Ensuring Compliance Across Controlled Groups: A BPMN-Based Approach

https://www.doi.org/10.56830/WRBA11202503

Sandeep Kumar Biradhara Nanagowda
Principle Software Engineer, NC, USA
Email: sandeepkumarnbs@gmail.com

Received September 16, 2025 Accepted October 25, 2025 Published November 11, 2025

Abstract

Compliance obligations for controlled groups collections of subsidiaries and affiliated entities under common ownership are increasingly complex in today's regulatory environment. Traditional approaches to managing compliance rely on fragmented processes, manual interventions, and siloed systems, which expose organizations to operational risk, reporting delays, and audit deficiencies. This paper presents a BPMN-based (Business Process Model and Notation) approach to modeling and automating compliance workflows across controlled groups. By leveraging BPMN as a standardized language, financial institutions and multinational enterprises can design transparent, auditable, and automation-ready processes that ensure consistent application of compliance rules across entities.

The paper highlights three critical dimensions of compliance reliability error rate minimization, reprocessing success, and audit completeness and illustrates how BPMN modeling supports these through retry mechanisms, compensating transactions, and full execution traceability. Practical scenarios, such as group-level regulatory filings, consolidated risk assessments, and distributed KYC checks, are used to demonstrate how BPMN-based models enhance accuracy, scalability, and resilience. Ultimately, this approach empowers organizations to achieve regulatory alignment, operational efficiency, and transparency, while reducing compliance risk and meeting the stringent expectations of global regulators.

Keywords: BPMN (Business Process Model and Notation), Compliance Reporting, Workflow Orchestration, Reliability and Accuracy, Audit Completeness, Compliance-as-Code, Process Automation.

1. Introduction

Regulatory bodies worldwide are placing increasing emphasis on ensuring that compliance procedures remain uniform, transparent, and fully auditable within groups of companies under common ownership. For banks, financial institutions, and multinational corporations, managing compliance at this scale presents significant challenges. Institutions often rely on disparate systems for routine tasks, while manual or semi-automated reporting and entity-specific workflows frequently lead to inconsistencies, increased risk of errors, and incomplete audit trails.

This is where Business Process Model and Notation (BPMN) can make a real difference. BPMN provides a standardized, visual way to design and document processes. Because it is both machine-executable and easy for humans to understand, it acts as a bridge between technical teams, business stakeholders, and regulators. Workflows BPMN to compliance with business processes across subsidiaries and affiliates helps ensure that critical activities like regulatory filings, risk assessments are carried out in a consistent manner across the entire organization.

1.1 **Problem Statement**

Organizations that operate as controlled groups (multiple entities under common ownership) have great difficulties in keeping their compliance reporting consistent and auditable. Existing systems often fall short in several ways. Automated tasks are prone to errors, frequently caused by temporary failures or mismatched system integrations. Many platforms lack the robust retry or compensation mechanisms needed to recover seamlessly (Benchmarks, 2025). When workflows do fail, recovering the workflow is often low as most systems do not provide automated recovery causing issues with robust reporting ((SOAPs), 2025). Above this compliance processes are often distributed across different entities which causes problems in creating a consistent and consolidated report which in turn increases regulatory risk (software, 2024).

With increase in regulatory norms each day, the legacy approach creates an expensive and resource intensive systems which are error prone. To overcome most of these inconsistencies, Business Process Mondel and Notation provides a way to standardize the workflows which are automated, auditable, recoverable and consistent across systems.

1.2 **Objective of the Study**

The goal of this study is to show how BPMN based modeling can be applied to compliance processes in controlled groups to make regulatory reporting more reliable, transparent, and consistent. Some of the common issues faced by institutions could be overcome by standardizing workflow mechanism that can handle failed retry and compensation mechanism which is an integral part of BPMN. BPMN tools have a inbuilt ability to retry failed tasks as well as run compensation workflows depending on the kind of failure. BPMN tool engines have inbuilt tracing mechanisms to record and track task beginning and completion along with metadata required to rebuild the whole workflow path on a need bases. This provides great capability of audit trails which can be used for reporting and tracking purposes.

