

IDENTIFYING AND ADDRESSING RESEARCH GAPS IN DEVOPS: TOWARD STANDARDIZED FRAMEWORKS, SECURITY INTEGRATION, AND ORGANIZATIONAL READINESS

* *Ms. Pramila .V. Bairagi*

* *Assistant Professor, Department of Computer Science & Information Technology, Sainath Education Trust's Rajiv Gandhi College of Arts, Commerce and Science, Plot No 16/17, Sector 10A, Vashi, Navi Mumbai.*

Abstract:

DevOps has become a central approach in contemporary software engineering, aiming to accelerate delivery cycles, enhance system reliability, and foster stronger collaboration between development and operations teams. However, despite its broad adoption, many organizations continue to experience inconsistent results, security shortcomings, and challenges in successful implementation. This study explores enduring research gaps in DevOps through the analysis of three closely connected areas: the absence of unified and standardized frameworks, the fragmented incorporation of security practices, and the limited attention given to organizational readiness. Using a survey-based research methodology supported by a critical review of existing literature, the study evaluates empirical insights gathered from DevOps practitioners across multiple industries in conjunction with prior academic research. The results indicate that current DevOps practices are predominantly driven by tools, security is unevenly integrated across the lifecycle, and organizational readiness remains insufficiently theorized and poorly operationalized. This research advances the field by conceptualizing DevOps as a socio-technical system and by outlining an integrative direction to inform future research and practical adoption. The study further discusses implications for theory building, organizational strategy, and the implementation of secure DevOps practices within post-pandemic, distributed work settings.

Keywords: *DevOps, DevSecOps, organizational readiness, standardized frameworks, software engineering*

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial Use Provided the Original Author and Source Are Credited.

Introduction:

DevOps has evolved from an informal, practitioner-led initiative into a foundational component of digital transformation efforts across a wide range of industries. Emphasizing practices such as continuous integration, automated delivery pipelines, and collaboration between development and operations teams, DevOps aims to address the limitations of traditional, functionally isolated software development approaches. Conceptually, it offers the potential for accelerated innovation, greater system reliability, and improved organizational learning. Yet, in real-world settings, DevOps adoption often produces uneven outcomes, with many organizations struggling to realize its anticipated benefits despite significant investments in automation tools and infrastructure.

At the heart of this challenge is a widening gap between the theoretical aspirations of DevOps and the way it is implemented in practice. Rather than being informed by cohesive and empirically validated frameworks that align technical processes, security mechanisms, and organizational capabilities, DevOps initiatives are frequently introduced in a piecemeal manner. Organizations tend to emphasize rapid delivery over long-term resilience, automation over governance, and tooling over human and organizational preparedness. As a result, security controls are commonly added late in the development lifecycle, and assumptions about organizational readiness replace systematic evaluation.

While existing research has examined aspects such as DevOps culture, maturity assessment models, and the emergence of DevSecOps, these contributions are often treated in isolation. Limited attention has been given to understanding how standardization, security integration, and organizational readiness interact as interdependent elements of a broader system. The lack of such an integrated perspective has tangible implications, including unsuccessful transformation initiatives, heightened exposure to security threats, and resistance from teams unprepared for DevOps-driven change. This study responds to these limitations by combining a critical synthesis of the literature with empirical insights from practitioners, with the aim of identifying persistent gaps in current DevOps research and practice and explaining their significance.

Identifying and Addressing Research Gaps in DevOps:

1. Lack of Standardized DevOps Frameworks

Existing DevOps implementations rely heavily on organization-specific practices, resulting in inconsistent outcomes and limited comparability across studies.

Most current frameworks emphasize tooling and automation while offering minimal guidance on governance, measurement, and long-term sustainability.

2. Fragmented Integration of Security (DevOps)

Security practices are often introduced late in the software lifecycle, undermining the core DevOps principle of continuous feedback and risk mitigation.

DevSecOps adoption remains uneven due to unclear role definitions, cultural resistance, and limited alignment between security and delivery teams.

Existing studies focus on tools and techniques rather than organizational and process-level integration of security.

There is insufficient empirical evidence on how continuous security practices influence delivery performance, resilience, and compliance outcomes.

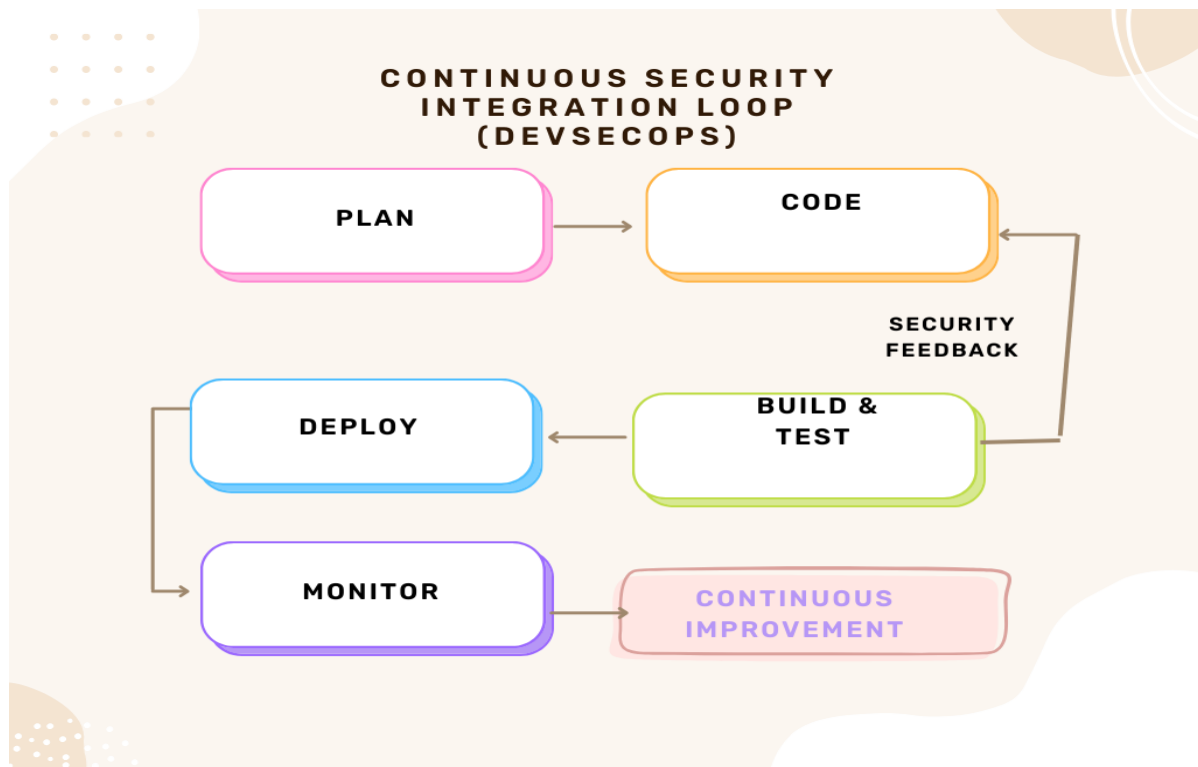
3. Underexplored Organizational Readiness

Organizational readiness for DevOps is frequently assumed rather than systematically assessed prior to adoption.

Human factors such as skills, leadership support, team autonomy, and cultural alignment are weakly operationalized in existing research. Current maturity models inadequately capture organizational change dynamics, especially in large, regulated, or distributed environments.

Limited attention is given to the impact of remote and hybrid work models on DevOps readiness and collaboration effectiveness.

Continuous Security Integration Loop (DevSecOps)



Literature Review:

Research on DevOps has progressed through largely disconnected streams. Initial work focused primarily on automation, infrastructure efficiency, and architectural optimization, whereas subsequent empirical investigations examined associations between DevOps practices and organizational performance outcomes. Although these contributions have expanded understanding of DevOps, efforts to formalize the approach through maturity models and standardized frameworks continue to be constrained by high levels of abstraction and limited adaptability to diverse organizational contexts.

The rise of DevSecOps signals increasing recognition of the security challenges created by rapid and continuous software delivery. While existing literature reviews indicate a growing emphasis on security automation and pipeline-level controls, comparatively little attention has been paid to organizational and governance-related factors. Empirical findings suggest that the effectiveness of security integration is strongly influenced by non-technical elements such as leadership engagement, workforce capabilities, and institutional support structures. Organizational readiness is often cited as a critical enabler of DevOps success, yet it is rarely translated into measurable or actionable constructs. Socio-technical research points to persistent issues including cultural resistance, coordination barriers, and misaligned incentives; however, these factors are seldom embedded within DevOps frameworks or assessment models. Taken together, the literature exhibits recurring tendencies toward

partial solutions, fragmented conceptualizations, and isolated methodological approaches, highlighting the need for integrative research perspectives consistent with the objectives of this study.

Methodology:

This research adopted a cross-sectional survey methodology to examine practitioner perspectives on DevOps frameworks, security integration, and organizational readiness. Data collection was conducted from March to July 2026 and involved DevOps practitioners representing diverse industries and geographic regions. A purposive sampling approach was applied to ensure that respondents possessed a minimum of one year of hands-on experience working within DevOps-oriented environments.

The survey instrument was designed by integrating established measures drawn from prior studies on DevOps maturity, DevSecOps practices, and organizational readiness, alongside newly formulated items intended to address gaps identified in the literature. Quantitative responses were analyzed using descriptive statistical techniques, internal consistency assessment, exploratory factor analysis, and regression analysis to explore relationships among key variables. Qualitative data obtained from open-ended questions were analyzed thematically to enrich and contextualize the quantitative results.

