Building High-Velocity Teams: The Business ROI of DevSecOps Adoption

Author Name: Arun Kumar Reddy Goli
Affiliation: Independent Researcher
Role: Cloud/DevOps Engineer
Email: goliarunredy6@gmail.com

Abstract- **This study explores the business ROI of DevSecOps integration in building high-velocity teams. DevSecOps increases collaborations, decreases deployment times, and increases the resilience of the system by applying security initially in the lifecycle of software development. Secondary quantitative and qualitative data collection and analysis methods were used in this paper, with case study examples of companies such as Dell, FlexiLoans, and UKHSA. Findings suggest that DevSecOps, with the application of security practices into DevOps, creates a business ROI through higher release speed, decreased threat, and cost-effectiveness, particularly when building high-velocity teams. Lastly, recommendations such as creating a collaborative culture, investing in automation, the proactiveness of leaders towards the application of DevSecOps, and others were included in this paper.**

Index Terms- ROI, Business ROI, DevSecOps, High-Velocity Teams, Pipelines, CI/CD

I. INTRODUCTION

A. Background to the Study

Building high-velocity teams includes developing teams and organisations that can adapt to changing landscapes, innovate, and create value seamlessly. Organisations need to accelerate software delivery while maintaining reliability and security in the fast-moving digital landscape. "Industrial IoT" and emerging technologies create a high-velocity environment that effectively destabilises firms' existing activities and capabilities [1]. Traditional software development processes commonly silo development, operations, and security departments causing vulnerabilities. By combining security and DevOps into DevSecOps, organisations can discover a workable solution. The importance of this study lies in its explanation of how DevSecOps enables teams to release and scale developments seamlessly and safely, which is significant for large enterprises. Identifying its effect on ROI or "return on investment" navigates decision-makers to validate its adaptation insight in strategic business planning.

B. Overview

DevSecOps, as a progression of the "DevOps methodology," applies security measures effectively around the lifecycle of development. "Transactional records and sensor feeds to social media" and customer interactions need advanced platforms capable of "high-velocity processing" and seamless interoperability [2]. Adopting continuous security through DevSecOps means that there are fewer risks and better compliance, and such teams use automation, CI/CD, and real-time monitoring to ensure software can be delivered in a fast and secure way. The study investigates how DevSecOps enhances a business's technology as well as its performance in the market, resulting in quicker products, less risk of breaches, and smoother day-to-day operations. This paper also examines how the approach cultivates a collaborative essence, coordinating IT purposes along with larger business objectives to create competitive advantages.

Doi:10.48047/ijiee.2023.13.3.2

C. Problem Statement

Apart from increasing awareness, most organisations face problems in quantifying the tangible business insights related to DevSecOps integration, leading to fragmented and hesitation in implementation. This paper refers to this specific issue of the poor coordination between business ROI and DevSecOps initiatives. The paradigm of DevSecOps refers to the application of security principles and practices in DevOps through rapid communication [3]. Standard measurements do not fully reflect how high-speed and secure software can benefit the business. Case studies and statistical data from the paper explain how DevSecOps improves a business's finances and operations. Further, this paper aims to decrease the gap between "executive buy-in" and "technological integration," creating evidence-oriented insights for companies approaching transformation through DevSecOps.

D. Objectives

The primary goals of this study are: 1. To identify practices and principles of DevSecOps and their contribution towards high-velocity team performance. 2. To highlight time-to-market, ROI, and incident reduction as measurable business outcomes correlated with the adoption of DevSecOps. 3. To highlight major challenges companies, face while applying DevSecOps. 4. To recommend corrective measures for organisations aiming to integrate DevSecOps to increase ROI and performance. These objectives, or RO, aim to evaluate how the integration of DevSecOps practices contributes to creating high-velocity teams and leads to measurable business ROI.

E. Scope and Significance

This study investigates the strategic incorporation of DevSecOps within organisations or businesses to create high-velocity teams and increase business ROI. This prioritises assessing both economic and technological effects, such as decreased security threats, speed of deployment, and operational credibility. DevOps movement, which merges “software development (Dev) and IT operations (Ops)” into a cohesive context [4]. This study discusses several case study insights, metrics analysis, and cultural transformations linked with the integration of DevSecOps. Additionally, the significance of this paper lies in limiting the gap in the knowledge between executive decision-making and technological integration, creating major insights for CIOs, stakeholders as well and IT leaders aiming to initiate secure digitalisation and competitive advantages.

