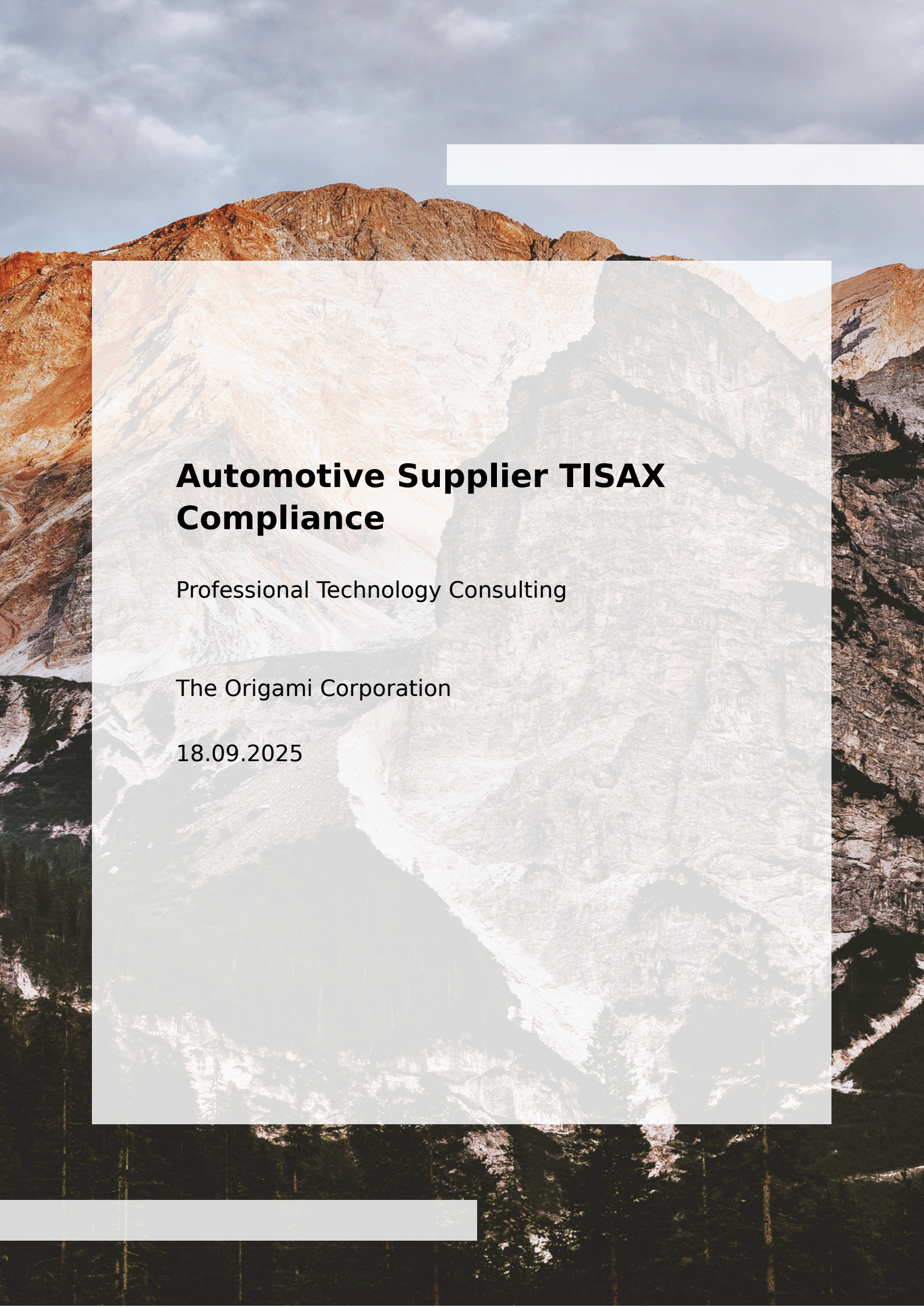




Automotive Supplier TISAX Compliance

Professional Technology Consulting

The Origami Corporation

18.09.2025

Table of Contents

1

From Risk to Resilience: Fast-Tracking TISAX AL3 for an Automotive Supplier

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

4

1.7

Conclusion

5

About The Origami Corporation

1 From Risk to Resilience: Fast-Tracking TISAX AL3 for an Automotive Supplier

1.1 Executive Summary

An EU-based automotive parts supplier faced an urgent mandate: obtain TISAX Assessment Level 3 (AL3) certification to continue supplying major German OEMs. We delivered an integrated program combining compliance-audit-tisax, penetration-testing, security-hardening, incident-response enablement, and staff-augmentation. Our team uncovered 18 vulnerabilities through comprehensive testing, hardened core infrastructure and applications, embedded three security specialists for six months, and built 24/7 incident response capabilities. The client achieved TISAX AL3 certification on the first attempt, retained contracts worth €15M annually, and prevented two potential breaches within weeks of standing up their new incident response processes.

1.2 The Challenge

The client operates across multiple sites with a mix of corporate IT and shop-floor systems supporting ERP, PLM, and vendor collaboration portals. Despite strong engineering capabilities, their information security program had grown organically and did not align with the rigor expected by TISAX (Trusted Information Security Assessment Exchange), which is based on VDA ISA and aligned with ISO/IEC 27001.

Key challenges:

- TISAX AL3 readiness required a formal ISMS, protection of highly sensitive information, and demonstrable controls for prototype protection and data protection.
- Gaps in security architecture (e.g., legacy configurations, insufficient network segmentation, incomplete logging) increased risk during audits and real-world threats.
- Limited internal capacity to accelerate remediation and operate

continuous monitoring and incident response. - The business risk was immediate: without certification, the client would risk losing multi-year contracts with German OEMs, representing €15M in annual revenue.

1.3 Our Approach

We designed a phased, outcomes-driven program focused on accelerating audit readiness while strengthening security posture:

- compliance-audit-tisax: Performed scope definition, VDA ISA gap assessment, risk treatment planning, and audit preparation, culminating in a readiness assessment and onsite audit support.
- penetration-testing: Conducted external, internal, and web application testing to expose exploitable weaknesses early and guide prioritized remediation.
- security-hardening: Established hardened baselines, reduced attack surface, and enforced least privilege across endpoints, servers, Active Directory, and network perimeters.
- incident-response: Built 24/7 monitoring and response processes, integrated critical log sources, authored playbooks aligned to MITRE ATT&CK, and ran tabletop exercises.
- staff-augmentation: Embedded three senior specialists for six months to work side-by-side with IT, compliance, and operations teams, accelerating delivery and knowledge transfer.

1.4 Implementation

Our work unfolded in five structured phases over six months.

Phase 1 — TISAX Scoping & Gap Analysis - Defined the TISAX scope to include HQ, two manufacturing sites, and core cloud services supporting customer data exchanges. - Conducted a VDA ISA 5.x gap assessment across governance, risk management, supplier security, prototype protection, and data protection domains. - Built an ISMS foundation: information security policy suite, asset inventory, classification schema, risk register, and a Statement of Applicability mapping controls to TISAX objectives. - Prioritized a remediation backlog focused on AL3-critical controls and high-impact vulnerabilities.

Phase 2 — Penetration Testing & Validation - External perimeter testing identified outdated VPN gateway firmware and unnecessary exposed services; internal testing highlighted Active Directory misconfigurations and legacy protocols. - Web application testing (aligned to OWASP) on the supplier collaboration portal revealed insufficient authorization checks and outdated libraries. - In total, 18 vulnerabilities were documented with evidence and proof-of-concept where safe to do so. Categories included: - Authentication/authorization weaknesses (e.g., session misman-

agement). - Patch-related exposures enabling potential RCE. - Insecure defaults in AD (e.g., unconstrained delegation, excessive privileges). - Transport security gaps (e.g., lack of TLS 1.2+ enforcement on certain endpoints). - We worked with system owners to triage by likelihood and impact, establishing target remediation timelines for each severity level.

Phase 3 — Security Hardening & Control Uplift - Active Directory: Implemented tiered administration, enforced MFA for privileged accounts, enabled LAPS for local admin password rotation, and reduced domain admin footprint. Hardened Kerberos settings and disabled legacy protocols (e.g., NTLMv1, SMBv1). - Endpoints/Servers: Applied CIS Benchmarks as a baseline, standardized build images, and integrated automated patch management. Enforced disk encryption and device control policies on engineering workstations handling sensitive CAD/PLM data. - Network: Introduced segmentation separating IT and OT networks with controlled inter-zone access. Hardened VPN, restricted RDP exposure, and applied geo-blocking and conditional access for remote users. - Applications: Implemented secure headers, tightened session management, upgraded cryptographic libraries, and deployed a WAF in front of internet-facing portals. - Logging & Monitoring: Centralized logs from AD, VPN, firewalls, EDR, and critical SaaS into a SIEM; normalized events and implemented detections mapped to MITRE ATT&CK.

Phase 4 — Incident Response Enablement - Designed a 24/7 IR operating model with on-call rotation, escalation paths, and SLAs for triage and containment. - Authored playbooks for phishing/BEC, ransomware, credential stuffing, and data exfiltration attempts, backed by runbooks for containment and eradication. - Conducted tabletop exercises with IT and executive stakeholders, clarifying decision points and communications flows with customers and OEMs. - Integrated EDR telemetry for rapid isolation and automated enrichment in the SIEM to reduce mean time to detect and respond.

Phase 5 — Audit Readiness & Support - Prepared evidence packages for TISAX objectives, including risk assessments, control implementations, supplier security reviews, and awareness training records. - Ran a mock audit against VDA ISA control sets and addressed final findings. - Coordinated with an accredited TISAX audit provider, provided audit-day support, and facilitated remediation clarifications in real time.

Throughout, our three embedded specialists—TISAX program lead, senior security engineer, and IR analyst—worked daily with the client's infrastructure and application teams, ensuring rapid knowledge transfer and sustainable operations post-engagement.

1.5 Results & Impact

- TISAX AL3 on first attempt: The client passed the assessment without major nonconformities, demonstrating mature governance, strong technical controls, and effective incident response capabilities.
- €15M annual revenue protected: Certification enabled continued engagement with key German OEMs and strengthened the client's competitive standing in the automotive supply chain.
- Vulnerabilities remediated: All 18 findings from penetration testing were addressed with validated fixes; critical exposures were mitigated within agreed timelines through configuration changes, patching, and compensating controls (e.g., WAF rules).
- 24/7 incident response operational: Within weeks of go-live, the team detected and contained two potential breaches—a targeted phishing attempt that was contained at the mailbox level, and a credential-stuffing attack against the VPN thwarted via MFA and geo-blocking—without data loss.
- Hardened security posture: Reduced attack surface by eliminating unnecessary external services, enforcing MFA for privileged access, segmenting high-value assets, and aligning systems to CIS baselines. The client now operates with centralized logging, defined playbooks, and tested response procedures.
- Sustainable ISMS: Policies, risk management, and supplier security processes are now institutionalized, enabling ongoing compliance, continuous improvement, and smoother re-assessments.

Beyond immediate certification, the client gained measurable resilience and a repeatable operating model, reducing audit fatigue and improving stakeholder confidence across engineering, IT, and customer teams.

1.6 Technologies & Services Used

Services - compliance-audit-tisax - penetration-testing - security-hardening - incident-response - staff-augmentation

Technologies and methods - VDA ISA control framework mapping to TISAX AL3 objectives - ISMS documentation (policy suite, risk register, Statement of Applicability) - SIEM for centralized logging and alerting; EDR for endpoint visibility and isolation - CIS Benchmarks for system hardening; secure baseline images and GPOs - Multi-factor authentication, privileged access management practices, LAPS - Network segmentation, VPN hardening, geo-blocking, conditional access - WAF and secure SDLC improvements for web applications - Penetration testing methodologies aligned with OSSTMM/OWASP; tooling including network, application, and AD-focused assessments - MITRE ATT&CK-aligned detections and incident response playbooks - Tabletop exercises and runbooks for high-impact scenarios

1.7 Conclusion

Under tight business timelines and stringent security expectations, we transformed the client's security program from siloed controls to a cohesive, audit-ready, and resilient posture. By combining compliance-audit-tisax with targeted penetration-testing, robust security-hardening, and a 24/7 incident-response capability—delivered through focused staff-augmentation—we enabled the client to achieve TISAX AL3 certification on the first attempt and safeguard €15M in annual revenue.

The outcome goes beyond a certificate. The client now operates an ISMS grounded in risk management, with measurable visibility, faster detection and response, and hardened infrastructure that supports safe collaboration with top-tier automotive manufacturers. As supply chain security expectations continue to rise, the organization is positioned to maintain compliance with confidence and to adapt proactively to emerging threats.

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.