iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71756

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

A Comparative Study of SSDLC Adoption: Challenges and Best Practices in Small and Medium-Sized Enterprises and Large Organizations

Bisola Kayode
Independent Researcher, UK

Abstract: ***The Secure Software Development Lifecycle (SSDLC) integrates security measures throughout the software development process. Despite its importance in minimizing vulnerabilities, adoption varies significantly across organizations. This paper examines the challenges and best practices associated with SSDLC adoption in Small and Medium-sized Enterprises (SMEs) compared to large organizations. Through a literature review, theoretical analysis, case studies, and comparative evaluation, the research identifies key barriers and proposes actionable strategies for improving secure development practices.***
Keywords: SSDLC, secure software development, DevSecOps, SMEs, enterprise security, software engineering

I. INTRODUCTION

With the rising frequency and sophistication of cyber threats, securing software during development has become a priority. The Secure Software Development Lifecycle (SSDLC) provides a proactive framework to integrate security at each phase of software creation—from requirements gathering to maintenance. However, adoption varies significantly between small and medium-sized enterprises (SMEs) and large organizations due to resource availability, technical capacity, and organizational structure. This paper investigates these differences to provide insights into effective SSDLC adoption strategies tailored to organizational scale.

II. BACKGROUND AND LITERATURE REVIEW

The SSDLC concept evolved in response to persistent security flaws resulting from reactive approaches to software protection. Prominent models such as Microsoft SDL, OWASP CLASP, and NIST SP 800-64 have provided structured guidelines for integrating security controls [1]. According to Singh [2], SMEs often lack the capacity to fully adopt these frameworks, while larger firms face challenges in coordination and tool management. Cheenepalli et al. [3] discuss the role of DevSecOps in streamlining SSDLC implementation, particularly in continuous integration/continuous delivery (CI/CD) environments.

III. THEORETICAL FRAMEWORK

Two principal frameworks underpin SSDLC integration: the NIST SP 800-64 Rev.2 and Microsoft SDL. These define best practices for incorporating security into each software development phase. Risk analysis techniques such as STRIDE and DREAD help organizations assess and prioritize vulnerabilities. Maturity models including OWASP SAMM and BSIMM serve as benchmarks for evaluating an organization's software security posture [4].

IV. METHODOLOGY

This study uses a qualitative comparative analysis approach, relying on secondary data from academic databases and industry sources. Materials were gathered from IEEE Xplore, ACM Digital Library, arXiv.org, and whitepapers from Veracode, OWASP, and Sonatype.

Thirty documents were selected using keywords like "SSDLC adoption," "DevSecOps in SMEs," and "software security frameworks." These were thematically coded to extract insights on tools used, training practices, maturity levels, and reported outcomes. Case studies from published and open-access sources were used to illustrate these patterns in real-world settings.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

V. RESULTS AND ANALYSIS

A. *Tool Adoption*

Around 80% of SMEs preferred open-source tools such as OWASP ZAP and SonarQube, citing affordability and ease of integration [2]. Larger firms favored commercial tools like Fortify and Veracode, which offer scalability and advanced analysis features [5].

B. *Training and Awareness*

Training in SMEs was typically informal and sporadic, whereas large firms established recurring training programs and certifications, often embedded within organizational performance metrics [2], [5].

C. *Security Maturity*

Maturity assessments via OWASP SAMM showed that large organizations commonly reached “Managed” or “Optimized” levels, while SMEs remained at “Initial” or “Repeatable” stages due to lack of formal processes [3].

D. *Outcome Metrics*

- TechNova (SME): Reduced post-deployment vulnerabilities by 40% within one year using open-source tools and basic training [2].
- GlobalSoft (Large Enterprise): Achieved a 30% decline in security incidents over 18 months following enterprise-wide DevSecOps integration and developer certification programs [5].

