Deep Science Publishing
https://doi.org/10.70593/978-93-49910-74-4_9

Chapter 9: The role of cloud and DevOps in accelerating insurance innovation

9.1. Introduction

Global investment in cloud computing services reached $498.2 billion in 2022, representing a year-over-year increase of 22.0%, and is projected to grow to $591 billion by 2023. As enterprises grow acclimated to cutting-edge capabilities offered by cloud service providers and identify shortages of traditional IT infrastructure as a bottleneck to faster innovation, more vertical segments are embarking on fast-paced cloud adoption journeys than ever before. Insurance is one of the most recent and perhaps intense examples of this evolving digital transformation dynamic. Insurance companies view cloud as the key technology driver for insurance transformation: Around 88% of survey respondents recognized cloud as the top modernization technology, followed by 82% pointing to artificial intelligence/machine learning platforms and 81% pointing to data analytics platforms (Bass et al., 2015; Gruhn & Schäfer, 2015; Erich et al., 2017).

The role of cloud platforms, however, extends much deeper and intrusively into the realms of enterprise innovation capabilities than being a mere modernization technology or a technology enabler for adjacent centralized or decentralized enterprise functions like data analytics or AI-microservices. Cloud Computing introduces a set of native capabilities built into the technology layer itself that enable the enterprise unlike any other past innovations to accelerate speed to innovation such as elastic scale-up and scale-down, push-button infrastructure provisioning, consumption-based costing for on-demand resources, infra-as-code, etc. Consequently, an entire family of newest technologies and applications such as software DevOps, microservices, data lakes, AI/ML, etc. that require these capabilities are native to the cloud. These capabilities and such newest technologies together intrinsically reshape organizational processes, team composition, resource, and scheduling decisions, in a way that acts to standardize, simplify and optimize core technology-heavy, business-critical, and innovation-rich enterprise functions of products and services Research and Development, core platform Engineering Hub Services for test, dev, and production, application development, business operations (Pahl & Xiong, 2018; Sousa & Gonçalves, 2020).

9.1.1. An Overview of Cloud Computing's Role in Modern Insurance

Cloud computing offers an extensive range of technological tools and options that power compelling insurance company capabilities. Yet at a fundamental level, the cloud enables an innovative, accident-prone sector to quickly and easily augment scarce IT skills with sophisticated capabilities, part of which is building their innovation chutzpah in the offices of their technology vendors, and part of which is gaining a deep and rich foundation of IT and analytical soft capabilities. The contemporary insurance company wishes to become flexible and agile, concentrating its own talents on risk selection and pricing. The development of risk category ratings, which optimize claims payouts and profits, is a key industry innovation, both for forcing the market to respond in real-time with potentially addictive variable premium moves, increasing trust, and the tickle-down effect on reserve balances. Much of the acceleration of profit recognition from these reserves flows from improved analytical tools enabled and powered by cloud-based IT,

Fig 9 . 1 : Cloud and DevOps in Accelerating Insurance requiring less expensive, scarce skill experts to develop and use. In addition, the pure premiums driven by technology incurs claims are sensitive to design, implementation, and control of technology infrastructure. No new technology has so rapidly transformed the competitive and operational nature of an industry as cloud computing has done to insurance. The magnitude is a ten-fold increase in the pace of profitable growth and costs per policyholder, increasing the use of analytical tools to both refine underwriting decisions regarding risk category and the increasing sophistication of incidental services to reduce loss ratios taken from other industries.

9.2. Understanding Cloud Computing

Cloud computing refers to the storage of data and programs on the Internet instead of the computer's hard drive. In the past, storing on-site data was more secure, as regulations and compliance focused on internal control over information. Thus, data breaches occurred more from the inside than from the outside. Cloud computing has made storage and computing power so cheap, abundant, and relatively secure, that firms as well as individuals are moving more to the cloud. With regards to cloud models, firms can select part or all of either of two deployment models, via a public cloud, a private cloud, or a hybrid cloud of both. A public cloud is the universal framework for cloud computing. Private clouds are done exclusively with in-house resources or via direct contracts with firms. The selection of a public, private, or hybrid cloud model depends upon business finances as well as sensitive information.

Infrastructure as a Service (IaaS) provides commodity hosting, Application Platforms as a Service (aPaaS) provide hosting for specific types of applications such as development, runtime, and orchestration, with access control, backup, and recovery, Software as a Service (SaaS) offers complete applications in the cloud, and Technology Enablers for Cloud Computing provide tools for the development, deployment, and management of cloud systems such as containers, microservices, and serverless computing. Cloud computing has made such resources relatively cheap and can offer advantages over in-house or server-based computing, such as low risk, high performance, and reduction of capital expenditure about investment. Cloud computing can also offer easy scaling for fluctuating workloads with faster time to market and better strategic focus, shifting IT focus to business issues.

9.2.1. Definition and Key Concepts

Cloud computing is an evolving technology driving business transformation in numerous domains. It provides a common infrastructure for performing distributed or large-scale data-centric computing, such as storage, management and analysis, at much lower costs and faster speeds than what are supported by traditional functions. It allows on-demand usage of shared configurable resources such as networks, servers, applications, and services, providing less expensive and more powerful solutions than what are available with in-house.

The three major models of cloud focus on who controls the major portion of the stack. Infrastructure-as-a-Service (IaaS) is an environment where a cloud provider sells raw compute power via a hypervisor with customers deploying their preferred environment stack in virtual machines atop that hypervisor. Platform-as-a-Service (PaaS) is a cloud model where development environments, including management and messaging tools, runtime environments, and libraries, are provided for building applications. Software-as-a-Service (SaaS) is a model where a cloud provider supplies fully workable applications available to customers with a browser. Cloud service models may be implemented with public or private clouds and may be serviced on a pay-as-you-go or subscription basis. Compared to in-house solutions, cloud services allow companies to quickly scale offering more configurations at lower costs without the burden of maintaining the infrastructure or worrying about security.

9.2.2. Types of Cloud Services

As cloud computing has matured, several forms have emerged to cater to the needs of cloud users. These can be broadly categorized into SaaS, PaaS, and IaaS. SaaS delivers software applications over the Internet, on-demand and on a subscription basis, providing a simple and affordable alternative for activating and deploying on-premise applications. Although developed by multiple independent software vendors, SaaS applications are mostly being offered by the leaders in the application software markets. Built on Web services, Software as a Service utilizes the Web as a delivery medium. But unlike Web applications, these applications boast of extremely rich user interfaces, akin to on-premise software.

Reducing the complexity of development and deployment, PaaS environments are replete with the infrastructure on which applications are built and deployed. By offering a set of software components and services for the developers to choose from, this model can greatly accelerate the development of Web-based applications. However, because of the design of these environments, developers are restricted to the architectural patterns, including data storage models, permitted by the PaaS vendor. Thus, for enterprise applications that are critical for business operations, the usage of such environments can run the risk of vendor lock-in. PaaS provides solution stacks or platforms optimized for building a specific class of solutions. It is aimed chiefly at enterprises interested in cloud-native application development.

9.2.3. Benefits of Cloud Computing in Insurance

The strategic impact of Cloud technology towards achieving IT and business goals has led organizations not only to experiment with Cloud technology, but also to jump on the Cloud bandwagon in droves. There are multiple reasons that impact this rapid growth towards Cloud, including Cost Benefits, Scalability, Efficiency, Rapid delivery of Infrastructure, Deploying crucial and critical applications faster, Failover, Disaster Recovery, Data Backup, etc. With Cloud computing, organizations can have many variations in their external access strategy, depending on their unique businesses model, the requirement for controllership of their infrastructure and applications, and need to leverage from Cloud computing's promise of scalability and flexibility.

Cloud's multiple variations provide both benefits and challenges for the insurance sector. The Public Cloud deployment model has compelling economics for applications that have a well-defined infrastructure cost-and-revenue structure; maximizing the Cloud's variable cost nature. Prospective benefits can include reduced time to market for new services, enhanced elasticity, and lower overall cost. Complexity comes from the multi-vendor dependency of public Cloud services firms face when building commercial solutions. Other challenges may arise regarding controllership and compliance, including regulatory issues, security, and customer protection. In contrast, the Private Cloud deployment model offers dedicated hardware for the Cloud services which shield companies from concerns over a multi-tenant Cloud design. With a dedicated infrastructure, companies control security and compliance. Similarly, Hybrid Cloud solutions provide companies the best of both worlds, allowing companies the flexibility of the Public Cloud for non-sensitive applications while retaining sensitive data in a Private Cloud.

9.3. Overview of DevOps

In the early 2000s, many software development teams started adopting a common set of practices, tools, and processes collectively known as Agile. Adopting Agile transformed the development of most web applications. But development was only one part of the process. Once ready, the software had to be released and made available to customers. Often, application updates were infrequent and users received new features now and then—and sometimes, not at all. Specialization of work meant that development and operations teams kept at arm's length. When software failed in production, it was often ops that took the brunt of the blame. Over time, this lack of collaboration contributed to a blame culture, where devs rushed to release a new feature, and ops deployed the code and watched it fail. As web applications became more important during the dot-com boom, the separation of duties was no longer sustainable. Users expected applications to be available all the time. They wanted new features and updates delivered quickly.

Teams could no longer afford to wait weeks or months between application updates. Frequent code changes had become a reality, driven early on by small companies, but more recently by tech giants that released new versions of their applications every night. Continuous delivery had become crucial for the success of organizations. As organizations became aware of how important frequent and fast releases were, they also became aware of how they could actually improve them after instituting a DevOps culture. DevOps combines the words "development" and "operations" and signifies a collaborative or shared approach to IT service delivery. DevOps is a cultural and professional movement that stresses communication, collaboration, integration, and automation among stakeholders at various stages of the service lifecycle, from design through the development, deployment, and operations, to the final decommissioning. By unraveling what makes tech organizations some of the highest performing organizations in the world at delivering software at speed and quality, the DevOps movement aims to reform the economics of technology.

9.3.1. Definition and Principles

DevOps originated in the late 2000s, launched by IT professionals who sought a better means of unifying responsible parties and processes in IT infrastructure development and launch to improve speed, minimize issues, and maximize availability of systems. The movement pioneered unification of the development and operations functions in IT, with developers taking more active interest and responsibilities in production, the software lifecycle post-code and build, and operations personnel getting involved in source code and testing decisions and processes that affect production. Through this collaboration, and experimentation with productivity improvement, automation, and formalization of shared processes, a culture evolved to aid in integration of the full software lifecycle, DevOps.

