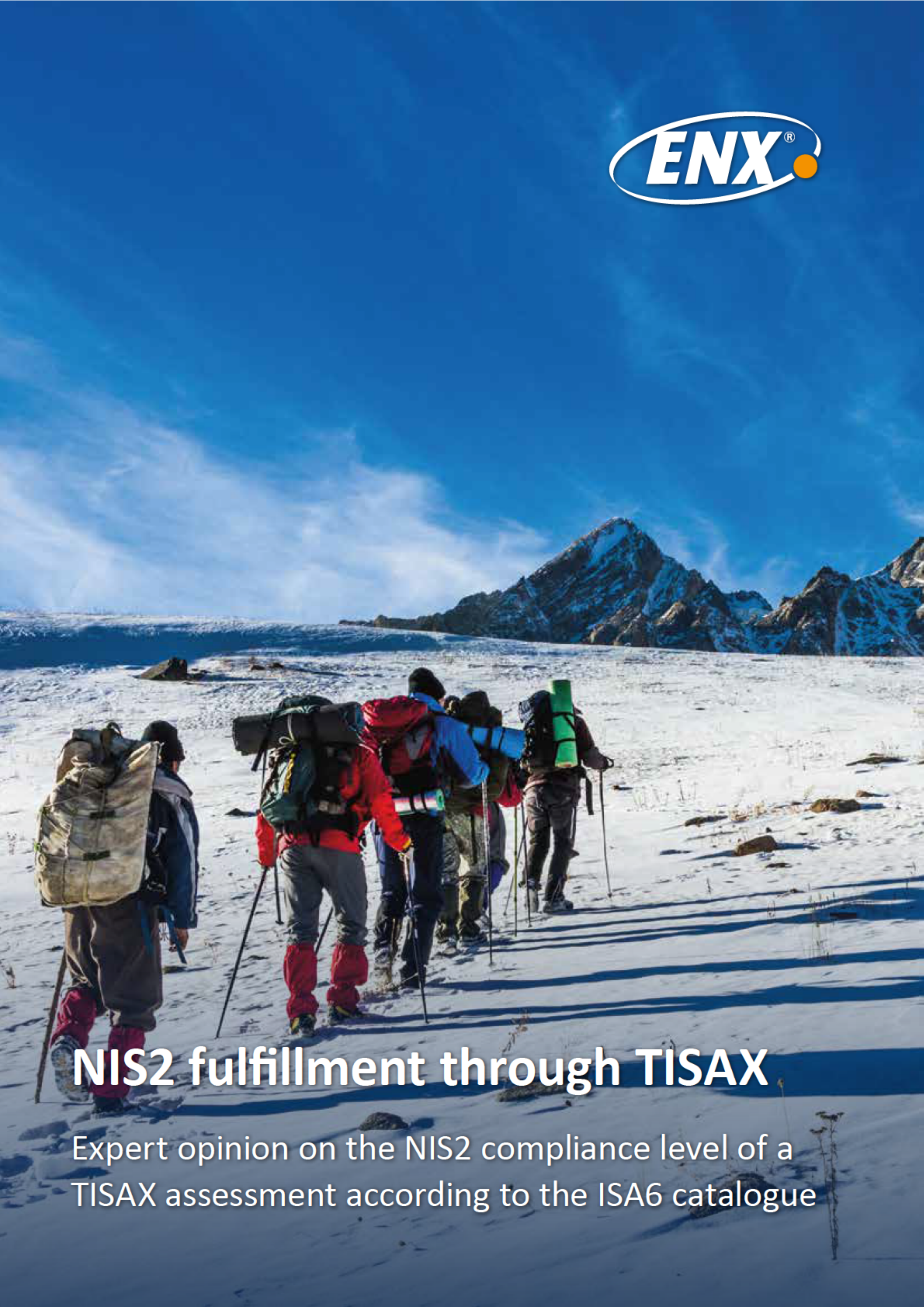

NIS2 fulfillment through TISAX

Expert opinion on the NIS2 compliance level of a TISAX assessment according to the ISA6 catalogue

Published by

ENX Association
Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany
20 rue Barthélémy Danjou, 92100 Boulogne-Billancourt, France

An Association according to the French Law of 1901, registered under No. W923004198 at the Sous-préfecture of Boulogne-Billancourt, France.

Editor

ENX WG ISA 2025

Contact

wg-isa@groups.enx.com

+49 69 9866927-79

Version

Date: 24.04.2025, Version: 1

Classification: public, ENX doc ID: 260

Legal Notices

The content of this document was prepared with utmost care. However, ENX Association does not guarantee the accuracy, completeness, or timeliness of the information provided.

ENX Association shall not be held liable for any direct or indirect damages arising from the use of, or inability to use, this information. All information is provided "as is." Any legal claims relating to this publication or its usage are subject to the laws of the Federal Republic of Germany.

This document may contain references or links to external websites. ENX Association has no influence on the content of external sites and assumes no liability for them. Responsibility for external content lies exclusively with the operators of the linked sites.

If you have questions about these legal notices, please contact legal@enx.com or
ENX Association, Bockenheimer Landstraße 97-99, 60325 Frankfurt am Main, Germany.

Table of contents

Executive Summary

The NIS2 Directive imposes requirements on a large number of companies in the automotive industry.

In the **automotive industry**, the need for industry-wide information and Cybersecurity has been recognized for years. The automotive industry has addressed the strengthening of **cyber resilience** in a structured manner. Measures of the industry include the establishment of the TISAX assessment standard in 2017 and its underlying ISA requirements catalogue, on the basis of which far more than 17,500 locations have already been assessed.

The structured analysis laid out in this document shows that companies that have set up their sites that are affected by NIS2 in a TISAX-compliant manner have fully implemented the requirements of NIS2. The catalogue of requirements (ISA) and its application in all TISAX assessments extends beyond the requirements for companies' information and Cybersecurity formulated in NIS2.

The catalogue of requirements is continuously developed by a committee of experts and used by thousands of companies worldwide. New insights from the field of information- and cybersecurity are taken into account. The catalogue of requirements and the assessment standard thus define the **state of the art** in information and cybersecurity for the industry and permanently uphold this claim.

The respective implementation is confirmed by independent auditors in a three-year cycle. According to experts in the automotive industry for information and Cybersecurity, the three-year cycle of the TISAX assessment is considered appropriate.

A common exchange mechanism enables the participating organizations to query the TISAX status of a supplier or partner - and thus also compliance with the NIS2 requirements - at any time.

Thanks to the automotive industry's intrinsically motivated involvement with information and Cybersecurity over the past few years, significant parts of the automotive supply industry and its partners are already prepared for the material requirements of regulation (NIS2).

It remains necessary for all organizations concerned to maintain and operate the different national reporting requirements in parallel.

1 Introduction and overview

1.1 Purpose of this analysis

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, abbreviated as NIS2 Directive, is an EU directive that aims to strengthen the level of cyber resilience in the European Union. It replaced the EU Network and Information Security (NIS 1) Directive from 2016.

Among other things, NIS2 takes up the standardization of the specification of the affected companies within the member states and expands the scope of the affected organizations. As a result, companies that were not affected by the NIS 1-Directive must now also deal with the content and requirements.

The automotive industry has recognized the need for industry-wide information- and cybersecurity for years and is addressed in a structured manner - among other things through the development of the TISAX Assessment standard and the ISA requirements catalogue on which it is based. The controls formulated in the ISA catalogue serve the same purpose as the measures defined in NIS2: Companies build up cybersecurity capacities and capabilities and ensure the continuity of services. The industry not only protects itself but also makes an essential contribution to the smooth functioning of the economy and society in the European Union.

To assist companies that need to comply with NIS2 in assessing measures to be implemented, ENX Association's Working Group (WG) ISA, a working group of leading experts in the automotive industry for information- and cybersecurity, has compared the current TISAX requirements catalogue ISA6 with the requirements resulting from NIS2.

The group analysed whether and to what extent the establishment and subsequent assessment of an organization in accordance with ISA and TISAX covers the requirements set out in NIS2.

1.2 Scope of this analysis

This analysis considers exclusively the requirements defined in the NIS2 Directive, which contain specific implementation guidelines for companies.

The document does not provide any assistance in the implementation or realization of an information security management system (ISMS) or in the preparation of a TISAX assessment, nor does it make any statement as to whether a company is sufficiently prepared to meet the requirements of NIS2.

When assessing the degree of compliance, the document refers to a TISAX assessment carried out in accordance with the information- and cybersecurity requirements formulated in the ISA catalogue. [1]

The analysis looks at the direct requirements of the NIS2 Directive. Country-specific implementations such as national cybersecurity regulations, competent national authorities, cyber crisis management authorities, central contact points for cybersecurity (central contact points) and computer security incident response teams (CSIRTs) and possible additional material requirements are not considered within this document.

It remains the responsibility of the companies to find out about possible country-specific additional requirements and to check these against the measures implemented.

[1] Pure assessments in the area of prototype protection do not provide sufficient information with regard to information- and cybersecurity.

TISAX assessments are based on the risk exposure of the assessed company. The classification of companies according to their degree of criticality in relation to their sector or the type of services they provide is in line with the requirements of NIS2.

A prerequisite for the applicability of the conclusions of this document is that the TISAX Assessment objectives reflect the overall risk to which the company is exposed and that all company sites affected by the requirements of the NIS2 Directive have corresponding TISAX labels.

1.3 Target group of the document

This document is aimed at experts from all companies that are affected by the NIS2 Directive and use TISAX for the risk management of their supply chains and value -added networks with regard to information- and cybersecurity or undergo a TISAX assessment themselves.

Furthermore, this analysis may serve as a basis for an assessment of compliance with the NIS2 requirements by authorities (competent authorities) or bodies responsible for cybersecurity and the supervisory tasks referred to in Chapter VII/NIS2.

1.4 Document structure and methodology

The structure of the document is designed to provide an objective evaluation of the extent to which a TISAX assessment can be seen as proof of compliance with the requirements of EU Directive 2022/2555 ("NIS2 Directive"). The underlying evaluation was carried out by leading information and cybersecurity experts from the automotive industry and market-leading audit providers.

The document follows the methodology of an expert opinion and allows the reader to work with the document at different levels of detail.

Structure:

1. Each relevant article of the NIS2 Directive is presented in a separate chapter
2. Each relevant paragraph of an article is presented in a sub-chapter with the following sections:
    a) Specification of the requirement from the NIS2 Directive
    b) Mention of the control questions from the ISA6[2] that deal with the question
    c) Detailing the control questions to the individual controls that relate to the question
    d) Concluding summary of the degree of fulfilment of the requirements of the paragraph

The last section (2d) of each sub-chapter thus provides an overview of the fulfilment.

For a more in-depth analysis, the second section (2b) can be used to draw conclusions about the associated control questions from ISA6 (Information Security spreadsheet, column H).

The highest level of detail is achieved by adding the other section (2c). The individual controls that contain the requirements of NIS2 are named and listed in detail here. The font colour of the control questions inserted from ISA6 has been adapted for better identification.

[2] https://portal.enx.com/de-DE/TISAX/downloads/

2 TISAX Assessment and underlying catalogue of requirements

2.1 Definition of the TISAX Assessment Scopes

In the assessment, the document refers to TISAX assessments conducted in accordance with ISA catalogue version 6 (ISA6). The audits are carried out by an independent auditor in a three-year cycle after being commissioned.

It is important to understand that the definition of the TISAX Assessment Scope differs from ISO management system certifications in terms of the requirements for defining the assessment scope.

