ORGANIZATIONAL CULTURE AND DEVSECOPS ADOPTION: A THEMATIC ANALYSIS

by

JULIE PREVETTE

B.S., Wesleyan College, 2002

M.B.A., Georgia College & State University, 2006

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment for the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA

2025

Organizational culture and DevSecOps adoption: A thematic analysis

Julie Prevette, *Middle Georgia State University, julie.prevette@mga.edu*

Abstract

Successfully adopting DevSecOps extends beyond mere technical integration; it profoundly impacts and is in turn impacted by organizational culture. This analysis explores key themes in the literature about implementing DevSecOps and the role organizational culture plays in its adoption. The review highlights the benefits of DevSecOps, such as better security integration, increased automation, and enhanced collaboration. It also identified challenges, including resistance to change, skill gaps, and the influence of leadership. This study provides valuable insights for organizations and leaders to understand better and address cultural barriers, ultimately strengthening their security and software development practices.

Keywords: DevSecOps, organizational culture, change management

Introduction

Security threats are increasing in number and impact, and recognizing the methods to combat them through security requirements and code quality puts development teams in a position where security must be considered from the beginning of a project (Lombardi & Fanton, 2023). This effort to shift security to the left in a DevOps environment is called DevSecOps (Zhou et al., 2023). It has become a way to ensure that security is brought into the planning process and continues throughout the project (Jeganathan, 2019). Implementing DevSecOps improves team communication, collaboration, and efficiency (Zhou et al., 2023). Its implementation is not without challenges, however.

While the technical aspects of DevSecOps, including automation, tools, and compliance enforcement, have been widely studied, its successful implementation requires a cultural shift in organizations (Lombardi & Fanton, 2023). DevSecOps promotes cross-functional collaboration, transparency, and shared responsibilities across teams handling development, security, and operations (Crouch, 2018). Studies on the implementation of DevOps revealed that organizations struggled with implementation because of silos, resistance to change, and leadership challenges (Mudadi & Lotriet, 2023).

The existing literature focuses on the technical and procedural elements of DevSecOps, but most of it does not delve deeply into how organizational culture can influence its adoption and success. Recognizing the impact of cultural factors is crucial for successfully adopting DevSecOps within an organization. This study seeks to address that gap by examining how organizational culture influences the adoption of DevSecOps.

Problem Statement

A review of the existing literature reveals the technical aspects of implementing DevSecOps are well documented. However, the effect that organizational culture can have on its successful implementation remains underexplored. Adopting a DevSecOps framework requires a shift in how teams collaborate, integrate security, and respond to continuous change (Leite et al., 2020). While the framework allows integrating security throughout the development process, challenges can hinder its adoption, including cultural resistance, skill gaps, cross-team collaboration, and balancing security with delivery speed (Zhou et al., 2023).

In a 2022 GitLab DevSecOps Survey, 53% of security respondents have difficulty getting development teams to prioritize fixing vulnerabilities, and 52% report that bureaucratic processes slow down

vulnerability remediation efforts (GitLab, 2022). This type of conflict could result in cultural or team dynamic challenges. With these challenges in mind, it is essential to understand the influence of organizational culture on the implementation of DevSecOps so that teams and organizations can anticipate issues and address them proactively.

Understanding the role of organizational culture in DevSecOps implementation is essential for bridging the gap. This research seeks to identify how cultural factors influence success, what barriers exist, and how organizations can foster a security-first mindset without compromising agility or efficiency. Addressing these issues can lead to a more robust and successful adoption of DevSecOps.

Purpose of the Study

This study aims to identify and analyze articles on DevSecOps implementation and examine the influence of organizational culture on its adoption. By analyzing critical themes in the literature, the study seeks to uncover how specific cultural factors enable DevSecOps practices. The findings will provide actionable insights for leaders, helping them develop targeted strategies and training programs to foster a culture of security, collaboration, and continuous improvement. By equipping organizations with a deeper understanding of cultural enablers and barriers, the study aims to support leadership in driving the behavioral changes needed for an effective DevSecOps environment.

Research Question

RQ1: What themes emerge from key articles on DevSecOps implementation and the influence of organizational culture, and how can these insights help organizations anticipate and mitigate cultural barriers to DevSecOps adoption?

Research Objectives

The findings of this study will reveal emerging themes in organizational culture's influence on the adoption of DevSecOps by identifying recurring themes from the literature. These insights will be used to develop strategies for organizations to anticipate and mitigate cultural resistance. Based on the findings, the study will guide organizations in aligning their cultural values with DevSecOps practices for successful adoption.

Review of the Literature

Origins of DevSecOps

DevOps strives to reduce development cycles, increase the frequency of releases, and enable automation throughout the development process, including testing and verification (Jha et al., 2023). DevOps originated in Agile methodology, with the goal of frequent releases with opportunities for stakeholders to review and give feedback on the product, and development teams can give frequent feedback about the process and their teamwork (Liete et al., 2020). The proliferation of cloud computing demands the ability to release frequently and with dependable results, with relative ease, compared to the manual deployments to production required in the past (Liete et al., 2020). Having security as an afterthought increases the potential of introducing flaws and vulnerabilities into production or, at best, delaying the release to production so security staff have the chance to review code quality or check for flaws or vulnerabilities (Jha et al., 2023).

