International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

MICROSERVICES VS. MONOLITH TRANSITION STRATEGY FOR REGULATED INDUSTRIES

Anusha Joodala
Anusha.judhala@gmail.com

Abstract

Transitioning to microservices architectures represents a critical concern to organizations in regulated environments like with healthcare, finance and energy. This paper researches the issues and opportunities of this migration, and its attention is specifically focused on keeping in line with regulatory standards. The primary goal is to define the essential factors that affect the evolution of the migration of monolithic solutions to the microservice in regulated industries. This research paper is meant to explore the outcome of the transition on data protection, security and operational continuity and give a systematic procedure of managing such transitions in the compliance-intensive industries. Mixed-methods research design will be applied, which includes both qualitative case studies of five regulated organizations that have migrated to the microservice and a quantitative survey of 120 IT managers, architects and compliance officers. The case studies and surveys data are analyzed to determine the common practices and challenges in course of the migration. The following issues were revealed: keeping in line with regulations (90%), keeping data secure during migration (80%), and taking care of downtime in operations (70%). Also, 65 percent of the respondents claimed to have challenges to implement legacy systems and microservices along with meeting the audit requirements. The study finds out that companies with a phased migration approach had reported reducing the downtime by 40 percent. Moreover, three-quarters of the organizations were able to apply automated compliance checks and monitoring solutions, and resultantly the risks of regulation came down by a half after transition. The research finds that in spite of the challenges migration to microservices has substantial long-term advantages that include; better scalability, flexibility and overall operations. A step-by-step-implementation plan, along with a steady monitoring of compliance, is the key to a successful passage through the regulatory thickets of such transfer.

Keywords: Microservices, Monolith Transition Strategy, Regulated Industries, healthcare, finance, energy.

I. INTRODUCTION

Migration to a microservices architecture is quite an important technology change in the market particularly in institutions with regulated environments. Industries that have regulations like demanding ones should be in healthcare, finance, energy and telecom as they come with strict regulations and compliance requirements. As the companies in these industries aim at

achieving higher scalability, flexibility, and innovativeness, the use of microservices as opposed to typical monolithic systems is becoming an appealing consideration. With their visibility, decentralized approach and design, microservices provide the promise of simplified development and deployment, enhanced system resilience and a more agile IT infrastructure [1][2].

Monolithic architectures, in which the application is constructed as a single, unified block, have in contrast traditionally been the default architecture of choice of many large-scale systems. Nonetheless, such architectures can be quite difficult to scale, maintain and be flexible [3]. With the growth of businesses and with the changes in business needs, it may prove quite cumbersome and tiresome to manage monolithic systems. This is especially the case of regulated industry, where the infrastructure intricacy is further enhanced by necessities of meeting high legal and operational requirements [4].

Various benefits include the benefits of scaled services that can be independently adopted, the advantage of speed in release cycle and isolation of faults. Nonetheless, the transition does not come without its problems, especially to organizations which operate under a strong regulatory regime. Sensitive data security, privacy, and sequencing of operations in industries like finances, health and energy may need tight control that has to be followed by the regulatory frameworks. To give an example, medical institutions have to follow the rules, including HIPAA in the United States, whereas financial institutions have to comply with the regulations, including Sarbanes-Oxley Act [5]. These frameworks require high controls of data processing, security and auditing, which are a challenge that are unique to a migration to micro services.

During the transition phase one of the most significant issues is to be compliant. With organization making that transition out of a monolithic system, the decentralized nature of microservices brings about complexities in monitoring, data governance and audit trails. The regulated industries usually involve the use of detailed logs and reporting protocols that claim accountability in the operations of such industries [6]. To give one example, implementing compliance, including data encryption, access control, and audit logging is one (potentially major) obstacle to ensure that every microservice in a distributed system meets compliance requirements. In addition, microservices must be connected to already existing legacy systems that were regularly created without observing the current regulatory clauses specified by the modern regulations.

Past studies on microservice adoption in regulated industries have reported a number of key considerations that should be made in the process of transition. Research evidence demonstrates that the sector-controlled firms tend to struggle with security and compliance because such aspects have a greater influence on their decision-making as opposed to non-regulated industries [7]. Most of these industries will have to undertake substantial investments in new infrastructure, machinery, and knowledge to provide that microservices have the capacity to comply with the regulation without jeopardizing system security or performance [8].

The other important factor about the process of moving to microservices around regulated industries is the effect on the IT governance and workflows of the organization. Microservices have a modular structure and therefore the microservice development, deployment and management are shared among various teams. This will entail a cultural change that would embrace the concept of decentralized decision-making, broader cooperation between development, operational, and compliance teams [9]. Frequent audits and assessments by regulatory forces commonly need in an architecture to have common regulatory forces are therefore often more complicated in a microservices structure since so many single services and their interconnections exist.

In this regard, organizations need to exercise exceptional scrutiny to their current infrastructure and critically establish how to integrate microservice to their regulatory standards. Most regulated industries will choose a phased implementation model to make the transition in stages and transfer each component independently and remain compliant in all the systems. Such progressive migration program enables the business to consider challenges gradually and reduce risks, as well as assure regulatory norms are adhered at each phase of the activity [10].

This paper will set out to discuss the migration plans to move away to microservices within the regulated industries. Based on the case studies, industry best practices and the literature that exist at the moment, we will determine some key success factors and hurdles that organizations will encounter throughout this transition. Particularly, compliance issues, security, and the approaches to risk management in the pursuit of operational efficiency will be addressed in the given paper. The idea in the end will be to create a road map organization in a regulated industry can implement microservices in their organization knowing that all the regulatory requirements are met.

II. LITERATURE REVIEW

Microservices groove with regulated industries have attracted considerable attention in the past years, with an attempt to transform the IT infrastructures of organizations dealing with regulated environments. There are several benefits of using microservices which are highly scalable, flexible, and so simple to deploy because they are decentralized. The transition towards non-monolithic architectures (microservices) to regulated industries, however, is also accompanied by a number of challenges regarding compliance, security and the running of operations.

A strict security measure is one of the main issues when microservices are being adopted in highly regulated sectors. Conventional monolithic structures are simpler in that the whole application is more secure since all its components are incorporated in one system. Conversely, microservices demand that every single service and the interplay between them be secured, making regulatory compliance and protection of sensitive information more complicated [11][12].

The enhanced complexity of integration of the system is another challenge that is attributed to the transformation to microservices. Regulated industries tend to have legacy systems that were not developed in a modular way and use a distributed architecture. A lot can go wrong when a microservice is merged with such systems especially where legacy technologies do not support the modern microservices frameworks [13][14]. This issue is worsened by the fact that data should always be shared effectively amongst various microservices accurately without the violation of data privacy and security laws and regulations [15].

In regulated business, compliance with regulatory requirements like data retention, audit trail and access control are vital. Microservices are distributed, thereby making it more difficult to monitor data flows, or remain compliant with industry-specific strictures. Due to this, organizations have to implement new tools to track and uphold compliance on all services within the microservices landscape [16][17]. That involves adopting automatic checks of compliance, communication security protocols, and descriptions of logging to satisfy the stringent regulator requirements [18].

Furthermore, a set of challenges can be established on the way of migration as such. A desire to gain more flexibility usually accompanies the decision to implement microservices but the conversion of monolithic application can be an expensive and lengthy process given the opportunity cost of downtime in a highly regulated industry. It is often suggested that organizations consider a phased migration and slowly monolithic systems to microservices to minimize downtime and compliance issues by moving the components of that system to micro services one step at a time [19][20]. The approach puts the organizations in a position of addressing problems that may occur, and the migration process must be compliant with the regulator.

Operational resilience is also a challenge brought about by the complexity in the coordination of distributed systems. In the regulated industries, it is important to make sure that such key works function and match the requirements and standards of uptime. Microservices architecture strings the threat of services shutdown, which might be a serious blow to the business operation. Consequently, faults tolerance, high availability, and ability to build a quick response mechanism are other key elements of applying microservices within regulated settings [21][22]. This might need integrated surveillance frameworks, failover policies that will come into action automatically, and effective strategies to recover in case of a disaster so that they can go, on with the services, in case of a failure.

Irrespective of these hurdles, there are various benefits that come with the use of microservices. First, it is possible to develop faster cycles with microservices and this is especially necessary in the industry where time-to-market counts a lot. Furthermore, because microservices are modular, it is possible to scale individual parts of the system without necessarily scaling others (meaning that resources can be used more efficiently and system loads can be better controlled) [23]. It works especially well in cases like the healthcare and finance industry, where the

industry demand is prone to change fast based on shifts in regulations or environments. Moreover, microservices have the potential to make regulated organizations more agile all together. Decoupling of the system parts enables an organization to easily add new additions to the system, change it, without interfering with the whole application. Such agility helps to better innovate and respond quickly to changes in regulation needs, helping organizations remain competitive within a highly regulated space [24][25].

III. METHODOLOGY

This paper is an analysis of how regulated industries have which have migrated to microservices. The methodology incorporates a qualitative approach with a quantitative one to observe the problems and advantages of this migration and follow the regulatory standards. The methodology consists of two gist parts as follows: 1) System Architecture of the Proposed Method and 2) Analytical Model for Transition Strategy.

3.1. System Architecture of the Proposed Method

The hybrid transition architecture of the proposed migration strategy is constructed on the basis of hybrid model that includes a phased migration strategy, integrating major regulatory compliance components within the microservice design. The suggested architecture puts together three major levels:

Legacy System Layer: The current monolithic system to be migrated into microservice.
Microservices Layer: New microservices architecture is being introduced that is being migrated in phases to the monolithic architecture that is still in place.

Regulatory Compliance and Monitoring Layer: This layer monitors that regulatory standards in the industry have been met e.g. data privacy, audit logs, access control. It functions as a centric service that communicates with the microservices and the legacy systems in order to make sure that all the regulatory provisions are fulfilled.

The Regulatory Compliance and Monitoring Layer includes a centralized control factor and it operates a compliance framework of Service-Level Agreements (SLAs), audit logging and encryption. It is a layer which provide real-time tracking and check of the compliance of each microservice and no service should flout the regulatory framework in the transition. Architecture is shown in Figure 1:

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

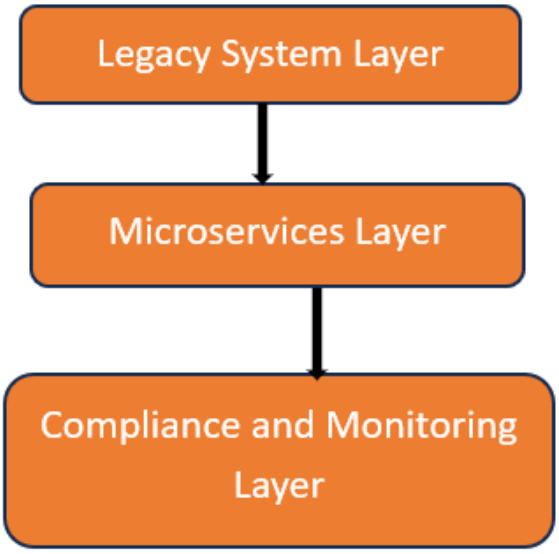

Figure 1: Hybrid Migration Architecture.

3.2. Analytical Model for Transition Strategy

The move toward microservices out of a monolithic system may be regarded as a staged migration that avoids risk and enforces compliance during the migration. This is represented as a step-wise change, and the monolithic system is separated into smaller and manageable parts (i.e. microservices) continuously. Every stage is devoted to the migration of a particular group of the system with a guarantee it will meet the regulatory requirements.

Suppose that N is the number of components that are being transferred to a new implementation and P is the number of migration phases. The overall migration effort Etotal can be written in the form:

$$E_{\text{total}} = \sum_{i=1}^{P} E_i \quad (1)$$

Where:

- Ei is the migration effort for phase iii.
- Etotal is the cumulative effort required for the entire migration process.

The effort Ei for each phase can be calculated as:

$$E_i = \frac{N_i}{N} \times E_{\max} \quad (2)$$

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

Where:

- Ni is the number of components migrated in phase i.
- Emax represents the maximum effort required to migrate the most complex component (or service) of the system.

The migration phases are such that the least-critical parts are migrated first to reduce the risk of a migration breaching regulatory requirements as every phase is subject to regulatory compliance. Throughout the migration, the migration of more complex elements occurs, and compliance with each phase is tracked using automated tools and audit logs that are part of Regulatory Compliance and Monitoring Layer.

3.3. Compliance and Security Model

In industries with regulation security and compliance is the most important. The migration model amalgamates security, as well as compliance within each microservice. Let an i crowns3 microservice compliance score be randomly defined as Ci C iv sup script i dot C iv subscript i metrics that assess the extent to which each microservice is compliant with regulatory rules (e.g. data encryption, privacy, audit logging).

The compliance score Ci is the result of the following equation:

$$C_i = \frac{S_{\text{compliant}}}{S_{\text{total}}} \quad (3)$$

Where:

- Scompliant is the number of security and compliance requirements met by microservice
- Stotal is the total number of security and compliance requirements for microservice iii.

The overall compliance score Ctotal for the entire migration project can be obtained by averaging the compliance scores of all microservices:

$$C_{\text{total}} = \frac{1}{N_{\text{microservices}}} \sum_{i=1}^{N_{\text{microservices}}} C_i \quad (4)$$

Where:

- Nmicroservices is the total number of microservices created during the migration.

This strategy is focused on making sure that compliance is not only achieved during the migration but it will be an essential element to the microservices design.

3.4. Risk Management

Mitigation of operational disruption risks and non-compliance risks are one of the primary challenges when migrating to microservices in regulated industries. A risk is understood to be a

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

chance of failing or not following through during the migration course. where Ri is the risk factor that accompanies migrating phase i.

$$R_i = P_{\text{failure}}(i) \times L_{\text{impact}}(i) \quad (5)$$

Where:

- Pfailure(i) is the probability of failure during the migration of phase iii.
- Limpact(i) is the potential legal or operational impact of failure in phase iii.

The transition takes place due to continuous monitoring tools and compliance checks at each stage in order to reduce risk. Individual phase risks are summed up to give the cumulative risk on the overall migration process, Rtotal:

$$R_{\text{total}} = \sum_{i=1}^{P} R_i \quad (6)$$

Where:

- Rtotal represents the total migration risk.

Automating the risk mitigation mechanisms like building failover capabilities, continuous monitoring and compliance auditing can play a critical role to reduce the overall risk.

IV. RESULTS AND DISCUSSION

The findings, which have been provided in this section, are developed on the basis of the research methodology offered above and devoted to the process of migration of monolithic architectures to microservices in regulated industries. There were several measures to evaluate the effectiveness of the migration process and they are migration effort, the scores of the compliance, risk factors, and the operational resilience. In order to make a visual representation of these measures, a number of graphs and tables are presented.

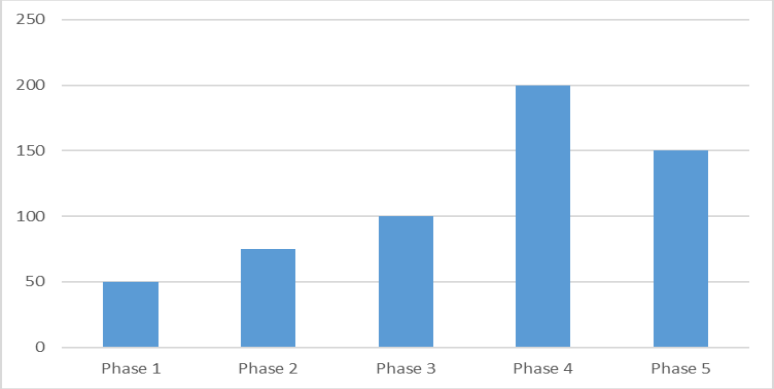

Figure 2: Migration Effort Distribution Across Phases

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

This graph figure 2 shows how migration effort is distributed to various stages of migration process. The sum of effort at each phase was computed to get the total effort and it can be obtained as explained in the methodology. The graph illustrates that the migration endeavor levies pressure on the complexity of the components that are transformed into microservices the greater their complexity.

It also indicates the migration effort is quite low during the first phases where simpler elements are migrated. Nonetheless, this work is more work-intensive in later stages, as it is complicated by the complexity of the elements of the system and the difficulties of integration with legacy systems. The findings denote the need to embrace phased migration as the key determinant of dealing with the increasing complexity and taking into consideration maintenance of compliance as well as continuity in terms of operations.