For ISO/IEC 27001 certification, the audited organization defines the scope of its ISMS (in the "scope statement"). The organization is completely free to define this scope. However, the scope of the audit (also known as the "audit scope") must be identical to the scope of the ISMS. In the case of ISO/IEC 27001 certification, the scope of the audit can be influenced by the way in which the scope of the ISMS is defined.

In contrast to ISO/IEC 27001, it was decided for TISAX that the following generally defined standard scope must be used for TISAX assessments:

"The TISAX scope defines the scope of the assessment. The assessment includes all processes, procedures and resources involved that are under the responsibility of the organization to be assessed and that are relevant to the security of the objects of protection defined in the stated assessment objectives and their protection goals at the listed locations.

The examination is conducted at least at the highest Assessment Level required in one of the listed TISAX Assessment Objectives. All criteria required in the listed TISAX Assessment Objectives are the subject of the examination."

The scope of the assessment can be equal to or smaller than the scope of the ISMS. However, it must be within the scope of the ISMS and must always include all elements that make up an ISMS.

This makes TISAX assessments comparable across companies and ensures a similar level of security. In contrast to other assessment mechanisms (e.g. ISO Management System certifications), there is no risk of a narrow view of the company to be assessed due to individually designed scopes.

What both standards have in common is, that the official statement of conformity only applies to the sites that have been included in the scope. If a company wishes to assess and improve its conformity with NIS2 on the basis of ISO/IEC 27001 or TISAX, all sites must be included in the scope in order to obtain a statement for the entire company. This assumption of identity between the company and the sites involved forms an important basis for the following statements in this report on NIS2 and TISAX.

2.2 TISAX Assessment Objectives

In TISAX assessments, Assessment Objectives specified in the standard within the assessment scope serve as a benchmark for the extent to which the information security management system is assessed. This allows the company being assessed to scale the assessment content based on the risks, i.e. the criticality and type of information processed. The assessment objectives standardized in TISAX are shown in Table 1.

Assessment Objective	Description
Confidential	Handling information with high protection needs in the context of confidentiality (access to confidential information)
Strictly Confidential	Handling information with very high protection needs in the context of confidentiality (access to strictly confidential information)
High Availability	Handling of information with high protection needs within the scope of availability (high availability of information)
Very High Availability	Handling of information with very high protection needs in the context of availability (very high availability of information)
Proto Parts	Protection of prototype parts and components
Proto Vehicles	Protection of prototype vehicles
Test Vehicles	Dealing with test vehicles
Proto Events	Protection of prototypes during events and film and photo shoots
Data	Data protection pursuant to Article 28 ("Processor") of the General Data Protection Regulation (GDPR)
Special Data	Data protection in accordance with Article 28 ("Processor") of the General Data Protection Regulation (GDPR) with special categories of personal data as specified in Article 9 of the General Data Protection Regulation (GDPR)

Table1 - TISAX Assessment Objectives

Based on the selection of the assessment objectives, various criteria with different characteristics from the ISA6 catalogue are used within the TISAX assessment. The scope of control and the assessment level (AL) to be used are thus specified via the assessment objectives.

2.3 TISAX Scope and Assessment Level (AL)

A distinction is made between Assessment Levels 1, 2 and 3. The Assessment Levels are explicitly assigned to the Assessment Objectives. Assessments at Assessment Level 1 usually play a role for internal purposes in the actual sense of a self-assessment. In an AL 1 assessment, an auditor checks whether a self-assessment has been completed. The auditor does not check the content of the self-assessment. No further evidence is required. The results of assessments with AL1 have a low confidence level and are therefore not used in TISAX. However, it is of course possible for your partner to request such a self-assessment outside of TISAX.

If Assessment Objectives with different ALs are used, the highest ranked Assessment Objective is used within the overall assessment. The assignment of Assessment Objectives to Assessment Levels can be found in Table 2.

In an AL 2 assessment, the audit provider carries out a plausibility check of the self-assessment of the company (for all locations in the assessment scope). It ensures this by checking evidence and conducting an interview with the person with overall responsibility for information security. The audit provider usually conducts the interview as a web conference.

TISAX test	**Assessment Level (AL)**
Confidential	AL 2
Strictly Confidential	AL 3
High Availability	AL 2
Very High Availability	AL 3
Proto Parts	AL 3
Proto Vehicles	AL 3
Test Vehicles	AL 2
Proto Events	AL 2
Data	AL 2
Special Data	AL 3

Table2 - Dependency between TISAX Assessment Objective and TISAX Assessment Level

In an AL 3 assessment, the audit provider conducts a comprehensive review of the assessed company's compliance with the applicable requirements. The auditor uses the self-assessment, and the documents submitted to prepare for the assessment. However, in contrast to an AL 2 assessment, the auditor will review everything:

- check documents and proof of implementation
- conduct planned interviews with the process owners
- consider the local conditions
- observe the implementation of processes
- conduct unplanned interviews with process participants

Methodologically, the two approaches differ considerably. In assessment level 2 examinations, the auditor does not verify everything, only checks the plausibility. An assessment in Assessment Level 3 generally takes place on site at all locations in the scope of the company to be assessed. An exception to this is the Simplified Group Assessment (SGA).

2.4 TISAX Group Assessments

2.4.1 Simplified Group Assessment

The TISAX Simplified Group Assessment is designed for companies with many locations, where going through the regular process with an individual assessment of each location would be immensely time-consuming. This procedure is only available to companies that have a centralized and highly developed ISMS.

In TISAX, "centralized and highly developed" is defined as follows:

- The main site must be able to ensure compliance with all ISMS-related rules and guidelines for all sites in the assessment scope.
- The dependent locations must have a reliable channel back to the main location.
- Their feedback must be consistent with the expectations set by the rules and guidelines of the main site.

There are two variants of the Simplified Group Assessment:

- The Simplified Group Assessment on a sampling basis (S-SGA) and
- the Simplified Group Assessment on a rotation plan basis (R-SGA).

The two evaluation procedures are explained below:

2.4.2 Sample based Simplified Group Assessment (S-SGA)

At the main site (usually the company's headquarters), the TISAX auditor assesses the ISMS more extensively than in the regular assessment procedure. For this purpose, the “Additional requirements for Simplified Group Assessments (SGA)” formulated in ISA6 are used. The aim of the additional assessment points is to determine that the company has a centralized and highly developed ISMS. Furthermore, an assessment of sample sites is carried out based on the number of total sites in the scope that are performed at the same assessment level. All other sites are assessed at one assessment level lower than in the regular assessment procedure.

2.4.3 Rotating Schedule based Simplified Group Assessment (R-SGA)

At the main site (usually the company's headquarters), the TISAX auditor assesses the ISMS more extensively than in the regular assessment procedure. For this purpose, the “Additional requirements for Simplified Group Assessments (SGA)” formulated in ISA6 are used. The aim of the additional assessment points is to determine that the company has a centralized and highly developed ISMS. All other locations are assessed at the same assessment level but evenly distributed over the three-year validity period of the TISAX label. The assessment process option R-SGA is NOT available for the Assessment Objectives of prototype protection (prototype parts, prototype vehicles, test vehicles, prototype events).

2.5 TISAX control questions and requirements

The control questions assigned to the assessment objective are detailed in requirements. For each control question, there may be requirements in the areas of must, should, additional requirements for high protection needs, additional requirements for very high protection needs and additional requirements for the simplified group assessment. The meaning of the individual requirement levels can be found in Table 3.

Requirement	**Description of the implementation**
Requirements (must)	The requirements in this column are strict requirements for which there are no exceptions.
Requirements (should)	The requirements in this column must always be implemented by the organization. However, under certain circumstances, there may be a valid justification for not fulfilling these requirements. The impact of deviations must be understood by the organization and the deviation must be justified in a comprehensible manner. It is at the auditor's discretion whether non-compliance is acceptable
Additional requirements for high protection needs	The requirements in this column must also be met if the tested organization has a high protection need.

Additional requirements for very high protection needs	The requirements in this column must also be met if the assessed organization has a very high protection need.
Additional requirements for the Simplified Group Assessment (SGA)	The requirements in this column must also be fulfilled for Simplified Group Assessments. They are then to be understood as "must" requirements.

Table3 - Implementation requirements

The requirements of the additional requirements category for high and very high protection needs are additionally subdivided into the protection objectives (confidentiality (C), integrity (I), and availability (A)). The classification into the protection objectives serves to differentiate the additional requirements according to the assessment objective. For example, in assessments with the Confidential and Strictly Confidential assessment objectives, control questions are used within the additional requirements that are characterized by the Confidentiality "C" protection objective.

In assessments with the assessment objective High Availability and Very High Availability, the control questions are applied within the additional requirements, which are identified by the protection objective Availability "A".

The integrity protection objective is also identified. The corresponding requirements are always checked within the Availability or Confidentiality assessment objectives.

In a regular TISAX assessment, it is expressly not possible to evaluate individual control questions of the assessment catalogue as not applicable (n/a) and thus exclude them. The control questions and their requirements must be implemented holistically by the company. TISAX only gives the auditors the necessary discretion when assessing what is considered appropriate implementation.

2.6 Dealing with deviations in the TISAX model

In addition to checking the existence of documents and processes, the TISAX assessment also includes checking the implementation and its documentation. In addition to the control questions, a maturity model has been established for this purpose that assesses the practical maturity of implementation independently of the formal assessment. The maturity model allows six assessment levels per control question.[3] The target maturity level for a successful TISAX assessment is level three "established". A detailed list of the maturity levels and the associated specification of the assessment requirements can be found in Annex I.

If deviations from the required content are identified during the assessment, these must be implemented within a reasonable period of time, starting with the completion of the assessment. The measures to be implemented to correct the deviations and the associated time periods for implementation are defined in a corrective action plan and approved by the auditor if the requirement is met by implementing the measure. The appropriateness of the implementation period is determined by the auditor. A period of up to three months is generally accepted without question. In justified cases due to particularly complex or long-term measures, this period can be extended to six months or, with appropriate justification, up to nine months.

The auditor checks compliance with the defined measures in a Corrective Action Plan Assessment at the end of the agreed period. If individual or all deviations are not corrected within the nine-month period, the audit is considered failed and must be repeated in full. The submission of a corrective action plan is the basis for the awarding of temporary labels, which are converted into permanent labels once all deviations have been rectified.

[3] The evaluation levels are: incomplete; implemented; controlled; established; predictable and optimizing.

2.7 Validity period of TISAX assessments

The validity period of a TISAX assessment is three years. After these three years, a new full audit of the controls defined in the ISA catalogue according to the defined scope is required to maintain validity. During this three-year period, the company is obliged to continue to pursue the measures specified in the audit and to document their implementation.

In addition, the company must carry out regular internal audits of information security policies and procedures and record and retain the results of the audits carried out. These documents are used as proof of active implementation in the next assessment or during interim assessments.

Interim assessments come into play when there have been changes within the company that directly affect the ISMS or the physical conditions of the company. In these cases, the company is obliged to report these and to commission an interim assessment with the audit service provider who also carried out the main assessment to maintain the status.

The maturity model described above has been established in the TISAX assessment process to quantify the maintenance of the processes over the entire label validity period.

3 NIS2 Article 20

3.1 Evaluation of the degree of fulfilment in accordance with NIS2 Article 20 (1)

3.1.1 Requirement from NIS2

NIS2 Article 20 (1) requires that the governing body of the organization has established relevant structures to implement risk management measures in the area of cybersecurity and to monitor their implementation.

3.1.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 20 (1) is checked in accordance with the following controls:

- 1.2.1: "To what extent is information security managed within the organization?"
- 1.2.2: "To what extent are information security responsibilities organized?"
- 1.4.1: "To what extent are information security risks managed?"
- 1.5.1: "To what extent is compliance with information security ensured in procedures and processes?"
- 1.5.2: "To what extent is the ISMS reviewed by an independent authority?"
- 7.1.1: "To what extent is compliance with regulatory and contractual provisions ensured?"