The realization that security requirements should be considered from the beginning of a project caused the integration of security into DevOps, creating DevSecOps, which shifts the considerations for security to the left in the process instead of addressing security only at the end of the development process or just prior to release (Jha et al., 2023). Dealing with security issues at a point where correction is more convenient, quicker, and cost-effective gives organizations an advantage over prior practices (Jha et al., 2023). As a result of seeing the benefits of shifting security left, the market for DevSecOps is growing. Estimates show it may increase by 24.1% annually to $17.24 billion by 2028 (Martin, 2023).

Principles of DevSecOps

The fundamental principles of DevSecOps include those that are also key to DevOps but highlight the integration of security earlier in the development process. Common to both is automation. DevSecOps aims to automate as much of the development process as possible (Jha et al., 2023). By automating, manual tasks that bring in risk for mistakes or omissions are minimized (Crouch, 2018). Along the same lines of automating development and testing, with DevSecOps, automated security testing and observability are essential to the process and can include automatic resolution of flaws or vulnerabilities (Crouch, 2018). Continuous Integration (CI) enables developers to merge their code into a central storage area with others on the team, commonly called pipelines (Donca et al., 2022). Continuous Delivery (CD) allows the compiled code to be built and deployed to an environment where automated testing can be completed (Donca et al., 2022). Tool usage is common in CI/CD, allowing teams to automate tasks and deliver code efficiently (Donca et al., 2022). By automating the pipeline process, organizations are in an excellent position when audited for compliance (Ramaj et al., 2022).

Collaboration is another foundational principle. Cross-functional teams comprising developers, operations, and security professionals work together from planning to execution, fostering shared responsibility for security (Leite et al., 2020). Communication improves since functions are shared more than handed off in past methodologies, breaking down traditional silos in the process (Zhou et al., 2023). The DevSecOps methodology enables collaborative integration between developers, operations, and security to ensure frequent releases can happen (Liete et al., 2020).

Continuous improvement is another common principle of DevSecOps and DevOps. In DevOps, the main point of continuous improvement is to improve the software development process by making it more efficient by evaluating the last cycle's results and adjusting. In DevSecOps, continuous improvement provides the opportunity to continually evaluate the security capabilities of the process by implementing improvements throughout the process (Zhou et al., 2023). Integrating Agile and DevSecOps provides quick cycles for iterative feedback from customers and opportunities to improve the development process (Almeida et al., 2022).

Differences between DevOps and DevSecOps

One of the main differences between DevOps and DevSecOps is the shift left of security into all stages of the software development lifecycle (Zhou et al., 2023). This facilitates the creation of a secure build for each integration into the pipeline (Ramaj et al., 2022). Incorporating security into the development process brings awareness and skill-building for developers and operations personnel, allowing the team to work more efficiently (Zhou et al., 2023). It allows collaboration with other teams, including legal and customer support, to tackle security and compliance issues (Ramaj et al., 2022). Bringing security into the process earlier means that security is every team member's responsibility (Jha et al., 2023).

Benefits and Drivers of DevSecOps Adoption

There are several advantages to adopting DevSecOps in software development. Improved communication and collaboration of teams enhance efficiency and product quality (Zhou et al., 2023). The efficiency gains in cost and time are another advantage since the methodology provides a collection of approaches and tools and security and compliance as code designed to address compliance and security issues (Ramaj et al., 2022). Because the methodology has a customer focus, the team can be sure they are building their products to maximize customer satisfaction (Jha et al., 2023). Continuous observability allows the team to catch flaws and vulnerabilities early to address them quickly (Ramaj et al., 2022). Teams can quickly address these flaws and vulnerabilities because of the shortened development cycles (Jha et al., 2023). DevSecOps fosters a culture of security where security is a shared responsibility rather than confined to a specialized team (Cram et al., 2020; Zhou et al., 2023).

Challenges of Implementing DevSecOps

Despite its benefits, DevSecOps presents adoption challenges. Organizational resistance to change is a common barrier as team structures and workflows shift to accommodate security integration (Zhou et al., 2023). There also may be some skill gaps to address with the team members as, historically, developers may not have the knowledge to address or consider security in their software, and security professionals may not know the intricacies of development (Zhou et al., 2023). The tools involved with CI/CD will require staff to learn new working methods, which will present a learning curve (Zhou et al., 2023). Maintaining the speed and agility of DevOps while ensuring robust security can be difficult but is doable once the team understands the concepts and learns the tools (Zhou et al., 2023).

Automating testing and distributing that testing throughout the process instead of breaking it into its phases, as some organizations may have done, will cause changes in processes and attitudes (Miller et al., 2022). Implementing automation may not work with legacy systems and cultures without substantial investment in time and training (Leite et al., 2020). Teams and organizations will also need to consider what measurements will be used to gauge success, and both the selection of the correct key performance indicators and their use may bring complexities (Lombardi & Fanton, 2023). As with any agile or related culture, teams are encouraged to fail quickly to identify ways of improving and avoiding failure in the future, but adopting that culture is not readily embraced and can be a challenge upon the adoption of agile or DevSecOps (Kendall et al., 2023).