1.3 Literature Review

BPMN (Business Process Model and Notation) has become the standard way to describe business workflows that are readable and executable. BPMN specification is maintained by Object Management Group (OMG) (BPMN-Business, (nd)). It was designed to act as a common language that is understood by business teams and technical systems, allowing processes to be modelled by business teams and automated consistently across organizations by the technical teams. The official specification and supporting guides emphasize clear notation, executable models, and alignment across stakeholders. These qualities make BPMN especially valuable in regulated industries, where transparency and precision are essential (Wazlawick, 2024). Within BPMN-based automation, reliability mechanisms such as retries, error events, and compensation are well documented. In Camunda 8/Zeebe, practitioners can define retry strategies per service task and handle deviations via BPMN error events; long-running transactional consistency is addressed through the Saga pattern and

BPMN compensation/compensation handlers. These patterns reduce effective error rates and enable robust reprocessing in distributed architectures (Developers, 2024). For auditability and transparency, the data governance literature stresses complete lineage and audit trails. Lineage platforms (e.g., Atlan) detail how end-to-end flow/transformations enable root-cause and impact analysis and support regulatory audits, vendor docs and guides frame lineage as essential evidence for compliance. In parallel, observability and audit-logging guidance (e.g., Splunk) describes best practices for capturing who/what/when/where and delivering scalable dashboards for compliance programs. Together, these works situate lineage, audit logs, and observability as the backbone of "audit completeness" (Lineage, (nd)).

2. Material and Methods

2.1. Architecture

2.1.1 Layers & Key Responsibilities

A compliance reporting system for controlled groups can be conceptualized as a multi-layered architecture, with each layer having distinct responsibilities and supported by BPMN-based orchestration.

At the Presentation and API layer, the system exposes dashboards, tasklists, and APIs for human interaction, reporting views, and regulatory submissions. This layer validates incoming requests and enforces authentication and authorization. The Orchestration and Workflow layer is the heart of the system, where BPMN models are executed by workflow engines such as Camunda 8 (Zeebe). This is where the processing logic, failure retry/ compensation and exception handling is done (Architecture, (nd)). The Business Logic/ Domain layer contains the actual compliance rules and validation logic. This is mostly made of microservices which handles one to many compliance tasks and are triggered by the orchestration engine as needed. The integration and connector layer interacts with external systems. It takes care of translating data formats, handling different communication protocols, and applying techniques like automatic retries or circuit breakers to keep processes stable even when systems fail temporarily. Camunda provides a connector framework to standardize these (Lingamallu & F. Oliveira, 2025).

Underneath these layers is the Persistence and Data layer. It keeps track of the workflow state, compliance data, and detailed audit trails for each workflow being executed. The reliability of audit reporting depends heavily on how well this layer can capture the data lineage (where the data came from and how it was transformed) and the decision traces (why certain choices were made along the way). To meet this need, organizations often rely on specialized platforms like Atlan, which provide strong data lineage and governance capabilities. Intercepting all layers is the Observability, Logging, and Audit trail (Connectors, (nd)). This keeps the system transparent and accountable. Each activity on the platform is tracked and recorded with timestamp. Enabling the microservices to emit the logs to a monitoring tool like Splunk (Lingamallu & F. Oliveira, 2025), will help teams create dashboards and troubleshoot issues as and when they come up. Having proper authentication and authorization in each module will act as a safeguard to the systems involved. This makes sure who can access the system and what they are allowed to see or do in the system. These governance measures ensure that compliance obligations are not only met but also applied uniformly across different systems (Chen, Yang, Chen, & H. Jiao, 2022).

The Reprocessing and Recovery layer is designed to make the system more resilient by automatically retrying failed tasks, triggering compensating workflows as needed (Guide, (nd)). This also allows manual exception handling/ intervention as needed. This approach follows industry best practices, which recommend achieving at least a 95% recovery rate for failed workflows. All this runs on top of the Platform and Infrastructure layer which is key for a robust and scalable system. Technologies like Kubernetes clusters, service meshes, Apache Kafka, and disaster recovery mechanisms ensure that compliance systems can handle large volumes of data while remaining stable and reliable (Self-Managed, (nd)). Together, these layers form a robust, transparent, and auditable compliance reporting architecture. By design, they address error rate, reprocessing success, and audit completeness.

2.1.2 Typical Flow

Let’s have a look at a typical flow for a BPMN centric compliance set up.

Data sources are typically systems that collect or generate data that needs to be consumed by different systems (Orchestration C. M., 2020). Data source systems can emit messages to Change Data Capture systems which can be put onto a event streaming bus like Apache Kafka. Any integrating system interested in consuming the message can subscribe to this message and consume to start processing on their end. A workflow engine like Camunda (BPMN compliant tool) works as a guide to coordinate different steps in a structured manner. This will have different validation steps, routing, SLAs, retries, and compensation to handle failures gracefully.