3.1.3 Detailed requirements within the control questions of ISA6

1.2.1 "To what extent is information security managed within the organization?"

The auditor checks whether the scope to be managed by the information security management system (ISMS) is defined *(Control 1.2.1; Requirements (must); first sub-item: "+ The scope of the ISMS (the organization managed by the ISMS) is defined")* and the requirements for implementation are determined *(Control 1.2.1; Requirements (must); second sub-item: "+ The organization's requirements for the ISMS are determined").* The auditor also checks that the organization's management has commissioned and approved the ISMS *(Control 1.2.1; Requirements (must); third sub-item: "The organizational management has commissioned and approved the ISMS")* to ensure that information security is not just the result of coincidence and individual commitment, but of sustainable management.

The implemented communication channels between the company management and the executors of the ISMS are also checked *(Control 1.2.1; requirements (must); fourth sub-item: + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review)")* to ensure that the control and management tools are also regularly used to maintain the effectiveness of the ISMS *(Control 1.2.1; requirements (must); sixth sub-item: "The effectiveness of the ISMS is regularly reviewed by the management")*.

1.2.2 "To what extent are information security responsibilities organized?"

It is also checked that the responsibilities for the ISMS are defined *(Control 1.2.2; Requirements (must); first sub-item: "+ Responsibilities for information security within the organization are defined, documented, and assigned ")* and communicated *(Control 1.2.2; Requirements (must); fourth sub-item: "+ The contact persons are known within the organization and to relevant business partners ")* and that the necessary resources are available

(Control 1.2.2; Requirements (must); third sub-item: “+ The required resources are available”). The auditor also checks whether an adequate information security structure is in place *(Control 1.2.2; Requirements (should); first sub-item: "+ There is a definition and documentation of an adequate information security structure within the organization")* and that other security roles are considered *(Control 1.2.2; Requirements (should); first sub-item: "- Other relevant security roles are considered")*. Furthermore, the auditor checks that the employees deployed in the area of the ISMS are or will be qualified for their task *(Control 1.2.2; Requirements (must); second sub-item: “+ The responsible employees are defined and qualified for their task”)* and that they are not subject to conflicts of interest *(Control 1.2.2; Requirements (additional requirements for high protection needs); first sub-item: "+ An appropriate organizational separation of responsibilities should be established in order to avoid conflict of interests (separation of duties). (C, I, A)")*.

1.4.1 "To what extent are information security risks managed?"

In order to ensure the functionality and continuous assurance and further development of the risk-based approach of the information security management system, the auditor checks the regular and event-related risk assessments *(Control 1.4.1; Requirements (must); First sub-item: “+ Risk assessments are carried out both at regular intervals and in response to events”)*, as well as the classification and allocation of the recognized risks *(Control 1.4.1; Requirements (must); Second sub-item: “+ Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage)”)* and the handling of security risks *(Control 1.4.1; Requirements (should); First three sub-items: + A procedure is in place defining how to identify, assess and address security risks within the organization. + Criteria for the assessment and handling of security risks exist. + Measures for handling security risks and the persons responsible for these are specified and documented: - A plan of measures or an overview of their state of implementation is followed.)*. The auditor also checks whether a responsible person has been assigned to the identified risks who is responsible for the assessment of the identified risk and its treatment through defined follow-up measures *(Control 1.4.1; Requirements (must); fourth sub-item: + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.)* and that a reassessment takes place in the event of changes to the environment *(Control 1.4.1; Requirements (should); Fourth sub-item: + In case of changes to the environment (e.g. organizational structure, location, changes to regulations), reassessment is carried out in a timely manner.).*

1.5.1 "To what extent is compliance with information security ensured in procedures and processes?"

In a further part of the assessment, the auditor deals with compliance with information security in procedures and processes *(Control 1.5.1; Requirements (must); First sub-item: + Observation of policies is verified throughout the organization)*. The auditor also checks that the assessments of compliance with information security in procedures and processes are carried out at regular intervals *(Control 1.5.1; Requirements (must); Second sub-item: + Information security policies and procedures are reviewed at regular intervals)* according to a defined plan *(Control 1.5.1; Requirements (should); First sub-item: + A plan for content and framework conditions (time schedule, scope, controls) of the reviews to be conducted is provided)* and documented in a traceable manner *(Control 1.5.1; Requirements (must); Fifth sub-item: + The results of the conducted reviews are recorded and retained)*.

1.5.2 "To what extent is the ISMS reviewed by an independent authority?"

The auditor also checks that an assessment is carried out by an independent body at regular intervals or in the event of significant changes *(Control 1.5.2; Requirements (must); First sub-item: + Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes)* and that the results are documented and reported to the organization's management *(Control 1.5.2; Requirements (should); First sub-item: + The results of conducted reviews are documented and reported to the management of the organization)*. Part of the assessment is also to ensure that corrective actions for possible deviations are initiated and pursued *(Control 1.5.2; Requirements (must); Second sub-item: + Measures for correcting potential deviations are initiated and pursued)*.

7.1.1 "To what extent is compliance with regulatory and contractual provisions ensured?"

Parallel to the specification and implementation of the objectives and content of the ISMS, knowledge of regulatory and contractual provisions affecting the organization and their consideration in the implementation of ISMS measures is also checked *(Control 7.1.1; Requirements (must); First sub-item: + Legal, regulatory, and contractual provisions of relevance to information security are determined at regular intervals)* in order to prevent risks to the enforceability of the organization's own information security arising from external influences of laws and regulatory requirements in the event of non-compliance with this requirement.

3.1.4 Summary:

The requirement that the governing body of an organization has created appropriate structures to implement and monitor the implementation of the cybersecurity risk management measures taken to comply with Article 21 (NIS2 Article 20 (1)) is described by the controls defined in the ISA6 assessment standard and is fully checked for existence and implementation by the responsible auditor within a TISAX assessment. By checking the relevant evidence, the auditor ensures that the defined content is implemented in a sustained manner.

Considering the obligation for operators of critical infrastructures in the sense of the IT Security Act in accordance with the German BSI-Law (BSIG) and German “BSI-Kritisverordnung” to submit proof of compliance of the requirements every two years and the risk-based approach of the NIS2 Directive, the three-year cycle of the TISAX assessment is considered appropriate.

3.2 Evaluation of the degree of fulfilment according to NIS2 Article 20 (2)

3.2.1 Requirement from NIS2

NIS2 Article 20 (2) requires that members of the governing body and other relevant members participate in regular training to acquire sufficient knowledge and skills to identify and assess risks and risk-management practices in the area of cybersecurity and its impact on the services provided by the organization.

3.2.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 20 (2) is checked in accordance with the following controls:

- 2.1.3: "To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?"

3.2.3 Detailed requirements within the control questions of ISA6

2.1.3: "To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?"

The auditor checks whether all employees (including the management level) of the company are comprehensively trained and sensitized regarding the risks involved in handling information *(Control 2.1.3; Requirements (must); first sub-item: + Employees are trained and made aware).* It is also checked that an awareness training concept exists that covers areas relevant to information security *(Control 2.1.3; Requirements (should); first sub-item: + A concept for awareness and training of employees is prepared. As a minimum, the following aspects are considered: - Information security policy, - Reports of information security events, - Reaction to occurrence of malware, - Policies regarding user accounts and login information (e.g. password policy), - Compliance issues of information security, - Requirements and procedures regarding the use of non-disclosure agreements when sharing information requiring protection, - Use of external IT services)* which takes into account the target groups for training concepts *(Control 2.1.3; Requirements (should); second sub-item: Target groups for training and awareness measures (i.e., people working in specific risk environments such as administrators, employees having access to customer networks, personnel in areas of manufacturing) are identified and considered in a training concept)* and the training measures are appropriate according to the criticality of the information processed. The auditor will also check whether the training and awareness-raising measures are carried out at regular intervals and in response to events *(Control 2.1.3; Requirements (should); fourth sub-item: + Training and awareness measures are carried out both at regular intervals and in response to events)* and that appropriate documentation is available *(Control 2.1.3; Requirements (should); fifth sub-item: + Participation in training and awareness measures is documented)*.

3.2.4 Summary:

The requirements that members of the management body and other relevant members participate in regular training to acquire sufficient knowledge and skills to identify and assess risks and risk-management practices in the area of cybersecurity and its impact on the services provided by the organization, NIS2 Article 20 (2), are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the auditor within a TISAX assessment. By checking the relevant evidence, the auditor ensures that the defined content is implemented permanently and regularly. Even if the direct reference to training for members of the management body and other relevant members is not explicitly listed in the ISA, the training of all employees and differentiation by target group is required. This requirement also fulfils the standard, as the members of the management body and other relevant members must be assigned a high level of relevance in the criticality classification according to the information processed by these members.

4 NIS2 Article 21

4.1 Evaluation of the degree of fulfilment according to NIS2 Article 21 (1)

4.1.1 Requirement from NIS2

NIS2 Article 21 (1) requires that companies have taken appropriate and proportionate technical, operational and organizational measures to manage the risks to the security of the network and information systems that those entities use for their operations or for the provision of their services and to prevent or minimize the impact of security incidents on the recipients of their services and on other services.

The measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the existing risk, considering the state of the art and, where appropriate, relevant European and international standards and the costs of implementation. In assessing the proportionality of those measures, due account shall be taken of the extent of the risk exposure of the facility, the size of the facility and the likelihood of security incidents occurring and their severity, including their societal and economic impact.

4.1.2 Applicable control questions of ISA6

The aim of the TISAX assessment is to verify whether a management system is in place that ensures that appropriate and proportionate technical, operational and organizational measures are always taken to manage the risks to information- and cybersecurity and to protect the organization and its customers from the effects of security incidents. A key aspect of this is the protection of network and information systems.

In the TISAX assessment in accordance with the current ISA6 standard, *fulfilment of the requirement of NIS2 Article 21 (1)* is *checked* in accordance with the following controls:

- 1.2.1: "To what extent is information security managed within the organization?" and
- 1.4.1: "To what extent are information security risks managed?*"*

4.1.3 Detailed requirements within the control questions of ISA6

1.2.1 "To what extent is information security managed within the organization?"

The auditor checks whether the scope of the ISMS is defined *(Control 1.2.1; Requirements (must); First sub-item: + The scope of the ISMS (the organization managed by the ISMS) is defined)* and that the ISMS is oriented towards the requirements determined by the company *(Control 1.2.1; Requirements (must); Second sub-item: + The organization’s requirements for the ISMS are determined).*

1.4.1 "To what extent are information security risks managed?"

The auditor also checks the existence of a risk assessment *(Control 1.4.1; Requirements (must); Third sub-item: + Information security risks are documented.)*, which is up to date and must be updated regularly or in response to incidents *(Control 1.4.1; Requirements (must); First sub-item: + Risk assessments are carried out both at regular intervals and in response to events.)*. During the assessment, the auditor checks that a risk owner is assigned to the identified risks *(Control 1.4.1; Requirements (must); Fourth sub-item: A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.)* and an action plan for dealing with the risks exists *(Control 1.4.1;*

Requirements (should); Third sub-item: + Measures for handling security risks and the persons responsible for these are specified and documented: - A plan of measures or an overview of their state of implementation is followed), which is implemented by the corresponding risk owner.

4.1.4 Summary:

The requirements of NIS2 Article 21 (1) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the auditor responsible during a TISAX assessment. Furthermore, the assessment of the ISA requirements catalogue in its entirety by the auditor helps to establish that the ISMS considers the circumstances of the company on a risk-based approach and is geared towards this.

The implemented and assessed ISMS ensures that companies have taken appropriate and proportionate technical, operational and organizational measures to control the risks to the security of the network and information systems that these entities use for their operations or for the provision of their services. And to prevent or minimize the impact of security incidents on the recipients of their services and on other services.

4.2 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2)

4.2.1 Requirement from NIS2

NIS2 Article 21 (2) requires that the measures must be based on a multi-hazard approach aimed at protecting the network and information systems and the physical environment of these systems from security incidents.

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

4.2.2 Implementation

The individual measures a to j required in NIS2 Article 21 (2) are summarized individually in the following chapters for the sake of clarity. Article 21 (2) does not contain any other measures to be implemented apart from those just mentioned.

4.3 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) a)

4.3.1 Requirement from NIS2

NIS2 Article 21 (2) a) requires existing policies on risk analysis and information system security.

4.3.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (2) a) is checked in accordance with the following controls:

- 1.4.1: "To what extent are information security risks managed?",
- 5.2.7: "To what extent is the network of the organization managed?" and
- 5.3.1: "To what extent is information security considered in new or further developed IT systems?"

4.3.3 Detailed requirements within the control questions of ISA6

1.4.1 "To what extent are information security risks managed?"

The auditor checks whether procedures are in place in the company to identify, assess and address security risks *(Control 1.4.1; Requirements (should); First sub-item: "+ A procedure is in place defining how to identify, assess and address security risks within the organization.")* and whether these are assessed and handled *(Control 1.4.1; Requirements (must); Fourth sub-item: "+ A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks")*.

5.2.7: "To what extent is the network of the organization managed?"

In addition, the auditor checks whether the requirements for the management and control of networks are determined and fulfilled *(Control 5.2.7; Requirements (must); First sub-item: "+ Requirements for the management and control of networks are determined and fulfilled "* and whether the necessary state of the art security aspects are implemented *(Control 5.2.7; Requirements (should); Second sub-item: "+ For a risk-based network segmentation, the following aspects are considered: - Limitations for connecting IT systems to the network, - Use of security technologies, - Performance, trust, availability, security, and safety considerations - Limitation of impact in case of compromised IT systems - Detection of potential attacks and lateral movement of attackers - Separation of networks with different operational purpose (e.g. test and development networks, office network, manufacturing networks) - The increased risk due to network services accessible via the internet, - Technology-specific separation options when using external IT services, - Adequate separation between own networks and customer networks while considering customer requirements - Detection and prevention of data loss/leakage ")*.

5.3.1: "To what extent is information security considered in new or further developed IT systems?"

The auditor checks that information security is taken into account in the new or further development of IT systems *(Control 5.3.1; Requirements (must); first sub-item: "+ The information security requirements associated with the design and development of IT systems are determined and considered "* and that the requirements of the ISMS for the systems are checked and ensured before they are used *(Control 5.3.1; Requirements (should); third sub-item: "+ The IT system is reviewed for compliance with specifications prior to productive use "*.

4.3.4 Summary:

The requirements of NIS2 Article 21 (1) a) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the auditor responsible during a TISAX assessment. The TISAX assessment standard goes beyond the required existing concepts and checks that these are implemented and active.

4.4 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) b)

4.4.1 Requirement from NIS2

NIS2 Article 21 (2) b) requires incident handling.

4.4.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (2) b) is checked in accordance with the following controls:

- 1.6.1: "To what extent are information security relevant events or observations reported?" and
- 1.6.2: "To what extent are reported security events managed?"

4.4.3 Detailed requirements within the control questions of ISA6

1.6.1: "To what extent are information security relevant events or observations reported?"

The auditor checks whether the parameters by which a reportable event can be measured are defined *(Control 1.6.1; Requirements (must); first sub-item: "+ A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders. The following aspects are considered: - Events and observations related to personnel (e.g., misconduct / misbehaviour) - Events and observations related to physical security (e.g., intrusion, theft, unauthorized access to security zones, vulnerabilities in the security zones) - Events and observations related to IT and Cybersecurity (e.g., vulnerable IT-systems, detected successful or unsuccessful attacks) - Events and observations related to suppliers and other business partners (e.g., any incidents that can have negative effect on the security of own organization)")* and that there is an obligation to report such events *(Control 1.6.1; Requirements (should); third sub-item: "+ Employees are obliged and trained to report relevant events")*. It is also checked that the necessary reporting channels are available *(Control 1.6.1; Requirements (must); Third sub-item: "+ Adequate channels for communication with event* *reporters exist") and (Control 1.6.1; Requirements (should); Second sub-item: "+ Different reporting channels according to perceived severity exist (i.e., real time communication for significant events / emergencies in addition to asynchronous mechanisms such as tickets or email) are available")* and the addressees of the report are known *(Control 1.6.1; Requirements (should); first sub-item: "+ A common point of contact for event reporting exists")*. Another part of the assessment is to ensure that reporting by parties external to the organization is also possible and that the necessary channels are available for the external reports *(Control 1.6.1; Requirements (should); Fourth sub-item: + Security event reports from external parties are considered. - An externally accessible way to report security events exists and is communicated, - Reaction to security event reports from external parties are defined"*).

1.6.2: "To what extent are reported security events managed?"

The review of the handling of reports includes categorization, qualification and prioritization *(Control 1.6.2; Requirements (should); First sub-item: "+ During processing, reported events are categorized (e.g. by responsibility into personnel, physical and cyber), qualified (e.g. not security relevant, observation, suggested security improvement, security vulnerability, security incident) and prioritized (e.g. low, moderate, severe, critical)")* and the response assigned to the class within a defined timeframe *(Control 1.6.2; Requirements (must); First two sub-items: "+ Reported events are processed without undue delay. + An adequate reaction to reported security events is ensured")* and involving the necessary responsible parties *(Control 1.6.2; Requirements (should); Second sub-item: "+ Responsibilities for handling of events based on their category are defined and assigned. The following aspects are considered: - Coordination of incidents and vulnerabilities across multiple categories - Qualification and resources - Contact mechanisms based on type and priority (e.g., non-time-critical communication, time-critical communication, emergency communication) - Absence-management*"). It is also checked that the reporting obligations and the associated contact information are known *(Control 1.6.2; Requirements (additional requirements for high protection needs); third sub-item: "+ Lawful, regulatory, and contractual reporting obligations and respective contact information are known. (C, I, A)")* and a communication strategy is in place that takes into account the addressees, reporting periods and reporting form *(Control 1.6.2; Requirements (additional requirements for high protection needs); Fourth sub-item: "+ A communication strategy for security related events exist. The following aspects are considered: (C, I, A) - To whom to communicate (e.g., shareholders, affected business partners and customers, other shareholders, general public) - When to communicate - Responsibilities for communication - Authorization and approval of communication - Legal and regulatory restrictions of communication - What to communicate (e.g. prepared templates and building blocks for specific scenarios) - How to communicate (e.g., communication channels)").*

4.4.4 Summary:

The requirements of NIS2 Article 21 (2) sub-item b) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor during a TISAX assessment. The processes for detection, reporting channels and procedures, classification, processing and escalation (if necessary), go beyond the requirements stipulated in NIS2.

4.5 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) c)

4.5.1 Requirement from NIS2

NIS2 Article 21 (2) sub-item c) requires business continuity, such as backup management and disaster recovery, and crisis management.

4.5.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, *fulfilment of the requirement of NIS2 Article 21 (2) c)* is *checked* in accordance with the following controls:

- 1.6.3: "To what extent is the organization prepared to handle crisis situations?",
- 5.2.8: "To what extent is continuity planning for IT services in place?" and
- 5.2.9: "To what extent is the backup and recovery of data and IT services ensured?".

4.5.3 Detailed requirements within the control questions of ISA6

1.6.3: "To what extent is the organization prepared to handle crisis situations?"

With regard to crisis management, the auditor checks whether the responsibilities and authorities for dealing with crises are defined in the organization and whether those responsible have the appropriate qualifications *(Control 1.6.3; Requirements (must); Third sub-item: "+ The responsible employees are defined and qualified for their task")* and that the needed resources are available *(Control 1.6.3; Requirements (must); First sub-item: "+ An appropriate planning to react to and recover from crisis situations exists. -The required resources are available ").* The framework conditions of a crisis *(Control 1.6.3; Requirements (should); First sub-item: "+ Methods to detect crisis situations are established. - General indications for the existence or imminence of a crisis situation and specific predictable crisis are identified)* and the process for declaring such a crisis *(Control 1.6.3; Requirements (should); Second sub-item: "+ A procedure to invoke and/or escalate crisis management is in place ")* are also part of the assessment.

5.2.8: "To what extent is continuity planning for IT services in place?"

The auditor checks whether there is continuity planning for IT services *(Control 5.2.8; Requirements (must); First sub-item: "+ Critical IT services are identified, and business impact is considered")* and IT systems *(Control 5.2.8; Requirements (should); First sub-item: "Critical IT systems are identified- the relevant systems are classified to have the appropriate protection need- adequate and appropriate security measures are implemented)*, which is based on an assessment of the criticality of the existing services or systems and which is known to the relevant responsible parties (*Control 5.2.8; Requirements (must); Second sub-item: "+ Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled")*.

In addition, the auditor checks the existence of specifications on different scenarios *(Control 5.2.8; Requirements (should); Second sub-item: "+ Continuity planning includes at least the following scenarios affecting critical IT systems: - (Distributed) Denial of Service attacks - Successful ransomware attacks and other sabotage activities - System failure - Natural disaster)* and backup strategies *(Control 5.2.8; Requirements (should); Third sub-item: "+ Continuity planning considers the following cases - Alternative communication strategies, in case primary communication means are not available - Alternative storage strategies, in case* *primary storage means are not available - Alternative power and network*") whose timeliness is checked by means of review protocols *(Control 5.2.8; Requirements (should); Fourth sub-item: "+ Continuity planning is regularly reviewed and updated").*

Another part of the assessment is to ensure that backups are in a recoverable state *(Control 5.2.8; Requirements (additional requirements for high protection needs); Fifth sub-item: "+ A backup and recovery strategy for critical IT services and information is defined and implemented. The following aspects are considered: - Backups are protected against unauthorized modification or deletion by malicious software. (I, A)- Backups are protected against unauthorized access by malicious software or operators (C, I)")* and the data in the backup is not corrupt and is protected against manipulation for the entire period of storage.

5.2.9: "To what extent is the backup and recovery of data and IT services ensured?"

To ensure backups and recoverability of data and IT services, the auditor checks the existence of backup concepts for relevant systems *(Control 5.2.9; Requirements (must); first sub-item: "+ Backup concepts exist for relevant IT systems. The following aspects are considered: - Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups")* and recovery concepts for relevant IT services, *(Control 5.2.9; Requirements (must); Second sub-item: "+ Recovery concepts exist for relevant IT services.")* which consider the dependencies during recovery. *(Control 5.2.9; Requirements (should); First sub-item: "+ A backup and recovery concept exists for each relevant IT service. - Dependencies between IT services and the sequence for recovery are considered").* Furthermore, for organizations where availability is essential, the auditor checks evidence that methodical reviews of the concepts take place *(Control 5.2.9; Requirements (additional requirements for high protection needs); first sub-item: "+ Backup and recovery concepts are methodically reviewed at regular intervals. (A)"),* the general recovery capacity is taken into account and checked *(Control 5.2.9; Requirements (additional requirements for high protection needs); Second sub-item: "+ General restore capability is considered and tested (e.g., sample testing, test systems) (I, A)")* and that relevant aspects are taken into account *(Control 5.2.9; Requirements (additional requirements for high protection needs); Third sub-item: "+ Backup and recovery concepts consider the following aspects: (A) - Recovery Point Objective (RPO). - Recovery Time Objective (RTO). - Required resources for recovery (considering capacity and performance incl. personnel and hardware). - Avoidance of overload scenarios during recovery. - Appropriate spatial redundancy (e.g., separate room, separate fire section, separate datacenter, separate site))").*

4.5.4 Summary:

The requirements of NIS2 Article 21 (2) subpoint c) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor as part of a TISAX assessment. The auditor determines the extent to which the organization is prepared to deal with crisis situations, whether continuity planning for IT services is in place and whether the backup and recovery of data and IT services is ensured.

4.6 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) d)

4.6.1 Requirement from NIS2

NIS2 Article 21 (2) subpoint d) requires the supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

4.6.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, *fulfilment of the requirement of NIS2 Article 21 (2) d)* is *checked* in accordance with the following controls:

- 1.2.4 "To what extent are the responsibilities between external IT service providers and your own organization defined?",
- 1.3.3 " To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?",
- 1.6.1: "To what extent are information security relevant events or observations reported?",
- 1.6.2: "To what extent are reported security events managed?",
- 1.6.3: "To what extent is the organization prepared to handle crisis situations?",
- 5.3.3 "To what extent is the return and secure removal of information assets from external IT services regulated?",
- 6.1.1 "To what extent is information security ensured among contractors and cooperation partners?" and
- 6.1.2 "To what extent is non-disclosure regarding the exchange of information contractually agreed?"

4.6.3 Detailed requirements within the control questions of ISA6

1.2.4 "To what extent are the responsibilities between external IT service providers and your own organization defined?"

The auditor verifies that IT services and services that are subject to information security measures are identified *(Control 1.2.4; Requirements (must); First sub-item: " + The concerned services and IT services used are identified*") , logged in a directory *(Control 1.2.4; Requirements (additional requirements for high protection needs); First sub-item: " + A list exists indicating the concerned IT services and the respective responsible IT service providers. (C, I, A)")* and that the organization responsible for implementing the measures is defined and aware of its responsibility *(Control 1.2.4; Requirements (must); Third sub-item*: "*+ The organization responsible for implementing the requirement is defined and aware of its responsibility")*. It is also checked that the allocation of joint responsibilities is regulated and implemented *(Control 1.2.4; Requirements (must); fourth sub-item:* "*+ Mechanisms for shared responsibilities are specified and implemented")* and that the organization responsible in each case fulfils these (*Control 1.2.4; Requirements (must); fifth sub-item: "+ The responsible organization fulfils its respective responsibilities"*). To check the functionality of the required measures, the auditor also checks that corresponding evidence is available (*Control 1.2.4; Requirements (additional requirements for high protection needs); fourth sub-item: "+ Proof is provided that the IT service providers fulfil their responsibility. (C, I, A)").*

1.3.3 " To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets? "

With regard to the use of non-organizational IT services, the auditor checks that these are not used without assessment and implementation of the measures resulting from the assessment *(Control 1.3.3; Requirements (must); First sub-item: "+ External IT services are not used without explicit assessment and implementation of the information security requirements: - A risk assessment of the external IT services is available,- Legal, regulatory, and contractual requirements are considered"*) and that the requirements for the services are appropriate to the protection needs of the information to be processed *(Control 1.3.3; Requirements (must); Second sub-item: "+ The external IT services have been harmonized with the protection need of the processed* *information assets")*. To ensure the implementation of and compliance with the measures, the auditor checks that a release procedure has been established (*Control 1.3.3; Requirements (should); Second sub-item: "+ A procedure for release in consideration of the protection need is established"*) and documented *(Control 1.3.3; Requirements (should); Third sub-item: "+ External IT services and their approval are documented ."*) and that a regular compliance check is carried out *(Control 1.3.3; Requirements (should); Fourth sub-item: "+ It is verified at regular intervals that only approved external IT services are used).*

1.6.1: "To what extent are information security relevant events or observations reported?"

The auditor checks that there is a communication channel through which reports can be received when security incidents occur within the supply chain and that these are then evaluated and processed accordingly *(Control 1.6.1; Requirements (should); Fourth sub-item: "+ Security event reports from external parties are considered. - An externally accessible way to report security events exists and is communicated, - Reaction to security event reports from external parties are defined").*

1.6.2: "To what extent are reported security events managed?"

The auditor also checks the existence of defined responses to such reports *(Control 1.6.2; Requirements (additional requirements for high protection needs); fifth sub-item: "+ Procedures for response to supplier security incidents are established. The following aspects are considered: (C, I, A) - Analysis of the impact on the own organization and invocation of appropriate internal mechanisms - The need for reporting according to own reporting procedures").*

5.3.3 "To what extent is the return and secure removal of information assets from external IT services regulated?"

Furthermore, the auditor checks within the assessment that information assets located in non-organizational services are securely returned and removed *(Control 5.3.3; Requirements (must); first sub-item: "+ A procedure for the return and secure removal of information assets from each external IT service is defined and implemented")* and that the contractual basis and the scheduling process for this is in place *(Control 5.3.3; Requirements (should); first sub-item: "+ A description of the termination process is given, adapted to any changes, and contractually regulated")*.

6.1.1 "To what extent is information security ensured among contractors and cooperation partners?"

With regard to contractors and cooperation partners and their information security standard, the auditor checks that a risk assessment is carried out with regard to these *(Control 6.1.1; Requirements (must); first sub-item: "+ Contractors and cooperation partners are subjected to a risk assessment with regard to information security ")* and that appropriate evidence of the level of information security is obtained *(Control 6.1.1; Requirements (additional requirements for high protection needs); first sub-item: "+ Proof is provided that the information security level of the supplier is adequate for the protection needs of the information (e.g. certificate, attestation, internal audit). (C, I, A)")*. It is also checked that the information security requirements are contractually agreed *(Control 6.1.1; Requirements (must); second sub-item: + An appropriate level of information security is ensured by contractual agreements with contractors and cooperation partners")* and passed on both to contractors and cooperation partners *(Control 6.1.1; Requirements (must); third sub-item: "+ Where applicable, contractual agreements with clients are passed on to contractors and cooperation partners ")* and to their subcontractors *(Control 6.1.1; Requirements (should); First sub-item: "+ Contractors and cooperation partners are contractually obliged to pass on any requirements regarding an appropriate level of information security to their subcontractors ")* and corresponding evidence of compliance with the contractual agreements is available *(Control 6.1.1; Requirements (must); Fourth sub-item: "+ Compliance with contractual agreements is verified ")*. The service reports and documents supplied by the contractors and cooperation partners are checked for compliance after receipt *(Control 6.1.1; Requirements (should); Second sub-item: "+ Service reports and documents by contractors and cooperation partners are reviewed")*.

6.1.2 "To what extent is non-disclosure regarding the exchange of information contractually agreed?"

The auditor checks that non-disclosure requirements are determined and fulfilled *(Control 6.1.2; Requirements (must); First sub-item: "+ The non-disclosure requirements are determined and fulfilled ")*, that procedures are in place for the use of non-disclosure agreements *(Control 6.1.2; Requirements (must); Third sub-item: "+ Valid non-disclosure agreements are concluded prior to forwarding sensitive information")* and that these are also known to all persons who disclose sensitive information *(Control 6.1.2; Requirements (must); Second sub-item: "+ Requirements and procedures for applying non-disclosure agreements are known to all persons passing on information in need of protection")*. The auditor also checks that the non-disclosure agreements are regularly reviewed *(Control 6.1.2; Requirements (must); Fourth sub-item: "+ The requirements and procedures for the use of non-disclosure agreements and the handling of information requiring protection are reviewed at regular intervals")*.

4.6.4 Summary:

The requirements of NIS2 Article 21 (2) sub-item d) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor within a TISAX assessment. The requirements in the ISA6 assessment standard go beyond the requirements of NIS2 and additionally include, for example, compliance with information security standards beyond the direct providers or service providers.

4.7 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) e)

4.7.1 Requirement from NIS2

NIS2 Article 21 (2) sub-item e) requires security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

4.7.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, *fulfilment of the requirement of NIS2 Article 21 (2) e)* is *checked* in accordance with the following controls:

- 1.2.3: "To what extent are information security requirements considered in projects??",
- 1.2.4: "To what extent are the responsibilities between external IT service providers and your own organization defined?",
- 1.3.4: "To what extent is it ensured that only evaluated and approved software is used for processing the organization’s information assets??",
- 5.2.1: "To what extent are changes managed?",
- 5.2.4: "To what extent are event logs recorded and analysed?",
- 5.2.5: "To what extent are vulnerabilities identified and addressed?",
- 5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?",
- 5.3.1: "To what extent is information security considered in new or further developed IT systems?",
- 5.3.2: "To what extent are requirements for network services defined?",

- 5.3.3: "To what extent is the return and secure removal of information assets from external IT services regulated?" and
- 5.3.4: "To what extent is information protected in shared external IT services?"

4.7.3 Detailed requirements within the control questions of ISA6

1.2.3: "To what extent are information security requirements considered in projects??"

The auditor checks whether a classification regarding information security is carried out during the implementation of any type of project *(Control 1.2.3 ; Requirements (must); first sub-item: "+ Projects are classified while taking into account the information security requirements")* and, as a result, appropriate measures for risk treatment are derived *(Control ; Requirements (should); third sub-item: "+ For identified information security risks, measures are derived and considered in the project")*.

1.2.4 "To what extent are the responsibilities between external IT service providers and your own organization defined?"

With regard to non-organizational IT services and IT services, the auditor checks that IT services and services that are subject to information security measures are identified *(Control 1.2.4; Requirements (must); first sub-item: "+ The concerned services and IT services used are identified"*), logged in a directory *(Control 1.2.4; Requirements (additional requirements for high protection needs); first sub-item: "+ A list exists indicating the concerned IT services and the respective responsible IT service providers. (C, I, A)*") and that the organization responsible for implementing the measures is defined and aware of its responsibility *(Control 1.2.4; Requirements (must); third sub-item:* "*+ The organization responsible for implementing the requirement is defined and aware of its responsibility")*. It is also checked that the allocation of joint responsibilities is regulated and implemented *(Control 1.2.4; Requirements (must); Fourth sub-item:* "*+ Mechanisms for shared responsibilities are specified and implemented")* and that the respective responsible organization fulfils them (*Control 1.2.4; Requirements (must); Fifth sub-item: "+ The responsible organization fulfils its respective responsibilities"*). To check the functionality of the required measures, the auditor also checks that corresponding evidence is available (*Control 1.2.4; Requirements (additional requirements for high protection needs); fourth sub-item: "+ Proof is provided that the IT service providers fulfil their responsibility. (C, I, A)").*

1.3.4: "To what extent is it ensured that only evaluated and approved software is used for processing the organization's information assets??"

To ensure that only approved software is used, the auditor checks whether such approval has taken place *(Control 1.3.4; Requirements (must); first sub-item: "+ Software is approved before installation or use. The following aspects are considered: - Limited approval for specific use-cases or roles - Conformance to the information security requirements - Software use rights and licensing - Source / reputation of the software"),* whether the types of software to be managed are identified *(Control 1.3.4 ; Requirements (should); First sub-item: "+ The types of software such as firmware, operating systems, applications, libraries, device drivers to be managed are determined")* whether a regular review of the released software to be up to date is carried out *(Control 1.3.4; Requirements (should); Fourth sub-item: "+ Approval of software is regularly reviewed")* and the current software versions and patch levels are known *(Control 1.3.4; Requirements (should); Fifth sub-item: "+ Software versions and patch levels are known")*. The auditor also checks the existence of software repositories *(Control 1.3.4; Requirements (should); Second sub-item: "+ Repositories of managed software exist")* and the protection of these against unauthorized manipulation *(Control 1.3.4; Requirements (should); Third sub-item: "+ The software repositories are protected against unauthorized manipulation")*.

5.2.1: "To what extent are changes managed?"

With regard to changes, the auditor checks that the information security requirements are determined and applied *(Control 5.2.1; Requirements (must); first sub-item: + Information security requirements for changes to the organization, business processes, IT systems are determined and applied ", and that* an assessment is carried out with regard to the impact on information security *(Control 5.2.1; Requirements (should); second sub-item: "+ Changes are verified and assessed for their potential impact on the information security")*. The auditor also checks that a formal approval procedure has been established for changes with an impact on information security *(Control 5.2.1; Requirements (should); first sub-item: "+ A formal approval procedure is established"), and that* these are planned and tested *(Control 5.2.1; Requirements (should); Third sub-item: "+ Changes affecting the information security are subjected to planning and testing")*, that they are verified during and after the changes *(Control 5.2.1; Requirements (additional requirements for high protection needs); First sub-item: "+ Compliance with the information security requirements is verified during and after the changes are applied. (C, I, A) ")* and the fallback in the event of errors is taken into account *(Control 5.2.1; Requirements (should); Fourth sub-item: "+ Procedures for fallback in fault cases are considered ")*.

5.2.4: "To what extent are event logs recorded and analysed?"

In order to ensure the traceability in the event of a security incident, the auditor checks that event logging takes place and that its handling takes into account the requirements of information security *(Control 5.2.4; Requirements (must); first sub-item: "+ Information security requirements regarding the handling of event logs are determined and fulfilled")* and ensures appropriate monitoring and recording of all information security-relevant actions in the network *(Control 5.2.4; Requirements (should); third sub-item: "+ Adequate monitoring and recording of any actions on the network that are relevant to information security are established")*. In addition, the auditor determines whether security-relevant requirements for logging the activities of system administrators and users are determined and fulfilled *(Control 5.2.4; Requirements (must); second sub-item: "+ Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled")*. The auditor also checks that the IT systems used are assessed with regard to logging *(Control 5.2.4; requirements (must); third sub-item: "+ The IT systems used are assessed regarding the necessity of logging")* and that the monitoring options are known and taken into account, especially for IT systems outside the organization *(Control 5.2.4; requirements (must); fourth sub-item: "+ When using external IT services, information on the monitoring options is obtained and considered in the assessment")*. The auditor also checks that the accesses set up when establishing and terminating network connections from outside the organization are logged *(Control 5.2.4; Requirements (additional requirements for high protection needs); second sub-item: "+ Cases of access during connection and disconnection of external networks (e.g. remote maintenance) are logged. (C, I, A)")*. The auditor also checks the existence of evidence of regular checks of event logs *(Control 5.2.4; Requirements (must); Fifth sub-item: "+ Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions")* and that an escalation procedure is used for relevant events *(Control 5.2.4; Requirements (should); first sub-item: "+ A procedure for the escalation of relevant events to the responsible body (e.g. security incident report, data protection, corporate security, IT security) is defined and established")*. The auditor also checks that the information security requirements relevant to security during handling are defined and implemented *(Control 5.2.4; Requirements (additional requirements for high protection needs); first sub-item: "+ Information security requirements relevant to the security during the handling of event logs, e.g. contractual requirements, are determined and implemented. (C, I, A)")* and that the logs are protected against changes *(Control 5.2.4; Requirements (should); Second sub-item: "+ Event logs (contents and meta data) are protected against alteration. (e.g. by a dedicated environment)")*.

5.2.5: "To what extent are vulnerabilities identified and addressed?"

With regard to the vulnerability analysis, the auditor checks that information on technical vulnerabilities is gathered and evaluated *(Control 5.2.5; Requirements (must); First sub-item: "+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS* *database) and evaluated (e.g. Common Vulnerability Scoring System CVSS)")*, and that the findings obtained are used to address such vulnerabilities *(Control 5.2.5; Requirements (must); Second sub-item: "+ Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed ")* and that risks are minimized *(Control 5.2.5; Requirements (should); Second sub-item: "+ Risk minimizing measures are implemented, as necessary ")*. The auditor also checks that patch management is established *(Control 5.2.5; Requirements (should); First sub-item: "+ An adequate patch management is defined and implemented (e.g. patch testing and installation)")* and that the successful installation is verified (*Control 5.2.5; Requirements (should); Third sub-item: "+ Successful installation of patches is verified in an appropriate manner")*.

5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?"

To verify the technical review of IT systems and services, the auditor checks that the requirements for assessing these systems and services are defined *(Control 5.2.6; Requirements (must); First sub-item: "+ Requirements for auditing IT systems or services are determined")*, that these are performed regularly *(Control 5.2.6; Requirements (should); Second sub-item: "+ Regular system or service audits are performed - carried out by qualified personnel - suitable tools (e.g. vulnerability scanners) are used for system and service audits (if applicable) - performed from the internet and the internal network")*, that the assessments are defined in scope *(Control 5.2.6; Requirements (must); Second sub-item: "+ The scope of the system audit is specified in a timely manner"* and evaluated with regard to the security risks that arise *(Control 5.2.6; Requirements (should); First sub-item: "+ System and service audits are planned taking into account any security risks they might cause (e.g. disturbances)")*. The auditor also checks that they are coordinated with the operators and users *(Control 5.2.6; Requirements (must); third sub-item: "+ System or service audits are coordinated with the operator and users of the IT systems or services")*. For critical IT systems or services and companies whose availability is essential in the supply chain, the auditor also checks that additional requirements for the assessment have been identified and taken into account *(Control 5.2.6; Requirements (additional requirements for high protection needs); first sub-item: " + For critical IT systems or services, additional system or service audit requirements have been identified and are fulfilled (e.g., service specific tests and tools and/or human penetration tests, risk-based time intervals) (A))* ".

The assessment also includes the control of evidence of performance *(Control 5.2.6; Requirements (should); Third sub-item: "+ Within a reasonable period following completion of the audit, a report is prepared)* as well as the storage and reporting of the results to management *(Control 5.2.6; Requirements (must); Fourth sub-item: "+ The results of system or service audits are stored in a traceable manner and reported to the relevant management")* and the derivation of appropriate measures based on the report *(Control 5.2.6; Requirements (must); Fifth sub-item: "+ Measures are derived from the results")*.

5.3.1: "To what extent is information security considered in new or further developed IT systems?"

The auditor checks the consideration of information security during planning and development of IT systems *(Control 5.3.1; requirements (must); first sub-item: "+ The information security requirements associated with the design and development of IT systems are determined and considered ")* as well as during acquisition or extension of IT systems and IT components *(Control 5.3.1; Requirements (must); second sub-item: "+ The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered")* and the further development of IT systems *(Control 5.3.1; Requirements (must); third sub-item: "+ Information security requirements associated with changes to developed IT systems are considered ")*. The auditor also checks whether requirement specifications have been created *(Control 5.3.1; Requirements (should); first sub-item: "+ Requirement specifications are prepared. The following aspects are considered: - The information security requirements. - Vendor recommendations and best practices for secure configuration and implementation - Best practices and security guidelines - Fail safe (designed to return to a safe condition in the event of a failure or malfunction)")* and these have been checked against information security *(Control 5.3.1; Requirements (should); Second sub-item: "+ Requirement specifications are reviewed against the information security requirements ").* The auditor also checks whether which data has been used for test purposes and, if productive data has been used, whether sufficient security mechanisms have been implemented *(Control 5.3.1; Requirements (should); fourth sub-item: "+ The use of productive data for testing purposes is avoided as far as possible (if applicable, anonymization or pseudonymization): - Where productive data are used for testing purposes, it shall be ensured that the test system is provided with protective measures comparable to those on the operational system, - Requirements for the lifecycle of test data (e.g. deletion, maximum lifetime on the IT system), - Case-related specifications for the generation of test data are defined ")*. The Assessment also includes checking evidence that audits of the IT systems were carried out prior to their productive use *(Control 5.3.1; Requirements (should); Third sub-item: "+ The IT system is reviewed for compliance with specifications prior to productive use")* and that system acceptance tests are carried out taking into account the information security requirements *(Control 5.3.1; Requirements (must); Fourth sub-item: "+ System approval tests are carried out under consideration of the information security requirements ")*.

5.3.2: "To what extent are requirements for network services defined?"

With regard to network services, the auditor checks that the information security requirements are identified and fulfilled *(Control 5.3.2; Requirements (must); first sub-item: "+ Requirements regarding the information security of network services are determined and fulfilled")* and that these are agreed in the form of SLAs *(Control 5.3.2; Requirements (should); second sub-item: "+ The requirements are agreed in the form of SLAs")*. The auditor also determines whether a procedure for protection and utilization *(Control 5.3.2; Requirements (should); First sub-item: "+ A procedure for securing and using network services is defined and implemented")* and, in the event that availability is essential, a procedure for monitoring the quality, are defined and implemented *(Control 5.3.2; Requirements (additional requirements for high protection needs); First sub-item: "+ Procedures for monitoring the quality of network traffic (e.g. traffic flow analyses, availability measurements) are defined and carried out. (A)*.

5.3.3 "To what extent is the return and secure removal of information assets from external IT services regulated?"

Furthermore, the auditor checks within the assessment that information assets located in non-organizational services are securely returned and removed *(Control 5.3.3; Requirements (must); first sub-item: "+ A procedure for the return and secure removal of information assets from each external IT service is defined and implemented")* and that the contractual basis and the scheduling process for this is in place *(Control 5.3.3; Requirements (should); first sub-item: "+ A description of the termination process is given, adapted to any changes, and contractually regulated").*

5.3.4: "To what extent is information protected in shared external IT services?"

The auditor also checks that an effective segregation of information prevents unauthorized access to shared IT services *(Control 5.3.4; Requirements (must); first sub-item: "+ Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organization ")* and that the provider's segregation concept is documented and is subject to adjustment if necessary *(Control 5.3.4; Requirements (should); first sub-item: "+ The provider's segregation concept is documented and adapted to any changes. The following aspects are considered: - Separation of data, functions, customer-specific software, operating system, storage system and network, - Risk assessment for the operation of external software within the shared environment")*.

4.7.4 Summary:

The requirements of NIS2 Article 21 (2) sub-item e) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor within a TISAX assessment. Within the assessment, the complete utilization cycle of network and information systems is mapped and checked for the existence of processes and control mechanisms to ensure information security at every stage of utilization. The assessment goes beyond the requirements of NIS2 by considering the return and secure removal of information assets from IT services outside the organization.

4.8 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) f)

4.8.1 Requirement from NIS2

NIS2 Article 21 (2) subpoint f) requires policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

4.8.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (2) f) is checked in accordance with the following controls:

- 1.2.1: "To what extent is information security managed within the organization?",
- 1.4.1: "To what extent are information security risks managed?",
- 1.5.1: "To what extent is compliance with information security ensured in procedures and processes?",
- 1.5.2: "To what extent is the ISMS reviewed by an independent authority?",
- 1.6.2: "To what extent are reported security events managed?" and
- 5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?"

4.8.3 Detailed requirements within the control questions of ISA6

1.2.1 "To what extent is information security managed within the organization?"

In the assessment in accordance with the current ISA6 standard, the auditor checks that communication channels have been implemented between the company management and the executors of the ISMS *(Control 1.2.1; requirements (must); fourth sub-item: + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review)")* to ensure that the control and management tools are also regularly used to maintain the functionality of the ISMS *(Control 1.2.1; requirements (must); sixth sub-item: The effectiveness of the ISMS is regularly reviewed by management)*.

1.4.1 "To what extent are information security risks managed?"

The responsible auditor checks the existence of a risk assessment *(Control 1.4.1; Requirements (must); Third sub-item: + Information security risks are documented)*, which is up to date and must be updated regularly or in response to incidents *(Control 1.4.1; Requirements (must); First sub-item: + Risk assessments are carried out both at regular intervals and in response to events.)*.

1.5.1 "To what extent is compliance with information security ensured in procedures and processes?"

Furthermore, the auditor checks that the assessments of compliance with information security in procedures and processes are carried out at regular intervals *(Control 1.5.1; Requirements (must); Second sub-item: + Information security policies and procedures are reviewed at regular intervals*).

1.5.2 "To what extent is the ISMS reviewed by an independent authority?"

The auditor also checks that an assessment is carried out by an independent body, which takes place at regular intervals and in the event of significant changes *(Control 1.5.2; Requirements (must); First sub-item: + Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes)*.

1.6.2: "To what extent are reported security events managed?"

The examination of the handling of reports includes the processing of reported events without unnecessary delays *(Control 1.6.2; Requirements (must); First sub-item: "+ Reported events are processed without undue delay")*, using an appropriate response *(Control 1.6.2; requirements (must); second sub-item: "+ An adequate reaction to reported security events is ensured")*, and the use of findings for continuous improvement *(Control 1.6.2; requirements (must); third sub-item: + Experience gained in this regard is incorporated into continuous improvement")*.

5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?"

To verify the technical review of IT systems and services, the auditor checks that the requirements for assessing these systems and services are defined *(Control 5.2.6; Requirements (must); First sub-item: "+ Requirements for auditing IT systems or services are determined"), and that* these are carried out regularly *(Control 5.2.6; Requirements (should); Second sub-item: "+ Regular system or service audits are performed - carried out by qualified personnel - suitable tools (e.g. vulnerability scanners) are used for system and service audits (if applicable) - performed from the internet and the internal network")*. For organizations where availability is essential, the auditor also checks for critical IT systems or services that additional assessment requirements have been identified and taken into account *(Control 5.2.6; Requirements (additional requirements for high protection needs); first sub-item: "+ For critical IT systems or services, additional system or service audit requirements have been identified and are fulfilled (e.g., service specific tests and tools and/or human penetration tests, risk-based time intervals) (A))"*.

The assessment also includes the control of evidence of performance *(Control 5.2.6; Requirements (should); Third sub-item: "+ Within a reasonable period following completion of the audit, a report is prepared)* as well as the storage and reporting of the results to management *(Control 5.2.6; Requirements (must); Fourth sub-item: "+ The results of system or service audits are stored in a traceable manner and reported to the relevant management")* and the derivation of appropriate measures based on the report *(Control 5.2.6; Requirements (must); Fifth sub-item: "+ Measures are derived from the results")*.

4.8.4 Summary:

The requirements of NIS2 Article 21 (1) f) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor within a TISAX assessment.

Considering the obligation for operators of critical infrastructures within the meaning of the IT Security Act in accordance with the German BSI Act (BSIG) and the German BSI-Kritisverordnung to submit proof of fulfilment of the requirements every two years and the risk-based approach of the NIS2 Directive, a three-year cycle is considered appropriate.

4.9 Evaluation of the degree of fulfilment in accordance with NIS2 Article 21 (2) g)

4.9.1 Requirement from NIS2

NIS2 Article 21 (2) subpoint g) requires basic cyber hygiene practices and cybersecurity training.

4.9.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirements of NIS2 Article 21 (2) g) is checked in accordance with the following controls:

- 1.1.1: " To what extent are information security policies available?",
- 2.1.2: "To what extent is all staff contractually bound to comply with information security policies?",
- 2.1.3: "To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?",
- 4.1.3: " To what extent are user accounts and login information securely managed and applied?",
- 4.2.1: "To what extent are access rights assigned and managed?",
- 5.1.1: "To what extent is the use of cryptographic procedures managed?",
- 5.1.2: "To what extent is information protected during transfer?",
- 5.2.1: "To what extent are changes managed?",
- 5.2.2: "To what extent are development and testing environments separated from operational environments?",
- 5.2.3: "To what extent are IT systems protected against malware?",
- 5.2.4: "To what extent are event logs recorded and analysed?",
- 5.2.5: "To what extent are vulnerabilities identified and addressed?",
- 5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?",
- 5.2.7: "To what extent is the network of the organization managed?",
- 5.2.8: "To what extent is continuity planning for IT services in place?",
- 5.2.9: "To what extent is the backup and recovery of data and IT services ensured?",
- 5.3.1: "To what extent is information security considered in new or further developed IT systems?",
- 5.3.2: "To what extent are requirements for network services defined?",
- 5.3.3: "To what extent is the return and secure removal of information assets from external IT services regulated?" and
- 5.3.4: "To what extent is information protected in shared external IT services?"

4.9.3 Detailed requirements within the control questions of ISA6

1. 1.1 " To what extent are information security policies available?"

In the TISAX assessment in accordance with the current ISA6 standard, the auditor checks that the information security requirements have been defined and documented in a policy *(Control 1.1.1; Requirements (must); First sub-item:* "*+ The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals, - A policy is prepared and is released by the organization.")*, and that this information security policy is made available to employees *(Control 1.1.1; Requirements (should); Fifth sub-item: "+ The policies are made available to employees in a suitable form (e.g. intranet")*, and that they are informed of relevant changes *(Control 1.1.1; Requirements (should); Sixth sub-item: "+ Employees and external business partners are informed of any changes relevant to them")*.

2.1.2: "To what extent is all staff contractually bound to comply with information security policies?"

The auditor also checks whether the employees are obliged to comply with the information security guidelines *(Control 2.1.2; Requirements (must); Second sub-item: "+ An obligation to comply with the information security policies is in effect")* and to maintain confidentiality *(Control 2.1.2; Requirements (must); First sub-item: "+ A non-disclosure obligation is in effect")* beyond the duration of the employment relationship or assignment *(Control 2.1.2; Requirements (should); First sub-item: "+ A non-disclosure obligation beyond the employment contract or order is in effect")*. The auditor also checks that information security is taken into account in employment contracts *(Control 2.1.2; Requirements (should); Second sub-item: "+ Information security aspects are considered in the employment contracts of the staff")* and that a procedure is described in the event of violations *(Control 2.1.2; Requirements (should); Third sub-item: "+ A procedure for handling violations of said obligations is described ").*

2.1.3: " To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?"

The auditor checks whether the company's employees are comprehensively trained and sensitized regarding the risks involved in handling information *(Control 2.1.3; Requirements (must); first sub-item: + Employees are trained and made aware)*. It is also checked that a training concept exists that covers areas relevant to information security *(Control 2.1.3; Requirements (should); first sub-item: + A concept for awareness and training of employees is prepared. As a minimum, the following aspects are considered: - Information security policy, - Reports of information security events, - Reaction to occurrence of malware, - Policies regarding user accounts and login information (e.g. password policy), - Compliance issues of information security, - Requirements and procedures regarding the use of non-disclosure agreements when sharing information requiring protection, - Use of external IT services)*, which takes into account the target groups for training concepts and *that* the training measures are appropriate according to the criticality of the information processed *(Control 2.1.3; Requirements (should); second sub-item: Target groups for training and awareness measures (i.e., people working in specific risk environments such as administrators, employees having access to customer networks, personnel in areas of manufacturing) are identified and considered in a training concept)* and which has been approved by management *(Control 2.1.3; Requirements (should); third sub-item: + The concept has been approved by the responsible management)*. The auditor will also check whether the training and awareness-raising measures are carried out at regular intervals and in response to events *(Control 2.1.3; Requirements (should); fourth sub-item: + Training and awareness measures are carried out both at regular intervals and in response to events)* and whether corresponding documentation is available *(Control 2.1.3; Requirements (should); fifth sub-item: + Participation in training and awareness measures is documented)*. To check that the assessment is effective, the auditor checks that the Contact persons for information security are known to employees *(Control 2.1.3; Requirements (should); sixth sub-item: + Contact persons for information security are known to employees)*.

4.1.3 "To what extent are user accounts and login information securely managed and applied?"

Part of the assessment is to check that access to information and IT systems takes place via validated user accounts and that login information is protected and the traceability of transactions and access is ensured. To this end, the auditor checks that user accounts are managed throughout their life cycle *(Control 4.1.3;*

Requirements (must); First sub-item: "+ The creating, changing, and deleting of user accounts is conducted"). The auditor also checks that user accounts are blocked immediately after the user leaves the organization *(Control 4.1.3; Requirements (must); Fourth sub-item: "+ User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract)")* and that a regular check is carried out to ensure that the allocation is up to date *(Control 4.1.3; Requirements (must); Fifth sub-item: "+ User accounts are regularly reviewed")*. The auditor also checks that the accounts are personalized *(Control 4.1.3; requirements (must); second sub-item: "+ Unique and personalized user accounts are used")* or, if necessary, that the allocation of collective accounts is subject to regulation *(Control 4.1.3; requirements (must); third sub-item: "+ he use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable)")*. The secure transmission of account information *(Control 4.1.3; Requirements (must); Sixth sub-item: The login information is provided to the user in a secure manner")*, ensuring the confidentiality of the credentials *(Control 4.1.3; Requirements (must); Eighth sub-item: "+ The login information (e.g. passwords) of a personalized user account must be known to the assigned user only")* and the associated behaviors *(Control 4.1.3; Requirements (must); Seventh sub-item: "+ A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used)*.

With regard to user profiles, the auditor checks that a standard profile exists *(Control 4.1.3; Requirements (should); first sub-item: "+ A basic user account with minimum access rights and functionalities is existent and used")*, also checks that manufacturer default accounts are deactivated *(Control 4.1.3; Requirements (should); Second sub-item: Default accounts and passwords pre-configured by manufacturers are disabled (e.g. by blocking or changing of password)")*, that there is a defined process for creating accounts *(Control 4.1.3; Requirements (should); fourth sub-item: "+ Creating user accounts is subject to an approval process (four-eyes principle)")*, and that the accounts are created by an authorized body *(Control 4.1.3; Requirements (should); third sub-item: "+ User accounts are created or authorized by the responsible body")*. The auditor also checks that blocking and deletion periods are defined *(Control 4.1.3; Requirements (should); Sixth sub-item: "+ Deadlines for disabling and deleting user accounts are defined")* and implemented for service provider accounts *(Control 4.1.3; Requirements (should); Fifth sub-item: "+ User accounts of service providers are disabled upon completion of their task")*. The auditor also checks that the use of default passwords is prevented *(Control 4.1.3; Requirements (should); Seventh sub-item: "+ The use of default passwords is technically prevented")*, that interactive login to service accounts is technically prevented *(Control 4.1.3; Requirements (should); Tenth sub-item: "+ Interactive login for service accounts (technical accounts) is technically prevented")*, that the medium is used securely when strong authentication is used *(Control 4.1.3; Requirements (should); Eighth sub-item: "+ Where strong authentication is applied, the use of the medium (e.g. ownership factor) is secure")* and finally that a regular check of the accounts takes place *(Control 4.1.3; Requirements (should); Ninth sub-item: "+ User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems")*.

4.2.1 "To what extent are access rights assigned and managed?"