Organizational Culture's Influence on Technology Changes

Organizational culture affects the successful adoption of new technology work processes, such as DevSecOps. Organizational culture is a set of shared fundamental assumptions developed over time as the group addresses the challenges of adapting externally and integrating internally, and, having proven effective, these assumptions are accepted as valid and passed on to new members as the proper way to interpret, think about, and respond to such challenges (Schein, 2010). Any time change is attempted, it can be met with resistance by employees, including disconnection and animosity toward the new way of working (Siddiq et al., 2024). Leadership that provides a model for acceptance and openness to change can positively affect employee confidence about workflow changes, which can benefit organizational culture (Siddiq et al., 2024). The success of digital transformation hinges on leadership's dedication and strategic vision, which affect organizational culture (Mihu & Herciu, 2024). An environment open to learning and adaptation can also lead to successful technology implementation and innovative workflows (Awad & Martín-Rojas, 2024). Learning enhances creativity and enables innovation, which draws on the organization's collective knowledge (Awad & Martín-Rojas, 2024).

The organizational members are the drivers who shape and uphold the organizational culture. They understand the norms and values of the organization and have a unified sense of purpose and loyalty (Lissillour & Wang, 2021). With that in mind, the members must have their values aligned with the new processes and technologies being implemented (Lissillour & Wang, 2021). Mihu and Herciu found that engaging employees in digital transformation is crucial for change management and leads to acceptance and engagement in new technologies, as well as prioritizing training to help adopt innovative ways of working, which eases the implementation of changes (2024).

While existing research explores DevSecOps' technical benefits and challenges, it does not comprehensively examine cultural barriers to adoption. Prior studies acknowledge organizational culture's role in digital transformation, but the specificities for implementing DevSecOps need further exploration. Leadership strategies for overcoming resistance and fostering cultural alignment with DevSecOps remain underexplored. This study aims to fill these gaps by identifying cultural factors affecting DevSecOps adoption and offering actionable insights for organizations to effectively anticipate and mitigate cultural barriers.

Research Methodology

This study employed a qualitative thematic literature review on organizational culture's influence on adopting DevSecOps. Research published in English was reviewed to limit the impact of language interpretation, and publication dates were set within the past ten years. Databases such as ProQuest and IEEE Xplore were searched using keywords such as "DevSecOps," "SecDevOps," and "organizational culture" in multiple combinations utilizing Boolean search strategies to retrieve peer-reviewed articles for analysis. Some sources older than ten years were used in portions of this paper for their historical context, foundational theories, or widely accepted models that are relevant to the analysis. These established models and theories are key tools for contextualizing and validating the study's findings.

Table 1: Included Articles

Author	Year	Title	Theme(s) Identified
Anjaria, D. & Kulkarni, M.	2022	Effective DevSecOps Implementation: A systematic literature review.	Collaboration & Communication Skills & Training Security Culture
Ashenden, D. & Ollis, G.	2020	Putting the Sec in DevSecOps: Using social practice theory to improve secure software development.	Collaboration & Communication Benefits of DevSecOps Security Culture
Diaz, J. et al.	2019	Self-service cybersecurity monitoring as enabler for DevSecOps	Collaboration & Communication
Jayakody, J. & Wijayanayake, W.	2023	Critical success factors for DevOps adoption in information systems development	Collaboration & Communication Transparency & Integrity Leadership Benefits of DevSecOps
Kainulainene, S. et al	2024	Requirements risk management for continuous development: Organisational needs	Collaboration & Communication Skills & Training Leadership Benefits of DevSecOps Organizational Barriers
Lacek, J.M.	2019	Changing the DevOps culture one security scan at a time	Security Culture
Nisha, T. & Khandebharad, A.	2021	Migration from DevOps to DevSecOps: A complete migration framework, challenges, and evaluation	Collaboration & Communication Security Culture Benefits of DevSecOps
Prates, L. & Pereira, R.	2025	DevSecOps practices and tools	Collaboration & Communication Security Culture
Rahman & Mehnaz	2022	DevSecOps: Integrating Security into the DevOps pipeline	Collaboration & Communication Security Culture Skills & Training Organizational Barriers Leadership
Rajapakse et al.	2022	Challenges and solutions when adopting DevSecOps: A systematic review	Collaboration & Communication Skills & Training Security Culture
Saeed, H. et al.	2025	Review of techniques for integrating security in software development lifecycle	Security Culture
Ticu-Jianu, R.	2024	Continuous Resilience: DevSecOps Strategies for cloud and quantum platforms	Collaboration & Communication Organizational Barriers Benefits of DevSecOps
Zhao, X. et al.	2024	Identifying the primary dimensions of DevSecOps: A multi-vocal literature review	Collaboration & Communication Skills & Training

Inclusion criteria focused on studies that explicitly discussed DevSecOps and the role that culture has on its adoption. Articles were selected based on their relevance and contribution to the research objectives. Themes were identified through an iterative thematic analysis process, following Braun and Clarke's five-phased approach to qualitative thematic analysis (2006).