II. LITERATURE REVIEW

A. DevSecOps Principles and High-Velocity Team Performance

The incorporation of “development, security, and operations” or DevSecOps has redirected how contemporary organisations create “high-velocity teams”. DevSecOps highlights collaboration, automation, continuous application (CI/CD), and “security as code,” specifying rapid and secure delivery of software. DevOps-based organisations benefit from the “existence of change management” or CM [5]. Automated security testing, shifting security to the early stages of development, and using Infrastructure as Code all help detect problems initially, hence releases can be fast without any issues. Cross-functional teams that move fast benefit from less manual work, improved ways of working, and clearer communication.

For example, Capital One gained many benefits from its digital setup by adopting DevSecOps with the "mission to help customers succeed by bringing ingenuity, simplicity, and humanity" [6]. As the company ensured security from the beginning of each step in development, it

Doi:10.48047/ijiee.2023.13.3.2

experienced more frequent deployments and a drop in incidents. The achievement of the company demonstrates how important DevSecOps is for meeting the challenges of changing markets. This has been emphasising the core principles of DevSecOps to help teams eliminate silos, automate more processes and share responsibility which leads to their ability to act seamlessly and efficiently.

B. Measurable Business Outcomes of DevSecOps Adoption

The integration of DevSecOps has been effectively correlated to increased operational and financial performance within organisations. Organisations that follow DevSecOps report increasing their deployment rate, recovering more quickly from issues, and seeing fewer changes fail. ROI has been incorporated as a primary measure for delineating declining firms [7]. Time-to-market, ROI, and incident reduction indicators help the business achieve real-world results by giving fewer network failures, higher customer satisfaction for customers, and larger profits. DevSecOps is described as integrating security initiatives within companies [8]. Additionally, early integration of security due to DevSecOps makes it less expensive and time-consuming to repair vulnerabilities once the system is deployed. Using automated pipelines, continuous monitoring, and policy-as-code, organisations can both speed up the software release process and keep everything in compliance. Businesses that have security at every part of the DevOps cycle are exposed to fewer security issues. Moreover, these insights show how DevSecOps increases agility in operations while creating tangible financial benefits, making it a strategic focus for companies that value forward-thinking.

C. DevSecOps Implementation Challenges

The application of DevSecOps, apart from its several benefits, has major challenges for companies. ***Cultural resistance*** is identified as one of the most signified challenges, where security, operations, and development teams face problems to incorporate shared thinking and to divide silos. ***Integration of toolchains***, which means that one needs to ensure that CI/CD tools, security scanners, and cloud resources are well-aligned; challenges in that area can lead to issues in how companies operate. Thus, the ***tool selection challenge*** is highly encouraged in the DevSecOps paradigm as its practices heavily rely on tools [8]. Furthermore, ***the skill gap*** has been identified as another issue, specifically with the requirement to upskill developers in the security department. Organisations fail to ***fully identify resilience and agility*** without cross-functional experience. These challenges indicate that DevSecOps requires changes in leadership, financing, and education, going beyond technology.

D. Strategic Measures

Organisations can create "***cross-functional leadership coalitions***," urgency, and authorise teams with the help of "***targeted upskilling***" based on the parameters of "Kotter's Change Management Theory". Additionally, to include DevSecOps in an enterprise strategy, companies can phase in ***tools, change job responsibilities, and encourage secure coding methods*** [10]. Metrics-based evaluations and ***ongoing feedback loops*** can be introduced to monitor ROI, deployment speed, and security enhancements, specifying sustainability and scalability in business.

III. METHODOLOGY

A. Research Design

Research design is identified as a strategy to answer research questions by determining the data collection and analysis process. "***Explanatory research design***" has been

Doi:10.48047/ijiee.2023.13.3.2

selected in this research to evaluate how the integration of DevSecOps practices contributes to creating high-velocity teams.

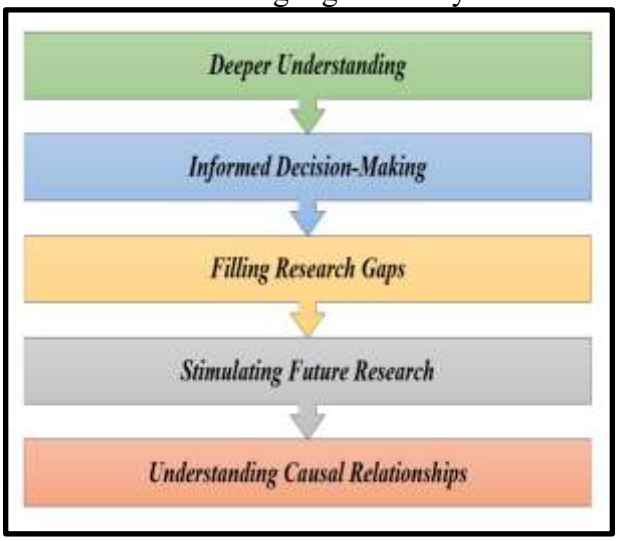

Figure 1: Benefits of Explanatory Research Design

[Source: Self-Created]

The above figure shows the benefits of incorporating an Explanatory research design, such as identifying Causal Relationships, filling the Research Gaps, Informed Decision-Making, and others. "Explanatory research design" helps to fulfil research objectives by highlighting "cause-and-effect relationships" between business outcomes and DevSecOps integration. Explanatory design is used to merge and mix different datasets to be collected and interpreted [11]. This enables in-depth integration of how certain practices encourage security efficiency, team-based performance, and ROI. Additionally, this research design validates the investigation of threats and strategic enablers, creating evidence-based evaluations to refer to the proactive integration of DevSecOps.

B. Data Collection

This study has used a "***multi-research method***" with the selection of both "***secondary quantitative and qualitative data collection and analysis techniques***". Data sources used for the secondary qualitative research are journal articles, case study examples, as well as industry reports. Statistical charts and graphs are collected and further interpreted in a secondary quantitative method. Moreover, the incorporation of multi-methods improves the reliability and validity of this paper by creating diverse observations, cross-verifying the outcomes, and specifying a stabilised, evidence-oriented comprehension of the DevSecOps effect and results.

C. Case Studies/Examples

Case Study 1: Scaling Security Automation

Dell has highlighted how they used DevSecOps at its scale. Through using automation and encouraging teamwork, Dell enhanced their view and status of security. As a result, it became faster to respond to security threats, an improvement in release success rate, and to manage operations in every section of its large infrastructure [12].

Case Study 2: Accelerating Deployment and Reducing Costs

FlexiLoans, a fintech company, struggled to maintain and oversee its platform effectively due to having more than 400 partners and 140 microservices [13]. Through their partnership with DevSecCops.ai, they set up a DevSecOps pipeline that allowed the company to finish faster, with savings once the complete migration was done. Due to automation, the team did not have to grow by hiring many new staff.

Case Study 3: Enhancing Efficiency and Reducing Incidents

UKHSA, in association with Capacitas, introduced improved DevSecOps procedures. Owing to the initiative, the company improved how quickly deliveries were made and reduced the number of production incidents by 89%. Making 'shift left' changes across the company helped save over £1 million, and more than £2 million was saved on cloud services as a result [14].

Doi:10.48047/ijiee.2023.13.3.2

D. Evaluation Metrics

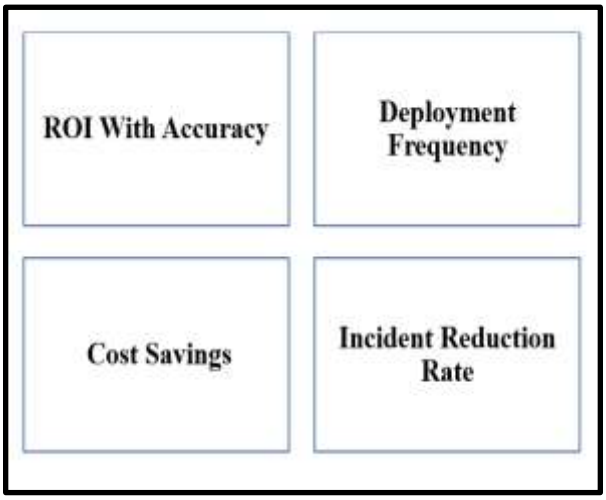

Figure 2: Evaluation Metrics

[Source: Self-Created]