Table I: SSDLC Adoption Comparison

Component	SMEs	Large Organizations
Tools	OWASP ZAP, SonarQube	Fortify, Veracode
Training	Informal, ad hoc	Structured, recurring
Threat Modeling	Seldom used	Standardized and routine
Automation	Partial CI/CD integration	Fully integrated DevSecOps

VI. CASE STUDIES

A. *TechNova Solutions (SME)*

A mid-sized software firm, TechNova adopted SonarQube and ZAP for vulnerability scanning. Security workshops were provided to developers, aligning practices with OWASP guidelines. The company reported a 40% reduction in critical vulnerabilities within 12 months [2].

B. *GlobalSoft Inc. (Large Organization)*

A multinational software provider, GlobalSoft implemented a security champion model, formal training programs, and enterprise tools like Fortify SCA. Over 1,000 developers participated in security training, resulting in a 30% drop in breach incidents [5].

C. *GovIT (Public Sector)*

This mid-sized government IT agency conducted a baseline security maturity assessment using OWASP SAMM. Policy reforms and targeted developer training followed, leading to improved audit outcomes and measurable increases in compliance metrics [4].

VII. DISCUSSION

Findings confirm that organizational size significantly impacts SSDLC implementation. SMEs benefit from agility and simplified hierarchies but face barriers like cost and expertise shortages. Large firms enjoy resource availability but are challenged by organizational inertia and tool complexity.

Tailoring SSDLC adoption strategies—such as open-source toolchains for SMEs and centralized governance for enterprises—can bridge these gaps. Emerging technologies like AI-based code scanning and behavior-based risk analytics present future integration opportunities.

VIII. BEST PRACTICES AND RECOMMENDATIONS

1) For SMEs: Use phased SSDLC adoption, leverage community-supported tools, and offer role-based security training.
2) For Large Organizations: Standardize tooling across departments, embed security in performance reviews, and maintain centralized policy enforcement.
3) Universally: Employ DevSecOps, adopt risk-based testing, and conduct periodic maturity assessments.

IX. LIMITATIONS

This research is limited to secondary data sources and may not represent all global regions or industries. Empirical validation through interviews or field studies would provide stronger evidence.

X. FUTURE WORK

Future research should explore:

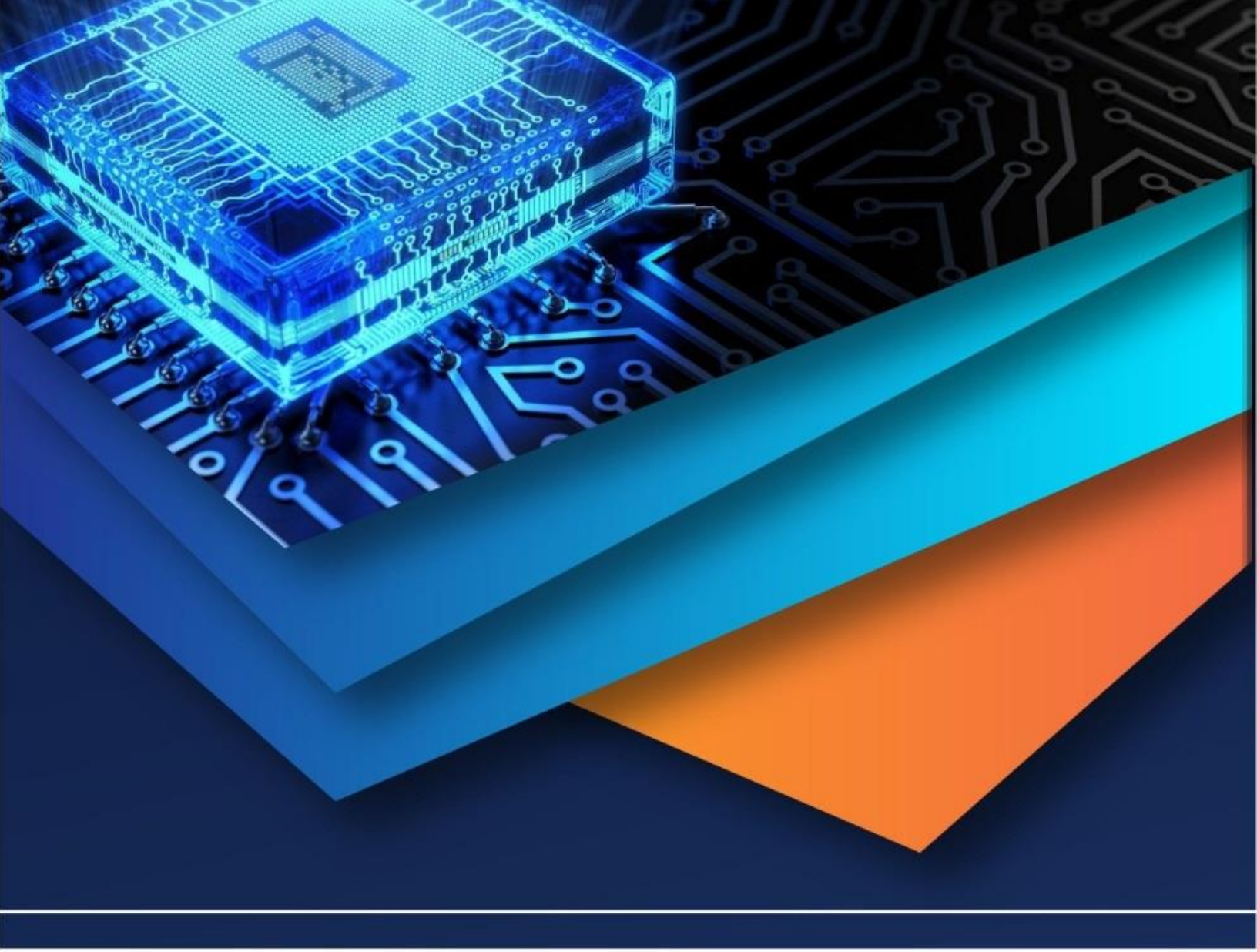
- The role of AI and machine learning in SSDLC.
- Longitudinal studies on SSDLC ROI.
- Cross-sector benchmarks and standardized metrics for SSDLC effectiveness.

XI. CONCLUSION

SSDLC adoption is critical in today's digital landscape. While SMEs and large enterprises face distinct challenges, both can significantly benefit from tailored, proactive security strategies. This paper offers a comparative lens and practical roadmap for integrating SSDLC into diverse organizational contexts.

REFERENCES

[1] OWASP Foundation, “CLASP: Comprehensive, Lightweight Application Security Process.” [Online]. Available: https://owasp.org (accessed: May 28, 2025).
[2] S. Singh, “Secure Software Development Life Cycle: Implementation Challenges in Small and Medium Enterprises (SMEs),” TechRxiv, Apr. 2025. [Online]. Available: https://www.techrxiv.org/doi/full/10.22541/au.174585836.63395541/v1 (accessed: May 28, 2025).
[3] J. Cheenepalli, A. Williams, M. K. Lee, and S. Desai, “Advancing DevSecOps in SMEs: Challenges and Best Practices,” arXiv preprint, arXiv:2503.22612, Mar. 2025. [Online]. Available: https://arxiv.org/abs/2503.22612 (accessed: May 28, 2025).
[4] OpenSSF, “Why are Organizations Struggling to Implement Secure Software Development?” OpenSSF Blog, Jul. 2024. [Online]. Available: https://openssf.org/blog/2024/07/05/why-are-organizations-struggling-to-implement-secure-software-development/ (accessed: May 28, 2025).
[5] Devoteam, “Common challenges when adopting DevSecOps in your organisation,” Devoteam Expert View, 2024. [Online]. Available: https://www.devoteam.com/expert-view/common-challenges-when-adopting-devsecops-in-your-organisation/ (accessed: May 28, 2025).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY