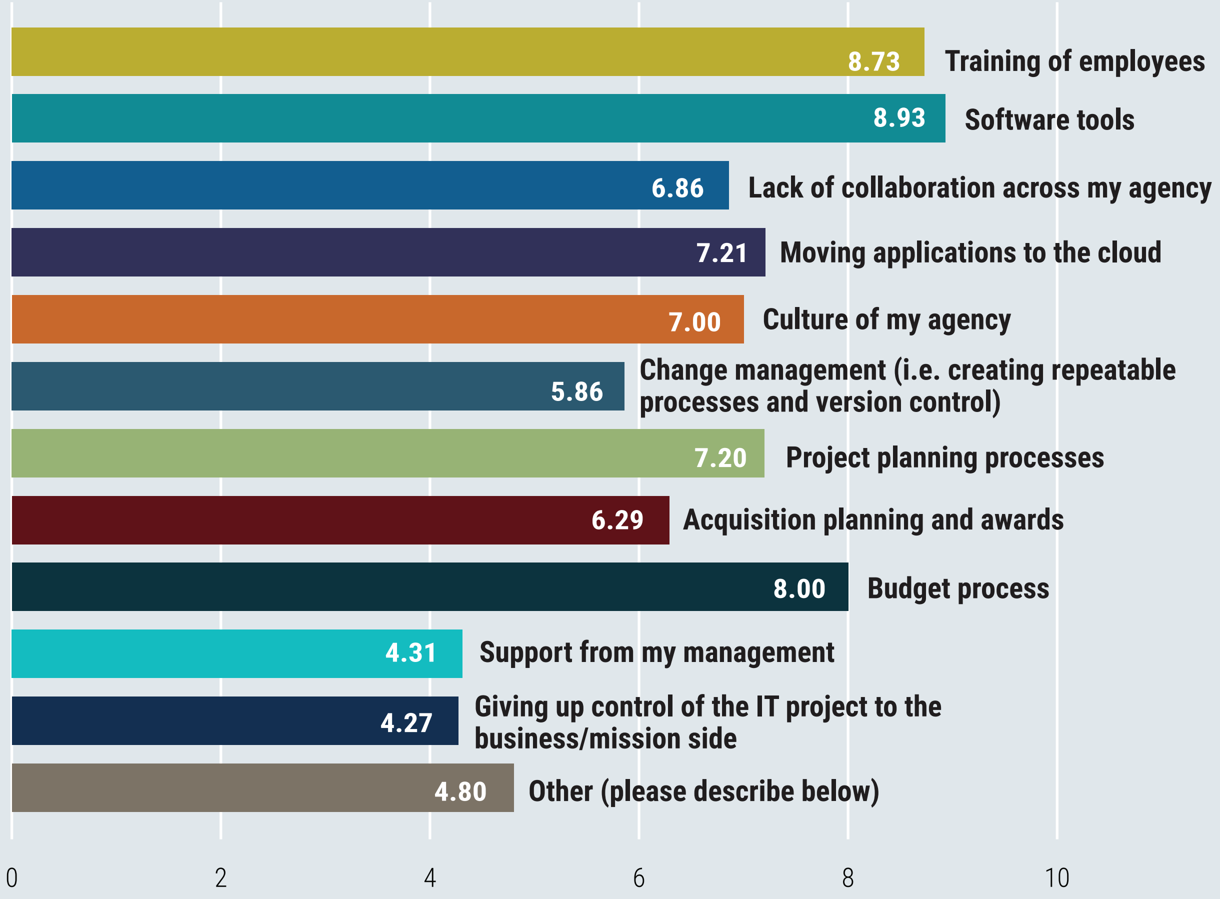
My office often gets to review and comment on new technology capabilities that are under development and before they are launched to the general public or broad internal audience.



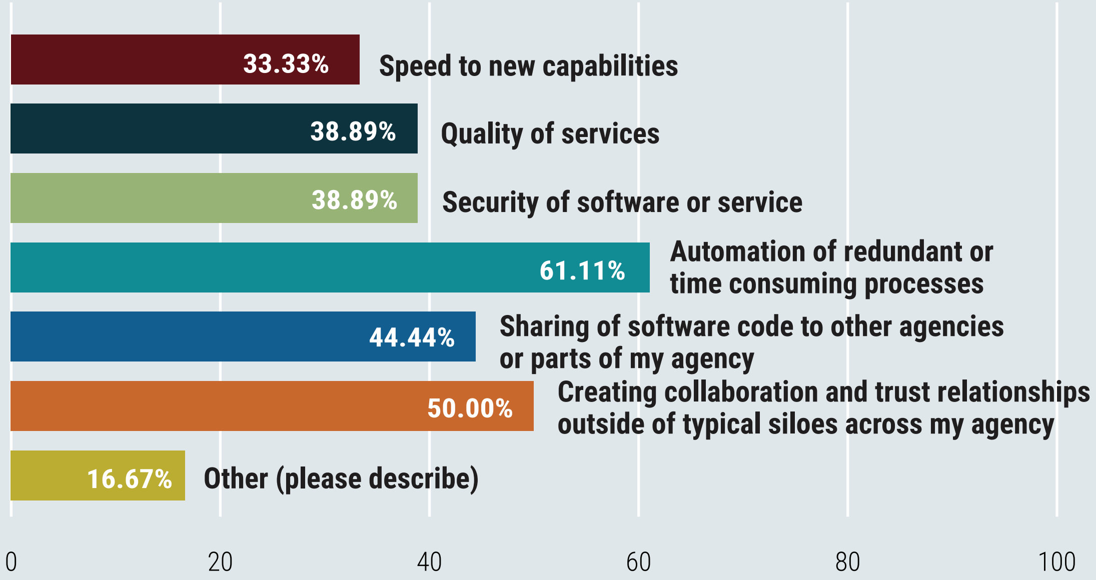
Do you think your agency is ready for the processes that underlie DevSecOps of automation, short time frame to release new capabilities, user centered design and similar approaches?



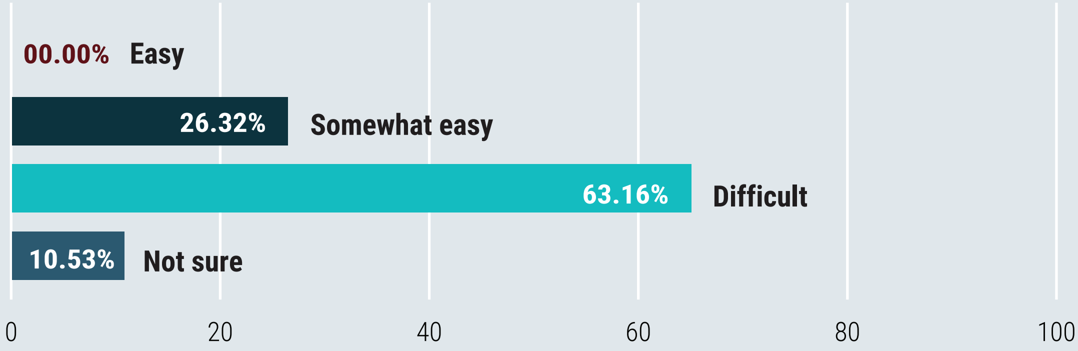
What are the biggest challenges that your agency faces to moving toward this culture of DevSecOps? (Rate from biggest challenge to smallest challenge)



What are the biggest benefits of moving toward a DevSecOps approach? (Check all that apply)



How would you rate the collaboration with others inside your agency?



COMMENTS:

- IT has been taken to department level unilaterally, and the people there neither know nor care what works or why things work the way they do.