To extract themes, after familiarization with the information in the sources, key findings and statements from the literature were categorized into a spreadsheet, summarized, and refined into key phrases through inductive coding. Coding followed Saldaña's first and second cycle coding methods, where initial descriptive codes were generated and then grouped into broader conceptual themes based on frequency, consistency across studies, and relevance to the research objectives (2015). By synthesizing findings from multiple sources and applying a structured validation approach, this study provides a credible narrative on how organizational culture impacts the implementation of DevSecOps.

Results

The data analysis revealed several themes that influence the adoption of DevSecOps implementation. The themes illustrate the interaction between technical, organizational, and cultural factors in integrating security into DevOps practices. The following sections provide an in-depth exploration of the themes, supported by relevant insights from the data.

Collaboration and Communication

Collaborative culture and effective communication emerged as the most prominent themes associated with the success of DevSecOps adoption. Of the sources evaluated, 76% addressed team collaboration and communication issues. Researchers such as Jayakody and Wijayanayake (2023) consistently identified effective collaboration, frequent communication, and shared responsibility as critical enablers of security integration. "Successful adoption of the new, collaborative way of working can be supported by tools and processes but depends on having and fostering a collaborative culture" (Ashendon & Ollis, 2020, p.38).

Prior research revealed conflicts between developers and security professionals can arise when developers perceive security teams as critical and feel that their work is scrutinized by the security team (Rajapakse et al., 2022). The authors point out that this dynamic contributes to mistrust and reluctance to engage in security practices, leading to cultural misalignment and hampering success (Ashendon & Ollis, 2020). Studies also showed when teams worked in isolation or silos, the lack of visibility and cross-functional cooperation slowed development cycles and increased friction (Rajapakse et al., 2022). Some studies indicate that organizations implementing shared responsibility models experience fewer challenges balancing speed and security (Anjaria & Kulkarni, 2022).

Studies showed that consistent communication fostered a shared understanding, clarified roles, and facilitated the early identification of security risks (Ticu-Jianu, 2024). Rajapakse et al. point out that automated communication, spurred by automated monitoring and alerting, is an essential communication trigger, promoting transparency and continuous feedback (2022).

Skills and Training

As organizations integrate security into the development process, studies have revealed that continuous learning and upskilling are essential. Anjaria and Kulkarni mentioned cross-training developers and operations personnel in security practices as vital to successful DevSecOps implementation (2022). Research highlights various training activities that can assist in upskilling, including online courses, boot camps, and internal security workshops (Rajapakse et al., 2022). Knowledge sharing in areas such as security incident handling and response is also noted in the research as a way to involve developers in the security functions so they recognize security threats early and incorporate secure coding practices proactively, as well as improve team collaboration and shared responsibility (Rajapakse et al., 2022). Another training initiative mentioned in prior studies to help ease the cultural shift needed is human resource

management (HRM) programs administered side-by-side with technical training to ease anxieties that come with changes in the workplace related to job security or loss of autonomy (Rajapakse et al., 2022).

Security Culture

The literature highlights integrating security into daily workflows as a common practice in DevSecOps adoption. Organizations report security champions, developers who advocate secure practices and bridge the gap between security and development, promoting a security-first mindset throughout the development lifecycle (Prates & Pereira, 2025). While teams integrate development, security, and operations, separating duties for critical security controls ensures oversight and compliance, balancing autonomy with accountability (Rajapakse et al., 2022). However, studies indicate that security is often deprioritized as it offers little value, but leadership commitment is a factor in addressing that perception (Rajapakse et al., 2022).

Lacek describes continuous feedback loops, including automated security checks and real-time testing, as mechanisms to reinforce security behaviors and contribute to the culture change needed for successful DevSecOps operations (2019). Studies identify these feedback mechanisms as a factor in software security and fostering a security-conscious mindset within development teams (Ashenden & Ollis, 2020). Blameless security retrospectives are described in the research as emphasizing learning from security incidents rather than assigning fault, with associations to psychological safety and incident response (Rajapakse et al., 2022).

Knowledge and process sharing emerged as a key theme in developing a culture of security. Jayakody and Wijayanayake observed that open communication on security practices, cross-team information sharing, and visibility into logs, metrics, and code traceability help teams proactively address vulnerabilities (2023). According to Anjaria and Kulkarni, transparency should extend across teams and even to customers when appropriate, and feedback, including customer satisfaction data, should be shared with DevSecOps teams to drive continuous improvement (2022). Rajapakse et al. explain that data integrity frameworks monitor access and enforce role-based permissions to manage insider threats and maintain data security and reliability (2022).

Organizational Barriers

Organizational barriers related to change implementation have been identified as factors affecting the adoption of DevSecOps. Ticu-Jianu notes that large organizations navigate complex structures and established procedures, which can affect implementation timelines (2024). In contrast, smaller organizations may face financial constraints that influence investing in tools, training, and personnel (Ticu-Jianu, 2024). Rahman and Mehnaz discuss how an organization's ability to adapt structures, processes, and tools is associated with collaboration, automation, and security integration in DevSecOps adoption (2022). Studies discussed approaches to modifying processes, addressing security resources, and conducting risk management to address barriers to DevSecOps success (Ticu-Jianu, 2024).