As per the above figure, time-to-market, ROI with accuracy, deployment frequency, cost savings, and incident reduction rate have been identified as evaluation metrics. ROI segmentation highlights that metrics such as accuracy have no value for interpreting certain scenarios [15]. These research-based evaluation metrics create quantifiable validation related to the efficacy of DevSecOps, leading to an objective assessment of business effects. These metrics improve the credibility of research by coordinating performance-based improvements to quantify outcomes around operations, security, and financial areas.

IV. RESULTS

A. Data Presentation

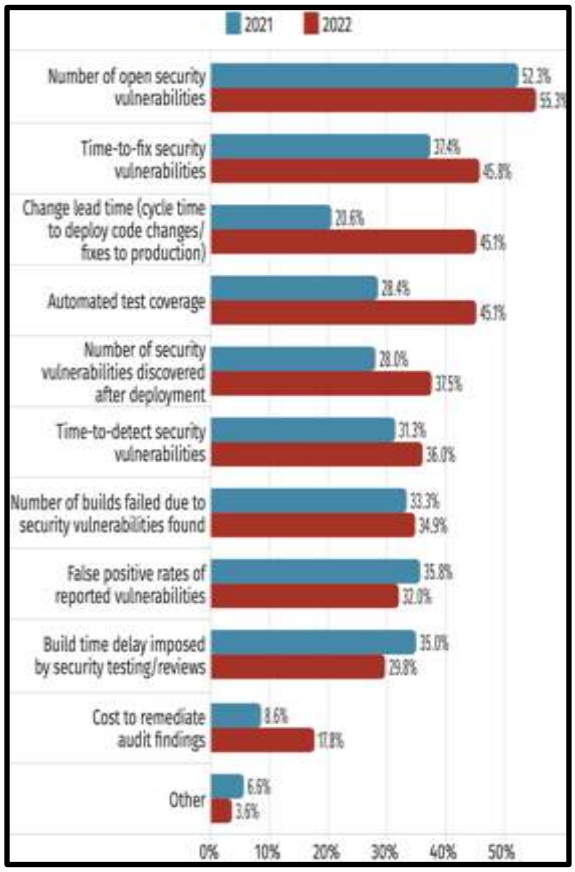

Figure 3: Measure the Success of DevSecOps Activities

[16]

Figure 3 highlights the KPIs that DevSecOps teams use to observe the success of DevSecOps in 2021 and 2022. Most of the analysts follow the trend of open security vulnerabilities the most, with 55.3% in 2022 [16]. Time-to-fix vulnerabilities and the time for delivering changes increased from 37.4% to 45.8% and from 20.6% to 45.1%, suggesting that speed and quick reactions are now given more importance [16]. After the product was deployed, there was an improvement in both automated testing and handling vulnerability issues, which suggested a growing focus on continuous checks for quality and security. This has become difficult to find organisations measuring false positives or cost-related metrics, which implies a preference for running well rather than for earning a profit.

Doi:10.48047/ijiee.2023.13.3.2

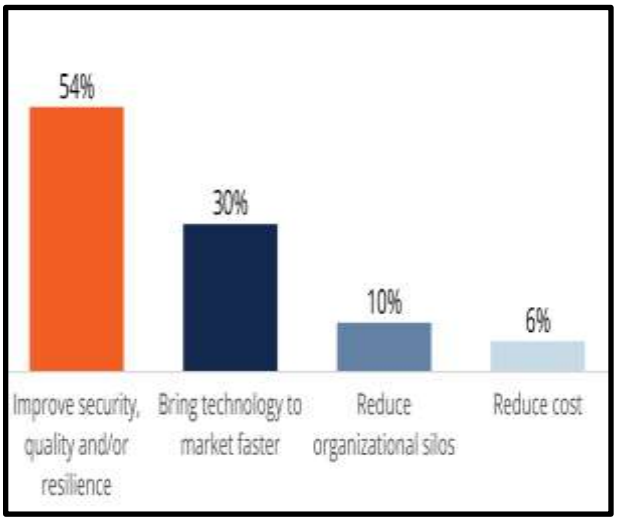

Figure 4: Motivators for DevSecOps Adoption

[17]

