1. Executive Summary

The Port Authority of Cotonou (PAC), one of West Africa's most strategic maritime hubs, faces the pressing challenge of modernising its financial and operational processes to improve efficiency, transparency, and regulatory compliance. In particular, its accounts payable process, traditionally paper-based, manual, and labour-intensive, has become a bottleneck in achieving digital transformation. To address these challenges, this report proposes a hybrid cloud architecture that integrates Artificial Intelligence (AI), automation, and Infrastructure as Code (IaC) principles to create a secure, scalable, and sovereign digital ecosystem.

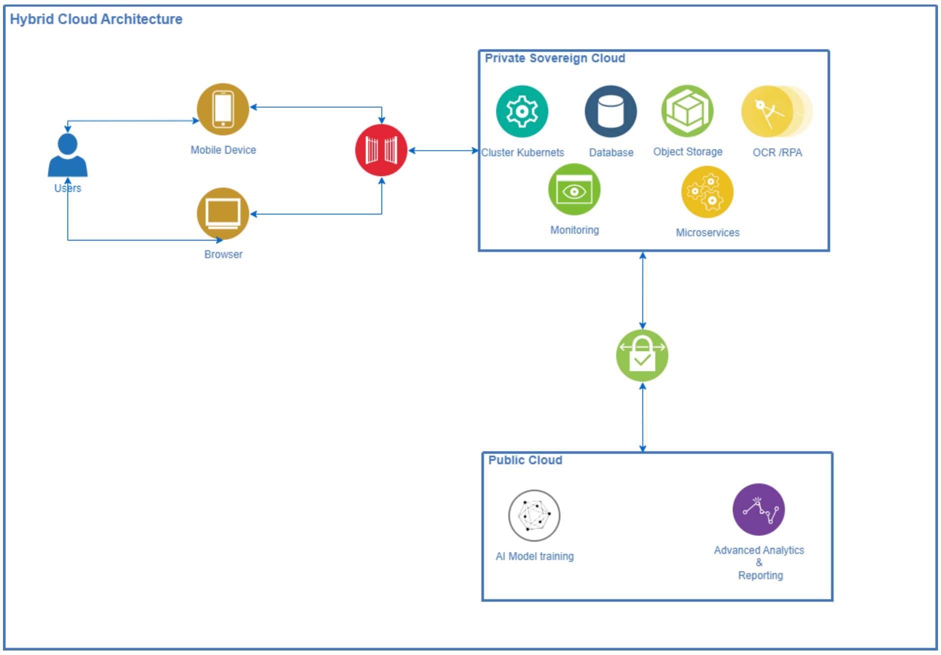
The proposed solution combines a sovereign national data centre for sensitive operations with selective use of public cloud services, notably Microsoft Azure, for advanced AI capabilities. Using technologies such as Terraform and Ansible, the solution automates infrastructure deployment, ensuring consistency, recoverability, and compliance with data governance policies. Within this framework, AI services such as Azure Form Recogniser are leveraged to automatically extract and structure invoice data, eliminating manual entry while improving speed and accuracy. The automation layer then orchestrates the entire workflow—from data ingestion to validation within the JD Edwards ERP system—creating an intelligent, end-to-end process.

This approach not only enhances operational efficiency but also enforces strict governance, ensures business continuity, and maintains complete data sovereignty. Ultimately, the synergy between hybrid cloud infrastructure, AI-driven data extraction, and workflow automation redefines PAC's back-office operations, positioning the organisation as a benchmark for digital transformation within a regulated public sector environment.

2. Cloud Solution Design

The proposed solution adopts a hybrid cloud architecture, a model extensively documented for its ability to balance scalability with control over sensitive data (Dillon et al., 2023). This approach is particularly relevant for public sector organisations that must comply with stringent data residency regulations.

2.1 Architectural Overview



The solution is designed as a cloud-native system that integrates AI services, automation workflows, and hybrid connectivity between sovereign and public environments. The architecture guarantees that sensitive data never leaves the national data centre. At the same time, computationally intensive tasks, such as AI-based optical character recognition (OCR) and document understanding, are assigned to the public cloud using anonymised copies of documents.

At the heart of the sovereign cloud is a Kubernetes cluster that hosts containerised microservices responsible for document management, workflow orchestration, and system integration with JD Edwards ERP. The cluster is supported by a PostgreSQL database for structured data, a MinIO object storage repository for document archives, and a central monitoring service that continuously oversees performance, availability, and security metrics.

User access is managed through a secure gateway (an API Gateway or a reverse proxy) that authenticates clients and enforces organisational policies. End-users, whether internal staff or external suppliers, can connect via web browsers or mobile applications. This controlled entry point ensures a consistent user experience while maintaining strong access governance.

The public cloud component, hosted on Microsoft Azure, offers supplementary services, including the Form Recogniser API, which performs intelligent data extraction from scanned invoices, and Azure Service Bus, which handles asynchronous communication between the two cloud environments.

2.3 Infrastructure as Code and Deployment Automation

To guarantee repeatability, transparency, and scalability, the entire infrastructure is deployed and managed through Infrastructure as Code (IaC) principles using Terraform and Ansible. Terraform defines and provisions both sovereign and public cloud resources declaratively, ensuring the environment remains consistent across all stages—development, testing, and production.

The use of IaC tools like Terraform and Ansible is supported by DevOps research, which highlights their role in achieving reproducible environments, reducing configuration drift, and enabling reliable disaster recovery (Morris, 2021).

Within the sovereign cloud, Terraform modules provision the Kubernetes cluster, virtual networks, storage, and security groups, while a separate module manages the minimal configuration required for Azure AI services. Once the infrastructure is deployed, Ansible playbooks automate the setup of operating systems, application dependencies, and security benchmarks. This separation of responsibilities between provisioning (Terraform) and configuration (Ansible) improves maintainability and minimises operational risk.

The combination of IaC tools also supports immutable infrastructure, in which environments are rebuilt from code rather than manually altered. This approach reduces configuration drift and aids disaster recovery, as environments can be re-provisioned identically within minutes. In accordance with DevSecOps principles, sensitive credentials such as database passwords and API keys are securely stored in HashiCorp Vault, which is deployed within the sovereign environment to ensure secrets never cross insecure boundaries.

2.4 Security and Compliance Design

Security is a fundamental design principle of the proposed system. The architecture employs a defence-in-depth approach, implementing layered controls across the network, infrastructure, and application levels. The zero-trust network model divides workloads into isolated subnets, ensuring that no database or internal service is directly exposed to the Internet. Strict firewall policies and identity-based authentication mechanisms manage access between layers.

From a compliance perspective, the design complies with international standards, including ISO 27001 for information security management and GDPR principles for data privacy. The sovereign cloud stores all sensitive data, including original PDF invoices, supplier records, and financial metadata. Only anonymised, temporary copies are sent to the public cloud for AI processing, ensuring that personally identifiable or financial information remains protected.

2.5 Scalability and Performance Optimisation

The system is built for horizontal scalability, ensuring performance remains stable during fluctuating workloads. The Kubernetes cluster automatically adjusts the number of pods for core services like document processing and workflow orchestration based on CPU and memory utilisation. This auto-scaling feature enables the Port to handle higher invoice volumes during peak times, such as fiscal closing months, without manual intervention.

2.6 Cost Efficiency and Resource Governance

Beyond scalability, the architecture encourages long-term cost management through automation and intelligent resource oversight. By adopting IaC, the Port establishes a single source of truth for all cloud assets, facilitating precise cost estimation, tagging, and monitoring. Automated scripts can detect idle or underutilised resources, prompting scale-down actions during off-peak times such as nights or weekends.

