Management Research Studies Journal
Volume, Number (), ISSN:
https://journal.perbanas.id/index.php/mrsj

PERBANAS INSTITUTE
MRSJ
Management Research Studies Journal
E-ISSN: 2746 - 0231

Operational Continuity in the Age of Digital Insurance: Evaluating BCP and DRP Readiness in GHN System

Ridawati Justina Simanullang,[1, *] Theodorus Sendjaja[2]

[1,2] Perbanas Institute, Jakarta, Indonesia

*Corresponding author: ridawati.justina37@perbanas.id

Article history

Received:
31-05-2025

Accepted:
07-08-2025

Published:
10-10-2025

Abstract

The digital transformation in the insurance industry demands high system resilience to ensure continuous service delivery to customers. This study aims to analyze the integration of Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP) within a digital insurance system, using the Generali Hospital Network (GHN) of Generali Indonesia as a case study. Employing a qualitative descriptive approach based on a case study, the primary data is derived from the author's direct experience as a backend developer of the GHN system. The results reveal that an outage in the Kafka cloud broker caused a failure in transmitting inpatient and outpatient registration data from hospitals, disrupting the printing of key documents and hindering claim processes. The incident highlighted the absence of formal RTO/RPO documentation, lack of Kafka failover, and the absence of disaster recovery simulations. However, as part of the recovery effort, the DevOps team has implemented a monitoring system on GCP integrated with Telegram and email alerts. This study concludes that a well-integrated BCP and DRP are essential to maintaining service continuity and mitigating operational disruption in digital insurance environments.

Keywords: *Business Continuity Planning, Disaster Recovery Plan, Kafka, Digital Insurance, GCP Monitoring*

Introduction

In the era of digital transformation, modern insurance companies face new challenges and opportunities in managing their services and business processes. Information technology has become the backbone in supporting the company's operational sustainability, from policy data management, customer service, to the claims process. Especially in the life and health insurance sector, the availability of reliable and sustainable information systems is an absolute should, considering that the services provided are highly dependent on speed, accuracy, and security of information access. In this context, digital systems that support key services such as customer care registration in hospitals and participant claims submission processes must be designed to have high availability, scalability, and resilience to disruptions.

The high dependence on digital systems raises the urgent need for technology-based risk management strategies. One of the approaches used to anticipate potential disruptions is the implementation of Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP). BCP focuses on the sustainability of the overall business process in the face of unexpected events, while DRP emphasizes more on the recovery aspect of information technology and data systems after disruptions. Both are not only important in the financial sector in general, but have become particularly vital in the insurance industry, where response times to claims and participant services have a direct impact on customer reputation and trust.

Organizations in the insurance sector are required to maintain a high and reliable Service Level Agreement (SLA) at all times. Failure to meet service standards can have serious consequences, both in terms of legal, financial, and reputation. In addition, in an increasingly regulated era, many financial supervisory authorities including the OJK in Indonesia have established an obligation for insurance companies to have real documentation and implementation related to BCP and DRP. International standards such as ISO 22301 even set out in detail a framework for business continuity management, which includes risk identification, prioritization of critical services, and periodic testing of recovery scenarios. According to Cahaya et al. (2022), in digital financial services, the effective application of technology applications directly influences customer satisfaction and service continuity. In addition, OJK regulations such as POJK No.12/POJK.03/2018 emphasize the importance of digital banking and financial service readiness in ensuring fast, safe, and uninterrupted services. Therefore, the implementation of BCP and DRP is not only a technical necessity but also a regulatory imperative.

One of the insurance companies that is undergoing digital transformation is Generali Insurance Company Indonesia, which focuses on life and health insurance services. As part of its operational system modernization, Generali Indonesia developed a digital portal called Generali Hospital Network (GHN). This portal is designed to be used by hospitals in carrying out the registration process of insurance participants, both for outpatient and inpatient services. The GHN portal has two main components: a frontend developed by the vendor, and an API backend along with a database system developed and managed by the company's internal information technology team. The backend system is hosted in the cloud and connected to the claims submission system through Apache Kafka technology, which is in charge of transferring registration data in real-time from GHN to the claims processing system.

