Each issue of the *Defense Acquisition Research Journal* will bring to the attention of the defense acquisition community a topic of current research, which has been undertaken by the DAU Virtual Research Library team in collaboration with DAU’s Director of Research. Both government civilian and military Defense Acquisition Workforce readers will be able to access papers publicly and from licensed resources on the DAU Virtual Research Library Website: https://dau.libguides.com/daukr.

Nongovernment Defense Acquisition Workforce readers should be able to use their local knowledge management centers/libraries to download, borrow, or obtain copies. We regret that DAU cannot furnish downloads or copies.

*Defense Acquisition Research Journal* readers are encouraged to submit proposed topics for future research by the DAU Virtual Research Library team. Please send your suggestion with a short write-up (less than 100 words) explaining the topic’s relevance to current defense acquisition to: Managing Editor, *Defense Acquisition Research Journal*, DefenseARJ@dau.edu.
DevSecOps Practices for an Agile and Secure IT Service Management

Mounia Zaydi & Bouchaib Nassereddine

Summary:
Without appropriate consideration of security best practices, the continuous delivery of Information Technology (IT) services facilitated by Development Operations (DevOps) is risky. On the other hand, Security Operations (SecOps) offers the possibility to reduce security risks if security is integrated into the continuous delivery pipeline according to best practices. The purpose of this paper is to investigate how Development Security Operations (DevSecOps) culture can be applied in IT Service Management (ITSM). We interviewed representatives of five Middle East and North Africa (MENA) organizations that are adopting SecOps in their ITSM daily activities. We note that the majority of respondents expressed the potential of common DevSecOps such as automated monitoring to improve ITSM. The findings of this study imply that organizations need a framework for understanding the DevSecOps culture before they can adopt these practices in their ITSM. Likewise, this study explores the main DevSecOps practices relevant to efficient ITSM.

APA Citation:
Kessel Run: An Analysis of the Air Force’s Internal Software Development Organization

Jenny Aroune, Robert Hollister & Nathan Taylor

Summary:

The current method of acquiring custom, innovative software through traditional contracting methods is an outdated practice. These traditional methods are time-consuming, and could be improved with the Air Force’s Kessel Run, an internal software development organization. With the Air Force’s Kessel Run, the time from software inception to operation can go from years to days. Unfortunately, neither most of the Air Force nor the rest of the Department of Defense (DoD) has yet to catch up to the forward thinking of those involved in the creation of Kessel Run. Most of the Air Force and the DoD are still outsourcing for most of their innovative acquisitions, whether it be research and design or product (software) development. This case study offers insight to the new organization and identifies the potential to apply the concepts learned during its creation to benefit other DoD organizations when considering insourcing as opposed to the traditional outsourcing acquisition approach.

APA Citation:


From Waterfall to OASIS: Navy Command’s Excursion through Kessel Run Brings DevSecOps to Marine Corps

Steve Ghiringhelli

Summary:

A Naval Information Warfare Center (NIWC) Atlantic enterprise engineering team recently began deploying in earnest its paradigm-shifting methodology for developing software. Modeled after the U.S. Air Force’s
“Kessel Run,” the newly accredited Operational Application and Service Innovation Site (OASIS) enables NIWC Atlantic's Expeditionary Warfare (ExW) Department to provide “DevSecOps”—development, security, and operations—to the U.S. Marine Corps for the first time. DevSecOps is a commercial best practice that has revolutionized the software industry and only recently made inroads in the U.S. military.

APA Citation:

DevSecOps Puts Security at the Heart of Program Development

Henry S. Kenyon

Summary:
The Department of Defense is rethinking how it approaches software and systems development in its technology programs by using more flexible methods to streamline the process and to improve cybersecurity from the start. Because traditional DoD program development processes don’t have the speed and flexibility to keep up with rapid technological changes or fast-paced modern adversaries, new methodologies are being considered. DevSecOps versus Agile Development methodologies that emphasize iterative development cycles and feedback to find and correct errors throughout the software building process have become more common in federal government technology programs. While DevSecOps does build on some Agile Development principles, such as the continuous integration and delivery of software systems in cycles, its key emphasis from the beginning of the process is to integrate security features: DoD Applications and Changing Culture DevSecOps fits into the DoD’s modernization strategy to upgrade legacy systems and incorporate new capabilities such as machine learning or artificial intelligence into its mission.

APA Citation:
DoD Enterprise DevSecOps Reference Design: Version 1.0

Thomas Lam & Nicholas Chaillan

Summary:

Legacy software acquisition and development practices in the DoD do not provide the agility to deploy new software “at the speed of operations.” In addition, security is often an afterthought, not built in from the beginning of the life cycle of the application and underlying infrastructure. DevSecOps is the industry best practice for rapid, secure software development. DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software life cycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. In DevSecOps, testing and security are shifted to the left through automated unit, functional, integration, and security testing—this is a key DevSecOps differentiator since security and functional capabilities are tested and built simultaneously.

APA Citation:

Jeremy D. Kramer & Torrey J. Wagner

Summary:
This article provides insights into the current state of developmental testing (DT) and requirements management in Department of Defense information systems employing Agile Development. The authors describe the study methodology and provide an overview of Agile Development and testing. Insights are described for requirements, detailed planning, test execution, and reporting. This work articulates best practices related to DT and requirements management strategies for programs employing modernized Software Development Life Cycle practices.

APA Citation: