The OSCAR PUBLISHING Services
American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 10 2025
PAGE NO. 362-367

Architecting Secure DevSecOps Pipelines for Cloud-Native Retail Platforms: A Compliance-Driven and Resilience-Oriented Research Framework

Liam Hawthorne

University of Melbourne, Australia

Received: 01 October 2026; **Accepted:** 16 October 2026; **Published:** 31 October 2025

Abstract: The rapid migration of retail enterprises toward cloud-native architectures has transformed how software is built, deployed, and governed, but it has also intensified exposure to security, compliance, and operational resilience risks. DevSecOps has emerged as a dominant paradigm intended to embed security across the entire software delivery lifecycle while preserving the speed and agility promised by DevOps. Yet, in highly regulated and data-intensive retail environments, conventional DevSecOps practices frequently fail to align with sector-specific compliance obligations, multi-cloud operational complexity, and the continuous threat landscape that accompanies customer-facing digital platforms. This study develops an integrated theoretical and methodological framework for secure DevSecOps in cloud-based retail systems by synthesizing contemporary scholarship with compliance-driven operational realities. Drawing extensively on Gangula's analysis of secure DevOps in retail cloud ecosystems, this research situates compliance and resilience not as external constraints but as endogenous design principles that reshape how pipelines, teams, and technologies are organized (Gangula, 2025). The article advances the argument that retail DevSecOps maturity depends less on the mere adoption of automated security tools and more on the institutionalization of governance, risk management, and cross-functional accountability within continuous delivery processes.

Through an interpretive research design grounded in multi-vocal literature analysis, this work examines how security controls, vulnerability management, container hardening, and cloud governance mechanisms co-evolve with organizational learning and innovation cycles. Prior DevSecOps research has largely emphasized technical automation, such as container scanning and pipeline security, but has insufficiently theorized the compliance-centric pressures that define retail, including data protection, financial regulations, and customer trust imperatives. By integrating insights from cloud security frameworks, vulnerability management research, and DevSecOps maturity models, this article constructs a comprehensive conceptual model that explains how compliance and resilience become operationalized through continuous integration and continuous deployment pipelines.

The findings demonstrate that secure DevSecOps in retail is best understood as a socio-technical system in which automation, metrics, and policy are mutually reinforcing. Rather than treating security as a gatekeeping function, advanced retail organizations embed regulatory requirements directly into pipeline logic, making compliance auditable, repeatable, and adaptive. This research further reveals that resilience in cloud-native retail is inseparable from security, as system availability, customer data integrity, and incident response capability are tightly coupled. The study contributes to theory by reframing DevSecOps maturity as a dynamic capability that allows retail firms to continuously reconfigure their security posture in response to shifting threats and regulatory landscapes. Practically, the work offers a roadmap for organizations seeking to move beyond ad hoc security integration toward a strategically governed, metrics-driven DevSecOps ecosystem.

Keywords: DevSecOps, cloud-native retail, compliance engineering, cybersecurity governance, operational resilience, secure software delivery

INTRODUCTION

The digital transformation of the retail sector has been one of the most profound shifts in contemporary enterprise computing, driven by the convergence of cloud platforms, data-driven personalization, and omnichannel customer engagement. Retail organizations increasingly depend on cloud-native architectures to support e-commerce, supply chain coordination, real-time inventory management, and

customer analytics, which together create unprecedented demands for scalability, reliability, and security. At the same time, the highly sensitive nature of retail data, which includes payment information, personal identifiers, and behavioral profiles, subjects these organizations to stringent regulatory and reputational pressures that far exceed those faced by many other industries. Within this context, the adoption of DevOps practices has promised faster time-to-market and continuous innovation, but it has also exposed a critical tension between speed and security that cannot be resolved through traditional, siloed governance models (Kim et al., 2016). The emergence of DevSecOps reflects an attempt to address this tension by integrating security practices directly into the software delivery lifecycle rather than treating them as external checkpoints.

The theoretical foundations of DevSecOps are rooted in the recognition that software development, operations, and security form an interdependent socio-technical system whose performance depends on feedback loops, automation, and shared accountability (Auth et al., 2021). Early DevOps scholarship emphasized the cultural and organizational dimensions of collaboration between developers and operations teams, arguing that continuous delivery requires not only tools but also a reconfiguration of professional identities and workflows (Wiedemann et al., 2019). As security breaches and compliance failures became more visible, scholars and practitioners began to argue that security must be integrated into this collaborative model, leading to the rise of DevSecOps as both a technical and managerial paradigm (Zhao et al., 2024). However, much of the early DevSecOps literature treated security primarily as a set of automated checks, such as vulnerability scans and configuration audits, without fully engaging with the broader governance and regulatory contexts in which enterprises operate.

Retail cloud environments present a particularly challenging setting for DevSecOps because they combine rapid feature deployment with strict compliance regimes and high customer expectations for service availability and data protection. Gangula's detailed examination of secure DevOps in retail cloud ecosystems provides one of the most comprehensive accounts of how these pressures intersect, demonstrating that compliance and resilience are not external constraints but intrinsic drivers of pipeline design and organizational structure (Gangula, 2025). In this view, secure DevSecOps is not merely about preventing breaches but about sustaining trust and operational continuity in an environment where even minor disruptions can have cascading economic and reputational consequences. The retail sector thus offers a critical testbed for evaluating whether DevSecOps can fulfill its promise of reconciling agility with security at scale.

Despite the growing body of work on DevSecOps tools, metrics, and cultural practices, a significant literature gap remains regarding the integration of compliance engineering and resilience management within cloud-native retail pipelines. Cloud security guidance frameworks emphasize shared responsibility and control layering, but they often stop short of explaining how these principles can be operationalized through continuous delivery systems (CSA, 2017). Similarly, research on container security and shift-left vulnerability detection provides valuable insights into technical risk mitigation but does not adequately address how regulatory requirements are translated into automated policy enforcement across heterogeneous cloud platforms (Chintale et al., 2024; Tigera, 2022). This gap is especially problematic for retail organizations, where compliance with data protection laws and payment standards is not optional but foundational to market participation.

The problem statement that motivates this research is therefore twofold. First, there is a lack of a coherent theoretical framework that explains how DevSecOps practices in retail cloud environments can simultaneously achieve high levels of security, compliance, and operational resilience. Second, existing empirical and conceptual studies have not sufficiently connected the micro-level mechanics of pipelines and tools with the macro-level governance structures that shape organizational behavior and risk management (Caniglia et al., 2025). Without such integration, DevSecOps risks devolving into a fragmented collection of technologies rather than a transformative organizational capability.

This article seeks to address these gaps by developing a comprehensive research framework that situates secure DevSecOps within the broader context of retail cloud governance and resilience engineering. Building on Gangula's compliance-centric perspective, the study argues that effective DevSecOps in retail must be designed as a continuous compliance system in which regulatory controls, security policies, and operational metrics are embedded into automated workflows (Gangula, 2025). By synthesizing insights from cloud security guidance, vulnerability management research, and DevSecOps maturity models, this work aims to articulate a nuanced

understanding of how secure software delivery can be achieved without sacrificing innovation velocity.

The contribution of this research is both theoretical and practical. Theoretically, it reframes DevSecOps as a dynamic capability that enables retail organizations to adapt their security and compliance posture in response to evolving threats and regulatory demands, rather than as a static set of best practices. Practically, it provides a roadmap for designing and governing cloud-native pipelines that make compliance and resilience measurable, auditable, and continuously improvable. Through extensive engagement with the literature and a detailed methodological exposition, the study offers a foundation for future empirical research and for the refinement of DevSecOps strategies in highly regulated digital industries (Pakalapati et al., 2023).

Methodology

The methodological orientation of this study is grounded in interpretive and design-oriented research traditions that are well suited to the analysis of complex socio-technical systems such as DevSecOps in cloud-native retail environments. Rather than relying on experimental or survey-based approaches, which often struggle to capture the contextual and institutional dimensions of security and compliance, this research adopts a multi-vocal literature synthesis combined with a conceptual modeling strategy. This approach allows for the integration of academic scholarship, practitioner frameworks, and industry case studies into a coherent analytical narrative that reflects the lived realities of retail DevSecOps implementation (Nikolov and Aleksieva-Petrova, 2023).

The first methodological pillar is a systematic multi-vocal literature review that encompasses peer-reviewed articles, industry white papers, security frameworks, and open-source maturity models. The rationale for this inclusive approach lies in the recognition that DevSecOps is an applied field in which much of the most actionable knowledge is produced outside traditional academic venues (Zhao et al., 2024). By examining sources such as cloud security guidance documents, container security best practice guides, and DevSecOps maturity models, the study captures the practical constraints and design choices that shape real-world pipeline architectures (CSA, 2017; OWASP, 2024). This literature was analyzed thematically, with particular attention to how compliance, vulnerability management, and resilience are conceptualized and operationalized across different contexts.

The second methodological pillar involves the construction of an integrative conceptual framework that maps the relationships between organizational governance, pipeline automation, and security outcomes in retail cloud environments. This framework is informed by Gangula's detailed analysis of secure DevOps strategies in retail, which highlights the centrality of compliance engineering and resilience planning as organizing principles for pipeline design (Gangula, 2025). Rather than treating Gangula's work as a standalone case, the methodology positions it as a theoretical anchor that guides the interpretation of other sources and the synthesis of broader patterns across the literature. This anchoring ensures that the framework remains grounded in the specific challenges and regulatory realities of the retail sector.

The analytic process involved iterative coding and abstraction, in which concepts such as shift-left security, continuous compliance, and vulnerability management were examined across multiple sources to identify convergences and divergences. For example, container security best practices emphasize image scanning and runtime enforcement, while cloud vulnerability management literature focuses on asset discovery and risk prioritization (Scannell, 2024; Tigera, 2022). By situating these technical practices within a governance-oriented framework, the methodology seeks to explain not only what organizations do but why they do it and how these actions contribute to compliance and resilience objectives.

A key limitation of this methodology is that it does not generate new empirical data in the form of interviews, surveys, or direct observations. However, this limitation is mitigated by the depth and breadth of the literature base, which includes detailed case studies and action research that provide rich contextual insights into DevSecOps implementation (Accenture, 2023; Nikolov and Aleksieva-Petrova, 2023). Moreover, the interpretive synthesis allows for the identification of theoretical gaps and practical tensions that may not be visible through quantitative methods alone.

Another methodological consideration is the dynamic nature of cloud technologies and regulatory regimes, which means that any static framework risks becoming outdated. To address this challenge, the conceptual model developed in this study emphasizes adaptability and continuous learning as core

principles, aligning with the DevSecOps ethos of iterative improvement and feedback-driven governance (Kim et al., 2016). By grounding the analysis in widely accepted security and DevSecOps principles, the methodology aims to produce insights that remain relevant even as specific tools and platforms evolve.

Results

The results of this interpretive synthesis reveal a set of interrelated patterns that characterize secure DevSecOps implementation in cloud-native retail environments. Across the literature, there is a consistent recognition that compliance, security, and resilience cannot be treated as discrete objectives but must be integrated into a single, continuously evolving delivery system (Gangula, 2025). This integration is achieved through the embedding of policy and control logic directly into automated pipelines, transforming regulatory requirements from external constraints into executable code that governs how software is built and deployed (CSA, 2017).

One of the most salient findings concerns the central role of vulnerability management as a bridge between technical security and compliance assurance. Cloud vulnerability management frameworks emphasize the need for continuous asset discovery, risk scoring, and remediation tracking across dynamic cloud infrastructures (Scannell, 2024). When these practices are integrated into DevSecOps pipelines, they enable retail organizations to demonstrate compliance with data protection and payment standards through auditable, real-time metrics rather than periodic manual assessments. This aligns with Gangula's observation that compliance in retail cloud environments must be operationalized as a continuous process rather than a point-in-time certification (Gangula, 2025).

Another key result is the importance of container security and shift-left practices in reducing the attack surface of retail applications. The literature on container image scanning and vulnerability detection shows that early identification of insecure dependencies and misconfigurations can significantly reduce the likelihood of production breaches (Chintale et al., 2024; Tigera, 2022). In a retail context, where microservices architectures are often used to support rapid feature deployment, these practices become essential for maintaining both security and system stability. The integration of container security tools into continuous integration workflows exemplifies how technical controls can be aligned with compliance objectives by ensuring that only approved, policy-compliant artifacts are promoted to production.