The workflows invoke microservices for enrichment of data, run validation and rules (DMN) against the data and integrate with external systems (like risk, regulator APIs). One also has a flexibility to use DROOLS (Ikegwu, Nweke, Anikwe, Alo, & O. R. Okonkwo, 2000) as there rule engine as well instead of Camunda DMN. Drools is a high-performance, open-source business-rules management system (BRMS) written in Java, enabling organizations to externalize decision logic from application code and execute complex rule flows with full support for Decision Model and Notation (DMN) (Goossens, Smedt, & J. Vanthienen, 2023).

Results persisted in a data lake/warehouse set up with immutable audit logs. Meta data related to each step in the process could be queried and used in reports as needed.

BI dashboards are produced using the persisted data and regulatory submissions are sent to portals/gateways depending on the use case.

Observability module handles metrics, logs and traces while Security/Governance module operate across all layers. The platform (like Kubernetes) provides scalability and resilience for the system.

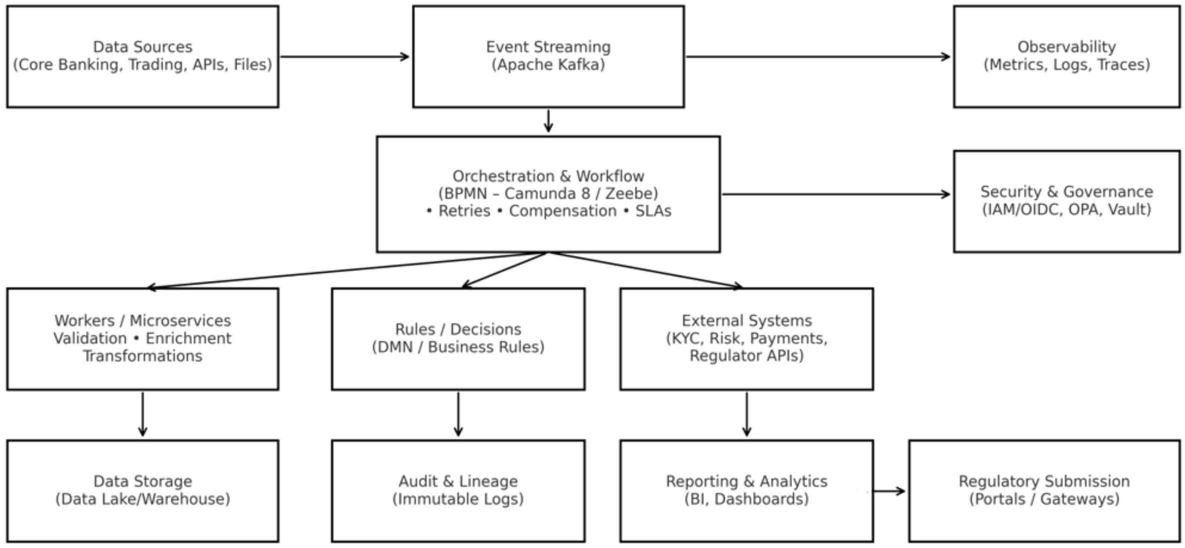

Figure 1. Overview of a standard BPMN environment

2.2 Implementation

The implementation of a BPMN-based compliance reporting system for controlled groups begins with defining BPMN 2.0 models that represent end-to-end workflows such as entity-level validation, group aggregation, exception handling, and reprocessing (Polančič & B. Orban, 2023). These models make use of gateways, subprocesses, compensation, and error events to build in reliability and recovery logic. A governance process for versioning and change management ensures that BPMN workflows are tested and deployed consistently, while DMN (Decision Model and Notation) can be added to capture complex business rules (Leoni, Felli, & M. Montali, 2021). The next step is to set up the workflow engine, typically Camunda 8 (Zeebe). A Zeebe cluster consists of brokers, gateways, and exporters, and can be deployed in a self-managed or cloud environment. Clients and microservices communicate with Zeebe via gRPC or REST APIs to deploy workflows, start process instances, and activate jobs.

To execute the actual business logic, worker microservices are implemented to subscribe to BPMN service tasks (Kocher, Miguel, & A. Fay, 2022). These services handle validations, transformations, KYC checks, and external API calls. Workers should be idempotent, handle retries and errors and enable BPMN error events or compensations when required. At the same time, connectors or adapters integrate the orchestration engine with external systems and regulatory APIs. Many implementations combine BPMN orchestration with an event-driven backbone such as Kafka, creating a hybrid orchestration–choreography pattern that balances reliability with loose coupling (Self-Managed, (nd)). Reliability is further supported through retry policies, compensation events, and reprocessing logic modeled directly in BPMN. Failed tasks can be retried automatically, rolled back through compensation, or recovered manually using administrative tools (Lopes & S. Guerreiro, 2023). This supports high reprocessing success rates, which are critical for compliance reporting.

Equally important is observability, audit, and lineage tracking. All workflow events, variable history, and decision traces are exported to monitoring platforms such as Prometheus, Grafana, Elasticsearch, or Splunk. These tools provide dashboards and alerts to track key KPIs like error rates, SLA breaches, and recovery metrics, while ensuring that regulators have access to full audit trails.

Finally, the system is deployed on a resilient platform and infrastructure layer, typically using Kubernetes with high availability, service mesh, and autoscaling. Zeebe clusters can be partitioned to scale throughput, and BPMN updates can be deployed using blue/green or canary strategies. Disaster recovery, backup, and monitoring round out the operational setup (Orchestration C. M., 2020) (Concepts, (nd)). All the systems together (BPMN modeling, workflow orchestration, microservices, event-driven patterns, observability and governance) provides a robust compliance architecture.

2.2.1 Metrics (Evaluation Criteria)

The effectiveness of a BPMN-based compliance system can be measured through three key metrics (Drools, (nd)). The first is the error rate of automated tasks, which tracks how often workflow steps fail during execution. As per industry standards this value should be less than 2. With retry mechanisms and compensation logic the actual impact of failures to close to zero. The second metric is the reprocessing success rate. This shows how well the system can recover from failures. Industry benchmarks suggest aiming for at least 95% successful recovery (through automated retries or compensating workflows that keep reporting processes on track).

The third is audit completeness to ensure every workflow produces a full record of its execution. This includes both data lineage (where the data came from and how it was transformed) and decision traces (why certain decisions were made). Together, these records provide the transparency needed to build reliable system.

2.2.2 Scope and Limitations

The scope of this study is to explore how BPMN-based modeling can be applied to compliance reporting in controlled groups. Multiple entities under common ownership must navigate complex and overlapping regulatory obligations. The focus is on how workflows can be designed, orchestrated, and automated using BPMN (supporting technologies like Camunda) The study also looks at how these workflows connect with external systems like regulatory APIs, and data warehouses. This also addresses the overall need for observability, governance and security. While BPMN provides a standardized modeling language, its success depends on the maturity of an organization’s IT infrastructure and governance processes. Institutions with legacy systems that lack strong integration capabilities may see fewer benefits from orchestration in general. The analysis focuses mainly on technical workflows and process reliability. Broader organizational challenges such as regulatory interpretation, change management, or staff training are not handled in this study. Tshe scenarios assume access to modern platforms, containerized environments, and observability tools, which may not be realistic for every organization.

3.1 Operational Performance KPIs

Below are some of the key’s metrics to look for in Operational Performance KPI.

System throughput is a measure of how much workflow the systems can process in each unit of time. This gives an idea of how the system will cope with heavy loads. Since compliance systems can undergo a lot of loads during certain window time frames it’s essential that the system should handle varied amounts of data with ease. Benchmarks from tools like Camunda show that modern workflow engines can maintain strong throughput even under stress.

Latency is a message of how quickly a workflow completes its execution. Though it’s normal to have a workflow that runs from few seconds to days (depending on the different steps involved), its essential that it completes each transaction within the workflow in a more consistent manner. Any failed transactions within the workflow will be retried as part of the workflow engine framework. This makes sure that not a lot of time gets lost during error scenarios (Medium, (nd)).

Resource allocation and utilization are another key factor in any IT system. Efficient resource allocation and utilization will reduce the operational cost as well as make sure that the system is reliable to handle load and failures. Using Kubernetes in a distributed environment is useful as it can be scaled up quickly.

Together, these three KPIs throughput, latency, and resource utilization, ensure that compliance reporting platforms remain reliable, scalable and cost-efficient.

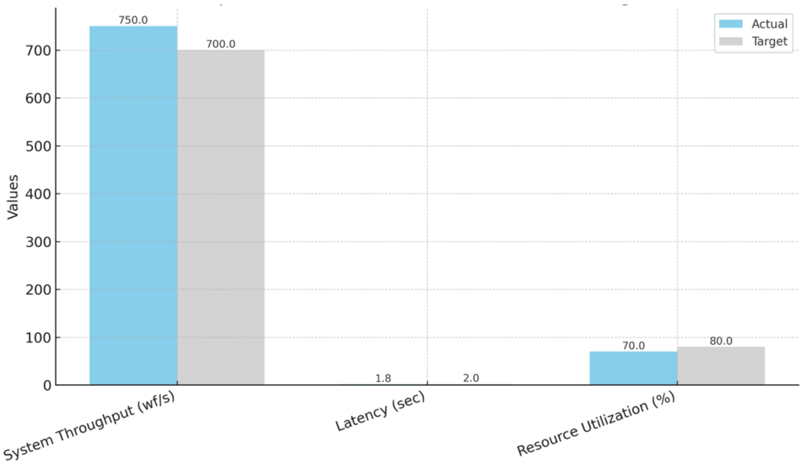

Figure 2. Operational Performance KPI’s – Actual vs Target

3.2 Efficiency Gains KPIs

Efficiency gains in BPMN-based compliance reporting systems can be measured across three important metrics.

The first is automation coverage. This reflects the percentage of workflows that run end-to-end without human intervention. The higher this number, the more consistent the results are. Lower the chance of human error and the faster the reporting cycles. Automation rates above 80% could be achieved by BPMN and workflow automation tools like Camunda (Orchestration W. i., (nd)).

Another metric to track is the manual effort involved in completing the tasks. This could be tracked used how many man hours and needed to complete a compliance reporting task. By automating the tasks like gathering the data, running validations on the collected data, implementing error handling and retry mechanism in the workflow, the manual effort could be brought down to a minimum. This will help in reducing human error as well as allowing the knowledge workers to focus on oversight and analysis (Orchestration W. i., (nd)). Though it could be costly to set up the initial workflow for compliance purposes, and when the automation coverage increases and manual effort decreases the cost per workflow will decrease. This will also deliver long-term efficiency.

3.3 Reliability & Accuracy KPIs

Reliability and accuracy are prerequisites for any system let along compliance systems. They make sure that the workflows run as intended and any regulatory submissions happen on time with zero errors. This is achieved by keeping the failed task to a minimum during workflow execution. With the help of auto retries or compensation mechanisms, one can achieve an error rate of less than 2%. Camunda platform provides automatic retry as well as compensation workflows that will make the applications robust and reliable (Automation C. B.–P., (nd)). The second metric is the reprocessing success rate, 95%, and above is the industry accepted success rate. This measures how many workflows are completed successfully. The workflows could be completed either without fail, or with retries or with compensation mechanisms. These options will make sure that the workflows complete successfully even when the underlying systems experience stability issues. The third metric is audit trails. Any BPMN compliant Workflow engine will persist its state at each level along with any other metadata that is needed by the applications. This data could be queried to generate or to be used in any reporting as part of audit trails. With all the of the above-mentioned metrics will determine the accuracy and robustness of the systems.

3.4 Scalability KPIs

Any system needs to be designed to handle increased amount of data volume for a prolonged period and not break. Though there could be lean periods where there is not much activity on the system, there could be periods where there is extreme amount of load on the system during any deadline. If the systems were broken or behaved in an inconsistent way during those periods, that will cause financial loss to the institutes. Hence, it’s of utmost importance that the system can scale up and handle the volume as needed. BPMN compliant workflow engines like Camunda show linear scalability in clustered environments. This makes it highly effective to set up large scale compliance workloads. By making use of Kubernetes the system can scale up quickly to handle incoming load. Kubernetes provides ways in which the scale up can happen dynamically based on the load without any human intervention which makes it best suited for mission critical applications. The last metric for scalability is concurrency. This measures how many workflows can run in parallel without affecting the overall performance of the system. An orchestration engine has inbuilt message management capability, co-related capabilities and coordination with distributed systems capability. This makes it a better choice compared to a purely choreographed approach.

4. Challenges and Risks

Many of the financial institutions still have legacy systems like mainframes and applications that lack modern APIs. This is one of the biggest challenges to integrate this with BPMN workflows with critical compliance processes. This integration efforts would become costly and time consuming to implement. This will affect efficiency adversely (Automation, (nd)). Getting proper scalability across platforms could become increasingly complex or costly. Even if the BPMN infrastructure is built for high throughput, if the integration systems need to cope up with the high volume if not will face higher latency, bottleneck which will reduce the reliability. Any compliance applications deal with sensitive information (data that is classified as highly confidential personal information). With robust authentication, authorization, encryption, audit trail institutions risk noncompliance penalties.

Transitioning from manual, ad-hoc compliance processes to BPMN-driven automation often requires significant staff training, stakeholder buy-in, and cultural change. Resistance to automation, particularly in highly regulated industries, may slow adoption and dilute the potential benefits

5. Future Perspective and Strategic Recommendations

Looking ahead, BPMN-based compliance modeling is poised to play an increasingly central role in the digital transformation of regulatory reporting. As compliance obligations expand in both volume and complexity, scalability, automation, and transparency will remain critical priorities for financial institutions. Emerging technologies such as AI-driven anomaly detection and predictive analytics are expected to complement BPMN workflows, allowing organizations to proactively identify risks, anticipate compliance breaches, and optimize process performance (Concepts C. D.–Z., (nd)). From a strategic standpoint, organizations should prioritize cloud-native deployment models for their BPMN engines to enable elastic scaling and global accessibility. Platforms like Camunda 8, when combined with container orchestration frameworks such as Kubernetes, will allow firms to handle fluctuating reporting demands while maintaining resilience and cost efficiency. A second strategic recommendation is the adoption of “compliance-as-code” principles, where regulatory requirements are codified directly into executable BPMN and DMN models. This shift helps reduce interpretation errors and speeds up the implementation of regulatory changes. This also provides auditable evidence of how compliance logic is applied. Using this approach institutions can get to more adaptive compliance landscape that aligns with evolving regulations (Challenges, (nd)). Looking forward to the future of compliance points to cloud-native, model driven AI- augmented systems.

6. Conclusions

This paper shows how BPMN based modeling can be applied to compliance in controlled groups to improve reliability, accuracy, efficiency and scalability. Since the compliance rules are directly embedded in workflows which have built in features to handle audit trail/ retry/ reprocess/ compensation mechanism, error rates, improved recovery of failed task and traceability is achieved. The analysis highlights that a BPMN compliant workflow engine like Camunda provides a strong foundation for a resilient, traceable, scalable compliance systems. With key KPI’s such as automation coverage, latency and resource utilization, entities can measure efficiency games along with cost reduction. It also talked about some of the challenges faced in integrating with legacy systems which causes issues with governance, scaling and organizational resistance. A good governance model, security controls, effective change management and a robust technical landscape is what is needed to overcome this. BPMN-based compliance modeling provides a forward-looking path for financial institutions facing growing regulatory complexity. By adopting model-driven, cloud-native and auditable compliance frameworks, organizations can shift compliance from being a reactive burden to a strategic capability.

References:

Architecture. ((nd)). *(https://docs.camunda.io/docs/components/zeebe/technical-concepts/architecture/)*.

Automation, C. B.–P. ((nd)). *(https://camunda.com/blog/)*.

Automation, D. –T. ((nd)). *(https://www.deloitte.com/us/en/pages/risk/articles/automation-in-compliance.html)*.

Benchmarks, C. (2025). *(https://camunda.com/blog/2025/02/state-of-zeebe-performance)*.

BPMN-Business, P. M. ((nd)). *https://www.omg.org/spec/BPMN/2.0.2/About-BPMN)*.

Challenges, G. –O. ((nd)). *(https://www.gartner.com/en/information-technology/glossary/legacy-system)*.

Chen, Z., Yang, J., Chen, L., & H. Jiao. (2022, Mar.). *"Garbage classification system based on improved ShuffleNet v2,"* . Retrieved from Resources, Conservation and Recycling: vol. 178, p. 106090, Available at: https://doi.org/10.1016/j.resconrec.2021.106090

Compliance-to-Code: Enhancing Financial Compliance Checking via Code Generation. (2025). *(https://arxiv.org/abs/2505.19804)*.

Concepts, C. D.–T. ((nd)). *(https://docs.camunda.io/docs/components/zeebe/technical-concepts/technical-concepts-overview/)*.

Concepts, C. D.–Z. ((nd)). *(https://docs.camunda.io/docs/components/zeebe/technical-concepts/technical-concepts-overview/)*.

Connectors, A. D.-D. ((nd)). *(https://camunda.com/blog/2023/06/architecture-connectors/)*.

Developers, E. t. (2024). *(https://camunda.com/blog/2024/12/exploring-the-new-features-in-camunda-8-for-java-developers/)*.

Drools. ((nd)). *(https://docs.drools.org/latest/drools-docs/drools/release-notes/index.html)*.

Goossens, A., Smedt, J. D., & J. Vanthienen. (2023). "Extracting Decision Model and Notation models from text using deep learning techniques,". *Expert systems with applications*, vol. 211, pp. 118667–118667, Jan. 2023, Available at: https://doi.org/10.101/j.eswa.2022.118667.

Guide, A. L. ((nd)). *(https://www.splunk.com/en_us/blog/learn/audit-logs.html)*.

Ikegwu, A. C., Nweke, H. F., Anikwe, C. V., Alo, U. R., & O. R. Okonkwo. (2000). "Big Data Analytics for data-driven industry: a Review of Data sources, tools, challenges, solutions, and Research Directions,". *Cluster Computing*, vol. 25, no. 2, Mar. 2022, Available: https://link.springer.com/article/10.1007/s10586-022-03568-5.

Industry, H. I. (2025). *(https://www.straive.com/blogs/how-intelligent-automation-is-reshaping-the-banking-industry-in-2025)*.

Kocher, A., Miguel, L., & A. Fay. (2022). "Modeling and Executing Production Processes with Capabilities and Skills using Ontologies and BPMN,". *2022 IEEE 27th International*

Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1–8, Available at: https://doi.org/10.1109/etfa52439.2022.9921564.

Leoni, M. d., Felli, P., & M. Montali. (2021). "Integrating BPMN and DMN: Modeling and Analysis,". *Journal on Data Semantics*, vol. 10, no. 1–2, pp. 165–188, Jun. 2021 Available at: https://doi.org/10.1007/s13740-021-00132-z.

Lineage, D. ((nd)). *(https://docs.atlan.com/product/capabilities/lineage).*

Lingamallu, P. K., & F. Oliveira. (2025, accessed Nov 13). *"Google Books,".* Retrieved from Google.com, 2019. Available at: https://books.google.com/books?hl=en&lr=&id=zsm8EAAAQBAJ&oi=fnd&pg=PP1&dq=Intercepting+all+layers+is+the+Observability .

Lopes, T., & S. Guerreiro. (2023). "Assessing business process models: a literature review on techniques for BPMN testing and formal verification,". *Business Process Management Journal*, vol. 29, no. 8, pp. 133–162, Apr. 2023, Available at: https://doi.org/10.1108/bpmj-11-2022-0557.

Medium, E.-D. O. ((nd)). *(https://medium.com/%40brijesh_deb/event-driven-orchestration-using-camunda-bpm-and-kafka-1b8a195d69ee).*

Orchestration, C. M. (2020). *(https://camunda.com/blog/2020/02/the-microservices-workflow-automation-cheat-sheet-the-role-of-the-workflow-engine/).*

Orchestration, W. i. ((nd)). *(https://www.ibm.com/think/topics/microservices-orchestration).*

Polančič, G., & B. Orban. (2023). "An experimental investigation of BPMN-based corporate communications modeling,". *Business Process Management Journal*, vol. 29, no. 8, pp. 1–24, Jan. 2023, Available at: https://doi.org/10.1108/bpmj-08-2022-0362~.

Self-Managed, C. 8. ((nd)). *(https://docs.camunda.io/docs/self-managed/about-self-managed/).*

software, W. c. (2024). *(https://sbnsoftware.com/blog/what-challenges-do-organizations-face-in-implementing-compliance-software/).*

SOAPs, S. O. (2025). *Mandatory Features include Error Handling and Recovery, 2025 (https://www.gartner.com/reviews/market/service-orchestration-and-automation-platforms).*

Wazlawick, ".-O. A. (2024). *Available at: https://books.google.com/books?hl=en&lr=&id=KdPKEAAAQBAJ&oi=fnd&pg=PP1&dq=BPMN+specification+is+maintained+by+Object+Management+Group+book&ots=PaRbPaRbcpULcY&sig=aZQ2NlqrChisLnfQ808VDhQJaQ8 (accessed Nov. 13, 2025).*