3. Integration of Advanced Cloud Technologies

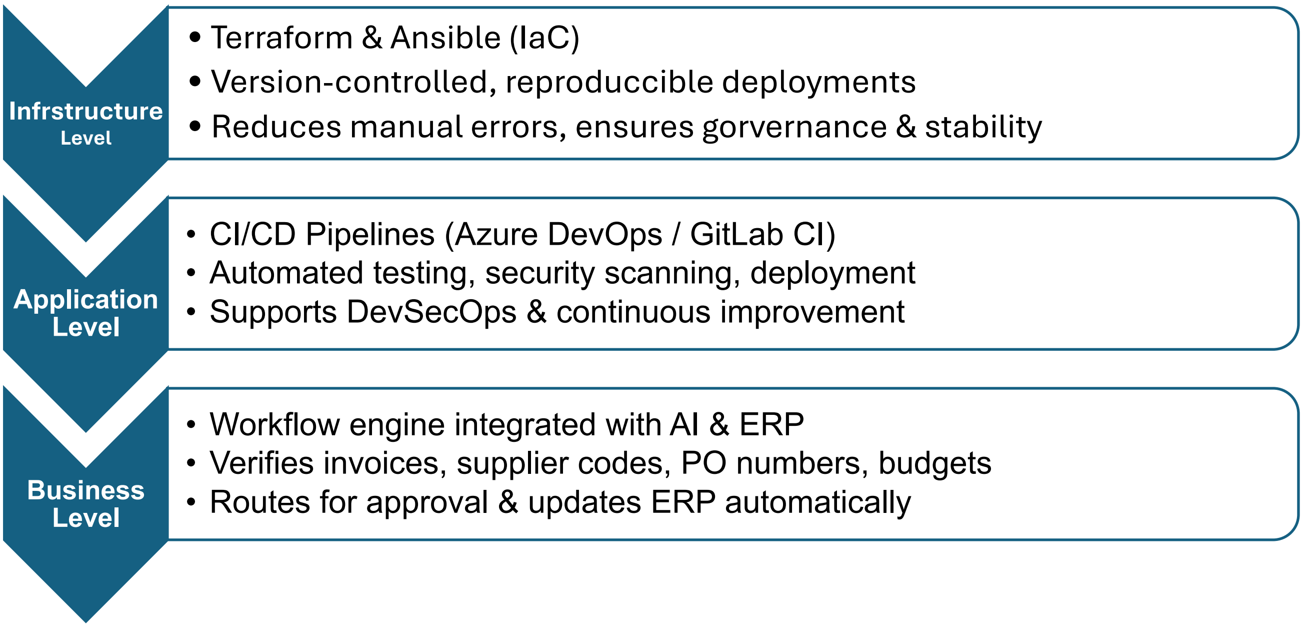
The integration of advanced cloud technologies forms the core of the proposed solution. Artificial Intelligence (AI), automation, and the hybrid cloud model interact within a synergistic ecosystem designed to optimise efficiency, reliability, and sovereignty.

3.1 Artificial Intelligence as a Catalyst for Intelligent Automation

The application of AI for document processing moves beyond simple Optical Character Recognition (OCR) to intelligent document understanding. This evolution is part of the broader trend of using AI to automate complex cognitive tasks, a key driver of the "hyperautomation" movement (Gartner, 2022, cited in Le Clair et al., 2023). The ability to transform unstructured document data into structured, actionable information is a foundational capability for modern business process automation (van den Burg et al., 2021)

3.2 Automation as the Operational Engine

Automation forms the operational backbone of the system. It influences the entire architecture—from infrastructure deployment to business process execution—ensuring tasks are performed consistently, securely, and efficiently. The automation framework is applied across three distinct but interconnected levels: infrastructure automation, continuous integration and deployment, and business process orchestration.



Infrstructure Level

- Terraform & Ansible (IaC)
- Version-controlled, reproduccible deployments
- Reduces manual errors, ensures gorvernance & stability

Application Level

- CI/CD Pipelines (Azure DevOps / GitLab CI)
- Automated testing, security scanning, deployment
- Supports DevSecOps & continuous improvement

Business Level

- Workflow engine integrated with AI & ERP
- Verifies invoices, supplier codes, PO numbers, budgets
- Routes for approval & updates ERP automatically

3.4 The Hybrid Cloud Model: Power and Sovereignty in Balance

The strategic partitioning of workloads between sovereign and public clouds aligns with the concept of "cloud federation." This model allows organisations to optimise for both performance and compliance by placing workloads in the most appropriate environment, a decision framework discussed by Dillon et al. (2023).

The hybrid cloud design acts as an architectural catalyst that aligns technological performance with the legal and ethical requirements of data sovereignty. This two-layer model separates the system into a sovereign cloud hosted within the national data centre and a public cloud (Azure) that offers specialised computational and AI services.

The two environments are linked through a secure gateway that employs end-to-end encryption, access control, and real-time monitoring. This separation of duties not only reduces compliance risks but also enhances performance and cost efficiency by assigning each workload to the most suitable environment.

Strategically, the hybrid approach allows the Port to harness the innovation and flexibility of the public cloud while maintaining the sovereignty and governance ensured by the national infrastructure. It also offers adaptability for future growth, such as the possible integration of advanced analytics, blockchain-based audit trails, or predictive financial modelling, as cloud regulations develop.

4. Risk and Compliance Considerations

For a public institution such as the Port Authority of Cotonou (PAC), operating within a regulatory environment that emphasises transparency, data protection, and national sovereignty, implementing a hybrid cloud solution requires a balanced approach between innovation and compliance.

ASPECT / LEVEL	RISK / CHALLENGE	MITIGATION MEASURES
INFRASTRUCTURE	Unauthorised access, data leakage, malicious intrusions across network boundaries	Defence-in-depth approach; network segmentation; firewall configurations; Zero Trust access policies; sovereign cloud isolated in national data centre; encrypted VPN tunnel (TLS 1.3 with mutual authentication)
IDENTITY & ACCESS MANAGEMENT	Credential compromise, unauthorised operations	Centralised authentication via Azure Active Directory (AAD); Multi-Factor Authentication (MFA); Role-Based Access Control (RBAC) enforcing least privilege
DATA	Exposure of sensitive supplier and financial data	AES-256 encryption at rest and in transit; Azure Key Vault for secure key generation, rotation, and auditing

THREAT DETECTION & RESPONSE	Delayed detection and response to incidents	Security Information and Event Management (SIEM) with Microsoft Sentinel; continuous log monitoring; real-time threat correlation and alerting; reduced mean time to detection (MTTD) and mean time to response (MTTR)
INTERNATIONAL COMPLIANCE	Non-compliance with information security and data protection standards	ISO/IEC 27001 (ISMS) and ISO/IEC 27018 compliance; structured risk management, incident response, and continuous auditing processes
NATIONAL COMPLIANCE	Legal violations regarding Beninese public sector data	Data stored and processed exclusively within sovereign data centre; anonymised/non-identifiable data used in public cloud for AI; alignment with APDP regulations; JD Edwards ERP integration for audit traceability
DATA RETENTION & ARCHIVING	Loss of auditability or non-compliance with accounting regulations	Policies aligned with national accounting and procurement rules; records remain accessible for audit and compliance checks
OPERATIONAL CONTINUITY	Service disruptions, infrastructure failures	Hybrid cloud architecture to avoid single points of failure; geo-redundant backups; replication to secondary site; routine backup verification and recovery testing
VENDOR DEPENDENCE	Lock-in to a single cloud provider	Multi-cloud capable infrastructure; provider-agnostic design; Terraform modular IaC templates support portability to Azure, AWS, Google Cloud, or regional clouds
SERVICE LEVEL AGREEMENTS (SLAS)	Unclear service commitments	Measurable commitments on availability, response times, and incident management; ensures provider accountability
AI GOVERNANCE	Algorithmic bias, lack of transparency in financial processes	Human-in-the-loop for critical verifications; regular AI model retraining and auditing according to OECD AI Principles
INSTITUTIONAL GOVERNANCE	Poor oversight, misalignment with ethical standards	Cloud Steering Committee to oversee data management, change control, and compliance audits; ensures alignment with institutional mission, ethics, and regulations

In conclusion, the risk and compliance framework supporting the proposed hybrid cloud solution adopts a comprehensive and proactive approach. Security measures, regulatory compliance, operational resilience, and ethical governance come together to form an architecture that is not only technologically advanced but also legally compliant, ethically responsible, and institutionally sustainable.

5. Future Recommendations

The proposed hybrid cloud solution provides a robust foundation for PAC's digital future. To maintain a competitive edge and operational excellence, PAC should consider the following emerging trends and technologies for phased adoption:

- **Edge Computing for Port Operations:** The integration of Edge Computing can address latency and bandwidth limitations. This aligns with the vision of "fog computing," where computing resources are distributed between the core cloud and the network edge (Bonomi et al., 2022), ideal for real-time IoT data processing in a port environment.
- **Expansion of AI and Predictive Analytics:** Evolve the AI capabilities from simple data extraction to predictive insights. Implement AI models to predict invoice approval times, identify potential fraud patterns in historical transaction data, and optimise cash flow management by forecasting payment cycles.
- **Adoption of Serverless Architectures:** For new, event-driven applications (e.g., real-time notification systems for suppliers, dynamic reporting dashboards), adopt a serverless computing model (e.g., Azure Functions). This approach further optimises costs by eliminating the need to manage underlying servers and ensuring automatic scaling.

By strategically planning for these technologies, the Port Authority of Cotonou can evolve from a digitally transformed organisation to an innovator and leader in the innovative port ecosystem.

6. Conclusion

The proposed hybrid cloud solution represents more than a mere technological upgrade for the Port Authority of Cotonou; it is a fundamental strategic realignment. By architecting a system that intelligently balances the power of the public cloud with the imperative of national data sovereignty, this initiative directly addresses the critical bottleneck of the accounts payable process. The integration of AI-driven automation and Infrastructure as Code does not simply streamline a single workflow—it establishes a modern, resilient, and scalable digital foundation for the entire organisation.

This transformation transcends operational metrics. It positions PAC as a benchmark for digital excellence in the public sector, demonstrating that rigorous compliance and innovative agility are not mutually exclusive but, in fact, synergistic. The robust risk and compliance framework ensures that this new capability is built on a foundation of trust, security, and ethical governance.

Ultimately, this cloud strategy is a pivotal investment in the Port's future. It unlocks immediate gains in efficiency, transparency, and cost-control while laying the groundwork for the next wave of innovation, from edge computing and blockchain to advanced predictive analytics. By embracing this vision, the Port Authority of Cotonou will not only optimise its operations but also significantly enhance its role as a vital, modern, and reliable engine of regional and global trade.

Words count : 2204 words

References

Bonomi, F., Milito, R., Natarajan, P. & Zhu, J. (2022). 'Fog Computing: A Platform for Internet of Things and Analytics'. In: Big Data and Internet of Things: A Roadmap for Smart Environments. Springer, Cham.

Dillon, T., Wu, C. & Chang, E. (2023). 'Cloud Computing: Issues and Challenges'. In: *2023 24th International Conference on Advanced Information Networking and Applications*. IEEE, pp. 27-33.

Morris, K. (2021). *Infrastructure as Code: Dynamic Systems for the Cloud Age*. 2nd edn. O'Reilly Media.

van den Burg, G., Rebel, D. & de Does, J. (2021). 'Improving Data Quality in Practice: A Case Study in Automated Invoice Processing'. *Data & Knowledge Engineering*, 134, p. 101909.