



Collaboration and Communication Drive DevOps Success

Among the key attributes of DevOps:

- Transparency of process
- Coordinated sharing of expert information
- Operational efficiencies through automation of project tasks
- Automating tasks that greatly reduce delivery time while increasing quality and confidence

ICF is a full-service IT provider, delivering innovative technology solutions to help government and commercial organizations reach their target audiences, make sense of complex data, and solve problems.

We enable digital transformation using the latest tools and technology platforms along with Agile and DevOps practices, philosophies that promote a higher standard of security and quality. From websites to legacy system modernization to new implementations, our specialized teams are leveraging automation solutions to solve clients' toughest challenges in areas of national importance that include health, cybersecurity, energy, and veterans' issues.

DevOps is an increasingly popular practice in system development that offers the benefits of an Agile approach beyond the realm of programmers. By breaking down barriers across the life cycle, DevOps facilitates collaboration from start to finish between those who request, those who create, and those who support a system post-launch.

Sharing a common roadmap, DevOps teams work with empathy for each other and are more vested in delivering a quality product. Rather than a manager determining when to engage team members, the team works together to share experiences and needs. By respecting and understanding each other's diverse requirements, team members are better able to plan their tasks.

Measuring and Monitoring

ICF has created a model to measure DevOps attributes to assess a given project team's DevOps maturity and level of quality over time. As new tools become available, or as defects are identified and resolved, additional levels of testing can be added to ensure that bugs are not reintroduced during future development. Real-time, streaming monitoring allows for systems that are able to scale up and down as demand requires so customers spend only what they need to on infrastructure when their stakeholders have their highest or lowest demand. An effective monitoring solution not only alerts administrators to issues, but also enable systems to self-heal without administrator intervention.









About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, technologists, researchers, digital strategists, social scientists, and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at **icf.com**.

For more information, contact:

Rami Aboushakra

rami.aboushakra@icf.com +1.703.272.6562

-  facebook.com/ThisIsICF/
-  twitter.com/ICF
-  youtube.com/icfinternational
-  plus.google.com/+icfinternational
-  linkedin.com/company/icf-international
-  instagram.com/thisisicf/

TANGIBLE EFFECTS ON PROJECT TEAMS

Before DevOps	With DevOps
<ul style="list-style-type: none"> ■ Project team creates a website, then submits a request to push the website live. ■ A day passes, the site is still not live, and frustration begins. ■ When the required security scan is executed, the team learns that vulnerabilities exist that must be corrected before the site can go live. ■ Consternation and resentment build. ■ Once the site is live, the user community does not use the site, and feedback indicates that the site fails to provide the user community with what it needs--even though the site technically meets the contractual obligation. 	<ul style="list-style-type: none"> ■ User experience (UX), design, application development, security, and systems administration work together to define the delivery roadmap. Team meets regularly and knows each other. ■ Through human-centered design and testing, the UX team informs the system design to create a solution that will meet user needs. ■ Design team creates a compelling, interactive, responsive design that performs on desktop, mobile, and other platforms identified by the user community. ■ Development team leverages a continuous deployment process automating unit, integration, functional, performance, and security tests. ■ Software release iterations layer features and interactions, informed by UX ■ Site launches and is well-received by the community. ■ During the first reporting period, site usage swells and the system scales easily to support the increased load. ■ Following the quarterly reporting, the system scales back to the baseline automatically avoiding downtime and unnecessary costs.
<p>Result: Frustrated development team and a dissatisfied client</p>	<p>Result: Customer is happy with the product and with the DevOps team.</p>

Efficiency from DevOps in the Federal Space

When infrastructure and applications are developed using code, security controls can be documented and versioned with the technology stack. Because automation is used to create the stack, it will be created identically each time the code is executed, with confidence. Taking this a step further, a system designed to be secure can be replicated with confidence that the new system will be equally secure. ICF refers to this as "technology control inheritance."

As a very simple example, a NodeJS application in AWS may include IAM control to manage access to components of the system, New Relic for application monitoring, in a locally-redundant and geo-redundant infrastructure created using CloudFormation. The system goes through the Federal Risk Management Framework (RMF) and the security controls are documented via a System Security Plan (SSP) in accordance with an Agency Information Security Office policy. When a new application of identical NIST impact level is created for the Agency leveraging automation, using the same technology stack, the controls documented in the SSP are inherited by the new system. While this does not eliminate the need to go through the process of obtaining an Authority to Operate (ATO) for the new application, it greatly reduces the burden of generating the required documentation to initiate the process.

