How Zero Networks Helps with TISAX Requirements

TISAX (Trusted Information Security Assessment Exchange) was established by the German Association of the Automotive Industry to serve as the automotive industry's information security standard, based on VDA ISA (Information Security Assessment) and managed by the ENX Association. TISAX certification is essential for automotive suppliers and service providers who work with German carmakers to demonstrate secure handling of sensitive data including vehicle designs, prototypes, and proprietary technologies.

Zero Networks enhances TISAX/VDA ISA 6.0 compliance through automated Zero Trust controls, adaptive microsegmentation, and comprehensive visibility across IT and OT environments – addressing core requirements while achieving 90% network segmentation in 90 days on average.

Who Must Comply

TISAX certification is required for automotive suppliers, manufacturers, IT service providers, and engineering firms handling sensitive OEM (Original Equipment Manufacturer) data. Certification level depends on data sensitivity: Assessment Level 1 (AL1) for self-assessment, AL2 for third-party validation, and AL3 for comprehensive on-site audits – typically required for highly confidential data such as vehicle prototypes, crash test results, and proprietary AI systems.

Specific requirements where Zero Networks can help you achieve TISAX compliance:

Requirement	Description	How Zero Helps	Impact
Information Security Management System (ISMS) *VDA ISA Controls: 1.1.x, 1.2.x*	Organizations must establish, implement, maintain, and continuously improve an information security management system aligned with ISO 27001 and VDA ISA requirements.	Zero provides automated policy enforcement and continuous compliance monitoring. The platform generates audit-ready evidence of security control effectiveness, documenting microsegmentation policies, access restrictions, and threat containment measures that demonstrate measurable risk reduction.	Provides documented proof of control implementation and effectiveness for TISAX audits.
Access Control & Identity Management *VDA ISA Controls: 4.1.1, 4.1.2, 4.1.3, 4.2.*	Access to information and IT systems must be restricted based on business and security requirements. Organizations must implement least-privilege access, protect privileged accounts, and enforce multi-factor authentication for critical systems.	Zero enforces identity-based access policies across all human and machine identities, applying just-in-time MFA at the network layer. The platform ensures least-privilege access for privileged accounts and service accounts, automatically restricting lateral movement and preventing credential-based attacks.	Prevents unauthorized access, credential theft, and privilege escalation across IT and OT environments.

Requirement	Description	How Zero Helps	Impact
Network Segmentation & Isolation *VDA ISA Controls: 5.1.3, 5.1.4*	Networks must be segmented based on risk levels and business requirements. Critical systems must be isolated from general networks, and communication between zones must be strictly controlled and monitored.	Zero automates network and asset microsegmentation by creating logical micro-perimeters around workloads, applications, and critical data. The platform blocks unauthorized east-west traffic, isolates production systems from development environments, and prevents lateral movement even if an attacker compromises an endpoint.	Reduces attack surface, contains security incidents, and protects critical automotive production systems.
Asset Inventory & Management *VDA ISA Controls: 2.1.1, 2.1.2*	Organizations must maintain a current inventory of all information assets, IT systems, and OT devices. Assets must be classified based on confidentiality, integrity, and availability requirements.	Zero provides automated discovery and real-time visibility into all network assets including devices, applications, users, and service accounts across IT, OT, and cloud environments. This comprehensive inventory helps identify critical assets requiring enhanced protection and supports accurate asset classification.	Enables complete visibility of attack surface and supports risk-based protection strategies
Incident & Crisis Management *VDA ISA Controls: 1.6.1, 1.6.2, 1.6.3*	Organizations must establish processes for detecting, reporting, managing, and responding to security incidents. This includes capabilities for rapid containment, investigation, and recovery from security events and crisis situations.	Zero enables rapid incident response through automated threat containment. When a security incident is detected, Zero can immediately isolate compromised systems while maintaining operational continuity for unaffected assets. The platform provides detailed forensic visibility including attack paths, lateral movement attempts, and containment boundaries.	Reduces incident duration, limits blast radius, and ensures business continuity during security events.
Vulnerability & Patch Management *VDA ISA Controls: 5.2.1, 5.2.2*	Organizations must identify, assess, and remediate technical vulnerabilities in a timely manner. Compensating controls must be implemented when patches cannot be applied immediately, particularly for legacy OT systems.	Zero provides virtual patching through network isolation for vulnerable or legacy systems that cannot be immediately patched. The platform restricts communication pathways to and from vulnerable assets, preventing them from being used as pivot points while maintaining necessary operational connectivity.	Reduces exploitation risk and provides compensating controls for unpatchable legacy systems.
Supply Chain & Third-Party Security *VDA ISA Controls: 1.3.1, 1.3.2, 1.3.3*	Organizations must manage information security risks arising from relationships with suppliers, service providers, and external partners. Third-party access must be monitored, controlled, and limited to only required systems.	Zero restricts third-party and vendor access to only required assets and ports through identity-based controls. The platform prevents vendors from moving laterally through internal networks and provides complete audit trails of all third-party access activities, ensuring traceable and least-privilege external connectivity.	Minimizes supply chain blast radius and prevents unauthorized vendor access to sensitive automotive data.

Requirement	Description	How Zero Helps	Impact
Prototype Protection *TISAX Module: Prototype Protection*	Organizations must protect pre-production vehicles, test vehicles, and prototypes during development, testing, and transportation. This includes preventing unauthorized access to prototype designs, specifications, and physical assets.	Zero creates isolated network zones for prototype development systems, restricts access to prototype data repositories based on role and need-to-know, monitors all access to sensitive prototype information, and prevents unauthorized data exfiltration through network controls.	Protects highly confidential vehicle designs from industrial espionage and competitive intelligence threats.
OT/ICS Availability *VDA ISA 6.0: OT/ICS Module*	Organizations must ensure resilience and availability of Operational Technology and Industrial Control Systems critical to automotive production. This includes protecting manufacturing systems, production lines, and robotics from cyber threats.	Zero provides automated microsegmentation for production networks following Purdue Model architecture, isolates critical control systems from IT networks, restricts lateral movement between production zones, prevents ransomware spread across manufacturing infrastructure, and maintains operational continuity during cyber incidents by containing threats without shutting down production.	Protects revenue-critical production operations from ransomware and ensures manufacturing resilience.

Achieve TISAX Compliance with Confidence

Zero Networks directly aligns with TISAX/VDA ISA requirements through automated Zero Trust controls, adaptive microsegmentation, and comprehensive visibility across IT and OT environments. By addressing core VDA ISA 6.0 controls – including access management, network segmentation, incident response, vulnerability management, supply chain security, prototype protection, and OT/ICS availability – Zero helps automotive suppliers achieve and maintain TISAX certification efficiently.

The average Zero customer achieves 90% network segmentation in 90 days. Zero deploys rapidly with automated discovery, policy generation, and enforcement that significantly reduces implementation time compared to traditional manual approaches. The platform provides continuous compliance monitoring, audit-ready documentation, and measurable risk reduction – giving automotive organizations the confidence to pass TISAX Assessment Level 3 audits while protecting critical production systems and sensitive vehicle data.

Catalyze compliance and protect your automotive supply chain.

Try Zero today

ZERO. Networks