

Trusted Information Security Assessment Exchange (TISAX®) ISA2027: The key changes

Greater clarity, greater planning certainty, a stronger focus on the supply chain

The publication of the new ISA2027 catalogue marks another important step in the further development of TISAX®. At the same time, the publication marks the tenth anniversary of the TISAX® standard, which, since its introduction in 2016, has established itself as the standard for information security management systems (ISMS) in the automotive industry.

Over the past ten years, more than 21,000 sites worldwide have been assessed against TISAX® requirements. Today, over 5,000 users from vehicle manufacturers and supplier companies use TISAX® results to assess their business partners and suppliers.

With ISA2027, the industry aims to make the catalogue clearer and easier to plan for. At the same time, the requirements for managing information security risks in supply chains are being more specified and upgraded.

What is ISA2027?

The ISA (Information Security Assessment) catalogue forms the basis for the required ISMSs. Its requirements are assessed during the respective TISAX® assessments, thereby demonstrating the maturity level of the ISMSs and, ultimately, the responsible handling of sensitive information within the supply chain.

Whilst the early versions of the ISA were closely modelled on ISO/IEC 27001, the catalogue has evolved in recent years into an independent industry standard. It specifically addresses the requirements and risks of automotive value chains and is continuously refined by experts from industry, trade associations and assessment providers.

The currently valid ISA 6 catalogue remains the basis for ongoing assessments. The new ISA2027 will become mandatory for all TISAX® assessments contracted to the assessment provider commissioned from 1 January 2027 onwards.



An overview of the key changes

1. NEW VERSIONING MODEL ENSURES GREATER TRANSPARENCY



One of the most notable changes concerns the naming of future ISA versions. Instead of sequential version numbers, the designation will in future be based on the year in which the respective version becomes mandatory for newly commissioned assessments. ISA2027 will therefore become mandatory from 1 January 2027. Future versions will follow the same principle.

In addition, the ENX Association is introducing an annual publication cycle:

- **New ISA versions will generally be published in the summer**
- **Mandatory application from the following 1 January**
- **A predictable and transparent development process for organisations and assessment providers**
- **Important for organisations**

The validity of TISAX® labels remains unchanged. Labels continue to be valid for up to three years. The annual publication of new catalogue versions will therefore not lead to more frequent re-assessments.

2. GREATER CLARITY AND IMPROVED READABILITY



A key objective of ISA2027 was to improve the readability and consistency of the catalogue. To this end, wording, definitions, translations and the structure of the requirements were comprehensively reviewed and standardised. This is intended to reduce ambiguities and differing interpretations that have arisen over time.

Of particular relevance is the now unambiguous definition of the phrase: 'The following aspects are taken into account.' In future, it will be clearly stated that all the aspects mentioned must be deliberately considered and that the respective implementation decision should be explained in a comprehensible manner within the assessment.

For organisations, this means, above all:

- **greater transparency,**
- **less scope for interpretation,**
- **more consistent assessment results.**

3. THE ROLE AND RESPONSIBILITY OF MANAGEMENT IS EMPHASISED MORE CLEARLY



Information security has always been a management responsibility. ISA2027 now makes this even more explicit. The catalogue explicitly states that executives and management levels are among the target groups for information security awareness and training initiatives. This does not introduce any fundamentally new requirements. Rather, it describes existing expectations more transparently and aligns them more closely with current regulatory developments.

For managing directors, this means in particular:

- **Information security remains a strategic management issue.**
- **Active support from senior management is becoming increasingly important.**
- **Security awareness should be embedded at all levels of the organisation.**

4. GREATER FOCUS ON SUPPLY CHAIN SECURITY



One of the key priorities of ISA2027 is the management of information security risks within the supply chain.

The automotive industry now operates within highly interconnected value chains. Security incidents at suppliers, service providers or development partners can have a significant impact on customers, manufacturers and other market participants. The new catalogue therefore places greater emphasis on the assessment and monitoring of business partners' information security.

Depending on the specific protection requirements, the requirements regarding:

- **the documentation of security requirements,**
- **the verification of evidence,**
- **the regular assessment of suppliers,**
- **the consideration of significant changes in the supply chain**

are specified in detail and, in some cases, expanded.

For information requiring a very high level of protection, additional, more stringent requirements for supplier management are set out. Evidence of compliance may include, for example, a TISAX® label, comparable independent assessments or appropriate supplier audits.

The key message is: information security does not end at the boundaries of one's own organisation.

5. COMPREHENSIVE REVISION OF PROTOTYPE PROTECTION



The section on prototype protection has also been revised. The previous structure, comprising several separate thematic sections, has been reorganised into two overarching areas:

1. Organisational matters:

requirements regarding processes, responsibilities, planning and management.

2. Physical and environmental security:

requirements for the physical protection of prototypes, components, vehicles and sensitive development items.

