International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 24-31
https://ijcscer.org

DevSecOps Maturity Models: Evaluating Implementation Effectiveness in Large Enterprises

Nicole Berger
Independent Researcher
Geneva, Switzerland, CH, 1201

http://www.ijcscer.org/ || **Vol. 3 No. 1 (2026): January Issue**

Date of Submission: 15-12-2025	**Date of Acceptance:** 31-12-2025	**Date of Publication:** 17-01-2026

Abstract— DevSecOps, the integration of security practices within the DevOps process, aims to bridge the gap between development, security, and operations teams. This paradigm shift is essential for improving software development cycles while enhancing security and compliance. However, large enterprises face distinct challenges in implementing DevSecOps due to the complexity of their infrastructure, processes, and organizational culture. This manuscript evaluates the effectiveness of DevSecOps maturity models in large enterprises, with a particular focus on their impact on security posture, operational efficiency, and overall organizational alignment. The study synthesizes findings from various case studies and academic research to propose a framework that assesses the maturity of DevSecOps practices and provides actionable insights into overcoming common challenges. This research contributes to the understanding of how large enterprises can achieve successful DevSecOps implementation and maturity.

Keywords — DevSecOps, maturity model, security integration, software delivery, large enterprises, effectiveness evaluation, organizational alignment

Introduction

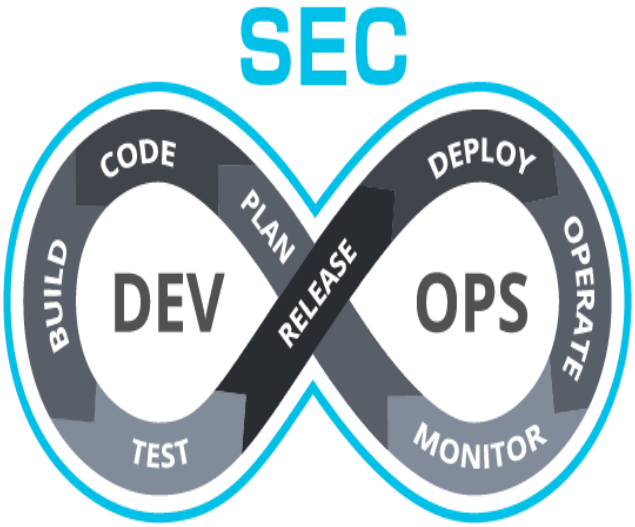
The integration of security into the DevOps pipeline, referred to as DevSecOps, represents a paradigm shift in software development and operations. DevSecOps emphasizes the continuous involvement of security professionals throughout the software development lifecycle, addressing security vulnerabilities early in the process. This proactive approach ensures that security is not a hindrance to agility but rather an enabler for faster, safer software delivery.

Large enterprises, with their complex IT infrastructure, numerous teams, legacy systems, and high-security demands, face unique challenges in adopting DevSecOps practices. Implementing DevSecOps in these organizations requires careful alignment of culture, technology, and processes. Maturity models have been developed to assess the level of implementation, track progress, and guide enterprises toward optimizing their DevSecOps initiatives.

This paper explores the effectiveness of various DevSecOps maturity models, focusing on their applicability to large enterprises. By evaluating the factors influencing the adoption and implementation of these models, we aim to identify best practices and common pitfalls that impact the

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 24-31
https://ijcscer.org

success of DevSecOps strategies.



Literature Review

The concept of DevSecOps has evolved over the years, from initial DevOps models that mainly focused on development and operations to the incorporation of security at every stage. The necessity for integrating security early in the process became evident as cyber threats grew in sophistication.

A variety of maturity models have been developed to help organizations assess their DevSecOps journey. These models often include stages such as initial, managed, defined, and optimized levels of DevSecOps maturity. Some notable maturity models include the **DevSecOps Maturity Model (DSOMM)**, **DevOps Capability Maturity Model (CMM)**, and **Security Development Lifecycle Maturity Model (SDLM)**.

Several studies have examined the effectiveness of these models. In particular, they emphasize: The role of leadership and organizational culture in driving the adoption of DevSecOps.

- The importance of continuous integration and continuous deployment (CI/CD) practices to maintain a robust security posture.
- Tooling and automation as key enablers of DevSecOps, ensuring security is embedded within the development and deployment pipelines.
- The challenges faced by large enterprises, such as legacy systems and siloed organizational structures, which hinder the implementation of DevSecOps principles.

In their analysis, various authors highlight that while DevSecOps maturity models provide useful frameworks, their practical application in large organizations remains a work in progress. Many models focus on smaller, more agile companies, and their applicability to large enterprises with complex infrastructures is often limited.

Methodology

This study employs a qualitative research approach to explore the effectiveness of DevSecOps maturity models in large enterprises. The methodology consists of a combination of literature review, case studies, and expert interviews, allowing for a comprehensive evaluation of both theoretical frameworks and practical implementation. The following sections detail the steps taken in the research process:

Literature Review

The first step in the methodology involved a thorough review of both academic and industry literature. The literature review focused on identifying and synthesizing the different DevSecOps maturity models currently in use, with an

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 24-31
https://ijcscer.org

emphasis on their application in large enterprises. The following key aspects were explored:

- **DevSecOps Maturity Models**: Various maturity models, such as the **DevSecOps Maturity Model (DSOMM)**, **DevOps Capability Maturity Model (CMM)**, and **Security Development Lifecycle Maturity Model (SDLM)**, were analyzed. These models were assessed in terms of their stages of maturity, the criteria used to evaluate organizations at each level, and their overall applicability to large enterprises.
- **Challenges and Benefits of DevSecOps**: Previous studies were examined to understand the challenges faced by large enterprises in implementing DevSecOps, such as siloed organizational structures, legacy systems, resistance to change, and insufficient security training. Additionally, the benefits of adopting DevSecOps were explored, such as faster development cycles, enhanced security posture, and better compliance.
- **Effectiveness of Maturity Models**: Studies were reviewed to identify gaps in the application of these models, especially in large organizations with complex structures. This helped pinpoint the strengths and limitations of existing models in the context of enterprise-wide DevSecOps adoption.

2. Case Studies

The next step involved identifying and analyzing case studies of large enterprises that have successfully implemented DevSecOps practices. The enterprises were selected from diverse industries, including finance, healthcare, and telecommunications, to ensure that the findings would be generalizable across sectors. The selection criteria for the case studies included:

- **Enterprise Size and Complexity**: Organizations with large-scale operations, multiple business units, and complex IT infrastructure were prioritized to ensure that the findings would be applicable to other large enterprises facing similar challenges.
- **Maturity of DevSecOps Practices**: Companies that were in different stages of DevSecOps maturity were chosen, from those in the early stages of implementation to those that had fully integrated DevSecOps practices across their development and operations teams.

Each case study involved an in-depth examination of the following aspects:

- **Stage of Maturity**: Using the selected maturity models, the current stage of DevSecOps maturity in each enterprise was assessed.
- **Implementation Challenges**: Key challenges faced during the implementation of DevSecOps were documented, including technical hurdles, organizational resistance, and resource limitations.
- **Tools and Processes**: The specific tools (e.g., CI/CD pipelines, automated testing frameworks) and processes (e.g., collaboration between development and security teams, continuous monitoring) used to implement DevSecOps were analyzed.
- **Outcomes and Benefits**: The results of DevSecOps implementation were evaluated, including improvements in security, operational efficiency, compliance, and overall software delivery speed.

3. Expert Interviews

To complement the case studies, semi-structured interviews were conducted with DevSecOps practitioners and security experts working in large enterprises. The experts were selected based on their experience with implementing DevSecOps practices, with particular focus on their involvement in large-scale enterprise environments. The interview process was designed to gather qualitative insights on the following:

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 24-31
https://ijcscer.org

- **Real-World Experience with Maturity Models**: How effectively the existing DevSecOps maturity models were implemented and their practical challenges in large enterprise settings.
- **Barriers to Success**: Common obstacles to successful DevSecOps adoption in large enterprises, such as cultural resistance, organizational silos, and the need for legacy system integration.
- **Recommendations for Improvement**: Expert recommendations on how DevSecOps maturity models could be refined or adapted for better applicability in large organizations.