DevOps, as a cultural movement, is based on principles for IT development and operations that is outside the purview of other silos-focused methodologies and solution suites, which emphasize optimization of individual focus areas rather than services as a holistic entity. Hence, therefore and as its name implies, the principles of DevOps imply integration of software of services delivery — key DevOps principles advocate collaboration across functional boundaries in IT, recognize that flexible systems are better for business, involve operations in IT decisions that have impact beyond development, regard error and correction as intrinsic to service delivery to ensure business objectives are met, emphasize automation of testing and deployment to ensure delivery consistency and match business objectives, and promote reduction of nonvalue-adding work to help ensure funding of capabilities that meet business objectives.

DevOps not only understands the impact IT decisions have outside the boundaries of development but encourages developers to optimize actions for all areas impacted to ensure positive results for the business. It’s a balancing act made easier by tools, automation of repetitive processes, simplified collaboration, and cultural acceptance all around, especially from the business.

9.3.2. DevOps Practices and Tools

DevOps implementation is ideally comprehensive. Most organizations do not pick a single practice to get started — they tend to use several tools and practices together to accelerate their software delivery while increasing the quality. Mainstream Practices and Their Tools are: CI/CD is a set of dev and operational practices designed to shorten the systems development lifecycle. CI is software developers integrate their code into a shared code repository several times a day with automated build testing run on the shared CI environment. Automated tools use the CI/CD pipeline. CI/CD is therefore the process and tools that allows for faster release of software, increased quality of software with lower costs. Continuous Integration focuses on automating the integration process. Continuous deployment flips the switch so that new code gets deployed to production the moment it has been integrated and built. Continuous delivery automates the integration and delivery process.

Infrastructure as Code (IaC) is a set of dev and operations processes that enable automating provisioning of IT infrastructure. IaC uses configuration files to define the infrastructure that’s needed to run various components of a given application. The files are stored in a version control system. IaC tools read these configuration files and automate the provisioning. Some use a declarative approach that says what the infrastructure should look like and some use an imperative or procedural approach that says how to get to that state. Declarative tools include various options. Examples of imperative IaC tools include various options. The software developers find it easier to talk in terms of code because they’re typically not domain experts. Automating everything means code is less prone to human error. The IaC paradigm enables rapid, massive scaling of infrastructure.

Collaborative Workflow and ChatOps refer to the tools and processes that enable ease of collaboration and communication between interested groups both within and across the organization. External communication is with customers and stakeholders. Internal communication is between development, operations, digital experience, quality, and security, etc. ChatOps tools allow this communication to happen in a structured and organized way so that it is easy for others to follow.

9.3.3. The Cultural Shift in Organizations

So, what requires an organization to truly adopt DevSecOps principles? The most important aspect is the culture shift. Organizations fall into two camps. A more traditional organization will have a siloed structure, whereby teams will be created around a specific domain of functionality. These organizations tend to prioritize individual component performance over the greater whole. Usually, they tend to have lengthy approval cycles, be made up of hierarchical complex structures, and have unclear, many-step processes.

They tend to have a lack of trust within organizations. This is evident through low levels of collaboration and communication between teams that can be found within silos. Individuals achieve goals between teams, but this is not seen as a collective success, and external politics might even run rife. When the organization is trusted for doing the right thing and when risk mitigation is a shared responsibility, people are informed, knowledgeable, and able to act with reasonable freedom. Underlying these activities is a greater understanding of how security is achieved and maintained, and how products are delivered: by working together. However, when planning solutions, organizations often overlook the associated security risks.

The second type of organization is the less mature company that does not have as significant divides between teams. Collaborative teams that trust each other and share an understanding of systems and techniques often push the DevOps innovations further. As an organization refines and develops its existing activities, whether this is automation or CI/CD pipelines or security reviews, the gains are fed back into the broader community. Even more than other types of organizations embarking on a DevSecOps shift, companies within this arena deal with security in a way that suits them. There are no clearly hard processes to follow; instead, teams are encouraged to express security as they see fit and combine it with their other activities that exist.

9.4. The Intersection of Cloud and DevOps

Accelerating innovation by removing silos across departments and creating a DevOps culture is the goal of most organizations, including insurers and reinsurers. But seldom can organizations fully realize this goal without external solutions and services typically supported by cloud computing. The increase in the amount of data; the rapidity and scope of technological changes such as AI and ML; the need to provide services seamlessly and on demand, as is being demanded by customers; and, in general, the uncertainty of the current business landscape are all reasons for organizations in the insurance ecosystem to incorporate cloud computing resources into their operations. Cloud eliminates many of the resource constraints traditionally imposed on organizations and helps them transition to DevOps.

Cloud computing can help automate and streamline software development and build pipelines, giving all the stakeholders visibility in the process. Automatic cloud scaling allows for testing and debugging of software at scale by multiple different users, testing for possible edge cases before the service goes live. Automated scaling and the existence of multiple copies of the software service in the cloud mean that business leaders can use newer algorithms and models when assessing the risk of loss, compute the business implications, and go live faster than ever. Coding, testing, and deployment can create multiple variants of the service on the fly to try out recommendation algorithms tailored to smaller customer segments.

The transition to the cloud should ideally be smooth, but integrating the two operations can introduce new challenges. New security models and new procedures to ensure that compliance requirements in terms of recordings or security are still being met are needed to foster confidence in a completely new operating model. Traditionally, security considerations come at the end of the development pipeline. Using cloud resources, the presence and potential flaws in the security of third-party modules used by the organization, of supplementary cloud native software services, and of the software services that the organization publishes to customers become even more critical. Integrating security in each step of the pipeline, at each stage in the life cycle of a service, from development to deployment and operation to decommissioning, is extremely important. Security solutions using ML and exploiting cloud computational power are being developed to make it possible.

9.4.1. How Cloud Supports DevOps Practices

Cloud is a foundational technology for DevOps. It accelerates every primary DevOps practice – drive resilience and security in software by default, deliver continuous feedback toward a stable release baseline, and build and test software in small batches – and supports those practices with shared cloud services. If virtualized compute was essential to Agile’s power, shared security and compliance, source code management, testing, collaboration, build, and monitoring services allow IT organizations to adopt and scale DevOps practices at high speed.

Shared cloud services accelerate primary DevOps practices. Resiliency and security in production by default. Functionality in deployment by default. Collaborative push-button testing at high speed. Shared services are not just faster and easier. They drive higher quality and productivity gains. Quality-aware software development and security checks before, and during the build, and before and during the test. Software written in small batches. The changing role of IT within the enterprise supports small batch software development. Software change estimated, scheduled, and planned over a release cycle supported by IT. Security and resiliency tasks at the smallest time scale. Monitoring and telemetry data shared by deployment teams, business executives, and other employees. Cloud destroys the asymmetry in development and operations cost and skill. DevOps releases and maintains software without the handoff, and without the overhead, the high cost, and the high stress.

9.4.2. Integration Challenges and Solutions

Cloud technologies, and especially public cloud services, make it easy for DevOps teams to deploy workloads quickly and easily. Services make it easy for teams with small IT budgets to create complex, multi-service applications. However, these public cloud services have their own integration challenges. Each cloud has its own set of tools and services for managing applications. Even multi-cloud solutions are unique to each implementation of these tools.

A small development team might need to develop, test, and deploy applications quickly after the idea for a solution is proposed. If the deployment is to a public cloud service, the ease of solutions from various providers might make sense. However, if the application needs to connect with a large ecosystem of other applications sitting on-premises or across multiple corporate networks, the overhead of using multiple cloud technologies can create more difficulty than benefit for the organization.

In this type of situation, a good solution to consider are integration tools that the organization is already familiar with across its DevOps lifecycle. Tools make it easy for teams creating solutions without heavy budgets to build, integrate, manage, and iterate on applications inside the cloud. Using these types of solutions lets teams use the cloud for its lower barrier of entry without the drawbacks of managing microservices, decentralized applications, or other challenges of cloud-first infrastructures.

9.5. Case Studies in Insurance Innovation

Transforming business operations in technology-driven ways is one of the main methods by which firms in various industries are open to innovation. Insurance is traditionally subject to the Dual Control principle promulgated by the state. With respect to the status quo and further advancements related to insurance, it has long been taught that the insurance industry is a latecomer to the digital world and that the insurance industry has so far been lagging behind other Financial Services. One of the reasons is the long lead time for product development coupled with industry-wide mild-oligopolistic conditions.

Nevertheless, during the past decade insurance companies have made significant investments in information technology to increase efficiency, improve customer relationships, and develop new and sophisticated products. This development paved the way for the establishment of InsurTech and for platforms that promise increased user and customer experience. More particularly, opportunities in InsurTech are founded in digitizing back-office processes and in providing service enhancements for customer interaction at the front office.

Fig 9 . 2 : Insurance Innovation

Previously, transformation was associated with long implementation phases. With cloud as the chosen platform and continuous delivery as the right methodology, improvements to business model operations, partner interactions and customer experiences can be brought about on a nearly monthly basis. This has led to some of the multi-billion dollar InsurTech valuations observed in the latest round of funding. However, those valuations are based on the expectation of being able to execute upon their growth plans without IT platform risks. Companies that are expected to rely upon a traditional corporate architecture, such as having to rely upon legacy systems for billing and claims, cannot command premium valuations. Demand requirements for speed, integration, and customer-centricity imply a pressure for back-end modernization and leveraging of API and microservices-enabled architectures.

9.5.1. Successful Cloud Implementations

Successful cloud implementations are becoming a hallmark of insurance innovation. The first wave of accessible, cheap cloud frameworks, providers, and resources has opened new ways of doing business to fresh-faced InsurTech startups, although implementation is still heavily influenced by the experience of the organizing team. However, these talent-filled companies have complemented incumbent leaders and now hundreds of partnerships between startups and carriers have formed, using applicable data and new entry points to transform static, packaged insurance into algorithmically priced, dynamically activated coverage. Real-time connections between insured, sensors, and policy management are moving car insurance to user-optioned, app-driven experiences. Then, claim events can be ported in real time to insurers to ensure safety, deploy contingency resources, and settle with all parties – which is proven to dramatically reduce the cost of claims logistics; and the costs of reinsurance for downtown car activity riders can quickly be deployed to settle risks of net downtown-nonproductive activity. Commercial and residential property insurance is moving to demographic-mapped algorithms for risk acceptance and limit diagnostics combined with AI-optimized baselining models of current risk. After a trigger event, loss settlements can be preprogrammed to come at policyholder discretion to flow with the insured risk. Use of the digitized log of risk can help multicarrier and various-event coverages served by an InsurTech to smoothly allocate risk cost burdens during large settlement events to incrementally drive down the losses as care flow increases. Cloud storage and GPU-enhanced models can forecast and proximate settlement flows probabilistically for various conditions on a project basis enabling excess co-insurance coverage to be expediently put in place.