The figure reveals which aspects motivate organisations to use DevSecOps, depending on their level of "Security by Design" implementation. The main motivator, at 54%, is ensuring better security, quality, and/or resilience, which points to organisations wanting strong protection and reliable systems [17]. 30% refers to the faster technological aspect [17]. Interestingly, although both are important, only 10% point to combating siloed groups, and the same 6% mention cost savings as their main reason for embarking on the path [17]. This means that although being practical and using resources wisely plays a part, the biggest factor behind using DevSecOps is the desire to make systems secure and products reliable.

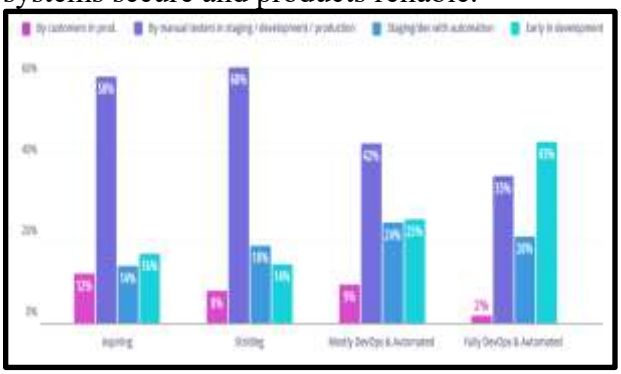

Figure 5: DevOps Maturity Drives Initial Detection - Issue Identification

[18]

Figure 5 highlights software issues that are shown in the four phases of DevOps maturity, such as "Mostly DevOps & Automated, Striding, Fully DevOps & Automated, and Aspiring." When DevOps is developed further, issues are found earlier in the process, using automation and development tools. Fully automated teams spot 43% of the issues early in development, and aspiring teams find only 16% [18]. As a result, DevSecOps and automation are helping to advance the quality of software as well as making feedback come faster and lessening problems later.

B. Findings

Figure 3 shows that implementing DevSecOps involves focusing on resolving vulnerabilities, using automation, and investing time in deployment. During this period of 2021 and 2022, changes in lead time and automated test coverage seemed more important, supporting the move toward fast and secure development [16]. Despite the achievements, only a few teams pay attention to controlling costs and false positives, hence, better ways to track financial results are required to help the organisation achieve its goals. According to Figure 4, increasing quality, resilience, and security are core drivers in the integration of DevSecOps as selected by 54% [17]. The faster technological aspect is secondary, as per the graph. There is a smaller focus on making teams work together and saving money, which implies that security outcomes matter more than any operational or financial benefits in implementing DevSecOps. Lastly, on mature teams, machines can highlight most issues earlier than non-mature teams, which still depend on users or testers to catch most bugs [18]. This shows that being able to test code quickly and automatically boosts the speed and reliability of software development.

Doi:10.48047/ijiee.2023.13.3.2

C. Case Study Outcomes

Case Study Name	Case Study Company	Case Study Outcome	Relevance to Current Research
Scaling Security Automation	Dell Technologies	Scaled security automation, improved collaboration, enhanced visibility, and response [12].	Demonstrates how enterprise-scale DevSecOps boosts security posture and operational agility.
Accelerating Deployment and Reducing Costs	FlexiLoans	Reduction in project time, cost savings, and efficient environment handling [13].	Highlights ROI through time and cost efficiency, key metrics of DevSecOps business value.
Enhancing Efficiency and Reducing Incidents	UK Health Security Agency	Faster delivery, 89% fewer incidents, £ 2 M+ in cost savings through shift-left practices [14].	Validates how DevSecOps enhances performance, security, and cost-effectiveness in public systems.

Table 1: Case Study Outcome
[Source: Self-Created]

Case study examples in Table 1 show how the application of DevSecOps leads to major developments in deploying speed, cost-effectiveness, and overall security assessments.

D. Comparative Analysis

Author	Aim	Findings	Gaps identified
[5]	This article aims to identify the relationship between leadership and DevOps practices.	DevOps is a development methodology aimed at bridging the gap between Development and Operations [5].	Lack of descriptive research
[7]	This article "examines the effects of two specific contextual factors: environmental velocity and decline	There is a relationship between retrenchment speed and turnaround in situations of rapid downfall [7].	Accounting for timing in the turnaround system is a research gap.