The synthesis also reveals a strong emphasis on metrics and maturity models as mechanisms for governing DevSecOps performance. Frameworks such as the DevSecOps maturity model and FOBICS metrics provide structured ways to assess how well organizations integrate security into their delivery processes (OWASP, 2024; Caniglia et al., 2025). In retail environments, these metrics are increasingly used to support executive-level oversight and regulatory reporting, linking pipeline performance to broader governance and risk management structures. This supports Gangula's argument that secure DevSecOps in retail requires not only technical excellence but also institutionalized accountability and transparency (Gangula, 2025).

A further result concerns the role of artificial intelligence and machine learning in enhancing DevSecOps capabilities. Emerging research highlights how AI-driven analytics can improve vulnerability prioritization, anomaly detection, and compliance monitoring within complex cloud environments (Fu et al., 2024; Pakalapati et al., 2023). While these technologies are still maturing, they offer significant potential for retail organizations to manage the scale and complexity of their digital operations without sacrificing security or regulatory compliance.

Collectively, these results indicate that secure DevSecOps in retail cloud environments is best understood as a layered system in which automation, governance, and organizational culture are mutually reinforcing. Technical tools provide the means to enforce policy and detect risk, while metrics and frameworks provide the language through which these activities are interpreted and managed at the organizational level. This holistic view aligns closely with Gangula's compliance-driven model of secure retail DevOps, reinforcing its relevance as a foundational perspective for both research and practice (Gangula, 2025).

Discussion

The theoretical and practical implications of these findings extend far beyond the technical details of pipeline configuration, touching on fundamental questions about how organizations govern risk and innovation in digital ecosystems. From a theoretical standpoint, the integration of compliance and resilience into DevSecOps challenges the traditional dichotomy between control and agility that has long

dominated discussions of software governance (Auth et al., 2021). Rather than viewing regulatory requirements as impediments to innovation, the evidence synthesized in this study suggests that, when properly engineered, compliance mechanisms can actually enhance organizational learning and adaptability by providing continuous feedback on system performance and risk exposure (Gangula, 2025).

This reframing has significant implications for how DevSecOps maturity is conceptualized. Existing maturity models often emphasize the progressive adoption of automation and collaboration practices, but they do not always account for the institutional and regulatory dimensions that shape organizational behavior in sectors such as retail (OWASP, 2024). By embedding compliance metrics and policy enforcement into the core of pipeline operations, retail organizations can transform regulatory oversight into a source of strategic insight, enabling them to anticipate and respond to emerging risks more effectively (Caniglia et al., 2025). This aligns with dynamic capability theory, which posits that firms achieve sustained competitive advantage by continuously reconfiguring their resources and routines in response to environmental change (Wiedemann et al., 2019).

At the same time, the discussion must acknowledge the counter-arguments and limitations associated with this integrated approach. Critics of heavy compliance automation argue that it can lead to rigidity and over-reliance on predefined rules, potentially stifling creativity and slowing down development teams (Kim et al., 2016). In fast-moving retail markets, where customer expectations and competitive pressures evolve rapidly, there is a risk that overly prescriptive controls could undermine the very agility that DevSecOps is meant to support. However, the literature reviewed here suggests that this risk can be mitigated through the use of adaptive, metrics-driven governance frameworks that allow policies to be updated and refined in response to real-time data (Scannell, 2024).

Another important debate concerns the role of organizational culture in sustaining secure DevSecOps practices. Technical tools and automated pipelines cannot, by themselves, ensure compliance and resilience if teams do not share a common understanding of security responsibilities and risk tolerance (Accenture, 2023). Gangula's analysis underscores the importance of cross-functional collaboration and leadership commitment in aligning security objectives with business goals in retail cloud environments (Gangula, 2025). This suggests that future research should pay greater attention to the social and institutional dynamics that shape how DevSecOps is enacted in practice, complementing the technical focus of much existing scholarship.

The discussion also highlights the need for further empirical investigation into how AI and advanced analytics can be leveraged to enhance compliance and resilience in DevSecOps pipelines. While the potential benefits of these technologies are widely acknowledged, there is still limited evidence on how they can be integrated into existing governance structures without introducing new forms of opacity and risk (Fu et al., 2024; Pakalapati et al., 2023). For retail organizations, where transparency and auditability are paramount, this represents a critical area for future research and experimentation.