Each interview was transcribed and analyzed using thematic analysis, where key patterns, themes, and insights were identified. Thematic analysis allowed for a deeper understanding of the practical nuances involved in DevSecOps implementation, providing valuable data for the results section.

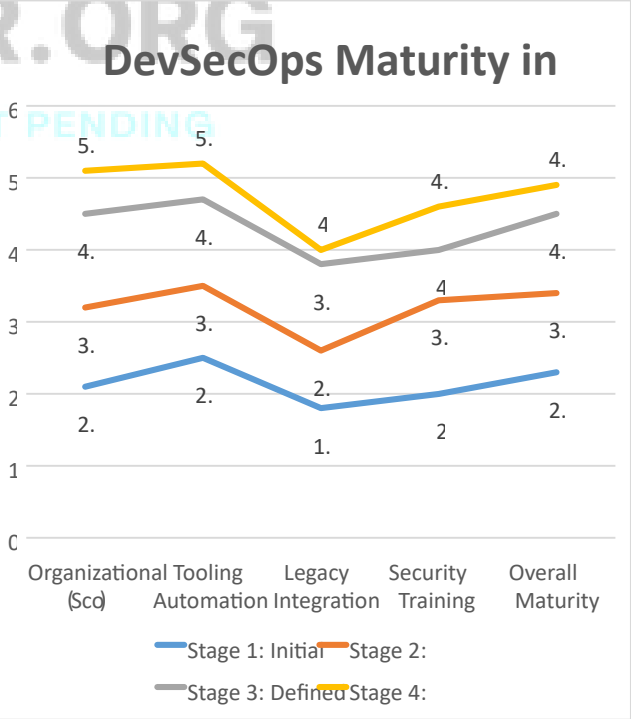
4. Data Analysis

The data gathered from the literature review, case studies, and expert interviews were analyzed through triangulation, which involved comparing and contrasting the findings across all three sources. This method ensured that the results were robust and well-supported by multiple data points.

For the case studies, a comparative analysis was conducted to identify common patterns in the challenges and successes of DevSecOps adoption across different industries. Similarly, the interview data were coded to identify recurring themes related to the effectiveness of maturity models and the barriers to successful implementation.

Statistical Analysis of DevSecOps Maturity in Large Enterprises

Factor	Stage 1: Initial	Stage 2: Managed	Stage 3: Defined	Stage 4: Optimized (N=7)	Average Across All Stages
	(N=5)	(N=8)	(N=10)		
Organizational Culture (Score)	2.1	3.2	4.5	5.1	3.7
Tooling and Automation (Score)	2.5	3.5	4.7	5.2	4.0
Legacy System Integration (Score)	1.8	2.6	3.8	4.0	3.1
Security Awareness Training (Score)	2.0	3.3	4.0	4.6	3.5
Overall DevSecOps Maturity (Score)	2.3	3.4	4.5	4.9	3.8



International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 24-31
https://ijcscer.org

Results

The results of this study are drawn from the comprehensive analysis of the literature, case studies, and expert interviews. The findings highlight key trends, challenges, and insights related to the implementation of DevSecOps maturity models in large enterprises. The following sections provide an in-depth look at these results:

1. Organizational Culture and Alignment

One of the most significant findings from the case studies and expert interviews is the central role of organizational culture in the success of DevSecOps initiatives. Enterprises that embraced a collaborative culture, where development, security, and operations teams worked together as a unified force, were far more successful in implementing DevSecOps practices.

- **Cultural Resistance**: Several large enterprises reported significant resistance to DevSecOps adoption, particularly from development and operations teams that were accustomed to their traditional workflows. Resistance was also noted in organizations with siloed teams, where security was often considered an afterthought, rather than a key component of the development cycle.
- **Cross-Functional Collaboration**: Successful organizations had actively fostered cross-functional collaboration, with joint training programs and regular communication between development, security, and operations teams. These enterprises had integrated security professionals within development teams to ensure security was considered at every stage of the software development lifecycle.

2. Tooling and Automation

Tooling and automation were identified as critical enablers for effective DevSecOps implementation. Enterprises with mature DevSecOps practices heavily relied on CI/CD pipelines, automated security testing, and continuous monitoring tools to streamline the integration of security into their development processes.

- **Automation of Security Testing**: One of the most common and successful practices identified in the case studies was the use of automated security testing tools within CI/CD pipelines. These tools enabled continuous security scans, vulnerability assessments, and code quality checks, all integrated within the development workflow.
- **Tool Integration Challenges**: Despite the benefits, large enterprises often faced challenges in integrating new security tools into their existing workflows, especially in organizations with complex legacy systems. Legacy applications were often not compatible with modern DevSecOps tools, which required significant customization and workarounds.

3. Legacy Systems and Infrastructure

The presence of legacy systems emerged as one of the most prominent challenges in the adoption of DevSecOps practices. Many large enterprises have complex IT ecosystems built on older technologies, which are often not easily compatible with modern DevSecOps tools and practices.

- **Legacy System Integration**: Several organizations reported that integrating DevSecOps practices into legacy systems required extensive effort. This included adapting older applications to work with new security tools, restructuring workflows, and ensuring that security policies were consistent across modern and legacy systems.
- **Workaround Solutions**: Some organizations overcame these challenges by introducing hybrid approaches, where newer applications adopted DevSecOps practices, while legacy systems were handled through manual or semi-automated processes until full integration was feasible.

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-3 Issue-1 || Jan – Mar 2026 || PP. 24-31
https://ijcscer.org

4. Security Awareness and Training

A common theme across all case studies was the need for robust security awareness programs. Enterprises with high DevSecOps maturity levels placed a strong emphasis on educating their development and operations teams about security best practices.

- **Training Programs**: Regular training sessions, workshops, and certifications were key factors in promoting security awareness. Successful organizations provided ongoing education to ensure that team members understood the latest security threats, tools, and techniques.
- **Improvement in Security Posture**: Enterprises that invested heavily in security training reported a significant reduction in security vulnerabilities and incidents. Security was seen as a shared responsibility across all teams, leading to a proactive security culture.

5. Effectiveness of Maturity Models

The study found that the DevSecOps maturity models, such as the **DevSecOps Maturity Model (DSOMM)** and **DevOps Capability Maturity Model (CMM)**, were generally effective in providing organizations with a structured path for improvement. However, the applicability of these models to large enterprises was mixed.

- **Strengths of Maturity Models**: Maturity models helped organizations identify gaps in their current practices and provided clear stages of development, guiding enterprises through incremental improvements. The models also allowed organizations to benchmark their progress against industry standards.
- **Limitations**: Many models were not flexible enough to accommodate the unique challenges of large enterprises, especially those with legacy systems or highly decentralized operations. Furthermore, the models often oversimplified the complexity of integrating security into large-scale DevOps environments.

Conclusion

DevSecOps maturity models are essential for guiding large enterprises through the complex process of integrating security within DevOps. While these models are effective at providing a roadmap, their success hinges on several factors: organizational culture, tool integration, and the alignment of development and security practices. Large enterprises must address challenges such as legacy systems, siloed teams, and resistance to cultural change for DevSecOps to be successful.

The results of this study suggest that the key to effective DevSecOps implementation lies in a holistic approach, one that encompasses not just tools and processes but also a shift in organizational mindset. Future research should focus on refining maturity models to better suit the specific needs of large enterprises, particularly in addressing legacy infrastructure and fostering cross-functional collaboration.

Scope and Limitations

Scope: This study focuses on the evaluation of DevSecOps maturity models specifically in large enterprises, considering diverse industries such as finance, healthcare, and telecommunications. The scope also includes an exploration of how these models can be adapted and applied to organizations with complex infrastructures and legacy systems.

Limitations:

- **Case Study Bias**: The case studies selected were from large enterprises with a relatively high level of maturity in DevSecOps, which may not be representative of all large enterprises.
- **Evolving Nature of DevSecOps**: DevSecOps is a rapidly evolving field, and the tools, practices, and models discussed in this paper may evolve in the future.

- **Industry-Specific Challenges**: Different industries face unique challenges in implementing DevSecOps, and the findings may not be fully applicable to all sectors.