Leadership

Leadership emerged as a theme affecting the adoption of DevSecOps. Rahman and Mehnaz describe leadership as influencing organizational culture, collaboration, and security prioritization in development (2022). Also noted in the research is that leadership involvement, including resource allocation, is associated with security integration within organizational culture (Rahman & Mehnaz, 2022). Leaders with change management expertise help guide their teams through resistance and align stakeholders (Jayakody & Wijayanayake, 2023). Kainulainen et al. examine how hierarchical structures may contribute to conflicts between teams and management and influence autonomy in self-management (2024).

Benefits of DevSecOps Adoption

A recurring theme in the literature is the benefits associated with DevSecOps adoption. Studies highlight how integrating security into development workflows influences team performance, software quality, and overall business outcomes (Ticu-Jianu, 2024). Research shows that DevSecOps adoption is associated with changes in team efficiency and fewer late-stage security interventions (Saeed et al., 2025). Saeed et al. describe how cross-functional collaboration, automation, and continuous feedback loops contribute to early security issue detection (2025). Authors discuss how integrating security into the development lifecycle relates to compliance, security incident frequency, and market positioning (Saeed et al., 2025). Studies also explore how DevSecOps implementation supports experimentation, iteration, and deployment while incorporating security considerations (Saeed et al., 2025).

Discussion

The findings confirm that DevSecOps adoption is not just a technical shift but a cultural transformation, highlighting both barriers and advantages. This study identified key themes that illustrate the impact of organizational culture on security integration. By analyzing these findings through the lens of Schein's model, this discussion explores how organizations can anticipate and mitigate cultural barriers while maximizing the benefits of DevSecOps adoption.

A key finding is that open communication and cross-collaboration are essential for DevSecOps' success. This aligns with prior studies, such as that by Zhou et al., which states that the people dimension, including breaking down silos and coordination of functions within teams is essential (2023). Studies suggest that security is often seen as a separate function rather than an integrated responsibility, leading to friction between development, security, and operations teams, making it difficult to fully embed security practices (Rajapakse et al., 2022). To bridge these gaps, organizations must create communication structures encouraging transparency, shared accountability, and knowledge transfer (Jayakody & Wijayanayake, 2023). Fostering an environment where the whole team learns to trust each other is also key to success, and open communication is one element of that process (Ashendon & Ollis, 2020). Another key to creating an environment of trust is ensuring teams have the necessary security expertise, which requires ongoing investment in training and education.

The research highlights the role of continuous learning in fostering a security-first culture. Studies emphasize the importance of structured learning, including cross-training initiatives that expose developers and operations teams to security best practices (Anjaria & Kulkarni, 2022). Training should be comprehensive and role-specific, covering secure coding, threat modeling, incident response, and compliance to ensure the whole team can effectively support security initiatives (Rahman & Mehnaz, 2022). Prior research on security integration in DevSecOps environments supports formal training and knowledge sharing, showing that organizations with implemented security training have teams that share responsibilities and effectively communicate (Zhou et al., 2023). Studies also suggest implementing HRM programs to supplement the implementation of DevSecOps to address concerns like job security, recognition, and loss of control (Rajapakse et al., 2022). A gap remains in how organizations measure training effectiveness, suggesting future research opportunities. Even with proper training, security culture must be reinforced throughout the software development process to ensure it remains a priority. Developing security knowledge is important, but integrating security values into the entire workflow can create the culture change essential for success.

A recurring challenge in DevSecOps adoption is shifting security from an afterthought to an ingrained part of the development lifecycle. The presence of security champions and automated security checks are positive moves, but leadership commitment is an essential factor (Prates & Pereira, 2025). Security policies often clash with deep-seated assumptions prioritizing speed over security, creating a disconnect between stated values and actual practices, leading to tension between development and security team members (Rajapakse et al., 2022). For instance, while organizations claim to prioritize security, teams often feel

pressure to deliver software quickly, leading them to bypass security protocols. The realignment of these stated policies and behaviors must be a priority for teams and leadership to ensure a continued focus on security as a value-added element. A culture of learning from and about security is essential to success, and this can be accomplished not just by security training but also through blameless security retrospectives, team monitoring of their processes, and metrics that reflect secure development (Jayakody & Wijayanayake, 2023; Rajapakse et al., 2022). An essential aspect of DevSecOps is its iterative cycles, driven by continuous feedback, which can help reinforce secure practices throughout the development lifecycle, ensuring security remains a priority and fostering greater awareness (Lacek, 2019). Another key to DevSecOps is automation and tools, making security an automated part of the development lifecycle once fully implemented (Jayakody & Wijayanayake, 2023). Organizations may see the benefit of shifting security left but face organizational barriers impeding implementation.