This architecture is expected to support fast, efficient, and flexible digital service processes. Nevertheless, the success of technology implementation is not only measured by the adoption of modern platforms, but also by the readiness of the system in the face of risks and disruptions. Despite adopting cloud technology and real-time data streaming, the implementation of BCP and DRP on the GHN system is not yet fully mature. This was proven when in 2025 there was an incident of disruption at the Kafka cloud broker, which caused registration data from hospitals to fail to be sent to the claims system. As a result of this incident, hospitals were unable to access participant case data, were unable to print Letters of Authorization (LOA), and were also unable to carry out the input billing process. Services have come to a complete halt, causing complaints from participants and hospitals, and creating potential reputational losses for the company.

This incident shows that the GHN system does not yet have a reliable technical recovery mechanism. There is no failover configuration for Kafka, no retry mechanism or fallback logic in the API, and no formal documentation related to the Recovery Time Objective (RTO) or Recovery Point Objective (RPO) parameters. The absence of this risk mitigation infrastructure and procedures illustrates the weak readiness of Generali Indonesia's information technology architecture in dealing with critical incidents. In fact, in the midst of digital business dynamics, companies need to have a fast, systematic, and coordinated response in restoring services in order that the impact does not spread.

From a technical point of view, the incident also marked a lack of integration between system design and IT risk management. In best practice, the system architecture used for critical services such as GHN should already include Kafka failover with multi-region replication, retry queues, and monitoring and alerting systems that is able to provide early warning of potential system failures. Meanwhile, from a procedural perspective, the absence of DR drills or disaster simulations makes the operational team not have a structured escalation and emergency response path. This causes a slow response and tends to be reactive.

Furthermore, the importance of integration between BCP and DRP is not only incidentally reactive, but should also be part of the strategic design in system development from the beginning. In the context of the insurance industry, the sustainability of digital services is an integral part of the value promised to customers. Therefore, recovery strategies should not be ad-hoc, but must be embedded in organizational culture, standardized, and tested regularly. Companies must be able to ensure that IT systems can continue to serve customers even in crisis conditions, with a clearly defined and realistic data loss recovery time and tolerance.

Based on this context, this study was conducted to analyze the extent to which the integration between BCP and DRP is applied to the digital system at Generali Insurance Company Indonesia, especially in the case of GHN system disruption. This research also aims to describe the technical challenges faced during downtime incidents, as well as formulate strategic and technical recommendations to strengthen system resilience in the future. This study was prepared with a case study approach based on the author's direct experience in the development and management of the GHN system, and enriched with a literature review from the scientific literature and best practices in the industry.

Research Methods

This research uses a descriptive qualitative approach with a case study method, which aims to dig deep into real conditions and direct experience in the field. The focus of the research is directed at the author's empirical experience as an IT Backend Developer at Generali Insurance Indonesia, who is actively involved in the process of developing, integrating, and maintaining the API backend system for the Generali Hospital Network (GHN) digital portal. The GHN portal is used by hospitals to carry out the outpatient and inpatient registration process for insurance participants, as well as being the starting point for the process of submitting cashless claims digitally.

The data in this study is divided into two main categories, namely:

1. **Primary data**, obtained directly through the author's involvement in day-to-day technical activities, including system development, system monitoring, troubleshooting, as well as handling of tampering incidents on Kafka integration and GHN backend APIs.
2. **Secondary data**, which is in the form of academic literature, scientific journals, and other reliable sources related to the concept and implementation of Business Continuity Planning (BCP), Disaster Recovery Plan (DRP), information technology risk management, as well as cloud-based service architecture and event streaming such as Apache Kafka.

The data collection technique is carried out through three main approaches, namely:

1. **Participatory Observation**
   The author is directly involved in the process of developing and maintaining the GHN system, which provides access and comprehensive understanding of the technology architecture structure, communication schemes between systems, as well as the business processes involved in the registration system and participant claim submission process system. This experience is the main foundation for analyzing incidents, team responses, and the effectiveness of existing system security.
2. **Internal Documentation Study**
   The authors analyze technical documents such as Kafka configurations, architectural diagrams, system logs, and downtime incident reports. Although these documents cannot be attached to the publication because they are internal and subject to the company's confidentiality policy, the important information from the documents is presented narratively in support of the validity of the findings.
3. **Literature Review**

Scientific literature and academic references are used to build a conceptual framework and compare field findings with the results of previous research. This literature covers international standards such as ISO 22301 for business continuity management, IT disaster recovery principles, and best practices in applying Kafka in enterprise cloud environments.

A. Business Continuity Planning (BCP) dan Disaster Recovery Plan (DRP)

Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP) are two key pillars in an organization's resilience strategy, especially in the face of operational disruptions caused by disasters, system failures, or other unexpected incidents. BCP refers to a set of policies and procedures designed to ensure that critical business functions is able to continue to run or be restored in the shortest possible time during and after a crisis occurs. BCP's main focus is to maintain service continuity, minimum required operations, and the sustainability of the company's overall business value. Meanwhile, DRP is a sub-component of BCP which specifically focuses on the recovery of information and data technology systems. DRP covers technical aspects such as data replication, system failover, backup, as well as server recovery strategies and other digital infrastructure. In a complex and interconnected digital environment, DRP is a vital part of the tactical response to technological incidents.

According to Patel and Keerthana (2019), integration between BCP and DRP is essential to form a framework that is responsive to disruption. Without coordination between business strategy and technology recovery, companies risk losing important data, revenue, and trust from customers. The two cannot run apart; The BCP specifies what should be restored, while the DRP explains how to restore it technically.

Further, a case study by Redjack (2025) emphasizes that companies in the financial services and insurance sectors face unique challenges in terms of continuity of service, as they serve clients in time-sensitive real-time scenarios. The research shows that effective BCDR (Business Continuity and Disaster Recovery) planning, compiled based on data and regular testing, is able to accelerate the post-crisis recovery process and minimize business impact. Companies that successfully recover their services quickly are not only because they have a robust infrastructure, but because they implement holistic BCP-DRP planning, encompassing technical, procedural, and managerial strategies.

In the context of digital insurers such as Generali Indonesia, the integration of BCP and DRP has become increasingly important as digital services become the spearhead of operations, and even a small disruption can have a far-reaching impact on customer reputation and experience. Therefore, BCP and DRP should not be seen as mere administrative documents, but as a living framework that should be tested and improved regularly.

B. Recovery Time Objective (RTO) dan Recovery Point Objective (RPO)

The Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) are two fundamental metrics in Disaster Recovery Plan (DRP) planning that determine how quickly and how much data is able to be recovered after an outage occurs. RTO refers to the maximum time that an organization tolerates to restore a service or system after an incident, while RPO describes the maximum amount of data that can be lost, measured in units of time, from the last point of backup to the time of failure. The determination of RTO and RPO is critical in building a realistic and measurable recovery framework. A low RTO value usually indicates that the system is critical and requires instant remediation, such as a digital claims service or medical registration portal. Meanwhile, RPO serves as the basis for determining the frequency of data backups and system replication strategies. Both of these metrics should be tailored to the business needs and technology capacity of the organization.

According to Druva (2025), RTOs and RPOs are not just numbers in white papers, but are integral parts of strategic decisions that help organizations choose cloud-based, hybrid, and on-premise recovery solutions. In the context of digital transformation, a deep understanding of these two parameters helps IT management balance between the risk of data loss and recovery costs.

Case studies of various companies show that failure to clearly define RTOs and RPOs often leads to delayed responses, confusion during crises, and large financial impacts. Therefore, periodic testing of RTO and RPO assumptions is a best practice recommended by various international standards, such as ISO 22301.

C. The Use of Apache Kafka in the Insurance Industry

Apache Kafka is a large-scale event streaming platform that has been widely adopted by companies in the digital insurance sector to facilitate real-time data processing. This system allows for fast and asynchronous exchange of information between microservices, such as customer registration, medical service authorization, and claim verification processes. Kafka's publish-subscription-based architecture is well suited to modern insurance systems that require high scalability and cross-entity system integration.

According to Waehner (2021), Kafka not only speeds up the flow of internal data, but also allows insurers to build predictive and responsive services, such as automated claims notifications or fraud detection based on streaming data. Its use cases have evolved from just log aggregation to the backbone for mission-critical transaction systems. However, the use of Kafka also brings its own challenges. Kafka does not by default provide cross-region disaster tolerance, so in a large-scale production environment such as an insurance company, advanced configuration is required to guarantee system availability. Confluent (2025) recommends the implementation of Kafka in multi-datacenter mode or multi-region replication as a disaster recovery strategy, with an active-passive or active-active failover architecture. This practice not only prevents data loss when a disaster occurs, but it also supports rapid recovery scenarios without disrupting ongoing services.

In the context of Generali Indonesia's GHN system, Kafka functions as a link between hospital registration and digital claims systems. Therefore, the implementation of HA (high availability) strategies, automatic failovers, and Kafka performance monitoring are very important to ensure the continuity of the service process of insurance participants.

Results and Discussion

GHN (Generali Hospital Network) is a digital portal for Generali Indonesia that is used by hospitals to register inpatient and outpatient insurance participants. This portal plays an important role in the initial process of submitting a health insurance claim. The GHN system consists of two main components, the Frontend, which is developed by external vendors and used by hospitals, and the Backend API, which is developed by the internal team of Generali Insurance Company Indonesia, including the authors. The API backend is used to retrieve policy and participant data from the Generali Indonesia Company's database system, retrieve participant treatment data at hospitals, as a medium for the transfer of care registration data input, billing data from the GHN (Generali Hospital Network) portal to the database system and claim submission process system of Generali Insurance Indonesia Insurance Company. The data input by the hospital through the GHN portal is sent to the claim submission process system through Apache Kafka technology. The database infrastructure and backend APIs are already cloud-based, in line with the Company's digitalization strategy since 2024.

In a period in early 2025, there was a disruption in the Kafka cloud that caused registration data from hospitals to not be sent to the claims processing system. Because the frontend system relies on data responses from the backend, hospitals cannot conduct data inquiries of active participant cases, enter patient billing, print Letters of Authorization (LOA), or print statement letters. As a result of this incident, many participants and hospitals submitted complaints because the claim registration process service at the hospital could not be used. The analysis indicates several weaknesses in the system, where there is no Kafka failover, there exists no retry mechanism or local buffer in the API, and no DRP scenario has been implemented in real terms. There is no RTO/RPO documentation and no disaster recovery drill is conducted.

Table 1. System Readiness Analysis for Key Components of BCP and DRP

Component	Current Status	Findings
RTO and RPO	Not formally documented	No reference recovery time or data loss tolerance
Kafka High Availability	Not applied	System fails completely when Kafka gcp goes down
DR simulation	Never done before	No interference scenario testing
Monitoring & Alerting	Limited	No alert when Kafka gcp is unresponsive
Fallback Mechanism in API	Not available	There is no buffering or circuit breaker.

Source: Internal analysis based on the author's experience (2025).

The case of a glitch on the Kafka Google Cloud Platform (GCP) in the GHN system reveals the weakness of the system in the face of unexpected incidents that directly impact critical services. This unpreparedness is characterized by the absence of redundant infrastructure, such as multi-node Kafka clusters or inter-zone replication, which causes the entire hospital registration process to stall when Kafka goes down. In addition, the backend API lacks fallback mechanisms such as retry queue or buffering, so data fails to be delivered without a workaround. Recovery simulations have also never been carried out, with the absence of documented RTOs and RPOs, making the response to disruptions slow and unstructured. As a fix, the DevOps team has implemented a real-time monitoring dashboard on Google Cloud Platform (GCP) that provides automatic alerts via Telegram and email when potential downtime occurs. To strengthen the system in the future, it is recommended to implement Kafka HA, API retry mechanisms, DRP training, as well as strengthening monitoring based on technical metrics and service map visualization as part of the early detection and periodic evaluation system.

Conclusion and Recommendations

This research confirms that in the era of digital insurance that relies heavily on cloud-based systems and microservice architectures, such as the GHN (Generali Hospital Network) system, the evaluation of the readiness of Business Continuity Planning (BCP) and Disaster Recovery Plan (DRP) is the key to ensuring operational continuity. A case study conducted on Generali Indonesia's GHN system showed that the incident of disruption in the Kafka cloud broker significantly hampered the main service processes, including participant registration, LOA printing, and claim submission, due to the unavailability of Kafka failover, the absence of fallback on the backend API, and the absence of RTO/RPO or DR drill documentation.

Based on the results of system evaluation and literature review such as Patel & Keerthana (2019), Redjack (2025), and Kesa (2023), it can be concluded that operational readiness does not only rely on the technology used, but also highly depends on the extent to which the organization has adopted the BCP–DRP framework as a whole. The research emphasizes that the integration between business strategy and technical solutions is the foundation in accelerating the post-crisis service recovery and minimizing business impact. Meanwhile, Druva (2025) and ISO 22301 emphasized the importance of establishing and periodically testing the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) parameters, to ensure recovery speed and data loss tolerance limits according to business needs.

In the context of technology, the literature from Waehner (2021) and Confluent (2025) provides evidence that the application of Apache Kafka to mission-critical systems such as GHN, must be complemented by a multi-region replication, automatic failover, and real-time monitoring architecture. Without this configuration, the system will be highly vulnerable to downtime, which has a direct impact on customer reputation and trust.

Thus, the results of this study conclude that the evaluation of BCP and DRP readiness cannot be separated from the system design from the beginning. Generali Indonesia's GHN system requires strategic and technical improvements that include formalizing RTO/RPO, improving Kafka infrastructure, periodic DR drill training, and strengthening metric-based monitoring. These measures are important to ensure that the insurance digital service system can continue to operate even in disruptive conditions, and to ensure operational continuity that is standard in the modern financial industry.

References

Waehner, K. (2021). Apache Kafka in the insurance industry: Use cases and architectures for event streaming. Retrieved from https://www.kai-waehner.de/blog/2021/06/07/apache-kafka-insurance-industry-use-cases-architectures-event-streaming/

Clumio. (2023). The importance of Recovery Point Objective (RPO) in your Business Continuity Plan. https://clumio.com/rto/the-importance-of-recovery-point-objective-rpo-in-your-business-continuity-plan/

Confluent. (2025). Disaster recovery for multi-datacenter Apache Kafka deployments. Retrieved from https://www.confluent.io/blog/disaster-recovery-multi-datacenter-apache-kafka-deployments/

Druva. (2025). Understanding RPO and RTO: Definitions and differences. Retrieved from https://www.druva.com/blog/understanding-rpo-and-rto

Herbane, B. (2010). Small business research: Time for a crisis-based view. International Small Business Journal, 28(1), 43–64. https://doi.org/10.1177/0266242609350804

Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. World Journal of Advanced Research and Reviews, 18(3), 970–992. https://doi.org/10.30574/wjarr.2023.18.3.1166

Corrales-Estrada, A. M., Gómez-Santos, L. L., Bernal-Torres, C. A., & Rodriguez-López, J. E. (2021). Sustainability and resilience organizational capabilities to enhance business continuity management: A literature review. Sustainability, 13(15), 8196. https://doi.org/10.3390/su13158196

Patel, J. S., & Keerthana, V. (2019). Disaster recovery in business continuity management. International Journal of Trend in Scientific Research and Development, 3(4), 319–322. https://doi.org/10.31142/ijtsrd23607

Redjack. (2025). Case study: Financial services and insurance - Improving cyber resilience with BCDR. Retrieved from https://redjack.com/resources/case-study-financial-services-and-insurance

Waehner, K. (2021). Apache Kafka in the insurance industry: Use cases and architectures for event streaming. Retrieved from https://www.kai-waehner.de/blog/2021/06/07/apache-kafka-insurance-industry-use-cases-architectures-event-streaming/

Widodo, H. (2020). Case study of business continuity plan and disaster recovery plan for banking industry in Indonesia. Jurnal Teknik Industri, 21(2), 120–129.

Fitriawati, D., Sumarwan, U., & Prihandoko, A. C. (2021). IT disaster recovery plan dalam mendukung business continuity plan saat terjadi force majeure. Jurnal Sistem Informasi dan Bisnis Cerdas, 10(1), 50–57.

Muslimin, A., & Harjanto, N. (2022). Business impact analysis sebagai bagian dari perencanaan keberlangsungan bisnis pada perusahaan perbankan. Jurnal Ilmu Komputer dan Sistem Informasi, 10(3), 214–222.

Zaharia, M., Das, T., Li, H., Hunter, T., Shenker, S., & Stoica, I. (2016). Discretized streams: Fault-tolerant streaming computation at scale. Communications of the ACM, 59(11), 61–71. https://doi.org/10.1145/2984012

Cahaya, Y. F., Widyarsih, A. V. R., & Marlina, R. L. (2022). Customer service analysis, application of technology applications, product variations on customer satisfaction (Study on Livin by Mandiri KCP Jayapura Business Center Products). *Management Research Studies Journal, 3*(2), 58–67. https://journal.perbanas.id/index.php/mrsj