DEKRA

Whitepaper

Aligning NIS2 with TISAX® and ISO/IEC 27001: **A Unified Strategy for Cybersecurity and Compliance in the Automotive Sector**



Table of **contents**

03	Introduction: The New Imperative of NIS2 for Automotive
04	Core Frameworks: A Primer on TISAX® and ISO/IEC 27001
05	The Strategic Convergence: Mapping NIS2 to Established Frameworks
06	ISO/IEC 27001: The Operational Engine for NIS2 Compliance
07	TISAX®: The Automotive Sector’s Compliance Accelerator
08	A Phased Implementation Strategy for Unified Automotive Compliance
09	Conclusion: Building a Coherent Cybersecurity Architecture

Abstract

The European Union's NIS2 Directive marks a watershed moment in cybersecurity regulation, imposing stringent new obligations on a vast range of entities in critical and important sectors, explicitly including the manufacturing of motor vehicles and their components. Concurrently, established frameworks like TISAX®, mandatory for securing the automotive supply chain, and the global standard ISO/IEC 27001 continue to set the benchmark for information security management.

This whitepaper deciphers the interconnected relationship between NIS2, TISAX®, and ISO/IEC 27001 specifically for OEMs, who typically mandate these frameworks, and their suppliers, who must implement and demonstrate compliance with them. It demonstrates how these frameworks are not competing mandates but complementary components of a mature security program. By leveraging the VDA ISA (TISAX®) foundation, we illustrate how automotive organizations can use existing ISO/IEC 27001 and TISAX® implementations as a powerful foundation to efficiently achieve NIS2 compliance, potentially reducing the effort required to close compliance gaps for essential and important entities, avoiding redundant efforts, and building a unified, resilient cybersecurity governance model.

Introduction:
The New Imperative of NIS2 for Automotive

The NIS2 Directive (EU 2022/2555) fundamentally elevates the cybersecurity landscape within the EU. **For the automotive industry, NIS2 brings most manufacturers of vehicles and their critical component suppliers directly into scope as 'essential' or 'important' entities**. This drastically expands the scope of regulation beyond previous standards, tightening security and reporting requirements, and significantly increasing the financial and liability penalties for non-compliance.

Under NIS2, essential and important entities must now demonstrably implement:

- A comprehensive, risk-based cybersecurity program.
- Active governance and oversight from top management. (NIS2 strengthens management accountability for cybersecurity oversight; the precise scope and mechanism of any personal liability depends on each EU member state's national implementing legislation.)
- Strict incident reporting within 24 hours of awareness, a crucial speed requirement for manufacturing supply chains.
- Robust business continuity and crisis management plans.
- Effective supply chain and third-party risk management. (This applies to sub-suppliers of critical ICT services and components.)

These mandates show strong alignment with the core principles of leading security frameworks, particularly ISO/IEC 27001 and the automotive industry'sTISAX®, which together enable more effective, sector-specific supply chain security measures.

Core Frameworks:
A Primer on TISAX® and ISO/IEC 27001

While closely related, the two frameworks reflect different vantage points: ISO/IEC 27001 provides a management view of an organization's own risk appetite, while TISAX® takes a customer-driven perspective, prescribing how information shared with suppliers across the automotive value chain must be protected.

- **ISO/IEC 27001:**
The internationally recognized standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). It provides a risk-based, holistic framework that integrates people, processes, and technology, serving as the foundational management structure.

- **TISAX® (Trusted Information Security Assessment Exchange):**
An assessment and interoperability mechanism for the automotive industry, managed by the ENX Association. Based on the VDA ISA (Information Security Assessment), which is developed and maintained by the ENX Working Group ISA and published by the VDA, TISAX® structures controls across core domains: Information Security, Prototype Protection and Data Protection. TISAX® not only takes ISO/IEC 27001 as a reference, but also other frameworks such as IEC 62443 into consideration.



The Strategic Convergence:
Mapping NIS2 to Established Frameworks

Official mappings confirm that a well-implemented ISO/IEC 27001 ISMS, particularly one that has been successfully assessed for TISAX®, covers the vast majority of NIS2 requirements. TISAX's inherent focus on the confidentiality of sensitive IP and the availability of systems is directly relevant to NIS2's mandate to secure critical manufacturing and transport functions.

The relationship between these frameworks can be visualized as a layered, integrated system:

NIS2 Requirement	ISO/IEC 27001 Coverage	TISAX® (VDA ISA) Leverage	NIS2 Specific Focus for Automotive
Risk Management	Clauses 6 & 8 (Planning & Operation)	Maturity level assessment (AL2/AL3) ensures rigor.	Focus on risks to production availability (OT systems).
Governance & Accountability	Integrated ISMS governance (Clause 5)	TISAX® applies a standard scope. Better setting responsibilities and execution of internal assessments.	Direct liability of the management body for compliance.
Incident Handling & Reporting	Annex A.5.24–A.5.28 (Incident Management, ISO/IEC 27001:2022)	Established Incident processes for sharing with partners.	Strict 24-hour early warning to national CSIRTs/authorities
Business Continuity	Annex A.5.29–A.5.30 (ICT Readiness for Business Continuity, ISO/IEC 27001:2022)	Inclusion of Availability label from VDA ISA 6.0 onwards for production	Mandatory redundancy for essential services (e.g., connected vehicle platforms).
Supply Chain Security	Annex A.5.19–A.5.22 (Supplier Relationships, ISO/IEC 27001:2022)	Mandatory and verified supplier security checks across the value chain.	Explicitly addressing third-party risks including software providers/ service integrators
Technical & Organizational Controls	Annex A.8.24–A.8.28 (Cryptography & Secure Development, ISO/IEC 27001:2022)	Information Security controls	Use of cryptography to protect sensitive technical data and in-transit information.