In sum, the findings of this study support a nuanced view of secure DevSecOps as a complex, evolving capability that requires the alignment of technology, governance, and culture. By situating compliance and resilience at the heart of pipeline design, retail organizations can move beyond reactive security measures toward a proactive, learning-oriented approach to digital risk management (Gangula, 2025). This perspective challenges simplistic narratives about speed versus security and offers a more sophisticated understanding of how cloud-native retail systems can be both innovative and trustworthy.

Conclusion

This research has developed a comprehensive framework for understanding and implementing secure DevSecOps in cloud-native retail environments, grounded in a synthesis of contemporary scholarship and anchored in Gangula's compliance-centric analysis of retail cloud security (Gangula, 2025). By integrating insights from cloud security guidance, vulnerability management, container security, and DevSecOps maturity models, the study has shown that compliance and resilience are not peripheral concerns but core design principles that shape how pipelines, teams, and technologies are organized. The central conclusion is that secure DevSecOps in retail is best understood as a dynamic, socio-technical capability that enables organizations to continuously adapt their security and compliance posture in response to evolving threats and regulatory landscapes.

Future research should build on this framework by

conducting empirical studies of retail organizations at different stages of DevSecOps maturity, exploring how compliance engineering and resilience practices influence performance outcomes and organizational learning. As cloud technologies and regulatory regimes continue to evolve, the ability to integrate security into the fabric of continuous delivery will remain a defining challenge for the retail sector and for digital enterprises more broadly.

References

1. Cloud Computing Security Consortium. CSA Cloud Security Guidance Document. 2017. https://clubcloudcomputing.teachable.com/courses/265372/lectures/4121893

2. Fu, M., Pasuksmit, J., and Tantithamthavorn, C. AI for DevSecOps: A Landscape and Future Opportunities. 2024.

3. Gangula, S. Secure DevOps in retail cloud: Strategies for compliance and resilience. The American Journal of Engineering and Technology, 7(05), 109–122. 2025.

4. Auth, G., Alt, R., and Kogler, C. Continuous Innovation with DevOps: IT Management in the Age of Digitalization and Software-defined Business. Springer Cham. 2021.

5. Scannell, E. Cloud vulnerability management: A complete guide. Network Security Journal. 2024.

6. Chintale, P., et al. Shift-Left Security Integration: Automating Vulnerability Detection in Container Images. Journal of Harbin Engineering University. 2024.

7. OWASP Foundation. OWASP DevSecOps Maturity Model. 2024. https://owasp.org/www-project-devsecops-maturity-model/

8. Caniglia, A., et al. FOBICS: Assessing project security level through a metrics framework that evaluates DevSecOps performance. Information and Software Technology. 2025.

9. Kim, G., et al. The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. ACM Digital Library. 2016.

10. Pakalapati, N., Konidena, B. K., and Mohamed, I. A. Unlocking the Power of AI and ML in DevSecOps: Strategies and Best Practices. 2023. https://doi.org/10.60087/jklst.vol2.n2.p188

11. Tigera. Container Security: 7 Key Components and 8 Critical Best Practices. 2022.

12. Accenture. Moving the enterprise to DevSecOps. 2023. https://www.accenture.com/ae-en/casestudies/about/cio-development-security-operations

13. Zhao, X., Clear, T., and Lal, R. Identifying the Primary Dimensions of DevSecOps: A Multi-Vocal Literature Review. Journal of Systems and Software, 214, 112063. 2024.

14. Nikolov, L. A., and Aleksieva-Petrova, A. P. Action Research on the DevSecOps Pipeline. International Scientific Conference on Computer Science. 2023.

15. Wiedemann, A., et al. Implementing the Planning Process within DevOps Teams to Achieve Continuous Innovation. Hawaii International Conference on System Sciences. 2019.

16. Debnath, B., et al. An Analysis of Data Security and Potential Threat from IT Assets for Middle Card Players, Institutions and Individuals. Sustainable Waste Management: Policies and Case Studies. 2019.

17. GitHub. sottlmarek DevSecOps Ultimate DevSecOps Library. https://github.com/sottlmarek/DevSecOps