

TERMS OF REFERENCE

Position:	DevOps Engineer
Rank / Classification:	Lead
Division	Technology, Product and Innovation Division
Duration / Post Type:	Contract (2 years)
Reporting Line:	Chief Technology Officer (CTO)

1. Background & Scope

The DevOps Engineer is responsible for operating, automating, and continuously improving on-premises hybrid infrastructure—Kubernetes, VMware vSphere, and AWS (via Terraform)—alongside delivery pipelines. Core duties cover GitOps, CI/CD security scanning, observability (Prometheus/Grafana/Loki), secrets management, and patch currency, ensuring high availability and compliance with PCI-DSS, ISO 27001, and applicable regulatory standards.

2. Key Responsibilities

- **On-Premises Kubernetes Operations:** Manage cluster lifecycles, CNI networking, ingress controllers, persistent storage, Helm/GitOps delivery (ArgoCD/Flux), RBAC, pod security standards, and Velero disaster recovery.
- **VMware vSphere Virtualisation:** Administer vCenter, ESXi hosts, HA/DRS, datastores, vMotion operations, snapshot retention, host patching, and VM backups.
- **AWS Cloud Infrastructure & IaC:** Provision AWS services (EKS, RDS, S3, VPC, IAM) using Terraform, manage landing zones, configure security tooling (GuardDuty, Security Hub), and execute cost optimization strategies.
- **Automation & CI/CD Pipelines:** Build GitLab CI/GitHub Actions pipelines with integrated vulnerability scanning (Trivy, SAST/DAST), enforce zero-manual-change policies and configuration drift remediation, develop Ansible playbooks for server hardening, build standardized machine images using Packer, and maintain peer-reviewed Git workflows to ensure environment parity across dev, staging, and production.
- **Observability & Incident Response:** Deploy Prometheus, Grafana, Loki/ELK stack, define SLIs/SLOs, route actionable alerts, participate in on-call rotation, and conduct post-incident reviews.

- **Security, Secrets & Compliance:** Administer HashiCorp Vault/AWS Secrets Manager, enforce PKI/cert-manager, apply CIS Benchmarks, maintain patch cycles, and produce audit evidence packages for PCI-DSS and ISO 27001.

3. Qualifications & Experience

- Bachelor's degree in computer science, Information Technology, Software Engineering, or a related field.
- Relevant certifications (CKA/CKS, VMware VCP-DCV, AWS Solutions Architect/SysOps, HashiCorp Terraform Associate, RHCSA) will be a distinct advantage.
- Minimum 3 years of hands-on experience in a DevOps, Platform Engineering, or Site Reliability Engineering role.
- Demonstrated production experience with Kubernetes, VMware vSphere, AWS, Terraform, and Linux administration.
- Proven track record of building secure CI/CD pipelines and automated observability stacks.
- Prior experience in a regulated environment such as fintech, banking, or payments is highly advantageous.

4. Deliverables

- **Strategic Assessments & Architecture:** Platform Gap Analysis Report across Kubernetes/VMware/AWS, Documented Kubernetes Cluster Architecture with RBAC & Pod Security, and VMware Health & Capacity Review.
- **Automation & Security Frameworks:** Terraform IaC Codebase for AWS, Ansible Playbooks for Server Hardening, GitOps Continuous Delivery Framework (ArgoCD/Flux), and Production Secrets Management Implementation.
- **Observability & Pipeline Integrations:** Full Observability Stack (Prometheus/Grafana/Loki), Production CI/CD Pipelines with Integrated Security Scanning, and SOPs/Runbook Suite.
- **Continuity & Cost Reports:** Disaster Recovery & Backup Assurance Test Reports for Clusters/vSphere/Databases, PCI-DSS/ISO 27001 Audit Evidence Packages, and Quarterly Capacity & AWS Cost Optimisation Reports.

Specific deliverables and timelines may be determined through annual or periodic work plans approved by the CTO.