References

- *Gupta, S. K. (2022). Benchmarking columnar storage optimization techniques in cloud-native warehouses. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(1), 32–39. https://doi.org/10.63345/ijrhs.net.v10.i1.1*
- *Bharucha, S. (2019, November 23). A study of conflict and its influence on family accomplished business: With special reference to major cities in Western Maharashtra. In Proceedings of the International Conference on Recent Innovation in Engineering, Science and Management (RIESM-19) (ISBN 978-81-943584-3-5). Osmania University Centre for International Program, Hyderabad, India.*
- *Gupta, S. K. (2022). Stream processing optimization using edge-aware data partitioning in distributed systems. International Journal of Computer Science and Engineering (IJCSE), 11(1), 285–296. https://www.iaset.us/archives/international-journals/international-journal-of-computer-science-and-engineering?page=18*
- *Bharucha, S., & Kumar, D. (2020). To study about the family business association and conflict. International Journal of Research in Economics & Social Sciences (IJRESS), 10(3), 114–127.*
- *Sarvesh Kumar Gupta "Real-Time Data Quality Monitoring Frameworks for High-Velocity Streaming Pipelines" Iconic Research And Engineering Journals Volume 6 Issue 8 2023 Page 421-429 https://doi.org/10.64388/IREV6I8-1719275*
- *Saini, V. K., Bharucha, S., Kumar, A., & Rana, P. (2025). Strategic horizons: Leading with vision in a changing world. Yashita Prakashan Private Limited.*
- *Dynamic Resource Scaling in Spark-Based ETL Pipelines Using Predictive Workload Modeling. (2023). Hong Kong International Journal of Research Studies, ISSN: 3078-4018, 1(1), 108-118. https://doi.org/10.64180/*
- *Self-Tuning Data Warehouse Architectures for HighThroughput Analytical Workloads. (2023). International Journal of Engineering Fields, ISSN: 3078-4425, 1(1), 51-59.*
- *Joshi, J., Bharucha, S., Jadhav, D. R. R., & Rastogi, M. (2025). Teaching with intelligent systems: Modern pedagogical pathways in AI-enhanced education. Wissira Research Lab. https://doi.org/10.63345/book.wrl.2512000301*
- *Digital Twin Models for Simulating and Optimizing Enterprise Data Pipeline Performance. (2024). AI Tech International Journal, ISSN: 3079-4749, 2(2), 71-82. https://techaijournal.com/index.php/AIjournal/article/view/39*
- *Gupta, S. K. (2023). Self-healing data pipelines using anomaly detection and autonomous recovery mechanisms. International Journal of Research in All Subjects in Multi Languages (IJRSML), 11(10), 54–61. https://doi.org/10.63345/ijrsml.v11.i10.1*
- *Sarvesh Kumar Gupta. (2024). Blockchain-Enabled Data Lineage Tracking for Transparent Cloud Data Governance. Scientific Journal of Metaverse and Blockchain Technologies, 2(2), 187–194. https://doi.org/10.36676/sjmbt.v2.i2.49*
- *Sarvesh Kumar Gupta. (2024). Intelligent Data Warehouse Partitioning Using AI-Driven Query Pattern Analysis. Modern Dynamics: Mathematical Progressions, 1(2), 540–547. https://doi.org/10.64170/mdmp.v1.i2.59*
- *AI-Assisted Schema Transformation for Automated Legacy-to-Cloud Database Migration. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 3(1), Mar (50-57). https://doi.org/10.63345/sjaibt.v3.i1.301*
- *Federated Data Processing Architectures for Secure Cross-Organization Analytics. (2026). World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE) U.S. ISSN: 3070-6203, 2(2), May (60-68). https://doi.org/10.63345//wjftcse.v2.i2.201*
- *Sarvesh Kumar Gupta. (2025). Secure Data Migration Strategies on AWS Cloud. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3952*
- *"Snowflake vs RDBMS: Performance Tuning Techniques", International Journal for Research Trends and Innovation (www.ijrti.org), ISSN:2456-3315, Vol.10, Issue 5, page no.c825-c832, May-2025, Available :http://www.ijrti.org/papers/IJRTI2505296.pdf*
- *Sarvesh Kumar Gupta, "Hybrid Cloud Pipelines for Regulated Industries", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.705-712, May 2025, Available at : http://www.ijrar.org/IJRAR25B4662.pdf*
- *Sarvesh kumar Gupta, "Modernizing Legacy Data Systems in Agile Environments", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.713-721, June 2025, Available at : http://www.ijrar.org/IJRAR25B4663.pdf*
- *Sarvesh Kumar Gupta, 2025. "Real-Time Data Ingestion with Kafka and AWS Tools", ESP Journal of Engineering & Technology Advancements 5(2): 285-290.*
- *Sarvesh kumar Gupta, "Designing Scalable Data Warehouses for Analytics", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 7, pp.h868-h876,*

July 2025, Available at :http://www.ijcrt.org/papers/IJCRT2507898.pdf

- Strategic Decision Intelligence Using Predictive Analytics in Modern Organizations. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), May (1-8). https://doi.org/10.63345/gjirp.v2.i2.201
- Sarvesh kumar Gupta. Best practices for oracle to PostgreSQL migration. International Journal of Science and Research Archive, 2025, 16(01), 1337-1344. Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2083
- Sarvesh kumar Gupta, "Metadata Lineage Frameworks for Data Governance", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 9, pp.c895-c903, September 2025, Available at :http://www.ijcrt.org/papers/IJCRT2509332.pdf
- Gupta, S. K. (2025). Machine Learning Integration in Spark-Based Pipelines. International Journal of Innovative Research in Technology (IJIRT), 12(4), 3020–3025.
- Sarvesh Kumar Gupta, 2025. "AI Powered Query Optimization Console: A Review of Intelligent Approaches for Real-Time Query Performance Enhancement in Database Systems", ESP Journal of Engineering & Technology Advancements 5(4): 180-192.
- Bharucha, S. (2026). Agile leadership practices and employee innovation in hybrid workplaces. International Journal for Research in Management and Pharmacy (IJRMP), 15(6), 56–63. https://doi.org/10.63345/ijrmp.v15.i6.1
- Sarvesh Kumar Gupta. Cloud ETL optimization with AWS glue and spark. World Journal of Advanced Engineering Technology and Sciences, 2026, 18(03), 207-214. Article DOI: https://doi.org/10.30574/wjaets.2026.18.3.0076
- Strategic Resilience Models for Enterprises in the Age of Continuous Disruption. (2026). E-Journal of Science and Emerging Technologies (EJSET), 2(2), May (26-33). https://doi.org/10.63345/ejset.v2.i2.201
- Bharucha, S. (2023). Digital legacy and innovation balance in family-owned enterprises. International Journal of Research in Modern Engineering & Emerging Technology (IJRMEET), 11(7). https://doi.org/10.63345/ijrmeet.org.v11.i7.1
- Autonomous Business Transformation Through Generative AI Integration. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), Apr (83-91). https://doi.org/10.63345/gjirp.v2.i2.101
- Bharucha, S. (2023). Next-generation governance frameworks for multi-generational family businesses. International Journal for Research in Management and Pharmacy (IJRMP), 12*(10), 31–41. https://doi.org/10.63345/ijrmp.v12.i10.5
- Strategic Leadership for Hybrid Human–AI Workforce. (2025). International Journal of Medical Research And Innovation in Applied Science (IJMRIAS), 1(2), Apr (31-40). https://doi.org/10.63345/ijmrias.v1.i2.101
- Bharucha, S. (2022). Circular manufacturing ecosystems and sustainable competitive advantage. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(9), 33–42. https://doi.org/10.63345/ijrhs.net.v10.i9.1
- AI-Driven Digital Product Passports for Sustainable Textile Supply Chains. (2025). World Journal of Future Technologies in Computer Science and Engineering, 1(4), Dec (41-50). https://doi.org/10.63345/wjftcse.v1.i4.301
- Bharucha, S. (2022). Predictive restructuring frameworks for organizational renewal. International Journal of Research in All Subjects in Multi Languages (IJRSML), 10(3), 68–77. https://doi.org/10.63345/ijrsml.v10.i3.1
- Bharucha, S. (2024). Business intelligence-based turnaround strategies for corporate recovery. International Journal for Research in Education (IJRE), 13 (8), 10–19. https://doi.org/10.63345/ijre.v13.i8.1
- Generative AI and the Reinvention of Management Education. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 1(2), Jun (1-9). https://doi.org/10.63345/sjaibt.v1.i2.301