

VCS One FinCloud

Integration Guide

Migration Setup & Fintech Integration Instructions



Step-by-Step Integration Instructions

Assessment Phase

Current State Assessment Process

Before beginning any migration, conduct a comprehensive assessment of your current infrastructure, applications, and compliance posture. This phase establishes the foundation for your migration strategy.

Step 1: Inventory Existing Systems

- Catalog all applications, databases, and infrastructure components in your estate
- Document technology stack: operating systems, programming languages, frameworks
- Map dependencies between systems using automated tools (dependency scanners)
- Identify data flows and integration points with external systems
- Classify systems by criticality: mission-critical, important, optional

Step 2: Performance Baseline

- Measure current transaction volumes, peak loads, and seasonal patterns
- Capture response times (P50, P95, P99) for key business processes
- Document current infrastructure utilization rates
- Establish availability and uptime SLAs for baseline comparison

Architecture Review Checklist

Systematically evaluate your architecture to identify modernization opportunities.

- ✓ Monolithic vs. microservices architecture assessment
- ✓ Database architecture: relational, NoSQL, data warehouse
- ✓ Security posture: encryption, access controls, network segmentation
- ✓ Integration patterns: APIs, message queues, file transfers
- ✓ Disaster recovery and backup procedures
- ✓ Testing and quality assurance practices
- ✓ Configuration management and deployment processes
- ✓ Logging and monitoring capabilities

Compliance Gap Analysis

Identify gaps between current compliance posture and target regulatory requirements.

Regulatory Mapping: Identify applicable regulations (PCI-DSS, ISO 27001, GDPR, SOC 2, etc.)

Control Assessment: Evaluate existing security and compliance controls against standard requirements

Gap Identification: Document deficiencies in current implementations

Remediation Planning: Develop roadmap for addressing identified gaps

Evidence Collection: Gather documentation for compliance audit trail

Cost Model Creation & Migration Roadmap

Develop detailed financial projections and phased migration timeline.

Cost Model: Calculate current OpEx vs. projected cloud costs including compliance overhead

Timeline Planning: Estimate migration duration with dependencies and risk buffers

Resource Planning: Identify team requirements and skill gaps

Risk Assessment: Document technical and business risks with mitigation strategies

Success Metrics: Define KPIs for measuring migration success

Pilot Migration Setup

Refactor Toolkit Installation

Install and configure the VCS One FinCloud Refactor Toolkit for automated legacy system modernization.

Installation Steps

- Download toolkit from VCS developer portal and verify checksums
- Install prerequisites: Docker, Kubernetes CLI, Terraform, Ansible
- Configure authentication credentials and API keys
- Initialize workspace with workspace initialization command
- Run connection tests to verify access to source systems

Configuration

- Source System Access:** Configure credentials for legacy system access with least-privilege principles
- Target Environment:** Set up cloud environment parameters (region, VPC, cluster details)
- Migration Patterns:** Select appropriate patterns from library for your workload types
- Schedule Settings:** Configure migration windows and maintenance schedules

Compliance Automation Configuration

Enable automated compliance validation and reporting.

- Install OPA (Open Policy Agent) and configure policy repository
- Import compliance policies for applicable regulations (PCI-DSS, ISO 27001, etc.)
- Configure automated compliance checks in CI/CD pipeline
- Set up audit logging and reporting destinations
- Enable real-time alerting for compliance violations

Observability Pack Setup

Deploy comprehensive monitoring and observability infrastructure for migration tracking.

Metrics Collection: Install Prometheus for metrics gathering and configure exporters for each microservice

Visualization: Deploy Grafana dashboards with pre-built templates for financial services

Logging: Set up ELK stack (Elasticsearch, Logstash, Kibana) for centralized log aggregation

Tracing: Configure Jaeger for distributed tracing across microservices

Alerting: Configure Alertmanager with notification channels (PagerDuty, Slack, email)

Canary Deployment Process

Execute gradual rollout with automated monitoring and rollback capabilities.

Phase 1: 5% Traffic

Route 5% of production traffic to new system. Monitor error rates, latency, compliance checks. Validate functionality with smoke tests.

Phase 2: 25% Traffic

Increase to 25% after 24-hour observation period with no issues. Continue monitoring and performance validation.

Phase 3: 50% - 100% Traffic

Gradually scale to 50%, 75%, and 100% over subsequent observation periods. Maintain parallel systems during entire process.

Rollback Procedures

Document and test rollback procedures before cutover:

Automatic rollback triggers: error rate > 1%, latency degradation > 20%, compliance violations detected

Manual rollback command with immediate DNS/load balancer cutover

Data synchronization verification to ensure no data loss

Post-rollback analysis and remediation before retry

Fintech Integration

KYC/AML Integration

Integrate identity verification and anti-money laundering screening services for regulatory compliance.

Onfido Integration

1. API Setup

Create Onfido account and obtain API key from dashboard

Install Onfido SDK: `pip install onfido` or `npm install @onfido/api`

Configure API client with your region (EU, US, CA)

Set up webhook endpoint for real-time verification results

2. User Onboarding Flow

```
# Create applicant
applicant = onfido.applicant.create({ first_name: "John", last_name: "Doe",
email: "john@example.com" })
# Create check (document + facial)
check = onfido.check.create({
  applicant_id: applicant.id,
  report_names: ["identity_enhanced", "facial_similarity"],
  document_ids: [document.id] })
```

3. Verification Workflows

Document capture: front/back of government ID via mobile SDK or web upload

Facial verification: selfie capture with liveness detection

Real-time screening: automated checks against watchlists and databases

Manual review: escalation to human reviewers for edge cases

Result notification: webhook callback with verification status and scores

Talon Integration

- Biometric Enrollment:** Capture fingerprint, voice, or facial biometrics during onboarding
- Secure Storage:** Store encrypted biometric templates in Talon's secure vault
- Authentication:** Use biometric matching for subsequent logins and transactions
- Fraud Detection:** Combine biometric data with behavioral analytics for enhanced security

Payment Rails Integration

Configure connections to payment networks for domestic and international transfers.

Connector Configuration

- SWIFT:** Obtain SWIFT code and BIC from your bank. Configure ISO 20022 message formats
- ACH:** Register with National Automated Clearing House Association (NACHA) and obtain Originator ID
- SEPA:** Obtain IBAN and BIC from European bank. Register with local payment scheme operator
- Faster Payments:** Partner with member bank or payment service provider for UK real-time payments

Transaction Processing

- Payment Initiation:** Create payment request with beneficiary details, amount, currency
- Validation:** Verify account numbers, perform sanctions screening, check velocity limits
- Execution:** Route to appropriate payment rail with routing logic
- Confirmation:** Receive status updates via webhooks and update transaction records
- Reconciliation:** Match returned files with sent transactions for daily reconciliation

Reconciliation Setup

- Automate file downloads from payment networks at scheduled times
- Parse returned files (MT940, CAMT.053 formats) and extract transaction details
- Match transactions using reference numbers with automated exception handling
- Generate reconciliation reports with unmatched items and investigation workflows

Legacy System Migration

Mainframe Migration Patterns

Strategies for migrating IBM mainframe systems (z/OS, CICS, IMS) to cloud platforms.

Strangler Fig: Gradually replace mainframe modules with cloud microservices, running in parallel until full cutover

Rehost: Use mainframe emulation (Micro Focus) to run COBOL applications in cloud without code changes

Refactor: Automated COBOL-to-Java conversion using tools, then containerize refactored applications

Replatform: Migrate databases from DB2/zOS to PostgreSQL with data transformation layers

Replace: Completely rebuild critical business logic in modern languages for long-term maintainability

AS/400 Modernization

Migration approaches for IBM AS/400 (IBM i) systems to cloud platforms.

Virtualization: Run IBM i in cloud VMs with Hyper-V or VMware

Database Migration: Move DB2/400 to DB2 LUW or PostgreSQL with ETL workflows

RPG Code Analysis: Use automated tools to analyze RPG/400 programs and generate refactoring recommendations

Web Service Extraction: Expose RPG programs as REST APIs for gradual modernization

Database Migration Tools

Tools and techniques for migrating relational databases to cloud platforms.

AWS DMS: Database Migration Service for MySQL, PostgreSQL, Oracle, SQL Server

Azure Database Migration Service: Lift-and-shift migrations with online cutover

Oracle GoldenGate: Real-time replication for Oracle and heterogeneous databases

Debezium: Change Data Capture (CDC) for streaming database changes to Kafka

Custom ETL: Use dbt, Talend, or Informatica for complex transformations

Application Refactoring & Data Migration

Code refactoring strategies and data migration procedures for legacy applications.

Identify bounded contexts using domain-driven design principles

Extract business logic from legacy code into independent microservices

Implement event-driven architecture with message queues for service communication

Migrate data using dual-write pattern ensuring zero data loss

Validate data integrity with automated consistency checks

Cloud Platform Setup

AWS Deployment Guide

Deploy VCS One FinCloud on Amazon Web Services infrastructure.

Prerequisites: AWS account, IAM roles with required permissions, Terraform installed

VPC Setup: Create VPC with public/private subnets across 3 availability zones

EKS Cluster: Deploy managed Kubernetes cluster with node groups and autoscaling

RDS PostgreSQL: Provision managed database with Multi-AZ deployment and automated backups

ElastiCache: Set up Redis cluster for session storage and caching

Application Load Balancer: Configure ALB with SSL certificates and path-based routing

CloudWatch: Enable logging and monitoring with custom dashboards and alarms

Azure Configuration

Deploy on Microsoft Azure platform.

AKS: Create Azure Kubernetes Service cluster with autoscaling and availability sets

Azure Database: Provision Azure Database for PostgreSQL with geo-replication

Azure Cache: Deploy Redis cache with clustering and persistence

Application Gateway: WAF-enabled load balancer with SSL offloading

Key Vault: Secrets management for API keys, certificates, and credentials

Monitor: Azure Monitor with Application Insights for APM

GCP Setup

Deploy on Google Cloud Platform.

GKE: Google Kubernetes Engine with regional clusters and node pools

Cloud SQL: Managed PostgreSQL with high availability and read replicas

Memorystore: Managed Redis for caching with automatic failover

Cloud Load Balancing: Global load balancer with SSL certificates from Google Managed Certificates

Secret Manager: Centralized secrets management with IAM integration

Cloud Logging & Monitoring: Stackdriver for metrics, logs, and APM

Multi-Cloud Architecture & Network Security

Design resilient multi-cloud deployments with secure networking.

DNS-Based Routing: Route53, Azure DNS, or Cloud DNS for intelligent traffic distribution across clouds

VPC Peering/VPN: Secure connectivity between cloud providers using VPN or dedicated links

Data Synchronization: Real-time replication of critical data across cloud providers

Failover Automation: Automatic DNS failover in case of regional outages

Network Segmentation: Private subnets for application tiers, NACLs, security groups restricting traffic

WAF: AWS WAF, Azure Application Gateway WAF, or Cloud Armor for DDoS and OWASP Top 10 protection

Private Endpoints: PrivateLink, Private Endpoints, or Private Google Access for cloud services

VPN/Zero Trust: Site-to-site VPN or Zscaler/Cloudflare Access for secure remote connectivity

Compliance Validation

Automated Compliance Testing

Continuous validation of infrastructure and code against regulatory requirements.

Policy Execution: Run OPA policies against infrastructure configurations and code commits in CI/CD pipeline

Security Scanning: Automated SAST/DAST scans for vulnerabilities with Blackduck, Snyk, or Veracode

Configuration Compliance: AWS Config, Azure Policy, or GCP Organization Policy for infrastructure compliance

Penetration Testing: Scheduled automated pentests using tools like OWASP ZAP or Burp Suite

Access Reviews: Quarterly automated access certification requests sent to resource owners

Audit Report Generation

Automated generation of compliance reports for regulatory audits.

Daily Reports: Automated generation of security logs, access reviews, and configuration changes

Monthly Reports: Compliance dashboard summaries, vulnerability status, patch management status

Quarterly Reports: Access certification results, penetration test findings, policy violation trends

Annual Reports: Comprehensive compliance posture assessment with evidence documentation

Evidence Collection & Certification Process

Systematic collection and organization of compliance evidence for certification.

Automated Evidence: Screenshots, logs, configuration exports captured on schedule and stored immutably

Documentation Management: Centralized repository of policies, procedures, and audit trails with version control

Third-Party Audits: Schedule independent audits with certified assessors (ForgeRock, Schellman, etc.)

Remediation Tracking: Issue tracking system for remediation of findings with deadline enforcement

Ongoing Monitoring

Continuous compliance monitoring and alerting.

Real-time dashboards for compliance posture with drill-down to specific controls

Automated alerts for policy violations, security incidents, and configuration drift

Trend analysis showing compliance improvements or degradations over time

Integration with SIEM for correlation of compliance events with security incidents

Migration Best Practices

- ✓ Start with non-critical systems for pilot migration
- ✓ Maintain parallel systems during cutover period
- ✓ Automate compliance validation at every stage
- ✓ Establish clear rollback procedures before starting
- ✓ Monitor costs continuously throughout migration
- ✓ Document all changes for audit trail compliance

Compliance Support

Expert Consultation:

Regulatory compliance guidance

Audit Support:

Evidence collection and reporting

Training:

Team enablement workshops

24/7 Support:

Migration assistance available

Value Creating Solutions Sdn Bhd

<https://vcsmv.com> | support@vcsmv.com