9.5.2. DevOps in Insurance Startups

Consider the Tekja startup in San Francisco, which has recently built a platform used by insurance carriers to automatically file claims made by personal lines policyholders. Because this startup faced some scaling issues, they engaged in what is called "Cloud with added momentum," which enabled Tekja to mitigate its growing pains and now deploy code with higher frequency and lower risk. Most insurance startups are already running on Cloud Plus DevOps, but speaking with executive Natalya Haskvitz and a handful of insurance carriers and brokers using Tekja's platform revealed the speed-up process they are experiencing thanks to the added momentum. "When we started, the velocity was much slower," Haskvitz said. Like many other startups, the company began by deploying its platform every couple of weeks, not even every week. "When something is deployed to production, it's a big deal. But at this point, we are deploying three or four times a day. We already know that this is how a large team operates, and we are just sizing up to that." Recently, it got a lot more interesting for Haskvitz, who joined the startup last autumn after leading engineering teams at various companies. The company went into the testing process of a new core product designed for brokers and underwriters to automate the personal lines quoting process. After the insurance company buys the policy, the new offering recommends changes to mitigate the risk further and reduce prices. According to a recent position paper published by a consultancy, only a handful of large or mid-sized insurance companies and brokers have been doing DevOps for a while. "In insurance, DevOps has been adopted mainly by visionaries," says a co-founder.

9.5.3. Lessons Learned from Industry Leaders

Cloud-first identifies a company that is fully adopting a cloud-based model for all new application innovations. The majority of traditional financial technology solutions were built on on-premises infrastructure, which required lengthy development cycles. However, innovation is occurring faster by defining a cloud-first strategy. Four industry leaders share their thoughts on this approach.

“We are only keeping the components that differentiate us. Everything that is a commodity is in the cloud.” – David Brear, CEO, 11:FS “We realized we couldn’t innovate the way we wanted in a traditional model and made a conscious decision to go full cloud.” – Doug Bouteiller, CIO, USAA “The best companies will be cloud natives. They will have nothing to do with legacy.” – Fred Goff, CEO, Jobcase “Everything we do from a technology point of view is built on the best of what SaaS has to offer.” – Paul Hounsell, CIO, Hiscox

Key Considerations for Investment in Cloud. Industry leaders express similar themes around the reluctance to invest further in on-premises infrastructure. Their businesses operate in a dynamic environment where small and medium enterprises (SMEs) and millennials have become more important to the strategy. The demands of SMEs and millennials are not the same as they once were. They expect quick responses with seamless digital interfaces. They expect the company to know them, understand their needs, and be easy to do business with. A cloud-first strategy enables a deeper level of flexibility and business responsiveness than a legacy IT model.

Risk Management of Cloud at Scale. Possible concerns with the cloud primarily revolve around risk. From a risk management and compliance perspective, proactive approaches are being undertaken to ensure the integrity of financial data is protected in the cloud. Enterprise companies with a cloud-first strategy are applying similar levels of oversight in their cloud investment that they would on a traditional technology investment.

Selecting security-aware cloud service providers and ensuring continuous compliance of all services is the approach being taken.

9.6. Regulatory Considerations

Understanding the applicable regulations governing data in the cloud is a core component of any organization's journey to the cloud. Organizations adopting cloud-native technologies for DevOps must consider not only the rules that apply to traditional IT outsourcing but also the specific features of the cloud that add new dimensions to the regulatory environment. This is especially critical for regulated industries such as the insurance sector that deal with sensitive information and the consequences of data breaches. Compliance considerations run through the process of cloud adoption and use for IaaS, PaaS, and SaaS as both customers and service providers.

At a high level, adoption of cloud-native technologies such as DevOps introduces new challenges for compliance and risk management and requires a new strategy for addressing these needs. Cloud service providers operate multiple customer environments in shared infrastructure, reducing the degree of control over compliance attestation that an insurance organization can conduct for cloud services. Furthermore, the speed with which organizations build, test, and deploy applications on these environments can accelerate their exposure in the event of an incident that does cause regulatory damage, and the security measures for cloud services are different than traditional IT systems. This means that companies must give significant consideration to automating and integrating security and compliance into cloud-native strategies for DevOps.

In addition to general considerations, the movement of information into the cloud creates unique compliance challenges for insurance organizations. Data movement into the cloud changes the responsible party for ensuring regulatory compliance, and the cloud provider is necessarily not privy to the specific requirements imposed by regulators. Too much assumption or misunderstanding of compliance requirements can lead to decisions that put insurance organizations in regulatory jeopardy. In some instances, the cloud service provider may have established industry-specific compliance programs, which allow customers to upload and run regulated use cases in the cloud, though both parties still must ensure appropriate safeguards and considerations are implemented as part of these programs.

9.6.1. Compliance Challenges in Cloud Adoption

Insurers are experts at managing risk. However, the cloud poses new risks that insurance companies have never faced before, challenges that stretch the definitions of security posture, cyber-risk, and risk management. Industry regulators and auditors have different views about the cloud. Some governments believe that cloud providers are now responsible for the security of customers' data, applications, and workloads; others give custodianship back to the customers. Insurers must work with each cloud provider to ensure compliance with the regulators and auditors. And because cloud regulations and auditors are evolving, the tasks of cloud compliance and audit will only become more complex over time.

Insurance data custodians are generally expected to implement common-sense best security practices. So, any new application deployed in the cloud should have encryption on the application, data protection controls to prevent unauthorized user access, and logging to enable audit. Access to the cloud should be secured via restrictions that are consistent (and equally enforced) with those required of internal applications. Data in the cloud itself should also be secured and encrypted, and any backend workloads should have their front-end posted behind a VPN or other secure access method. Penetration tests should also be done on a regular basis, especially if the cloud provider pushes any patches.

9.6.2. Data Privacy and Security Issues

The ownership, maintenance, and access of sensitive customer data stored in a cloud environment is a complex issue — one that often inhibits insurers from embracing the cloud. Insurance organizations collect and store vast amounts of data that require being handled with the utmost care. For executive leadership, allowing vendors access to sensitive customer information, concerns of system breaches, and employing ill-equipped resources to ensure protections are set in place to avoid unauthorized access or theft of personal data, is enough to cause them to halt any cloud adoption or advancement initiatives altogether. The fear of third parties accessing sensitive information or hackers circumventing infrastructures that are supposed to provide ultimate care and concern is enough to cause executive leadership to stall selection of cloud service providers. The threat of disaster recovery services not being in place to leverage data in viable forms for worldwide access in the event of an emergency is a deep-seated source of concern. Regulations that require federal agencies and their contractors to secure sensitive data often drive executive leadership to the private cloud.

However, the capabilities afforded insurers today through adoption of the cloud can be dampered by confusion of the need for complying to rules or redaction of any identifiers to independent, equate customers with linkage to health condition information prior to outsourcing any data for analysis to enhance engagement between providers and patients is paramount to preserving trust and subsequently generating sufficient amounts of revenue. Furthermore, executives – who are often overwhelmed by the pressing nature of other matters and have little to no experience with data security decisions – must also grapple with how to choose third-party vendors and/or cloud services that are the best fit for operations, whose capabilities they trust, and how to structure the business relationship.

9.7. Future Trends in Insurance Technology

As insurance sits at the crossroads of many industries providing coverage of varied services within industries such as health, transport, infrastructural and technology, the future could see a large advent of insurance companies diversifying their insurance product portfolios. Along with diversification, there will be many emerging technologies that would be reshaping the risk landscape. From crypto and blockchain technology offering instant trust for monetary transactions, to autonomous vehicles making new risks for road insurance with their introduction, we will be seeing new types of risks that would need to be covered and new technologies that would make it possible to verify and evaluate those risks. Examples of such emerging technologies include social, mobile, analytics, cloud and cyber. Such technologies will aid in identifying evolving customer preferences ahead of time. Disruption or evolution in social habits of customers are at the heart of many recent insurance disruptions, doing away with standard vehicle services and replacing it with IT services that rely on sharing economy. Interactive computing software on mobile, and capabilities on collaborative software elucidate insurance policies being formulated at point of sale on mobile with help of relationship managers, comparing policies between companies based on analytics on structured and unstructured big data across social and mobile. Feedback on products could be sent with immediate effect due to social media integration. Incoming data and flows on and from customers could be called cyber from sensor technology embedded across value chains. Such enabling technologies would make new types of products and services possible in the area of customization and personalization. Insurers and reinsurers that are nimble, agile and enter new non-restrictive partnerships can remain relevant and dominant in the marketplace. The ability to identify new digitally addressed, price-sensitive customer segments in fast-growing markets through the use of robotics, AI and chat technology makes the delivery of insurance solutions through ecommerce portals possible.

9.7.1. Emerging Technologies and Their Impact

The modern technological revolution is affecting every aspect of our waking life. Rapid technological innovation is paving the way for improvements in efficiency and speed of decision-making while improving response times for consumer needs. Memorialization of human experience in ever-increasing amounts of data has created opportunities for insights never conceived of before. The requirement for speed in decision-making and action has created disruptive business models across industries. Incumbents in every traditional market are investing in business transformation. Insurers are not exempt from the challenges and opportunities created by these new imperatives. Insurers who stand still in the face of changing consumer demands and emerging unregulated innovators do so at an existential peril.

Emerging technologies promise the capability to address these challenges, reshaping the industry. Blockchain, increased connectivity, automation, artificial intelligence, augmented reality, and an abundance of data are among the discussed technologies and their application via telematics, IoT sensors, connected devices, and drones are reshaping the competitive landscape. Imagine this: A consumer is sitting at home and a storm that vacationers are flocking to on a whim is about to hit where they are. After all, insurance companies are pro-accident, and that is exactly what consumers expect. They are expecting vacationers to be stranded in their beach houses with no power and no way out. That is the expectation every insurer is preparing to meet.

9.7.2. The Role of AI and Machine Learning

Insurance businesses are uniquely qualified to benefit from these machine learning and AI improvements. Algorithms thrive on data, and few industries have access to the amount of data generated by insurance transactions and claims as the insurance industry. This capability has allowed innovators to shorten significantly traditional underwriting and claims processes. Historically, these activities have taken quite some time, involving time-consuming data analysis and labor-intensive human analyses. Next-gen insurers can now use AI to predict unseen trends in underwriting data.

For example, many systems can quickly analyze previous years of extensive weather data through sophisticated natural language processing systems to predict the odds of highly localized weather events, from hailstorms to floods. Other AI-based systems can predict which variables have the most impact on property insurance loss, delivering guidance on regulation and compliance decisions.

AI also impacts fraud detection. Traditional fraud detection techniques typically focus on one small area within an enterprise. For instance, a common-issue automated fraud detection by travel booking and insurance provides tracking and detection of travelers flying to a disaster area, buying travel insurance, then returning to their homes immediately before the disaster occurs.

Significantly, AI and machine learning technology primarily comes from the digital retail and social media markets, and it enhances prediction capabilities in positively disruptive ways. Using near-term trends data from the social media market, these systems can narrow their search predictions by millions in a matter of seconds, allowing insurers to contact customers and change their policies before the customer even thinks about it.

9.8. Building a Cloud-First Culture

For insurance organizations to fully harness the value of cloud platforms and DevOps tools, they need to accelerate the transformation of the way they operate and navigate the cloud-centric world. They need to lay the groundwork for a cultural shift toward a cloud-first mindset to realize the transformational business outcomes from modernization. They need to encourage cloud operations to become the new norm, and use it as a reference for guiding all technology-related work and spending. Business and technology leaders should task their organizations with establishing a roadmap that enables the adoption of innovative cloud technologies and solution architectures.

So how do insurers cultivate a cloud-first culture? One fundamental strategy that sets the tone for the rest of the initiatives is to launch training and development initiatives that teach that cloud is the technology norm for any solution the company builds and deploys. A second tactic is to create formal and informal innovation channels that promote and support innovative minds to demonstrate the capabilities of the cloud by building cloud-first tools that help the organization solve challenges for operations and solve customers' pain points. Cloud tools should be among the first the company starts using as any product or service takes off. They help the company and customers feel and experience the ease and benefits of cloud-first approaches, architecting company and industry functions, products, and services to work with cloud-first functionality unique to their capabilities. Use of these products sets the groundwork for the marketer's value proposition to offer accelerated cloud-first security, performance, reliability, ease of use, and almost next to zero cost of ownership.

9.8.1. Training and Development Initiatives

Accelerating insurance innovation is no longer just a question of changing technology. To achieve the agility and adaptability that is required for establishing a cloud-first culture, an organization must also adapt its people, process, and procedures to align with its goals. A significant piece of that puzzle is scheduling and supporting necessary training and development to increase awareness and host knowledge share sessions across the organization. The first step is to help employees identify their gaps of knowledge and provide targeted training based on their role. These training initiatives should not only address the core concepts and tools of the cloud; they should also help the company cross the Devils Canyon Delta. To do that, organizations should host architectural decision-making workshops that help stakeholders go through the critical architectural decisions they need to make as they evolve into being cloud-first.

Once the organization has a foundation of knowledge on which to build, continuous support and development retargeted to the real-world problems that employees are facing in their roles is needed to not only build but also sustain development velocity. This active mentorship can be fulfilled through onboarding buddies, regular one-on-ones with managers, lunch-and-learn sessions, and hackathon events. Such development initiatives also have the added effect of breaking down siloes of knowledge within the company, allowing faster collaboration and solutions to difficult problems through shared understanding across teams, as well as easily integrating new people into the company. Given the rapid advancement in cloud-native technology, people are always going to need to learn in their roles, but by creating a culture of knowledge share and development, organizations can reduce ramp up time and not only ensure understanding but also excitement in using the technology.

9.8.2. Encouraging Innovation and Agility

Emerging from the global pandemic, customers of all types and backgrounds are changing. In the insurance industry, this change is dramatic. Insurers can no longer expect people, when faced with unexpected bills, to respond to business solicitations on social media, but instead, will initiate those conversations, compelled by comparative experience. They want easy onboarding and interactions, earlier resolution of premium

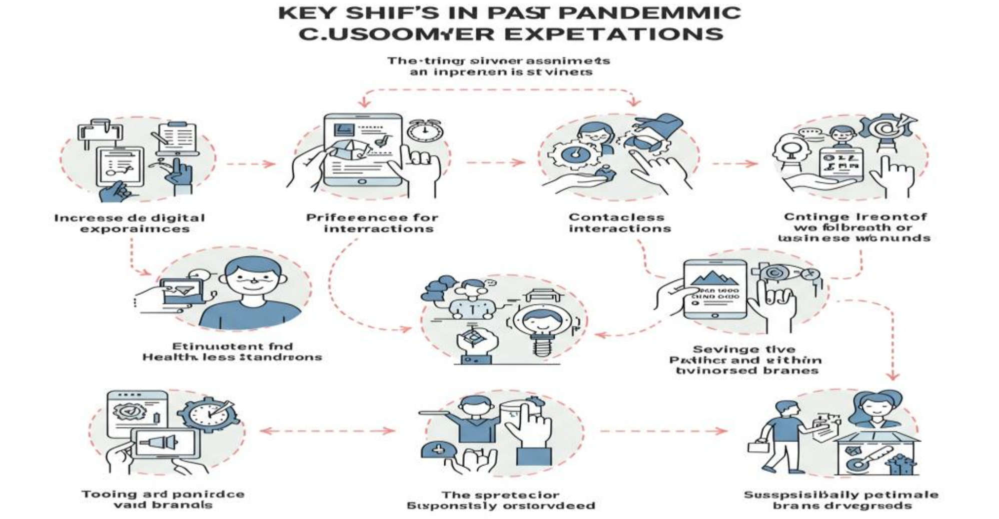

Fig 9 . 3 : Post-Pandemic Customer Expectations (1-10 Scale) disputes, asynchronous claims reporting complete with picture submission, direct deposits for approved claims… and all services available for self-service. For insurance, delivering these new experiences means changing what used to be “applied technologies” to a wide variety of original design and development software-defined solutions. Cloud opens the door to development agility. DevOps teams within and outside the enterprise can participate. And with cloud-based capabilities, your business units can take on experienced developers to craft and manage those solutions—if only for your unique use cases—and extend your innovation window. Win with the latest cloud capabilities. Start with your early moves to cloud, the ones that let you learn capabilities and processes as you make the big moves: that is, your quick applications, then back-end applications. You are cloud experts now.

Throughout this access, discover new and specialized capabilities in next-generation services like intelligent automation, machine learning models and government-supported marketplaces, blockchain, augmented reality/virtual reality, and radically new managed services like enterprise warehouses. Because cloud continues to change, you can discover cloud-native ways to implement anything. Through all this discovery, organizations gain the ability to change and respond. Decision makers have greater confidence to take risks on implementing emerging capabilities because there are so many available where none existed how few years ago. The investments involved express themselves through short time horizons, great business interest, available cloud professionals, and low code/nocode development platforms.

9.9. Conclusion

Historically, insurance has not been an industry associated with technological progress. On the contrary, its long-term and often slow-moving nature functioned as a restraint to radical changes. This perception changed with the advent of insure-tech ventures that emerged as alternative platforms to directly challenge the existing players. Through ingenious technological enablers, like mobility, cloud, and data, insure-techs challenged the insurance market on multiple fronts, including data analytics, underwriting, distribution, customer experience, reduced costs, and shorter times to market. Established insurers, already faced with their own internal shortcomings, risked losing market share, if not market dominance, to these nimbler and, therefore, potentially more successful players.

To counter the threats posed by insure-techs, large players invested heavily in the development of technological enablers. However, much of the investments were not seen through to successful completion. In the wake of the pandemic and the pivotal acceleration it caused in the adoption of the hybrid work model worldwide, our thesis is that the cloud and DevOps are not simply accelerators of innovation, but have emerged as the strategic foundation on which successful innovations must be built. Our recommendations to stakeholders in the insurance industry are that they should avoid the trap of viewing the cloud as just a cheaper or more flexible IT resource, or digital transformation as an evolution of IT. Embrace the central role played by the cloud and DevOps in accelerating innovation itself and rapid time-to-market as the key to ensuring the success of the chosen innovations. Consider these elements in all strategic decision-making, in particular, but not only, for the chosen enterprise architectural blueprint. Finally, and critically – sourcing talent with the right cloud, architectural, and Dev-Ops skills to lead and oversee the transition.

9.9.1. Final Thoughts and Strategic Recommendations

As insurers strive to fast-track business transformation, all the while balancing traditional business commitments against these modern operational and developmental pressures, a cloud-first strategy can help. The cloud provides the innovative infrastructure, pre-built and customizable developer tools, cost management solutions, and AI supercomputing resources that digital life requires. Insurers need to leverage the cloud as a means of paring down the infrastructure investments and buildup times associated with modern development and operational projects. Insurers can benefit from the dynamics of the shift to a cloud-first digital strategy. Insurers need to take advantage of the shift from in-house engineering of niche solutions to the curated delivery of low-code or prepackaged automation tooling.

The introduction of low-code automation tooling and prepackaged use-case specific automatics capitalizes on the focus of skilled IT engineering talent on the true differentiating capabilities of the insurer. Industry cloud use-case accelerators and true insurance industry expertise are in-demand in the niche areas of product design and distribution, but the majority of the technology that underpins the rollout of insurance innovations for customer involvement and engagement, and for the interaction of the insurer and partners supporting the insured and the product, is best sourced from third parties. In this context, giving development responsibilities to business partners for use case work benefits from supporting them with sufficient guidance, strategic direction, and knowledge of business objectives and standards. Understanding the lifecycle business objectives, the human interface requirements, the preconditions of development support, business transparency needs, and the economic tolerances for losses help target development efforts for successful long-term outcomes.

References

Sousa, R., & Gonçalves, P. (2020). Cloud Computing and DevOps in the Insurance Industry: A Strategic Enabler of Innovation. Journal of Cloud Computing: Advances, Systems and Applications, 9(1), 1–12. https://doi.org/10.1186/s13677-020-00221-0

Erich, F. M. A., Amrit, C., & Daneva, M. (2017). A Qualitative Study of DevOps Usage in Practice. Journal of Software: Evolution and Process, 29(6), e1885. https://doi.org/10.1002/smr.1885

Bass, L., Weber, I., & Zhu, L. (2015). DevOps: A Software Architect's Perspective. Addison-Wesley Professional. https://doi.org/10.5555/2849240

Gruhn, V., & Schäfer, C. (2015). DevOps for Insurance IT: Enabling Agile Transformation. In: 2015 IEEE 8th International Conference on Cloud Computing, 935–940. https://doi.org/10.1109/CLOUD.2015.135

Pahl, C., & Xiong, H. (2018). Cloud-Based DevOps Automation for the Insurance Industry. In: 2018 IEEE 11th International Conference on Cloud Computing, 97–104. https://doi.org/10.1109/CloudCom.2018.00031