The study identifies structural and cultural barriers that slow DevSecOps adoption, particularly in large enterprises with entrenched bureaucratic processes (Ticu-Jianu, 2024). Previous studies on agile transformations suggest overcoming resistance to change requires leadership-driven cultural shifts and restructured workflows (Ashendon & Ollis, 2020). Resource constraints in smaller organizations limit investment in security tools and training, highlighting disparities in adoption readiness across organizations of varying sizes (Ticu-Jianu, 2024). The success of implementing DevSecOps depends on organizations' capacity to adapt structures, processes, and tools (Kainulainen et al., 2024). Organizational barriers can be overcome with leadership commitment and action.

Leadership emerged as a crucial enabler of DevSecOps adoption. Leaders who actively advocate for security, allocate resources, and drive cultural change facilitate smoother transitions (Rahman & Mehnaz, 2022). However, implementation may be inconsistent if leadership only superficially supports security without aligning incentives or decision-making structures (Kainulainen et al., 2024). Some findings suggest that leadership commitment varies, with some organizations prioritizing short-term development speed over long-term security integration (Rajapakse et al., 2022). For example, leaders who mandate security metrics as part of performance evaluation reinforce security priorities, whereas those who focus solely on speed inadvertently discourage security integration. This finding aligns with broader discussions on digital transformation where executive buy-in determines the success of large-scale cultural shifts (Kainulainen et al., 2024). While each identified theme highlights critical cultural factors influencing DevSecOps implementation, Schein's model provides a structured way to understand how these elements interact at different levels of an organization.

Applying Schein's Model of Organizational Culture

While each of these themes highlights cultural factors influencing DevSecOps adoption, Schein's model provides a structured way to understand how these elements interact at different levels of an organization at three levels – artifacts, espoused values, and underlying assumptions – and provides a framework understanding cultural dynamics that influence the adoption and success of DevSecOps (2010). By applying Schein's model, these findings highlight the need for deliberate cultural interventions to ensure success, including how collaboration, training, leadership, and security culture can shape implementation and sustainability. Artifacts, such as security champions and training programs, demonstrate visible practices, but they must align with espoused values, such as leadership commitments, to be effective. However, underlying assumptions, such as prioritizing speed over security, often create barriers to adoption. Table 2 categorizes the key themes within Schein's framework.

Table 2: DevSecOps Adoption Themes Categorized Using Schein's Model of Organizational Culture

Schein's Level	Themes	Description
Artifacts (Visible Organizational Practices)	Collaboration & Communication	Observed practices such as cross-functional teamwork, frequent and automated communication, and shared responsibility models.
	Skills & Training	Tangible initiatives like security training, boot camps, HRM programs, and cross-training efforts.
	Security Culture	Observable behaviors include security champions, continuous feedback loops, automated security checks, and blameless security retrospectives.
Espoused Values (Stated Organizational Beliefs and Strategies)	Leadership	Leadership's commitment to security, advocacy for collaboration, resource allocation, and change management strategies.
	Benefits of Adoption	The stated importance of security integration for efficiency, compliance, and market competitiveness.
Underlying Assumptions (Deeply Embedded, Unconscious Beliefs)	Organizational Barriers	Implicit cultural norms include resistance to change, siloed structures, bureaucratic barriers, a focus on speed over security, and concerns about job security due to automation.
	Security Culture	Unspoken attitudes include seeing security as a blocker rather than an enabler, reluctance to integrate security early, and the perception that security adds little business value.

Applying Schein's model to DevSecOps adoption emphasizes aligning culture deeper than the surface level. Organizations must implement security practices and address deeper assumptions that hinder transformation. The gap between stated values and assumptions must be bridged. For example, leaders must ensure that security priorities are articulated and reflected in operational structures, incentives, and workflows (Rahman & Mehnaz, 2022). Cultural change must be reinforced to be sustained (Ashendon & Ollis, 2020). Security champions, cross-team knowledge sharing, and continuous feedback loops help shift cultural norms and reinforce security-conscious behaviors (Lacek, 2019). Resistance to change must be addressed through organizational support. Overcoming deep-seated resistance requires structured change management strategies, including leadership coaching, HRM programs, and transparent communication about integrating security throughout development (Rajapakse et al., 2022). Understanding DevSecOps adoption through Schein's organizational culture model helps organizations identify cultural misalignments, target specific interventions, and create an environment where security is seamlessly integrated into development and operations.

Implications

The findings of this study provide significant implications for research, practice, and policy, emphasizing that DevSecOps adoption is not just a technical challenge but a cultural transformation. From a theoretical perspective, this study reinforces the application of Schein's model in understanding security integration within DevSecOps and the cultural implications of that change in an organization. It highlights the need for future research on the alignment between espoused values and underlying assumptions regarding security, as discrepancies in these areas can hinder effective adoption (Rajapakse et al., 2022). Additionally, the study suggests that future research should explore how different industries experience and address cultural barriers in security adoption, providing a comparative analysis of DevSecOps implementation across sectors and organizations of varying sizes (Ticu-Jianu, 2024).