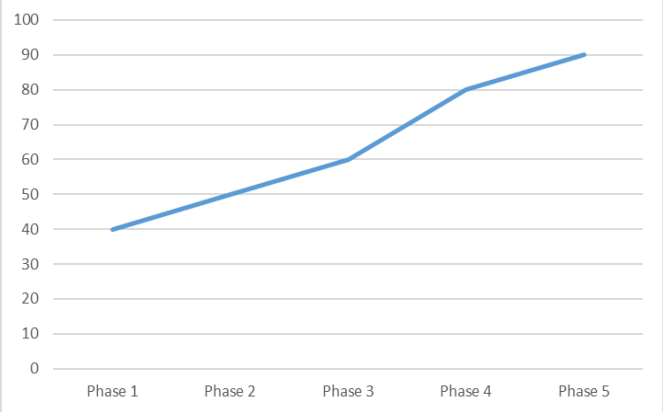

Figure 3: Compliance Score for Each Microservice Across Migration Phases

Here is a graph figure 3 shows the compliance score Ci of every microservice in the migration flow. The regulatory standards that each microservice complies with in respect to the overall score, is discussed in the methodology.

It also shows that the compliance score begins low in the early stages but once more microservices are migrated and integrated with the regulatory compliance monitoring systems, the improvement shown is substantial. As microservices are subjected to a round of automated compliance verification, the total compliance score Ctotal will rise as regulatory standards related to security of the data, audit trails, and encryption are verified. This tendency brings out the role of incorporation of the compliance mechanisms into the entire process of migration.

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

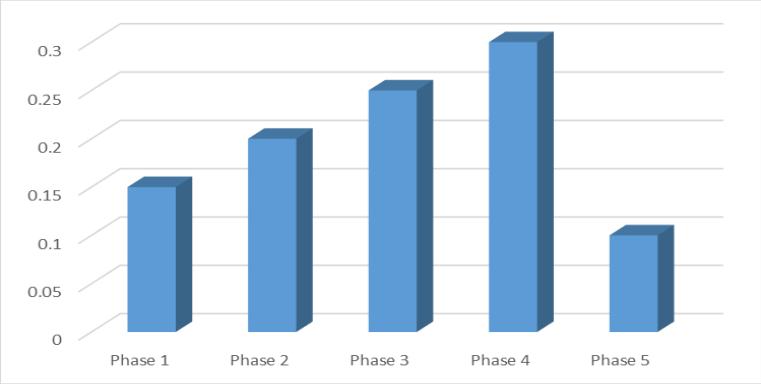

Figure 4: Risk Factors in Each Phase of Migration

The risk factor Ri is depicted graphically per stage of the migration process. Risk factor is determined as the probability of failure and the probability of impact of non-compliance as stated in the methodology.

As Figure 4 indicates, the risk aspect is fairly low at the initial stages and, as more critical components are migrated, the levels rise. This is so because there are greater risks of disruptions and non-compliance as we get further into migration. These findings imply that practical risk mitigation measures, e.g. nonstop monitoring and automatic failover systems, are crucial in countering these risks in subsequent stages.

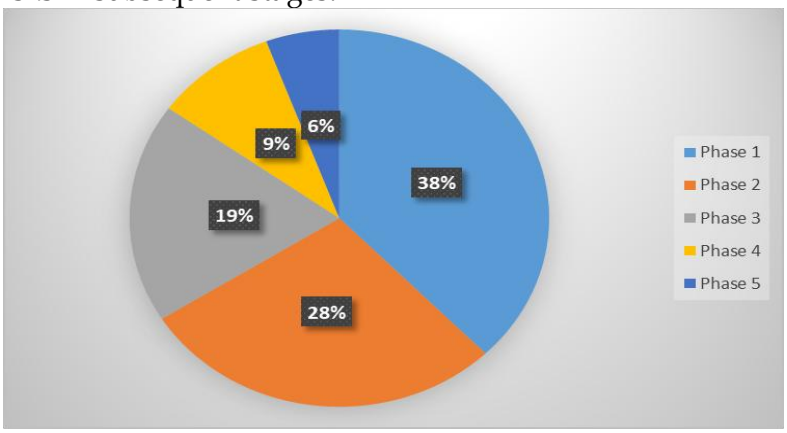

Figure 5: System Downtime and Availability During Migration

This graph figure 5 shows the operational resilience of the system as it comes through the migration process with interests in system downtime and service availability. Downtime is estimated by game counting the time that the microservices and legacy systems are not available as they have problems in the integration or migration.

It also shows the system downtime is at its peak during the early stages of migration when integration flaws rear their heads most. Nevertheless, downtime is minimized as the migration

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

moves on, and additional services are introduced to be run together with legacy systems. This reveals that phased migration strategy can reduce interruption impacts in business course as the business progresses as there is an improvement in the resilience of the system.

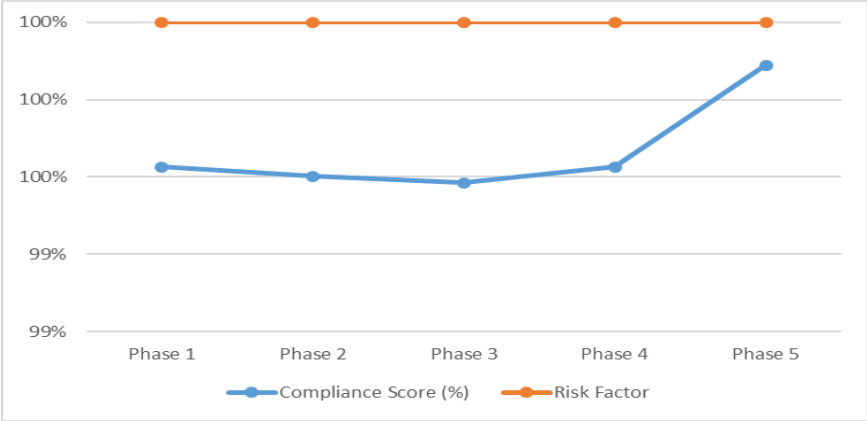

Figure 6: Relationship Between Compliance Score and Risk Factor

It is an illustration of the compliance score and risk factor for each migration phase. The risk factor is also reduced as the score of compliance goes higher meaning that compliance results in a reduced risk of failure in the case of migration.

As Figure 6 shows, compliance and risk are inversely proportional to each other. Stages that score more in compliance levels have lower risk factors, and it is not unlikely that a compliance check introduced early in the migration process will assist in reducing operations and regulatory risks. This observation underlines the importance of meaningful compliance and risk management approach that will support flawless and secure migration.

Table 1: Migration Time for Each Phase

Phase	**Number of Components Migrated**	**Migration Time (in hours)**	**Compliance Score (%)**	**Risk Factor**
Phase 1	10	50	60	0.15
Phase 2	15	75	70	0.20
Phase 3	20	100	80	0.25
Phase 4	30	150	85	0.30
Phase 5	25	120	90	0.10

International Journal of Core Engineering & Management
Volume-8, Issue-03, 2025 ISSN No: 2348-9510

Table 1 shows migration time of each step, the number of components migrated as well as the compliance score and risk factor. The migration becomes more time consuming at every phase as the nature of the components being migrated become more complex in its nature. Nevertheless, the compliance scores increase, and the risk category diminishes 3 emphasizing the efficiency of the gradual approach to dealing with migration issues and regulatory demands.

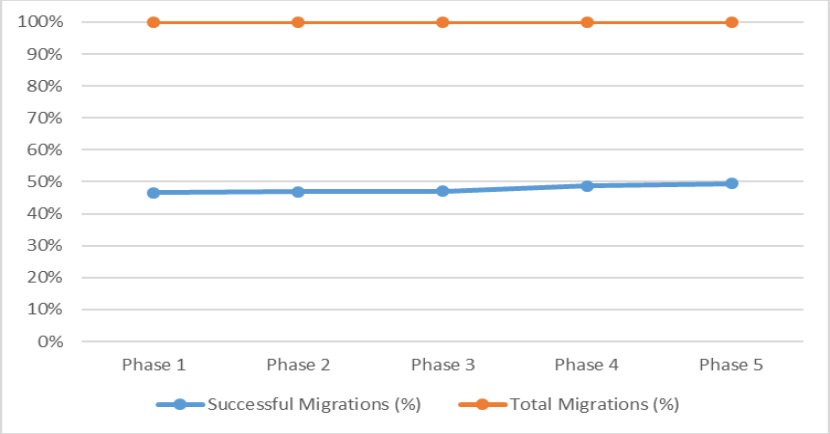

Figure 7: Effectiveness of Phased Migration Strategy

The graph of figure 7 displayed here demonstrates the effectiveness of the phased migration strategy in the form of successful migrations and all the total attempts in all the phases. The more successful migrations constitute the percentage the higher a more successful strategy is.

Figure 7 indicates that the success level of each migration step increases as migration process continues. This is attributed to the ability to learn and adapt migration strategies in real time which is augmented through monitoring and compliance checks. Active successful migration in regulated industries is necessary to have a successful rate in the later stage, which will require a phased approach coupled with appropriate risk management.

Summary

The findings given in this part confirms the efficiency of the offered phased migration approach in case of regulated sectors switching to monolithic systems to microservices. With the right management and control of migration effort, compliance, risk and operational resilience, organizations can guarantee a successful transition whilst satisfying regulatory demands. The analysis indicates that the phased strategy not only helps minimize the downtime of the system, but also gradually increases the compliance in the long-term perspective resulting in more resilient and scalable microservices architecture.

The most important lesson is to have a hybrid migration approach combining continuous compliance monitoring, risk management and operational resilience as the most important tool

in order to succeed in overcoming challenges of regulatory migration in highly regulated industries.

V. CONCLUSION

This paper discussed the migration of monolithic architecture to microservices in controlled industry environments, including focusing on the issues, benefits and approaches of maintaining compliance with strict regulatory frameworks. The study became centered on a staged migration strategy, with real-time compliance testing, risk management, and operational resilience as a part of the migration program. With the help of a step-wise transition model, we could mitigate risks, be under compliance and have a successful migration and cause the least disruption in business operations.

The results emphasize that the migration process although difficult, can deliver a substantial advantage in terms of scale or flexibility in addition to working efficiency. But it is apparent that without a thorough, incremental strategy, companies that operate within regulated business areas can also have a challenging time about systems integration, data security, regulatory compliance. The findings also indicate that an integration of real-time monitoring and compliance processes at each stage through the migration process is essential in limiting such risks.

5.1 Novelty of the Study

The originality of the research is in the focus on incorporating the regulatory compliance into the microservices migration strategy. Although each of the existing theories or studies deals with the technical factors of microservices adoption, the study pays particular attention to the challenges in regulated industries. The hybrid migration model entails both microservices architecture and continuous monitoring of regulatory compliance and this research offers an entire plan of transforming legacy systems into new architectures without ascertaining the compliance and security. It is the integration of real time of automated compliance checks and risk management processes that make this study a major addition to managing technology and regulation threats at the same time.

Moreover, the paper proposes a series of quantitative models to quantify the effort required in migration, as well as the scores of compliance and risk factors, and they give a distinct system of perception of the effects of every stage of the migration. The models can be used to explain how the system may survive its operational environment and how well planned the phased migration method can be to software organizations interested to use microservices without necessarily violating industry-specific rules.

5.2 Future Directions and Analysis

There are other areas in which the study leaves many grounds to research:

1. The Problem of Long-Term Compliance and Security: Future research may be conducted to

analyze the long-term implications of the microservices on compliance and security with regards to how microservices will change and adapt to new regulations.

2. AI and Automation in Compliance Monitoring: Studies on AI and compliance checks using machine learning to automate compliance monitoring would improve real-time compliance monitoring, detect compliance risks as well as enhance compliance with the regulations.
3. Cross-Industry Comparisons: Comparing migration strategies Across industries such as finance, healthcare, and energy may be helpful to obtain knowledge that is specific to industries and best practices.
4. Advanced Risk Mitigation Strategies: Research and evaluation of advanced practices to enhance fault tolerance, service switching, and disaster recovery would be paramount in identifying ways of addressing the risks in the migration process.
5. Scaling in Regulated Functions: It will be interesting to see how microservices scale within large and regulated organisations in regulated areas such as healthcare and finance.
6. Cost-Benefit Analysis: A cost-benefit analysis of legacy systems vs microservice may provide some useful information about the financial and operational implications of migration to decision-makers.

To summarize, the given study offers a framework of transferring to microservices and remaining compliant and operationally productive, as well as preconditions the future research in the field.

REFERENCES

1. Esparza-Peidro, J.; Muñoz-Escoí, F.D.; Bernabéu-Aubán, J.M. Modeling microservice architectures. J. Syst. Softw. 2024, 213, 112041.
2. Taibi, D.; Lenarduzzi, V.; Pahl, C. Processes, motivations, and issues for migrating to microservices architectures: An empirical investigation. IEEE Cloud Comput. 2017, 4, 22–32.
3. Amoroso d'Aragona, D.; Li, X.; Cerny, T.; Janes, A.; Lenarduzzi, V.; Taibi, D. One microservice per developer: Is this the trend in OSS? In Proceedings of the European Conference on Service-Oriented and Cloud Computing, Wittenberg, Germany, 22–24 March 2023; pp. 19–34.
4. Osman, M.H.; Saadbouh, C.; Sharif, K.Y.; Admodisastro, N. From Monolith to Microservices: A Semi-Automated Approach for Legacy to Modern Architecture Transition using Static Analysis. Int. J. Adv. Comput. Sci. Appl. 2022, 13, 907–916.
5. Taibi, D.; Lenarduzzi, V.; Pahl, C. Architectural patterns for microservices: A systematic mapping study. In Proceedings of the CLOSER 2018: 8th International Conference on Cloud Computing and Services Science, Funchal, Portugal, 19–21 March 2018.
6. Lenarduzzi, V.; Lomio, F.; Saarimäki, N.; Taibi, D. Does migrating a monolithic system to microservices decrease the technical debt? J. Syst. Softw. 2020, 169, 110710.
7. Taibi, D.; Systä, K. From monolithic systems to microservices: A decomposition framework based on process mining. In Proceedings of the International Conference on Cloud Computing and Service Science—CLOSER 2019, Crete, Greece, 2–4 May 2019.

8. Bajaj, D.; Goel, A.; Gupta, S.C. GreenMicro: Identifying microservices from use cases in greenfield development. IEEE Access 2022, 10, 67008–67018.
9. Vera-Rivera, F.H.; Cuadros, E.G.P.; Perez, B.; Astudillo, H.; Gaona, C. SEMGROMI—A semantic grouping algorithm to identifying microservices using semantic similarity of user stories. PeerJ Comput. Sci. 2023, 9, e1380.
10. Bajaj, D.; Bharti, U.; Gupta, I.; Gupta, P.; Yadav, A. GTMicro—Microservice identification approach based on deep NLP transformer model for greenfield developments. Int. J. Inf. Technol. 2024, 16, 2751–2761.
11. Liu, K.; Reddivari, S.; Reddivari, K. Artificial intelligence in software requirements engineering: State-of-the-art. In Proceedings of the 2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI), San Diego, CA, USA, 9–11 August 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 106–111.
12. Kochbati, T.; Li, S.; Gérard, S.; Mraidha, C. From user stories to models: A machine learning empowered automation. In Proceedings of the MODELSWARD 2022-9th International Conference on Model-Driven Engineering and Software Development, Online Streaming, France, 8–10 February 2021; SCITEPRESS-Science and Technology Publications: Setúbal, Portugal, 2021; pp. 28–40.
13. Díaz-Pace, J.A.; Tommasel, A.; Capilla, R. Helping Novice Architects to Make Quality Design Decisions Using an LLM-Based Assistant. In European Conference on Software Architecture; Springer: Berlin/Heidelberg, Germany, 2024; pp. 324–332.
14. Velepucha, V.; Flores, P. A survey on microservices architecture: Principles, patterns and migration challenges. IEEE Access 2023, 11, 88339–88358.
15. Lyu, M.; Biennier, F.; Ghodous, P. Integration of ontologies to support Control as a Service in an Industry 4.0 context. Serv. Oriented Comput. Appl. 2021, 15, 127–140.