The conclusion is clear: ISO/IEC 27001 establishes the foundational management system, TISAX® provides mandatory, sector-specific depth and customer-driven validation, and NIS2 sets the mandatory legal obligations.

ISO/IEC 27001:
The Operational Engine for NIS2 Compliance

ISO/IEC 27001 is the most effective operational framework for meeting NIS2's demands, acting as the bedrock for the TISAX® requirements.

- **Inherent Risk-Based Approach:**
NIS2 mandates risk management. ISO/IEC 27001's cycle of risk identification, assessment, and treatment provides the necessary structure, ensuring risks to the delivery of vehicle components or manufacturing services are systematically managed.

- **Governance & Leadership:**
NIS2 holds management directly accountable. ISO/IEC 27001 requires top management to lead the ISMS, which forms the basis for demonstrating the required cybersecurity oversight and training for the board/management.

- **Supply Chain Security Leverage:**
ISO/IEC 27001 establishes a risk-based framework for managing information security across the organisation, including supplier relationships and third-party access to sensitive information. ISO/IEC 27001's Annex A.5.19–A.5.22 (ISO/IEC 27001: 2022) establishes the policy framework, which is operationally realized through the contractual requirement of the TISAX® assessment for key partners.

- **Closing the NIS2 Reporting Gap:**
The incident management lifecycle defined in ISO/IEC 27001 (A.5.24–A.5.28, ISO/IEC 27001: 2022) provides the process template. However, organizations must specifically tune this process to meet NIS2's stringent 24-hour early warning deadline and report to the designated National Supervisory Authority—a step beyond TISAX's internal/partner notification focus.



TISAX®:
The Automotive Sector's Compliance Accelerator

For automotive organizations, TISAX® is not merely a customer requirement but can be the primary driver and demonstration of NIS2 readiness.

- **Direct Scope Overlap:**
  Entities required to hold a TISAX® label (OEMs and critical Tier 1/Tier 2 suppliers) are highly likely to fall under NIS2. Meeting TISAX® is proactive compliance with many of NIS2's technical and organizational measures.

- **Focus on Availability:**
  The inclusion of the Availability label from the TISAX® VDA ISA 6.0 onwards catalogue aligns perfectly with NIS2's requirement to maintain the continuity of essential and important services. This applies directly to Operational Technology (OT) systems used in manufacturing, which represents the core business of most automotive organizations where NIS2's Business Continuity and resilience requirements carry particular weight. A successful TISAX® assessment (especially AL2 or AL3) provides trusted, third-party verification of a mature security posture. This independent audit evidence is one of the strongest demonstrations an organization can provide to its national supervisory authority that it has implemented appropriate technical and organizational measures.

- **IP and Prototype Protection:**
  The TISAX® specific requirements for securing prototypes, highly sensitive designs, and intellectual property directly address a unique threat vector in the automotive sector that is not explicitly detailed in NIS2 but is critical to its security principles.

The simplification and reduction of TISAX® Prototype Assessment Objectives in the VDA ISA 2027 assessment catalogue does not affect NIS2 compliance.





A Phased Implementation Strategy for Unified Automotive Compliance

Automotive organizations can integrate these frameworks efficiently through a sector-specific phased approach:

Validate the Foundation and TISAX® Scope

- Ensure an ISO/IEC 27001 Information Security Management System (ISMS) is established, implemented and kept up to date.
- Confirm the required TISAX® Assessment Level (AL2/AL3) and Objectives (e.g., Information Security, Prototype Protection, Data Protection) dictated by key OEM customers, using the VDA ISA catalogue at this stage to scope the ISMS and avoid rework later.

Map and Close the NIS2 Gap

- Reuse the ISMS established in Phase 1 and the TISAX® VDA ISA catalogue as the primary control list, avoiding duplicate control mapping.
- Conduct a focused gap analysis specifically against the NIS2 requirements for Governance and Reporting.
- Implement the most critical procedural change: formalizing the 24-hour/72-hour reporting workflow to the national CSIRT/Authority (which goes beyond the TISAX® partner notification).

Operationalize and Demonstrate via TISAX®

- Implement all necessary controls, particularly in areas like secure development and OT security.
- Undergo and successfully complete the TISAX® assessment, generating the formal label which serves as sector-recognized proof of security implementation.

Formalize NIS2 Governance & Legal Accountability

- Assign clear legal accountability for NIS2 compliance to the board/senior management and ensure they receive mandatory cybersecurity training.
- Prepare the final documentation required for the supervisory authority, using the TISAX® assessment report and ISMS evidence as primary artifacts.

Conclusion:
Building a Coherent Cybersecurity Architecture

The NIS2 Directive is not a separate project for the automotive industry; it is the affirmation of the stringent security requirements already being enforced by the TISAX® framework.

- ISO/IEC 27001 provides the necessary organizational and risk management structure.
- TISAX® delivers the industry-specific rigor, independent validation, and the crucial protection layers for IP and prototypes.
- NIS2 sets the non-negotiable legal accountability and rapid reporting mandates.

By treating TISAX® as the operational compliance vehicle for NIS2, automotive organizations can achieve tangible benefits: accelerated time-to-compliance, minimized audit redundancy, and a stronger, legally defensible posture that meets both regulatory requirements and customer demands. This unified approach secures their position as a trusted, resilient partner in the digital automotive value chain.

Would you like more information?

Contact Us!

November 2026

DEKRA



dekra.com

DEKRA SE