



Digital Transformation for Regional Bank

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1 From Legacy to Leadership: Modernizing a Financial Services Platform with Hybrid Cloud, ISO 27001, and 35% Cost Savings

1.1 Executive Summary

1.2 The Challenge

1.3 Our Approach

1.4 Implementation

1.5 Results & Impact

1.6 Technologies & Services Used

1.7 Conclusion

About The Origami Corporation

1

1

2

2

4

5

5

1 From Legacy to Leadership: Modernizing a Financial Services Platform with Hybrid Cloud, ISO 27001, and 35% Cost Savings

1.1 Executive Summary

A regional financial services company needed to modernize a portfolio of legacy applications without disrupting operations or compromising regulatory compliance. We executed a phased program that migrated key workloads to a secure hybrid cloud, designed and implemented a defense-in-depth security architecture, and stood up a dedicated, co-sourced engineering and compliance team. The engagement culminated in ISO 27001 certification, a 35% reduction in IT operational costs, and markedly faster transaction processing—while strengthening governance, risk management, and operational resilience.

Services delivered: - Cloud migration to a hybrid architecture - Security infrastructure design and zero-trust alignment - ISO 27001 compliance audit preparation and certification support - Staff augmentation across cloud, security, DevOps, and compliance

1.2 The Challenge

The client’s core transaction processing and customer-facing applications ran on aging, monolithic systems hosted on-premises. Their environment presented several constraints common in financial services: - High cost base tied to end-of-life hardware, proprietary middleware, and underutilized capacity - Inconsistent security controls across applications, limited visibility into threats, and manual patching

cycles - Increasing regulatory scrutiny and a need to demonstrate a mature Information Security Management System (ISMS) aligned to ISO 27001 - Limited in-house expertise to execute a complex migration with stringent uptime, data-residency, and segregation-of-duties requirements - Pressure to improve transaction throughput and reduce latency during peak periods without service disruption

The client sought a partner who could modernize the platform, uplift security, build compliance-by-design, and transfer capability to internal teams.

1.3 Our Approach

We designed a holistic program anchored in three pillars—platform modernization, security-by-design, and compliance operationalization—supported by dedicated staff augmentation.

Key elements of the approach:

- Strategy and roadmap: Conducted an application and data discovery, TCO analysis, and risk assessment to define a hybrid target state. We prioritized workloads using business criticality, compliance impact, and technical complexity.
- Hybrid cloud reference architecture: Defined a landing zone with multi-account/subscription segmentation, centralized identity, and network hubs. Chose rehost, replatform, and refactor patterns per workload, applying the strangler-fig approach for monolith decomposition where appropriate.
- Security architecture: Implemented zero-trust principles, identity-first controls, pervasive encryption, and segmented network boundaries. Standardized logging, threat detection, and incident response across environments.
- ISO 27001 program build: Mapped controls to existing practices, established an ISMS with risk treatment plans and a Statement of Applicability, and orchestrated internal audits ahead of the external certification.
- Co-sourced delivery: Provided a blended team of cloud architects, security engineers, DevOps/SRE, and compliance specialists, operating in two-week sprints with embedded knowledge transfer.

1.4 Implementation

The engagement was delivered in phased waves over nine months to minimize change risk and ensure compliance remained intact throughout.

1) Foundation and Connectivity

- Built a cloud landing zone with guardrails (policies/SCPs), centralized identity federation (SSO/MFA), and least-privilege IAM roles.
- Established resilient connectivity between data centers and cloud via dual links (e.g., Direct Connect/ExpressRoute + VPN) and a hub-and-spoke network topology with network segmentation for prod/non-prod/regulatory zones.

- Implemented centralized DNS, certificate management, and key management (KMS/HSM-backed) to enforce encryption at rest and in transit (TLS 1.2+).

2) Security Infrastructure Design

- Adopted zero-trust patterns: device and workload identity, micro-segmentation, and just-in-time privileged access.
- Deployed a unified logging pipeline (e.g., Fluent/Beat to SIEM) covering cloud audit logs, OS logs, application logs, and VPC/VNet flow logs. Enabled real-time alerting with runbook-based response.
- Introduced WAF, IDS/IPS, endpoint protection/EDR, and secrets management for application credentials and DB connections.
- Automated vulnerability scanning (container and host), dependency scanning in CI, and regular patch baselines enforced via configuration management.

3) Application Migration and Modernization

- Grouped applications into migration waves. Low-risk services followed rehost + right-sizing; latency-sensitive services were replatformed to managed PaaS databases and containerized services.
- Containerized stateless components and orchestrated them on managed Kubernetes. Implemented autoscaling policies based on CPU/latency, health probes, and surge capacity for peak transaction windows.
- Optimized data services: introduced read replicas for heavy read paths, connection pooling, and application-level caching to reduce round-trips to databases.
- Built standardized CI/CD pipelines with infrastructure-as-code (Terraform), integrating static analysis, SAST/DAST, secrets scanning, and IaC policy checks prior to deployment. Deployments leveraged blue/green and canary strategies to minimize risk.

4) Resilience, DR, and Observability

- Defined and tested RPO/RTO targets per service tier. Implemented cross-zone high availability, cross-region backups for critical data, and automated failover for select services.
- Implemented end-to-end observability: metrics (application and infrastructure), distributed tracing for transaction flows, and SLOs with error budgets. Created runbooks and on-call rotations with clear escalation paths.

5) ISO 27001 Certification Support

- Established ISMS scope covering hybrid cloud and on-prem assets. Produced asset inventory, risk assessments, treatment plans, and control ownership.
- Authored and operationalized policies and procedures (access control, change management, vendor management, incident response, business continuity).

- Conducted internal audit and management review, closed findings, and coordinated with the external auditor for Stage 1 readiness and Stage 2 certification. Maintained evidence in a GRC system for continuous compliance.

6) Staff Augmentation and Knowledge Transfer

- Deployed a dedicated pod: lead cloud architect, security architect, DevOps/SREs, data engineer, and ISO 27001 lead implementer/auditor.
- Co-delivered with client engineers, introduced a Cloud Center of Excellence model, and ran hands-on training covering Kubernetes operations, incident handling, and compliance control execution.
- Transitioned operations with playbooks, RACI-defined responsibilities, and a backlog of continuous improvement items.

1.5 Results & Impact

- **ISO 27001 Certification:** The client achieved ISO 27001 certification on the first external audit cycle. The ISMS now provides ongoing risk management, formal control ownership, and audit-ready evidence.
- **35% Lower IT Operational Costs:** Savings realized through right-sizing, autoscaling, license optimization, decommissioning on-prem hardware, and reserved capacity commitments. Automation reduced manual effort across provisioning, patching, and deployments.
- **Faster Transaction Processing:** Containerization, database tuning, and caching reduced end-to-end latency during peak periods and increased throughput. The platform now scales elastically to meet demand, improving customer experience and reducing queue times.
- **Stronger Security Posture:** Identity-first controls, pervasive encryption, centralized logging, and continuous vulnerability management significantly reduced risk exposure. The organization improved threat detection coverage and standardized incident response.
- **Improved Reliability and Recovery:** High availability across zones and tested backups/failovers improved resilience. Defined RPO/RTO targets are met consistently, reducing operational risk.
- **Greater Delivery Velocity:** Standardized CI/CD and environment parity shortened release cycles and enabled safer, more frequent deployments—without compromising controls or segregation of duties.
- **Capability Uplift:** Internal teams now run the platform with support from comprehensive runbooks, SLOs, and a maturing Cloud Center of Excellence, reducing reliance on external contractors over time.

1.6 Technologies & Services Used

- Services:
 - Cloud-migration: discovery, TCO, wave planning, rehost/replatform/refactor, data migration
 - Security-infrastructure-design: zero-trust patterns, IAM federation, network segmentation, WAF, SIEM, IDS/IPS, EDR, secrets management
 - Compliance-audit-iso27001: ISMS design, risk treatment, SoA, policy/procedure authoring, internal audit, Stage 1/2 support
 - Staff-augmentation: cloud architecture, security engineering, DevOps/SRE, ISO 27001 lead implementer, training and knowledge transfer
- Platform and tooling:
 - Hybrid cloud landing zone with multi-account/subscription model and guardrails
 - Identity federation (SSO/MFA), least-privilege IAM, short-lived credentials
 - Network hub-and-spoke, private connectivity (Direct Connect/Express-Route), DNS, PKI, KMS/HSM
 - Managed Kubernetes, container registry, autoscaling, service mesh (where required)
 - Managed databases with read replicas, connection pooling, and caching tiers
 - CI/CD with IaC (Terraform), policy-as-code, SAST/DAST, artifact signing
 - Observability stack: metrics, logs, traces; SIEM integration and alerting
 - Backup, DR orchestration, and configuration management for patch baselines

1.7 Conclusion

By uniting cloud migration, security architecture, compliance operationalization, and a co-sourced delivery model, the client transformed a brittle legacy estate into a modern, compliant, and cost-efficient platform. Achieving ISO 27001 certification validated the maturity of the new operating model, while a 35% reduction in IT operational costs and significantly faster transaction processing delivered immediate business value. The organization is now equipped with a secure hybrid cloud foundation, measurable reliability, and an empowered internal team—positioned to innovate safely and scale confidently in a heavily regulated market.

About The Origami Corporation

The Origami Corporation is a leading technology consulting firm specializing in cloud migration, DevSecOps, cybersecurity, and digital transformation. We help organizations navigate complex technological challenges and achieve their business objectives through innovative, secure, and scalable solutions.

Connect With Us

Follow Us Online

LinkedIn: [The Origami Corporation](#)

Facebook: [@theorigamicorporation](#)

X (Twitter): [@OrigamiGlobal](#)

Telegram: [@theorigamicorporation](#)

Contact Information

Europe & Americas

- **Email:** office@theorigamicorporation.com
- **Phone:** +359 878 686 627

Asia-Pacific, Middle East & Africa (APMEA)

- **Email:** office.apmea@theorigamicorporation.com
- **Phone:** +41 77 924 2245

Ready to Get Started?

SCHEDULE A MEETING

Ready to transform your technology infrastructure? Contact us today to discuss how we can help your organization achieve similar results.