From a practical perspective, the findings underscore the necessity of viewing DevSecOps adoption as a cultural shift rather than merely a technical upgrade. Organizations must actively transform their culture by ensuring leadership commitment to security initiatives, fostering open team communication, and integrating

a security-first mindset into operational processes (Rahman & Mehnaz, 2022). Leadership must proactively promote security awareness through incentives, training, and clear communication strategies (Rahman & Mehnaz, 2022). Training and collaboration must be prioritized, with continuous education, security champions, and cross-functional teamwork as essential components (Rajapakse et al., 2022). Addressing gaps between espoused values and underlying assumptions is critical as organizations often express commitment to security while prioritizing development speed, creating conflicts that hinder integration (Rajapakse et al., 2022).

By understanding the cultural dimensions of DevSecOps adoption, organizations can proactively address challenges and create an environment where security is seamlessly integrated into development and operations. These findings provide a foundation for further research and offer actionable insights that organizations can use to refine their DevSecOps strategies, fostering a more secure and collaborative software development culture.

Conclusion

The findings of this study reinforce the notion that DevSecOps is more than a change in software development lifecycle strategies but a profound cultural transformation. By examining the role of organizational culture in implementing DevSecOps, the research highlights the significance of collaboration, leadership, training, and structural adaptability in overcoming barriers to DevSecOps implementation. Applying Schein's model of organizational culture provided a structured view through which to analyze the cultural dimensions, revealing how artifacts, espoused values, and underlying assumptions interact to facilitate or hinder implementation (2010).

This study contributes to the growing research on DevSecOps by demonstrating that successful adoption depends on aligning stated security priorities with organizational behaviors and deeply embedded cultural norms. Integrating security into development demands deliberate cultural interventions that address misalignments between leadership commitments, team perceptions, and operational realities (Rajapakse et al., 2022). The findings emphasize that leadership buy-in, continuous security training, and encouraging a culture of shared responsibility are essential to embedding security as a core organizational value (Rahman & Mehnaz, 2022). Beyond its theoretical contributions, this study offers practical implications for organizations striving to implement DevSecOps effectively. By identifying key cultural barriers, such as resistance to change, prioritization of speed over security, and siloed team structures, this research provides actionable insight for organizations to develop strategies that promote security-conscious development behaviors (Rajapakse et al., 2022).

While this study analyzes cultural factors in DevSecOps adoption, there are opportunities for future research. Additional empirical studies, such as case studies of organizations undergoing cultural shifts in security adoption, would offer deeper insights into the effectiveness of different implementation strategies. Additionally, examining industry-specific challenges in healthcare, finance, and government IT could offer valuable insights on how cultural factors influence security integration in different organizational settings.

As cybersecurity threats evolve, organizations cannot rely solely on technical solutions; they must cultivate a security-focused culture to ensure long-term resilience. This study lays the groundwork for future research and offers valuable insights to help organizations embed security into their development processes, creating a more secure and collaborative software development environment.

References

Anjaria, D., & Kulkarni, M. (2022). Effective DevSecOps implementation: a systematic literature review. *Cardiometry*, *24*, 410–417. https://doi.org/10.18137/cardiometry.2022.24.410417

Ashenden, D., & Ollis, G. (2020). Putting the sec in DevSecOps: using social practice theory to improve secure software development. *NSPW '20: Proceedings of the New Security Paradigms Workshop 2020*, 34–44. https://doi.org/10.1145/3442167.3442178

Awad, J. A. R., & Martín-Rojas, R. (2024). Digital transformation influences organisational resilience through organisational learning and innovation. *Journal of Innovation and Entrepreneurship*, *13(1),* 69. https://doi.org/10.1186/s13731-024-00405-4

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2020). Maximizing employee compliance with cybersecurity policies. *MIS Quarterly Executive*, 183–198. https://doi.org/10.17705/2msqe.00032

Crouch, A. (2018). DevSecOps: Incorporate security into DevOps to reduce software risk. *AgileConnection*. Birmingham: Pack Publishing. https://www.agileconnection.com/article/devsecops-incorporate-security-devopsreduce-software-risk

Diaz, J., Perez, J. E., Lopez-Pena, M. A., Mena, G. A., & Yague, A. (2019). Self-service cybersecurity monitoring as an enabler for DevSecOps. *IEEE Access*, *7*, 100283–100295. https://doi.org/10.1109/ACCESS.2019.2930000

Donca, I. C., Stan, O. P., Misaros, M., Gota, D., & Miclea, L. (2022). Method for continuous integration and deployment using a pipeline generator for agile software projects. *Sensors*, *22*(12), 4637. https://doi.org/10.3390/s22124637

GitLab. (2022). The GitLab 2022 global DevSecOps survey. https://learn.gitlab.com/dev-survey-22/2022-devsecops-report

Jayakody, J. A. V. M. K., & Wijayanayake, W. M. J. I. (2023). Critical success factors for DevOps adoption in information systems development. *International Journal of Information Systems and Project Management*, *11(3),* 60–82. https://doi.org/10.12821/ijispm110304

Jeganathan, S. (2019). DevSecOps: A systemic approach for secure software development. *ISSA Journal*, *17(11),* 20–27.

Jha, A. V., Teri, R., Verma, S., Tarafder, S., Bhowmik, W., Kumar Mishra, S., Appasani, B., Srinivasulu, A., & Philibert, N. (2023). From theory to practice: Understanding DevOps culture and mindset. *Cogent Engineering*, *10(1),* 2251758. https://doi.org/10.1080/23311916.2023.2251758

Kainulainen, S., Tuunanen, T., & Vartiainen, T. (2024). Requirements risk management for continuous development: Organisational needs. *Australasian Journal of Information Systems*, *28*. https://doi.org/10.3127/ajis.v28.4441

Lacek, J.-M. (2019). Changing the DevOps culture one security scan at a time. *ISSA Journal*, *17(11),* 32–37.

Leite, L., Rocha, C., Kon, F., Milojicic, D., & Meirelles, P. (2020). A survey of DevOps concepts and challenges. *ACM Computing Surveys*, *52(6),* 1–35. https://doi.org/10.1145/3359981

Lissillour, R., & Wang, J. (2021). Organizational subculture, constructive deviance and technology adoption: Post-implementation of an enterprise information system in China: *Recherches en Sciences de Gestion*, *145(4),* 153–181. https://doi.org/10.3917/resg.145.0153

Lombardi, F., & Fanton, A. (2023). From DevOps to DevSecOps is not enough. CyberDevOps: An extreme shifting-left architecture to bring cybersecurity within the software security lifecycle pipeline. *Software Quality Journal*, *31(2),* 619–654. https://doi.org/10.1007/s11219-023-09619-3

Martin, L. (2023). Growth is good. *ISSA Journal*, *21(4),* 8.

Mihu, C., & Herciu, M. (2024). Digital transformation: A quantitative analysis of Romanian SMEs. *Studies in Business and Economics*, *19(1),* 137–166. https://doi.org/10.2478/sbe-2024-0008

Miller, A., Giachetti, R., & Van Bossuyt, D. (2022). Challenges of adopting DevOps for combat systems development environment. *Defense Acquisition Research Journal*, *29(99),* 22–48. https://doi.org/10.22594/dau.21-870.29.01

Mudadi, A., & Lotriet, H. H. (2023). An analysis of DevOps' impact on information technology organisations: A case study. *South African Journal of Industrial Engineering*, *34(1).* https://doi.org/10.7166/34-1-2759

Nisha T. N., & Khandebharad, A. (2021). Migration from DevOps to DevSecOps: A complete migration framework, challenges, and evaluation. *International Journal of Cloud Applications and Computing*, *12(1),* 1–15. https://doi.org/10.4018/IJCAC.2022010102

Prates, L., & Pereira, R. (2025). DevSecOps practices and tools. *International Journal of Information Security*, *24(1),* 11. https://doi.org/10.1007/s10207-024-00914-z

Rahman, P., & Mehnaz, S. (2022). DevSecOps: Integrating security into the DevOps pipeline. *SSRN Electronic Journal*, *4(1),* 1–21. https://doi.org/10.2139/ssrn.5054029

Rajapakse, R. N., Zahedi, M., Babar, M. A., & Shen, H. (2022). Challenges and solutions when adopting DevSecOps: A systematic review. *Information and Software Technology*, *141*, 106700. https://doi.org/10.1016/j.infsof.2021.106700

Ramaj, X., Sánchez-Gordón, M., Gkioulos, V., Chockalingam, S., & Colomo-Palacios, R. (2022). Holding on to compliance while adopting DevSecOps: An SLR. *Electronics*, *11(22),* 3707. https://doi.org/10.3390/electronics11223707

Saeed, H., Shafi, I., Ahmad, J., Khan, A. A., Khurshaid, T., & Ashraf, I. (2025). Review of techniques for integrating security in software development lifecycle. *Computers, Materials & Continua*, *82(1),* 139–172. https://doi.org/10.32604/cmc.2024.057587

Saldaña, J. (2015). *The Coding Manual for Qualitative Researchers* (2nd ed.). SAGE Publications.

Schein, E. H. (2010). *Organizational Culture and Leadership* (4th ed.). Jossey-Bass.

Siddiq, S., Manzoor, K., & Rasheed, S. (2024). Transformational leadership with relation to change management: An underlying mechanism. *Abasyn University Journal of Social Sciences*, *17(1),* 49–58. https://doi.org/10.34091/AJSS.17.1.04

Ticu-Jianu, R. (2024). Continuous resilience: DevSecOps strategies for cloud and quantum platforms. *Informatica Economică*, *28(4),* 63–73. https://doi.org/10.24818/issn14531305/28.4.2024.05

Zhao, X., Clear, T., & Lal, R. (2024). Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *Journal of Systems and Software*, *214*, 112063. https://doi.org/10.1016/j.jss.2024.112063

Zhou, X., Mao, R., Zhang, H., Dai, Q., Huang H., Shen, H., Li, J., & Rong, G. (2023). Revisit security in the era of DevOps: An evidence-based inquiry into DevSecOps industry. *IET Software*, *17(4),* 435–454. https://doi.org/10.1049/sfw2.12132