Doi:10.48047/ijiee.2023.13.3.2

	speed, and timing of response on a firm's turnaround performance."		
[8]	This article has highlighted DevSecOps Adoption for Cloud Security.	DevSecOps involves developing a "Security as Code" culture with continuous, flexible collaboration between release engineers and security teams [8].	Lack of primary research
[9]	This paper aims to identify DevSecOps integration threats and their interventions.	The tool-oriented nature of DevSecOps and the availability of a substantial number of tools exacerbate the threats [9].	Lack of primary research

Table 2: Comparative Analysis of Literature Review Sources

[Source: Self-Created]

Moreover, these comparative interpretations help to fulfil research aims and objectives by identifying aims, findings, and gaps, specifying refined knowledge of the future business ROI of DevSecOps in creating high-velocity teams.

V. DISCUSSION

A. Interpretation of Results

Both secondary quantitative and qualitative outcomes have a direct correlation with the study objectives. Mature DevSecOps teams use automation and test early, demonstrating the contribution in supporting the speed of high-velocity teams, fulfilling objective 1. Additionally, faster identification of issues, less need for manual testing, and fewer bugs seen by customers show increases in released products, fewer incidents, and a great return on investment, referring to objective 2. The majority of bugs from newer groups are found towards the end of the development process, proving that less-established DevSecOps faces challenges (objective 3). Following this, strategies such as targeted upskilling, cross-functional leadership, incorporation of the ongoing feedback loops, and others were identified in this paper to fulfil the parameters of the 4th objective.

B. Practical Implications

This study creates actionable perceptions for companies wanting to scale and integrate DevSecOps for high-velocity team development. The development and integration of DevSecOps systems is currently a feasible organisational outline

Doi:10.48047/ijiee.2023.13.3.2

[19]. Studying case studies as well as measurable results helps leaders select policies to increase their ROI, speed up the setup process, and increase security. Additionally, the approach draws attention to correlating culture, automated builds, and regular integration as important practices. The learning from the study offers direction to IT leaders, developers, and security specialists for setting up fast, safe, and adaptable development environments.

C. Challenges and Limitations

The outcome of this paper effectively depends on secondary data, which decreases the reliability of outcomes in real-time or modifies them depending on current deployments. The incorporation of a few case study examples makes the study outcome difficult to generalise and the research area. Furthermore, because DevSecOps tools and methods are changing fast, the findings can get outdated quickly. The paper does not pay attention to organisations operating in less experienced markets or with fewer resources, which may restrain the findings. Thus, these elements need to be approached in further research.

D. Recommendations

Organisations that want to integrate DevSecOps need to start by creating a collaborative culture among "development, security, and operations departments." Organisations can invest in automation for ongoing testing, application, and development that accelerates the delivery with high security. Offering regular training and workshops is necessary to allow teams to face new changes in information security. This is also recommended to run some DevSecOps tests on pilot projects first and then roll them out throughout the company [20]. Set specific metrics such as return on investment, how often the system is deployed, and the number of incidents, to highlight if things are improving. Lastly, leaders can show proactive support towards the application of DevSecOps by correlating their business objectives and resource allocation for sustainability and accountability.

VI. CONCLUSION AND FUTURE WORK

DevSecOps, the application of security practices insight into the DevOps workflow, effectively leads to the creation of high-velocity teams by automating security tasks, enabling faster delivery, and fostering collaboration in software. Future efforts need to prioritise primary data gathering with surveys and interviews to collect accurate knowledge about DevSecOps adoption in various fields. Conducting a longitudinal approach allows companies to follow changes in practices, tools, and their return on investment. Furthermore, examining automation with AI and integrating it into DevSecOps processes could also boost future actions, making them more advanced, effective, and foreseeable.

VII. REFERENCE LIST

[1] Ghosh, S., Hughes, M., Hodgkinson, I. and Hughes, P., 2022. Digital transformation of industrial businesses: A dynamic capability approach. *Technovation*, *113*, p.102414.

[2] Olayinka, O.H., 2021. Big data integration and real-time analytics for enhancing operational efficiency and market responsiveness. *Int J Sci Res Arch*, *4*(1), pp.280-96.

[3] Rajapakse, R.N., Zahedi, M., Babar, M.A. and Shen, H., 2022. Challenges and solutions when adopting DevSecOps: A systematic review. Information and software technology, 141, p.106700.

[4] Immaneni, J., 2021. Securing Fintech with DevSecOps: Scaling DevOps with Compliance in Mind. *Journal of Big Data and Smart Systems*, *2*(1).

Doi:10.48047/ijiee.2023.13.3.2

[5] Maroukian, K. and Gulliver, S., 2020. Exploring the link between leadership and Devops practice and principle adoption. *Advanced Computing: An International Journal*, *11*(4).
[6] Capitalone.com, 2022. *Our Company,* Available at: https://www.capitalone.com/about/corporate-information/our-company/
[7] Francis, J.D., Desai, A.B. and Pett, T., 2021. Effects of Rapid Environmental Change and Speed of Decline on Distressed Firms and Turnaround Outcomes. *International Journal of Business & Administrative Studies*, *7*(4).
[8] Allen, A., Puchaty, E. and Zoghi, B., 2021. Challenges Cybersecurity Architects Are Facing In A Cloud Computing Environment. *International Journal of Computer Science and Information Security (IJCSIS)*, *19*(6).
[9] Rajapakse, R.N., Zahedi, M., Babar, M.A. and Shen, H., 2022. Challenges and solutions when adopting DevSecOps: A systematic review. *Information and software technology*, *141*, p.106700.
[10] Sittrop, D. and Crosthwaite, C., 2021. Minimising risk—the application of Kotter's change management model on customer relationship management systems: A case study. *Journal of Risk and Financial Management*, *14*(10), p.496.
[11] Othman, S., Steen, M. and Fleet, J., 2020. A sequential explanatory mixed methods study design: An example of how to integrate data in a midwifery research project. *Journal of Nursing Education and Practice*, *11*(2), pp.75-89.
[12] Yugandhar, M. B. D. (2022). Fintech Digital Products and Customer Consent-Ontrust solution. International Journal of Information and Electronics Engineering, 12(1), 5-15.
[13] Flexiloans.com, 2023. *Overview of the Company,* Available at: https://flexiloans.com/
[14] Capacitas.co.uk, 2021. *Large-scale transformation with DevSecOps,* Available at: https://www.capacitas.co.uk/ukhsa-case-study
[15] Müller, D., Soto-Rey, I. and Kramer, F., 2022. Towards a guideline for evaluation metrics in medical image segmentation. BMC Research Notes, 15(1), p.210.
[16] Deepfactor.io, 2022. SANS DevSecOps Survey 2022: 5 Key Takeaways, Available at: https://www.deepfactor.io/sans-devsecops-survey-2022-5-key-takeaways/
[17] Securitycompass.com, 2021. Research Report Survey: The 2021 State of DevSecOps, Available at: https://www.securitycompass.com/reports/2021-state-of-devsecops/
[18] Mabl.com, 2021. The State of Testing in DevOps, Available at: https://www.mabl.com/testing-in-devops-report-2021
[19] Kanstantsin, Z., 2022. Secure change management process: on the effectiveness of DevSecOps. Computer Science and Information Technology, 10(4), pp.37-51.
[20] Scanlon, T. and Morales, J., 2022, May. Revelations from an agile and DevSecOps transformation in a large organization: An experiential case study. In Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering (pp. 77-81).
[21] Chintale P: Optimizing data governance and privacy in Fintech: leveraging Microsoft Azure hybrid cloud solutions. Int J Innov Eng Res. 2022, 11:
[22] "The Role of Artificial Intelligence in Enhancing Data Security and Compliance in Cloud-Based Ecommerce Logistics Integration", int. J. Eng. Res. Sci. Tech., vol.

Doi:10.48047/ijiee.2023.13.3.2

18, no. 3, pp. 176–185, Aug. 2022, doi: 10.62643/.
[23] Venna, S. R. (2022). Global Regulatory Intelligence: Leveraging Data for Faster ECTD Approvals. *Available at SSRN 5283298*.

Doi:10.48047/ijiee.2023.13.3.2