Štefan Tóth

TRANSFORMATION OF THE INFORMATION SECURITY SYSTEM ON TISAX

TRANSFORMÁCIA SYSTÉMU INFORMAČNEJ BEZPEČNOSTI NA TISAX

Abstract

The paper is about the transformation and possible complications from the ISO / IEC27001 standard to the TISAX standard. The aim of the work is to point out the differences of similar but still different two standards, the modern attitudes of automobiles in order to create a standard that is not only in the financial but also in the automotive world and will bring a high level of information and personal data protection. Information security management is becoming a direct part of business as such and directly supports secure communication and protection of trade secrets.

Key words

ISO/ IEC 27001, TISAX, information security, information exchange, personal data, protection.

1. Introduction

TISAX or Trusted Information Security Assessment Exchange is a standard that came into force in 2017 as a novelty in the German automotive industry. It is a kind of modified successor to the ISO / IEC27001 standard. Perhaps Europe's largest supply chain for the automotive industry is working with a lot of sensitive information, such as prototypes. Improper treatment poses major business risks, which car manufacturers must avoid. Until now, the burden has been to verify compliance on the part of manufacturers, but this is gradually changing and this new standard leads to joint evaluation and data exchange. The beginnings of this reform date back to 2003, when the German Automobile Industry Association (VDA) created the so-called working group on information security. The aim of this project is to create a modern standard and the result was the VDA information security standard, including the ISA evaluation catalog. The catalog is anchored and part of the already mentioned ISO / IEC27001 standard. The catalog is freely available and serves for self-assessment of the state of information security. Requirements with control questions as well as risk assessment are the basis of the catalog, resp. cooperation of partners in this industry. The VDA has designated the French association ENX as the neutral, governing and supporting body of the TISAX standard. ENX is in the position of approver of audit providers and oversees the results of the audit.

2. Materials and Methods

In July 2020, the White Paper "Information Security Risk Management" was published, which talks about confidentiality, integrity and availability. Describes information assets, respectively. assets, processes or information that need to be protected, e.g. designs, constructions, development know-how of the company and the like. A threat is a circumstance or event that internally or externally threatens an asset and thus the protection of information security. Gaps in processes and systems are defined as vulnerabilities that can directly affect societal threats.

Therefore, if we miss the vulnerability in information security, which activates the threat, it can damage and disrupt the company's strategic goals. This manual only serves as a supplementary document when implementing the requirements of the ISO / IEC27001 and TISAX standards. It describes selected states in the field of information security, which in some way describes and guides the correct implementation of specific sub-areas of these standards. The following table compares some of the requirements of the White Paper and ISO / IEC27001, in the chapters where penetration is necessary, it is necessary to pay attention to both standards. The overall complex differences will be evaluated at the end of this work.

Table 1. Comparison of standards

ISO/IEC27001	VDA White Paper „Information Security Risk Management“
4.1 Understanding the organization and its context	Context of the organization, page 4
4.2 Understanding the needs and expectations of stakeholders	Context of the organization, page 4
4.3 Determining the scope of the information security management system	Scope of ISMS, page 6
4.4 Information security management system	
5.1 Leadership and commitment	
5.2 Policy	
5.3 Organizational roles, responsibilities and powers	Roles, competencies and responsibilities, representation in roles, page 6.
6.1 Activities to address risks and opportunities	Risk Management, pages 6 to 16
6.2 Information security goals and planning to achieve them	
7.1 Resources	
7.2 Competences	
7.3 Awareness	
7.4 Communication	
7.5 Documented information	Documentation and report, page 17
8.1 Operational planning and management	
8.2 Information security risk assessment	
8.3 Addressing information security risks	
9.1 Monitoring, measurement, analysis and evaluation	
9.2 Internal audit	

9.3 Management review	
10.1 Nonconformity and corrective actions	
10.2 Continuous improvement	

Source: own processing

3. Results

Let me describe a few basic rules of risk management under the VDA ISA. The role of the risk manager is to control the risk management in the company, consolidate them and report the current situation to the top management. The role of the manager is to define processes, appropriate methods, including tools for ensuring the target quality of risk management. Each defined risk has an assigned owner who is responsible and evaluates his risks. It can define the implementation of evaluation and treatment, but not responsibilities. The identification of threats is the responsibility of each employee, who must report such a fact to the risk owner or risk manager. Risks must be systematically recorded during the course of other processes, but must be taken into account in the short term in the context of risk management. The result of the collection is a risk register, where it is necessary to classify very high, high, medium and low risks and at the same time assign owners. The register is the absolute basis for risk management. Risk assessment consists of identification and analysis.

Identification has various aspects such as the identification of assets, threats and vulnerabilities. Possible tools for risk identification are workshops, self-assessments and the like. The identification of relevant threats consists primarily of the experience of technical experts in the information structure, the experience of previous incidents and standardized threat catalogs. An integral part of risk identification activity is regular testing of infrastructure vulnerabilities.

Risk analysis consists in assessing the existing risk in risk classes. The risk class can be defined, for example, by a multiple of the probability of occurrence and potential damage. Probability of occurrence defines the probability of exploiting a vulnerability. Each risk is therefore assessed according to the probability, occurrence and extent of the damage. Based on these properties, it is possible to define a matrix in which we can evaluate the significant risks that the organization should address. Ultimately, there are these options for dealing with the final risks, avoiding them through measures, mitigating the risks, transferring or accepting the risks. Risk avoidance is acceptance, resp. failure to take measures, processes that cause risks. Risk mitigation is the most common way to deal with risk. These are usually technical, organizational or procedural measures that mitigate the risk ultimately. The transfer, or transfer, of the risk is usually done through a third party, that is, instead of performing a specific risk process internally, the process is purchased. The owner decides on the acceptance of the risk, who must take into account the possible consequences. In order to continuously manage risk management, it is necessary to establish a procedure for monitoring the defined measures from the risk analysis. Where necessary, room for countermeasures must be guaranteed in the event of the original measures being ineffective.

We are moving directly to TISAX and thus a credible exchange of information security information. The research goal of my descriptive research design is to review the implementation of the TISAX standard in an automotive organization with ISO / IEC27001 certification. It is a process through which the partner demonstrates its level of information security according to the VDA ISA and will communicate these results securely, resp. exchange. TISAX is intended for all organizations that need or want to demonstrate their level of information security. One of the ways to prove an effective information security system is certification according to ISO / IEC27001. TISAX recognizes and recommends this standard for the creation of a management system. At the same time, the main actors of the VDA agreed to create a system by which suppliers and all partners in the chain can exchange information about the level of information security they meet. This system is called TISAX and purpose-built for the automotive industry. It consists of three main steps:

- test by provider,

- exchange of information on the result of the test with partners.

Registration means providing contact and billing information, accepting the terms and conditions and defining the scope of information security control on the ENX portal. The essential difference between the TISAX standard and ISO / IEC27001 is that we are only talking about participants in the information exchange. This means that we do not use the term customer or supplier. The organization that seeks to demonstrate the level of information security is in the position of an active participant, the organization that will require, respectively. exchanging result information is a passive participant. The following figure is an example from the above research sample.

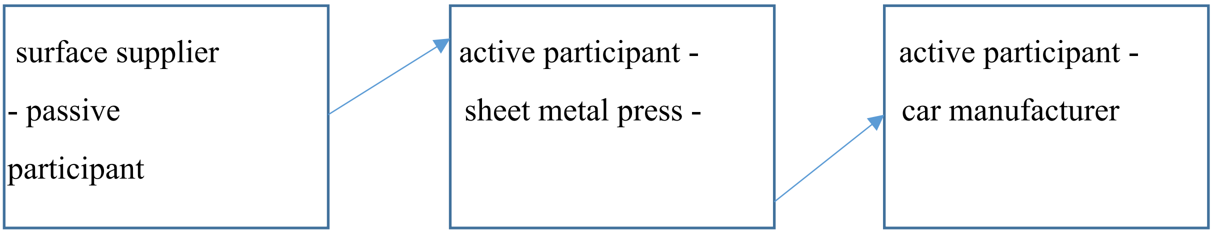


Figure 1. TISAX participants

Source: own processing

It is clear from the figure that participants can become both active and passive participants in the whole process. During registration, an agreement is concluded between the active participant and TISAX in this case, the general conditions of TISAX participation. The terms and conditions govern the relationship between the participants, including rights and obligations. The most important point of the conditions is the confidential treatment of the evaluation results. The rules are the same for everyone without distinction. As a next step, it is necessary to define the scope of evaluation, resp. SCOPE. Specifies what the provider must verify with the subscriber. It is essential to maintain a high degree of precision in defining the scope. Otherwise, the test result may not be a reflection of the current situation and the costs of the verification may differ from those planned. The scope of the test can be standard or custom, tailored to your own needs. It is usually a good idea to choose a standard range, as it is predefined and does not need to be modified.

The standard scope comprises all processes and involved resources at the sites defined below that are subject to security requirements from partners in the automotive industry. Involved processes and resources include collection of information, storage of information and processing of information.

Examples for involved resources: Work equipment, employees, IT systems including cloud services such as infrastructure/ platform/software as a service, physical sites, relevant contractors

Examples for sites: Office sites, development sites, production sites, data centres

Examples for involved resources: Work equipment, employees, IT systems including cloud services such as infrastructure/ platform/software as a service, physical sites, relevant contractors

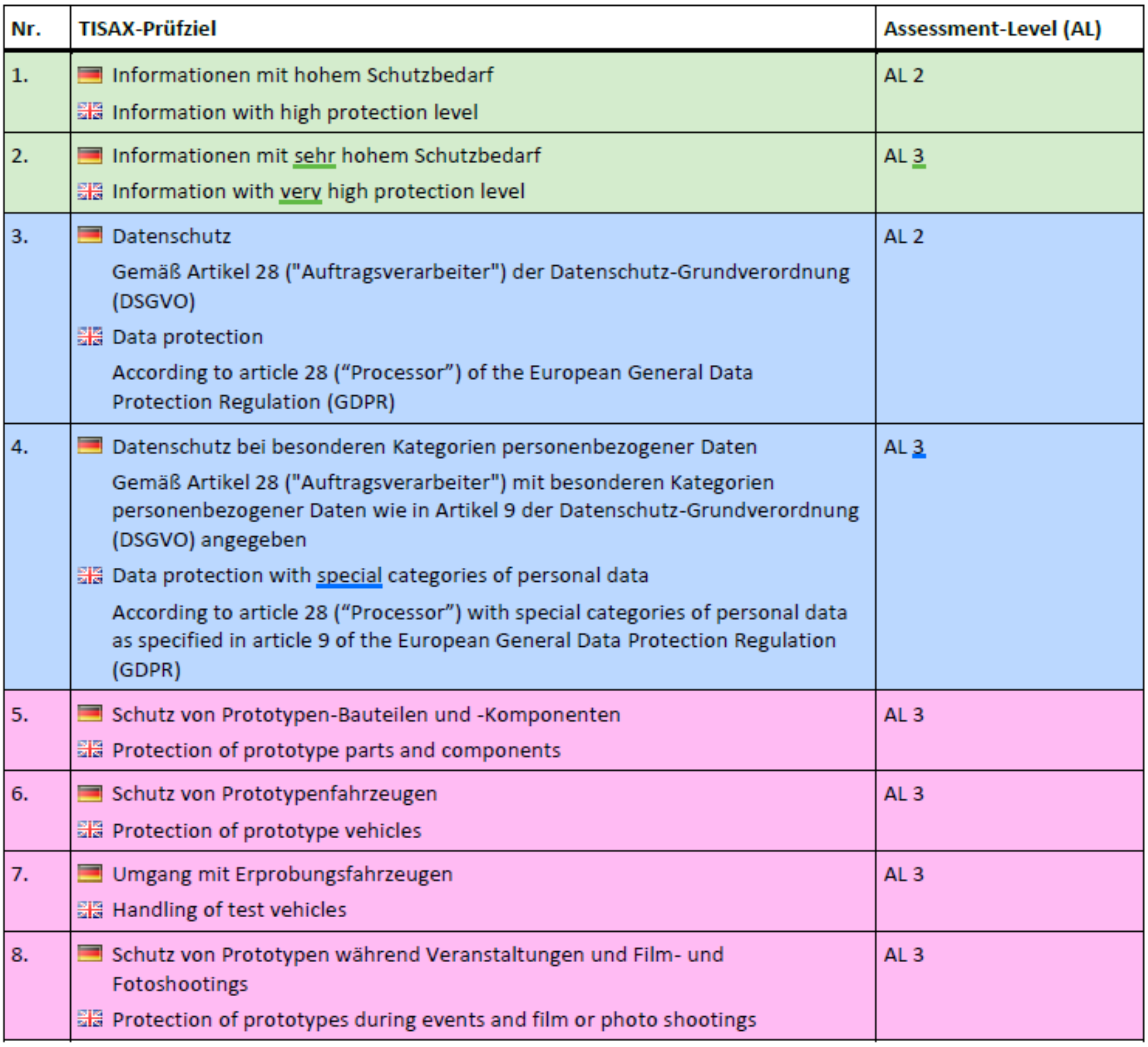
Examples for sites: Office sites, development sites, production sites, data centres

Figure 2. TISAX standard range

Source: TISAX-Teilnehmerhandbuch Version 2.2.pdf

The participant may also decide to shorten or extend the standard scope. As a rule, it is not recommended to shorten the scope, it may happen that other participants may not recognize the results. In case the participant, ie the company has more branches, it is necessary to consider how the scope will be defined. Sometimes it is better to define your own scope for each branch. The reason is, for example, the result of a branch, which conditions the issuance of a central result with one scope for all branches, or already verified branches will be blocked by the issuance of the result by branches that have not yet been audited. It is necessary to gather a lot of information about the company when registering and defining the scope, such as company name, supplier number, branches, company protection, area of operation, number of employees, number of employees in the information area and certificates issued. The clerk and his representative with whom the process will be communicated are also mentioned. It is necessary to know the ID of the active participant so that we can share the current status with him, resp. process results. The participant can decide with whom he wants to share his result and to what level.

During registration, the objectives of the evaluation are defined, determining the relevant requirements of the information security management system. It is based on the type of data that is processed with the partner. Another option, the most used, is to set the "AL" rating level, as shown in the next figure.



Nr.	TISAX-Prüfziel	Assessment-Level (AL)
1.	🇩🇪 Informationen mit hohem Schutzbedarf 🇬🇧 Information with high protection level	AL 2
2.	🇩🇪 Informationen mit sehr hohem Schutzbedarf 🇬🇧 Information with very high protection level	AL 3
3.	🇩🇪 Datenschutz Gemäß Artikel 28 ("Auftragsverarbeiter") der Datenschutz-Grundverordnung (DSGVO) 🇬🇧 Data protection According to article 28 ("Processor") of the European General Data Protection Regulation (GDPR)	AL 2
4.	🇩🇪 Datenschutz bei besonderen Kategorien personenbezogener Daten Gemäß Artikel 28 ("Auftragsverarbeiter") mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben 🇬🇧 Data protection with special categories of personal data According to article 28 ("Processor") with special categories of personal data as specified in article 9 of the European General Data Protection Regulation (GDPR)	AL 3
5.	🇩🇪 Schutz von Prototypen-Bauteilen und -Komponenten 🇬🇧 Protection of prototype parts and components	AL 3
6.	🇩🇪 Schutz von Prototypenfahrzeugen 🇬🇧 Protection of prototype vehicles	AL 3
7.	🇩🇪 Umgang mit Erprobungsfahrzeugen 🇬🇧 Handling of test vehicles	AL 3
8.	🇩🇪 Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings 🇬🇧 Protection of prototypes during events and film or photo shootings	AL 3

Figure 3. Assignment of TISAX targets to AL (Assessment-Leveln)

Source: TISAX-Teilnehmerhandbuch Version 2.2.pdf

The AL 1 assessment level is intended for internal self-assessment, in which the examiner checks the completeness of the self-assessment without providing evidence. It is the lowest level of reliability and therefore this level is not commonly used in TISAX.

The level of AL 2 assessment differs not only from the completeness check but also from the evidence presented at all sites examined. It is usually checked verbally or by conference and usually the on-site test is not performed except for exceptions such as prototype protection.

The AL 3 assessment level is a complete review of all tests as at the previous level, but all controls will be comprehensive and in-depth examined on site and through face-to-face interviews.

Table 2. Comparison of standards

Test method	AL 1 (normal)	AL 2 (high)	AL 3 (very high)
Self-propelled	Y	Y	Y
Evidence	N	Verification	Detailed verification
Interviews	N	Conference	Personally in place
On-site verification	N	As needed	Y

Source: vlastné spracovanie

TISAX does not require suppliers to be subject to the same requirements. However, it is necessary to follow all the principles that have been established in the field of information security when communicating with other parties.

We will move on to the VDA ISA form itself, which contains three sheets of criteria that need to be addressed. The main form is named "Information Security". The questions in it are mandatory for all levels of the TISAX exam. Other "Data Protection" and "Prototype Protection" sheets are optional. The generalization of the requirements is described in the following table.

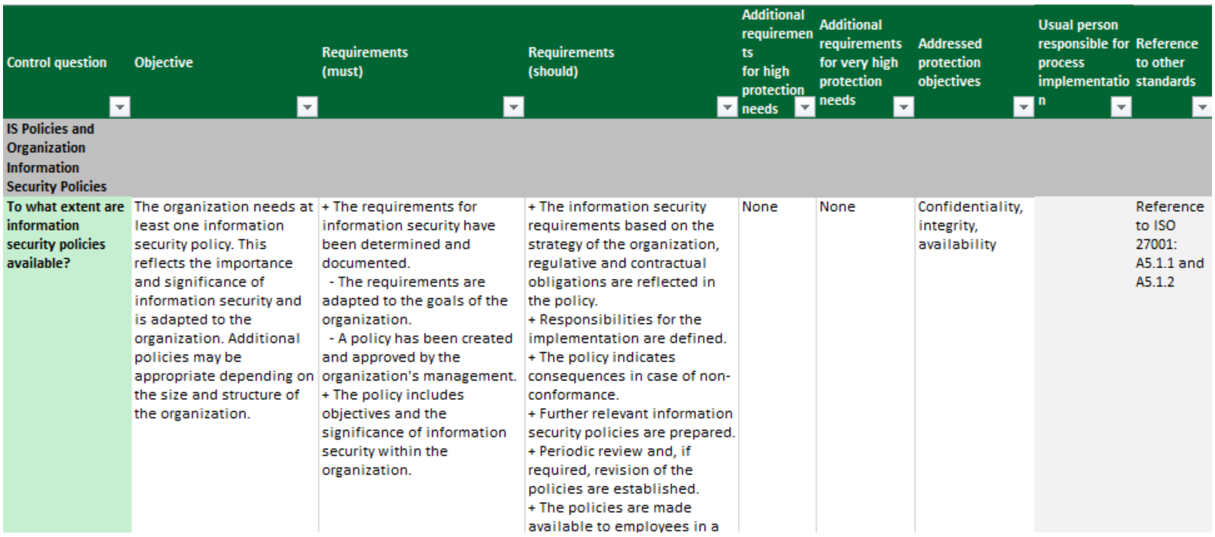
Table 3. General requirements of the standards

General requirements	AL 1 (normal)	AL 2 (high)	AL 3 (very high)
Requirements for access to information and applications are dedicated. The authorization procedure is defined and contains at least the following aspects: - application, inspection and approval procedure, - use of authorizations, - separation of functions, - the principle of minimization. The instructions are binding for all users. Access rights are constantly being tested and monitored.	x	x	x
Access rights are released through the responsible user. Access rights are regularly tested, for example on a quarterly basis.		x	x
Functions in applications are limited by users as much as possible and necessary. Prevent unauthorized access, such as passwords, physical locking, and the like.			x

Source: own procesing

The manual also mentions the method of payment, price list and the like. The price list is public and is available on the ENX portal. In principle, TISAX certification is cheaper than ISO / IEC27001 certification due to the fact that TISAX is inspected every three years, while after ISO / IEC27001 certification two more control audits are needed in an annual cycle, which makes the whole certification more expensive. However, it is important that even when tested according to TISAX, a complete implementation of the ISO / IEC27001 standard is required, on which TISAX is based and regulated by new rules.

After successful completion of all previous points, a self-assessment follows according to the current form from the ENX portal. Its version can change continuously, so it is necessary to monitor the portal and always use the current version. We are currently working with VDA version ISA 5.0.2, it is only available in German and English. The first sheet is welcome, it is necessary to fill in the second sheet with information about the organization, ID and the like. The third sheet describes in detail the levels of maturity of the information security system. For the organization, the research sample, we chose the highest level of AL3, which results in a level of maturity 3, ie an established information security management system. Sheets that are subject to self-assessment are highlighted in orange, the first is the area of information security, the second is focused on prototypes and the third on data protection. Levels AL1 and AL2 correspond to at least the first sheet, or the second if relevant. The third sheet is voluntary and mandatory for level AL3. In the information security sheet, it is first necessary to fill in the level of maturity, which in this case is level 3. The next column is for the self-assessor, who provides links to individual documents where the requirements of the line are implemented. In a provider test, the auditor will use these links to guide and review compliance. The following table translates the requirements of Chapters 1.1. Each subchapter has a main question and then a supplementary question according to the level. We chose the highest level of AL3, which means that all the supplementary questions are relevant.



Control question	Objective	Requirements (must)	Requirements (should)	Additional requirements for high protection needs	Additional requirements for very high protection needs	Addressed protection objectives	Usual person responsible for process implementation	Reference to other standards
IS Policies and Organization Information Security Policies								
To what extent are information security policies available?	The organization needs at least one information security policy. This reflects the importance and significance of information security and is adapted to the organization. Additional policies may be appropriate depending on the size and structure of the organization.	+ The requirements for information security have been determined and documented. - The requirements are adapted to the goals of the organization. - A policy has been created and approved by the organization's management. + The policy includes objectives and the significance of information security within the organization.	+ The information security requirements based on the strategy of the organization, regulative and contractual obligations are reflected in the policy. + Responsibilities for the implementation are defined. + The policy indicates consequences in case of non-conformance. + Further relevant information security policies are prepared. + Periodic review and, if required, revision of the policies are established. + The policies are made available to employees in a	None	None	Confidentiality, integrity, availability		Reference to ISO 27001: A5.1.1 and A5.1.2

Figure 4. Information security questions 1.1

Source: VDA ISA 5.0.2 EN

The requirements are very extensive and the form also serves as a guide for the first certification or for the first implementation of the requirements. The questions interpret all the requirements of ISO / IEC27001. It is good to note that an established system can occur only after a long period of operation of the information security management system. Logically, a passive participant cannot reach maturity level 3 or AL3 immediately after implementing the requirements. The participant must mature to this level through a living system. The requirements are structured up to chapter 7.1. After completing the entire questionnaire, respectively. all relevant sheets are passed the results to the mediator. The date of the audit will be agreed according to the specified scope.

The test consists of four steps, namely preparation, selection of the provider, examination of the security of the information and the result of the test. The TISAX audit has the same requirements as all other ISO audits. The auditor must comply with the requirements of ISO19001 and take into account the requirements of ISO / IEC27001 to which TISAX refers when auditing. The auditor goes through the individual questions and looks for compliance with the requirements in the documents to which the passive participant referred. According to the audit plan, the auditor also verifies the effectiveness of the system in practice, by observation, physical examination, interviews and the like. The scope of the audit is significantly shorter than that of ISO / IEC27001, which means that only the effectiveness of the operation of the information security management system is actually verified. If the audit does not show compliance, there is no room for further discussions, non-compliance is automatically evaluated, resp. a derogation which must be rectified in accordance with the rules by a specified date, until which time the TISAX label cannot be issued. The auditor after the audit of the report, resp. The ISA VDA form is sent to the provider's headquarters, and after an internal veto, the message is uploaded to ENX, where an independent check of the results and completeness of the form takes place. Only after the successful completion of this step can the results be exchanged between the participants.

The last step is the exchange, respectively. sharing the evaluation result with partners. The result is valid for three years and then needs to be renewed in the same way. For participants, this is an advantage in terms of a reduced frequency of audits, it can also result in a negative, where the system is not monitored by a third party and is less maintained. The results are easily shared with the partner ID on the ENX portal. This exchange concludes the TISAX process for a period of three years.

4. Conclusion

The research goal of my descriptive research design was to review the implementation of the TISAX standard in an automotive organization with ISO / IEC27001 certification. At the end of my work I evaluate the fulfillment of the goal. The following findings have been made. Obtaining the TISAX label is only possible after implementing the requirements of the ISO / IEC27001 standard. This extensive standard defines a number of documentary and technical measures that an organization has the ability to regulate in terms of selecting certain requirements that it will not implement. These unimplemented requirements may be assessed by the organization as accepted residual risks. The auditor must consider such acceptance and will not affect the outcome of the audit. With the TISAX standard, the regulation is strict and it is not possible to correct it from the participants. There are clear levels of AL to which the individual questions in the chapters belong. In case of non-compliance it is not possible to issue a TISAX label, the standard does not recognize exceptions or exclusions. From this point of view, TISAX is more efficient, is subject to active communication between the passive and active participants, and the scope of the requirements of the individual levels is identical for all applicants. The exchange of results is private, secure and directly bridges participants through the ENX portal. There is a presumption that this form of result exchange will be used in other international standards in the future. In my work, I pointed to a new standard in the automotive industry, where special emphasis is placed on the secure processing of sensitive information and personal data, a comparison of the standard with existing standards and a short manual to familiarize yourself with the verification process. In general, there is a smooth transition of participants from ISO / IEC27001 to the TISAX standard, provided that, depending on the level, requirements are added that may have been exempted as accepted in the original system.

References

[1] GRAUZEL, J. STN EN ISO 9001 Systém manažérstva kvality - Požiadavky. 2016, p. 60 [17-21] Bratislava: ÚpNMaS. 122449

[2] GRAUZEĽ, J. STN EN ISO19011 Návod na auditovanie systémov manažérstva. 2019. p. 76 [10-70] Bratislava: ÚpNMaS, 128839

[3] Manažérstvo rizika STN ISO 31000. 2019. p. 32 [20-25] Bratislava: ÚpNMaS, 127846

[4] Másilko, J. IATF Příručka auditora pro IATF16949. 2020. p. 43 [30-35] Praha: Česká společnost pro jakost, ISBN 978-80-02-02908-3

[5] Riadenie rizík informačnej bezpečnosti STN ISO/IEC 27005. p. 116 [20-100] Bratislava: Slovenský ústav technickej normalizácie, 114598

[6] STRNÁD, O. *Systémový prístup k riadeniu informačnej bezpečnosti.* 1. vyd. p. 233 [20-200] Trnava: SP Synergia, ISBN 978-80-89291-20-5

[7] STRNÁD, O. *Systém riadenia informačnej bezpečnosti – Aplikovanie procesného riadenia*. 2011. p. 241 [20-200] Ostrava: Amos, ISBN 978-80-904766-6-0

[8] Systémy riadenia informačnej bezpečnosti STN ISO/IEC 27001. 2014. p. 48 [5-40] Bratislava: ÚpNMaS, 119076

[9] VDA ISA catalogue version 5.0. 2020. Dostupné na internete: <https://www.vda.de/en/services/Publications/vda-isa-catalogue-version-5.0.html>

Kontaktná adresa autora, autorov:

PaedDr. Štefan Tóth

Katedra manažmentu

Fakulta manažmentu, Prešovská univerzita v Prešove

Ulica 17. Novembra č. 15

080 01 Prešov

stefan.toth@smail.unipo.sk

stefan.toth.sk@gmail.com