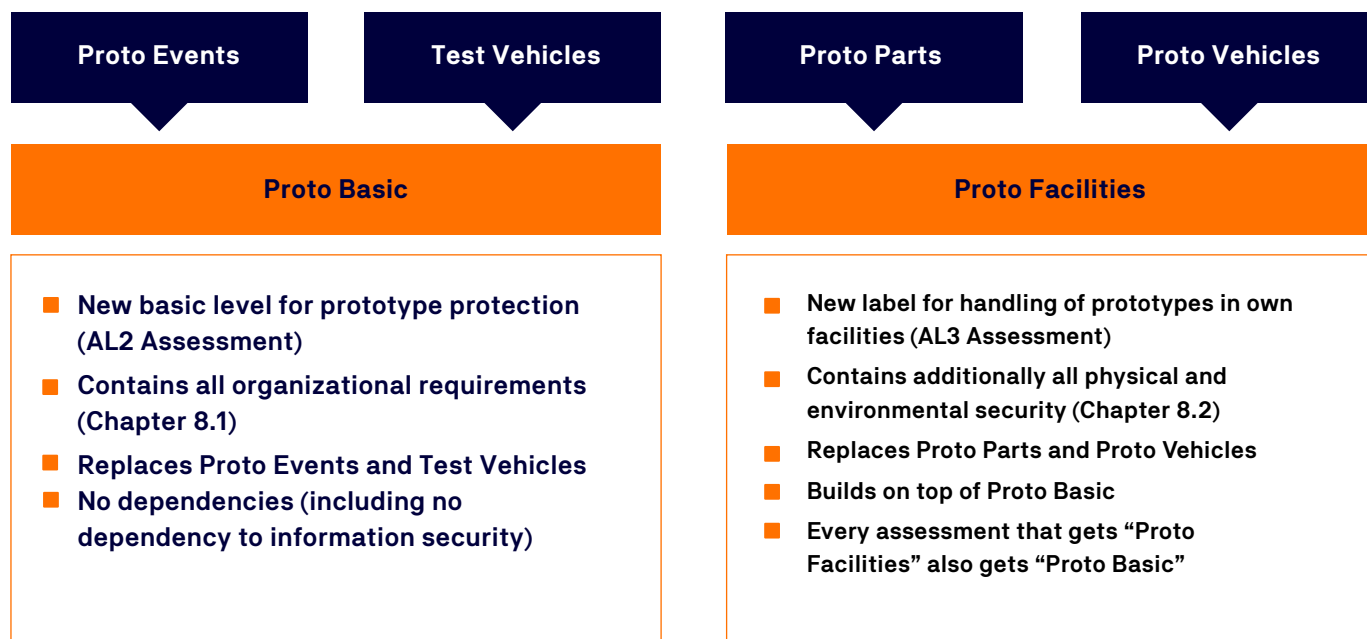
This reorganisation is intended to make the catalogue simpler, more comprehensible and easier to audit.

In addition, ISA2027 contains new requirements regarding:

- traceability of protected vehicles, components and parts,
- documentation throughout the entire life cycle,
- the regulated return, disposal or recycling of protected items and associated tools in accordance with customer specifications.

The prototype protection labels are being consolidated under ISA2027, resulting in two new prototype protection labels. In future, a distinction will only be made between 'Basic Prototype Protection' – to be verified by a Level 2 assessment – and 'Extended Prototype Protection including Facility Security' – to be verified by a Level 3 assessment.

The old prototype protection labels 'Proto Events' and 'Test Vehicle', which primarily applied to the handling of prototype vehicles, will be merged into the new 'Proto Basic' label, whilst the 'Proto Parts' and 'Proto Vehicles' labels, which primarily covered the development and manufacture of prototype parts and prototype vehicles, are being replaced by the new 'Proto Facilities' label, as the physical protection of the buildings and facilities where the prototype parts or vehicles are developed and manufactured plays a particularly important role.



Who should be looking into ISA2027 now?

The new version is particularly relevant for:

- current TISAX® participants,
- companies with re-assessments scheduled from 2027 onwards,
- suppliers and service providers to the automotive industry,
- development and engineering service providers,
- companies with increased security requirements,
- especially companies with requirements relating to prototype protection.
- Our recommendation: Prepare well in advance

Even though ISA2027 only applies to assessments commissioned from 1 January 2027 onwards, it is advisable to familiarise yourself with the changes well in advance.

In particular, companies should:

- ✓ review their supplier management
- ✓ analyse existing verification and documentation processes
- ✓ involve management and executives more closely in awareness-raising measures
- ✓ evaluate existing processes relating to prototype protection
- ✓ plan the transition from ISA 6 to ISA2027 at an early stage

Conclusion

ISA2027 does not fundamentally redefine TISAX®, but rather builds on it in a targeted manner. The focus is on greater clarity, improved consistency, better predictability and greater consideration of risks within the supply chain.

For companies, this means one thing above all: information security remains a crucial factor for success in the automotive industry. Those who take these developments into account at an early stage and adapt their processes in good time will lay the foundations for an efficient assessment and a resilient organisation.

As an experienced TISAX® assessment provider, TÜV NORD CERT supports companies in evaluating their information security. Drawing on our many years' experience in auditing information security management systems and conducting TISAX® assessments, we support companies with independent assessments and a transparent evaluation of their security maturity.



Contact

TUV NORD Thailand

1858/103-104 23rd Floor Interlink Tower, Debaratna Road, Bangna Tai, Bangna, Bangkok 10260

T +66 2751 4050-52

E thailand@tuv-nord.com



Further
information and
contact form: