



Securing Success Enterprise Cybersecurity Transformation

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1 From Reactive to Resilient: Transforming a European Fintech’s Cybersecurity and Achieving ISO 27001	1
1.1 Executive Summary	1
1.2 The Challenge	1
1.3 Our Approach	2
1.4 Implementation	2
1.5 Results & Impact	4
1.6 Technologies & Services Used	5
1.7 Conclusion	5
About The Origami Corporation	

1 From Reactive to Resilient: Transforming a European Fintech’s Cybersecurity and Achieving ISO 27001

1.1 Executive Summary

A fast-growing European fintech engaged us to move from a reactive security stance to a proactive, standards-driven posture. Through a coordinated program of penetration testing, security infrastructure design, ISO 27001 compliance audit support, and staff security training, we identified 23 critical vulnerabilities across applications, cloud, and internal networks. We then designed and implemented a robust security framework, established a fully operational Information Security Management System (ISMS), and trained over 150 employees. Within six months, the client achieved ISO 27001 certification, reduced security incidents by 95%, passed regulatory audits, and gained the confidence to expand into new markets.

1.2 The Challenge

The client’s rapid growth had outpaced their security controls. Key challenges included:

- Fragmented security tooling with limited visibility across hybrid cloud and on-premises assets.
- Increasing attack surface due to new open-banking APIs (PSD2), third-party integrations, and a predominantly remote workforce.
- No centralized ISMS or formal risk management framework; policies were ad hoc and inconsistently enforced.
- Limited security awareness among staff, leading to recurring phishing and access control incidents.
- An impending regulatory audit and market expansion plans requiring demonstrable controls aligned to ISO 27001, GDPR, and regional financial services expectations.

The client sought a partner to conduct comprehensive penetration testing, establish a scalable security architecture, drive ISO 27001 compliance, and uplift security culture organization-wide.

1.3 Our Approach

We structured the engagement into four integrated workstreams aligned to the requested services: penetration-testing, security-infrastructure-design, compliance-audit-iso27001, and staff-security-training.

- Risk-led assessment and prioritization: We began with a rapid risk assessment and asset inventory to define scope, criticality, and threat modeling for internet-facing apps, APIs, internal networks, and cloud services.
- Standards-based methodology: Testing and remediation were guided by OWASP ASVS, OWASP Top 10, NIST SP 800-115, and ISO/IEC 27001:2022 Annex A controls.
- Architecture and process uplift: We designed a zero-trust security model, deployed centralized detection and response, and embedded secure-by-design practices across the SDLC.
- Compliance orchestration: We established an ISMS, conducted gap analyses, built the Statement of Applicability (SoA), and prepared evidence for certification.
- Human factor strengthening: We delivered role-based training and simulations to drive measurable behavior change.

This approach enabled quick wins for risk reduction while laying the foundation for continuous improvement.

1.4 Implementation

1) Penetration Testing (VAPT)

- Scope and methodology: External and internal network testing, web and mobile application assessments, API testing, cloud configuration review, and limited social engineering. Techniques included black-box and gray-box testing, credentialed scans, and manual exploitation to validate impact.
- Findings (23 critical vulnerabilities):
 - Unauthenticated API endpoints allowing account enumeration and data exfiltration.
 - Broken access control enabling privilege escalation in a customer portal.
 - Stored XSS in admin reporting with session hijacking risk.
 - Misconfigured cloud object storage exposing logs with PII.

- Overly permissive IAM roles, including wildcard actions on production resources.
 - Weak JWT signing configuration and missing token rotation.
 - VPN access without enforced MFA; stale privileged accounts.
 - Flat internal network with insufficient segmentation around payment services.
- Remediation support: We provided proof-of-concept exploits, mapped each finding to CVSS v3.1 scores, and co-developed a prioritized remediation plan. We added DAST/SAST gates to CI/CD, tightened API auth (OAuth2 with PKCE), enforced MFA, hardened IAM with least privilege, implemented WAF rules, and segmented networks around crown-jewel systems.
 - Retesting: Post-remediation verification closed all critical and high findings, with medium/low issues tracked in the risk register and assigned SLAs.

2) Security Infrastructure Design

- Zero-Trust access: Implemented SSO with enforced MFA, device compliance checks, and context-aware access policies for all administrative and remote access.
- Network and workload security: Micro-segmentation of production networks; hardened Kubernetes clusters with network policies; container image scanning; secrets moved to a centralized vault with rotation and least privilege.
- Endpoint and email security: EDR deployed across servers and endpoints; enhanced email security with DMARC/DKIM/SPF and executive impersonation protection.
- Detection and response: Deployed a SIEM with normalized logging for cloud accounts, API gateways, authentication events, EDR telemetry, and application logs. SOAR playbooks automated containment for common alerts (credential stuffing, anomalous admin actions).
- Data protection and resilience: Encryption enforced in transit (TLS 1.2/1.3) and at rest (KMS-backed keys); immutable backups for critical systems; periodic recovery drills aligned to defined RTO/RPO.
- Vulnerability and patch management: Continuous scanning integrated with ticketing; risk-based SLAs (critical: 7 days, high: 14 days); executive dashboards for SLA adherence.

3) ISO 27001 Compliance Audit

- ISMS scope and governance: Defined scope covering customer-facing platforms, cloud infrastructure, and EU offices. Established the ISMS charter, governance committees, and roles (CISO, ISMS Manager, control owners).
- Gap analysis and SoA: Mapped current controls to ISO 27001:2022 Annex A, identified gaps, and produced a Statement of Applicability with risk-based justifications for inclusions and exclusions.

- Risk management: Built a risk register, conducted risk assessments using a qualitative/quantitative model, and documented treatment plans. Embedded risk acceptance criteria and review cadence.
- Policies and procedures: Authored and implemented policies across Access Control, Cryptography, Operations Security, Supplier Management, Secure Development, Asset Management, Incident Response, and Business Continuity. Created supporting SOPs, runbooks, and evidence templates.
- Internal audit and readiness: Conducted internal audits, management reviews, and corrective actions. Coordinated with an accredited certification body; prepared audit evidence and staff for interviews.
- Certification: Achieved ISO 27001 certification on first attempt and established a surveillance audit plan.

4) Staff Security Training

- Role-based curriculum: Delivered tailored content for engineering (secure coding, secrets management, threat modeling), operations (incident handling, log hygiene), and general staff (phishing, data handling, password hygiene).
- Simulations and drills: Quarterly phishing simulations; tabletop exercises for incident response and business continuity.
- Measurable outcomes: Baseline phishing susceptibility reduced from 21% to 2.5% within three months; secure coding assessment pass rates increased from 62% to 94%. Over 150 employees trained, with a “security champions” network in engineering.

1.5 Results & Impact

- 95% reduction in security incidents: Post-implementation, monthly incident volume fell sharply, with no critical incidents in the subsequent two quarters.
- Faster detection and response: Mean time to detect (MTTD) decreased by 68%, and mean time to respond (MTTR) by 54% due to centralized logging, EDR, and SOAR automation.
- Vulnerability posture improved: All 23 critical and all high findings remediated and verified; vulnerability SLA adherence rose to 98% for criticals and highs.
- ISO 27001 certification: Passed Stage 1 and Stage 2 audits on first attempt; established continuous improvement cycles and surveillance audit readiness.
- Regulatory audit success: Demonstrated compliance controls supporting GDPR and financial services expectations, enabling expansion into new EU markets.
- Cultural shift: Security embedded into daily operations; increased phishing reporting, improved privileged access hygiene, and consistent policy adherence.

Business outcomes included accelerated market entry, strengthened partner confidence, and reduced operational risk. The client also reported improved cyber

insurance terms due to measurable control maturity.

1.6 Technologies & Services Used

- Services:
 - Penetration-Testing: External/internal, web/mobile, API, cloud configuration review; OWASP, NIST SP 800-115 methodologies.
 - Security-Infrastructure-Design: Zero-trust architecture, micro-segmentation, SIEM/SOAR, EDR, WAF, secrets management, vulnerability and patch management.
 - Compliance-Audit-ISO27001: ISMS establishment, risk assessment, SoA, internal audit, audit readiness and evidence management.
 - Staff-Security-Training: Role-based curricula, phishing simulations, incident response exercises, security champions program.
- Tools and capabilities:
 - VAPT toolchain: Burp Suite, OWASP ZAP, Nmap, Nessus; Kubernetes and cloud security baselines and scanners.
 - Identity and access: SSO/MFA, least privilege IAM, privileged access management.
 - Observability and response: SIEM with normalized pipelines, EDR, alert tuning, automated containment playbooks.
 - SDLC security: SAST/DAST integration, dependency scanning, IaC scanning, pre-commit hooks.
 - Data protection and resilience: KMS-backed encryption, immutable backups, recovery testing.

1.7 Conclusion

By combining in-depth penetration testing, modern security architecture, ISO 27001-aligned governance, and targeted security training, we helped the client transition from reactive defenses to a proactive, measurable, and certified security posture. The program not only eliminated critical vulnerabilities and reduced incidents by 95%, it also established durable processes, technology controls, and a security-aware culture. With ISO 27001 certification and a robust ISMS in place, the fintech is now equipped to scale into new markets confidently, meet regulatory expectations, and sustain continuous improvement through ongoing monitoring, quarterly VAPTs, and annual ISMS reviews.

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.