Ethical clearance for the study was granted by the Institutional Research Ethics Committee of the authors' affiliated university. Participation was voluntary, and informed consent was obtained from all respondents prior to data collection.

Results and Analysis :

The findings demonstrate a predominant dependence on tool-focused DevOps practices, with relatively limited adoption of formally defined or externally standardized frameworks. Although a majority of participants reported some degree of automation within their deployment pipelines, substantially fewer indicated the presence of structured approaches for evaluating DevOps maturity or organizational readiness. The integration of security practices was inconsistent: while automated security testing was commonly implemented, issues related to governance structures, role clarity, and accountability for security responsibilities persisted across many organizations.

Inferential analysis identified statistically significant relationships between key organizational readiness dimensions particularly leadership commitment and workforce capability and perceived DevOps performance. Further analysis indicated that security integration played a mediating role in this relationship, implying that organizational readiness alone does not translate into effective DevOps outcomes without deliberate and continuous incorporation of security practices. Insights from open-ended responses supported these quantitative results, with respondents frequently highlighting cultural resistance, ambiguous role definitions, and regulatory compliance demands as major obstacles to achieving sustainable and secure DevOps adoption.

Discussion :

The results of this study underscore that DevOps performance emerges from the combined influence of technical practices, security integration, and organizational conditions, rather than from isolated improvements in any single area. The continued prevalence of tool-centered implementations aligns with patterns observed in earlier

research, yet the findings also highlight the inherent constraints of such approaches when broader organizational and governance factors are overlooked. These outcomes question linear interpretations of DevOps maturity and instead lend support to socio-technical viewpoints that position organizational readiness and governance as central determinants of success.

This research contributes to the existing body of knowledge by providing empirical evidence of security integration as a mediating mechanism between organizational readiness and DevOps effectiveness. By identifying organizational readiness as a foundational enabler and security as a critical integrating element, the study connects previously fragmented streams of DevOps, DevSecOps, and organizational transformation research. The resulting integrative perspective offers a more cohesive explanation of why DevOps initiatives succeed or fail and provides a basis for advancing both theory development and practical implementation.

Conclusion:

This study investigated persistent gaps in DevOps research by examining the roles of standardized frameworks, security integration, and organizational readiness. The findings reveal that contemporary DevOps practice remains largely fragmented and dominated by tool-focused implementations, with security considerations and readiness assessments applied inconsistently. From a theoretical standpoint, the study contributes to DevOps literature by conceptualizing DevOps as an integrated socio-technical system in which technical processes, security mechanisms, and organizational capabilities are interdependent. From a practical perspective, the results emphasize the importance of adopting readiness-sensitive and security-by-design frameworks, particularly within post-pandemic contexts marked by distributed collaboration and increased cybersecurity exposure. While the study is subject to limitations associated with its cross-sectional approach and reliance on self-reported perceptions, it establishes a solid platform for subsequent research. By identifying overlooked dimensions and clarifying their significance, this work deepens understanding of how DevOps initiatives can be structured to promote sustainable performance, organizational resilience, and long-term value creation in the evolving digital economy.

References:

1. Bass, L., Weber, I., & Zhu, L. (2015). *DevOps: A software architect's perspective*. Addison-Wesley.
2. Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). *DevOps*. *IEEE Software*, 33(3), 94–100. <https://doi.org/10.1109/MS.2016.68>
3. Forsgren, N., Humble, J., & Kim, G. (2018). *Accelerate: The science of lean software and DevOps*. IT Revolution Press.
4. Lwakatare, L. E., Kuvaja, P., & Oivo, M. (2016). *Relationship of DevOps to agile, lean and continuous deployment*. *International Conference on Product-Focused Software Process Improvement*, 399–415.
5. Myers, J., & Behl, A. (2020). *DevSecOps: A systematic literature review*. *Information and Software Technology*, 127, 106391. <https://doi.org/10.1016/j.infsof.2020.106391>
6. Rahman, A. A., Helms, T., & Williams, L. (2021). *Security practices in DevOps environments: An empirical investigation*. *Empirical Software Engineering*, 26(4), 1–34.

7. Weiner, B. J. (2009). *A theory of organizational readiness for change*. *Implementation Science*, 4(1), 67.
8. Wiedemann, A., Wiesche, M., & Krcmar, H. (2019). *Implementing DevOps in organizations: A multiple-case study*. *Information Systems Frontiers*, 21(6), 1291–1306.

Cite This Article:

Ms. Bairagi P.V. (2026). *Identifying and Addressing Research Gaps in DevOps: Toward Standardized Frameworks, Security Integration, and Organizational Readiness*. **In Educreator Research Journal: Vol. XIII (Issue II)**, pp. 188-193.