To ensure that only authorized users have access to information and IT services, the auditor checks that the requirements for the management of access rights have been determined and fulfilled *(Control 4.2.1; Requirements (must); first sub-item: "+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed")*, that authorization concepts have been created *(Control 4.2.1; Requirements (should); First sub-item: "+ Strategies for authorizing access to information are prepared")*, authorization roles are used

(Control 4.2.1; Requirements (should); Second sub-item: "+ Authorization roles are used"), that no privileged access rights are assigned to normal users *(Control 4.2.1; Requirements (should); Fourth sub-item: "+ Normal user accounts are not granted privileged access rights")*, and that the access rights have been approved by the information officer *(Control 4.2.1; Requirements (additional requirements for high protection needs); First sub-item: "+ The access rights are approved by the responsible internal Information Officer. (C, I, A)")*. The auditor also checks that the assignment of authorizations is needs-based *(Control 4.2.1; Requirements (should); Third sub-item: "+ Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility")*, that the rights are checked regularly *(Control 4.2.1; Requirements (must); second sub-item: "+ The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers")*, and that an update is also carried out in the event of changes to other areas of responsibility *(Control 4.2.1; Requirements (should); fifth sub-item: "+ The access rights of a user account are adapted after the user has changed (e.g. to another field of responsibility")*.

5.1.1 "To what extent is the use of cryptographic procedures managed?"

For the use of cryptographic procedures, the auditor checks that these comply with the recognized industry standard and take into account the laws and regulations affecting the company *(Control 5.1.1; Requirements (must); first sub-item: "+ All cryptographic procedures used (e.g. encryption, signature, and hash algorithms, protocols) provide the security required by the respective application field according to the recognized industry standard, - to the extent legally feasible")*. The auditor checks that a technical set of rules has been created *(Control 5.1.1; Requirements (should); first sub-item: "+ Preparation of technical rules containing requirements for encryption in order to protect information according to its classification")* and a utilization concept has been defined *(Control 5.1.1; Requirements (should); second sub-item: ""+ A concept for the application of cryptography is defined and implemented. The following aspects are considered: - Cryptographic procedures, - Key strengths, - Procedures for the complete lifecycle of cryptographic keys, including generation, storage, archiving, retrieval, distribution, deactivation, renewal, and deletion)*. It is also part of the assessment to check that the requirements for key sovereignty have been determined and fulfilled *(Control 5.1.1; Requirements (additional requirements for high protection needs); first sub-item: "+ Key sovereignty requirements (particularly in case of external processing) are determined and fulfilled. (C, I) ")* and an emergency process for restoring key material is established *(Control 5.1.1; Requirements (should); Third sub-item: + An emergency process for restoring key material is established ")*.

5.1.2 "To what extent is information protected during transfer?"

To ensure the protection of information during transmission, the auditor verifies that network services used for transmission are identified and documented *(Control 5.1.2; Requirements (must); First sub-item: "+ The network services used to transfer information are identified and documented ")*, that policies and procedures for the use of network services are defined and implemented *(Control 5.1.2; Requirements (must); Second sub-item: "+ Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented")*, and that measures to protect transmitted content are implemented *(Control 5.1.2; Requirements (must); Third sub-item: "+ Measures for the protection of transferred contents against unauthorized access are implemented ")*. In addition, for organizations for which confidentiality is essential, information must be transported or transmitted in encrypted form *(Control 5.1.2; Requirements (additional requirements for high protection needs); First sub-item: + Information is transported or transferred in encrypted form: (C) - Where encryption is not feasible, information must be protected by similarly effective measures. ") (Control 5.1.2; Requirements (should); second sub-item: "+ Electronic data exchange is conducted using content or transport encryption according to the respective classification ")* and it has to be ensured that the addresses used are correct *(Control 5.1.2; Requirements (should); first sub-item: "+ Measures for ensuring correct addressing and correct transfer of information are implemented")*. The auditor also checks that remote access connections have appropriate security features and capabilities *(Control 5.1.2; Requirements (should);*

Third sub-item: "+ Remote access connections are verified to possess adequate security features (e.g., encryption, granting and termination of access) and capabilities ").

5.2.1: "To what extent are changes managed?"

With regard to changes, the auditor checks that the information security requirements are determined and applied *(Control 5.2.1; Requirements (must); first sub-item: + Information security requirements for changes to the organization, business processes, IT systems are determined and applied ")*, *and that* an assessment is carried out with regard to the impact on information security *(Control 5.2.1; Requirements (should); second sub-item: "+ Changes are verified and assessed for their potential impact on the information security")*. The auditor also checks that a formal approval procedure has been established for changes with an impact on information security *(Control 5.2.1; Requirements (should); first sub-item: "+ A formal approval procedure is established")*, that these are planned and tested *(Control 5.2.1; Requirements (should); Third sub-item: "+ Changes affecting the information security are subjected to planning and testing")*, that they are verified during and after the changes *(Control 5.2.1; Requirements (additional requirements for high protection needs); First sub-item: "+ Compliance with the information security requirements is verified during and after the changes are applied. (C, I, A) ")*, and the fallback in the event of errors is taken into account *(Control 5.2.1; Requirements (should); Fourth sub-item: "+ Procedures for fallback in fault cases are considered ")*.

5.2.2: "To what extent are development and testing environments separated from operational environments?"

The auditor checks the existence of a risk assessment regarding the need to separate production and test systems *(Control 5.2.2; Requirements (must); First sub-item: + The IT systems have been subjected to risk assessment in order to determine the necessity of their separation into development, testing and operational systems ")*, the implementation of the results *(Control 5.2.2; Requirements (must); Second sub-item: + A segmentation is implemented based on the results of risk analysis ")*, and that requirements for development and test environments have been determined and implemented *(Control 5.2.2; Requirements (should); First sub-item: "+ The requirements for development and testing environments are determined and implemented. The following aspects are considered: - Separation of development, testing and operational systems, - No development and system tools on operational systems (except those required for operation), - Use of different user profiles for development, testing, and operational systems ")*.

5.2.3: "To what extent are IT systems protected against malware?"

In order to ensure the protection of IT systems against malware both technically and organizationally, the auditor checks that technical and organizational measures for protection against malware are defined and implemented *(Control 5.2.3; Requirements (must); second sub-item: "+ Technical and organizational measures for protection against malware are defined and implemented")* and that the requirements for protection against malware are determined *(Control 5.2.3; Requirements (must); first sub-item: "+ Requirements for protection against malware are determined*. The check also includes that unneeded network services are disabled *(Control 5.2.3; Requirements (should); First sub-item: "+ Unnecessary network services are disabled ")*, access to network services is restricted *(Control 5.2.3; Requirements (should); Second sub-item: "+ Access to network services is restricted to necessary access by means of suitable protective measures")*, software for protection against malware is installed and regularly updated *(Control 5.2.3; Requirements (should); Third sub-item: "+ Malware protection software is installed and updated automatically at regular intervals (e.g. virus scanner")*, and that received files and received software are automatically inspected for malware *(Control 5.2.3; Requirements (should); Fourth sub-item: "+ Received files and software are automatically inspected for malware prior to their execution (on-access scan)")*. The auditor also checks that regular checks for malware are carried out *(Control 5.2.3; Requirements (should); Fifth sub-item: "+ The entire data contents of all systems is regularly inspected for malware")*, that data transmitted from central gateways is automatically checked *(Control 5.2.3; Requirements (should); Sixth sub-item: "+ Data transferred by central gateways (e.g. e-mail, internet, third-party networks) is automatically inspected by means of protection software: - Encrypted connections are considered")*, and that encrypted connections are considered.

With regard to the user, the auditor checks that protection software is prevented from being deactivated or altered by users *(Control 5.2.3; Requirements (should); Seventh sub-item: "+ Measures to prevent protection software from being deactivated or altered by users are defined and implemented")* and that case-related awareness-raising measures take place *(Control 5.2.3; Requirements (should); Eighth sub-item: "+ Case-related staff awareness measures")*. For IT systems that are operated without malware protection software, the auditor checks that alternative measures have been implemented *(Control 5.2.3; Requirements (should); Ninth sub-item: "+ For IT systems operated without the use of malware protection software, alternative measures (e.g. special resilience measures, few services, no active users, network isolation) are implemented ")*.

5.2.4: "To what extent are event logs recorded and analysed?"

In order to ensure the traceability in the event of a security incident, the auditor checks that event logging takes place and that its handling takes into account the requirements of information security *(Control 5.2.4; Requirements (must); first sub-item: "+ Information security requirements regarding the handling of event logs are determined and fulfilled") and ensures appropriate monitoring and recording of all information security-relevant actions in the network (Control 5.2.4; Requirements (should); third sub-item: "+ Adequate monitoring and recording of any actions on the network that are relevant to information security are established")*. In addition, the auditor determines whether security-relevant requirements for logging the activities of system administrators and users are determined and fulfilled *(Control 5.2.4; Requirements (must); second sub-item: "+ Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled")*. The auditor also checks that the IT systems used are assessed with regard to logging *(Control 5.2.4; requirements (must); third sub-item: "+ The IT systems used are assessed regarding the necessity of logging")* and that the monitoring options are known and taken into account, especially for IT systems outside the organization *(Control 5.2.4; requirements (must); fourth sub-item: "+ When using external IT services, information on the monitoring options is obtained and considered in the assessment")*. The auditor also checks that the accesses set up when establishing and terminating network connections from outside the organization are logged *(Control 5.2.4; Requirements (additional requirements for high protection needs); second sub-item: "+ Cases of access during connection and disconnection of external networks (e.g. remote maintenance) are logged. (C, I, A)")*. The auditor also checks the existence of evidence of regular checks of event logs *(Control 5.2.4; Requirements (must); Fifth sub-item: "+ Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions")* and that an escalation procedure is used for relevant events *(Control 5.2.4; Requirements (should); first sub-item: "+ A procedure for the escalation of relevant events to the responsible body (e.g. security incident report, data protection, corporate security, IT security) is defined and established")*. The auditor also checks that the information security requirements relevant to security during handling are defined and implemented *(Control 5.2.4; Requirements (additional requirements for high protection needs); first sub-item: "+ Information security requirements relevant to the security during the handling of event logs, e.g. contractual requirements, are determined and implemented. (C, I, A)")* and that the logs are protected against changes *(Control 5.2.4; Requirements (should); Second sub-item: "+ Event logs (contents and meta data) are protected against alteration. (e.g. by a dedicated environment)")*.

5.2.5: "To what extent are vulnerabilities identified and addressed?"

With regard to the vulnerability analysis, the auditor checks that information on technical vulnerabilities is gathered and evaluated *(Control 5.2.5; Requirements (must); First sub-item: "+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS)")*, that the findings obtained are used to address such vulnerabilities *(Control 5.2.5; Requirements (must); Second sub-item: "+ Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed ")*, and that risks are minimized *(Control 5.2.5; Requirements (should); Second sub-item: "+ Risk minimizing measures are implemented, as necessary ")*. The auditor also checks that patch management is established *(Control 5.2.5;*

Requirements (should); First sub-item: "+ An adequate patch management is defined and implemented (e.g. patch testing and installation)") and that the successful installation is verified (*Control 5.2.5; Requirements (should); Third sub-item: "+ Successful installation of patches is verified in an appropriate manner")*.

5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?"

To verify the technical review of IT systems and services, the auditor checks that the requirements for assessing these systems and services are defined *(Control 5.2.6; Requirements (must); First sub-item: "+ Requirements for auditing IT systems or services are determined")*, that these are performed regularly *(Control 5.2.6; Requirements (should); Second sub-item: "+ Regular system or service audits are performed - carried out by qualified personnel - suitable tools (e.g. vulnerability scanners) are used for system and service audits (if applicable) - performed from the internet and the internal network")*, that the assessments are defined in scope *(Control 5.2.6; Requirements (must); Second sub-item: "+ The scope of the system audit is specified in a timely manner")*, and evaluated with regard to the security risks that arise *(Control 5.2.6; Requirements (should); First sub-item: "+ System and service audits are planned taking into account any security risks they might cause (e.g. disturbances)")*. The auditor also checks that they are coordinated with the operators and users *(Control 5.2.6; Requirements (must); third sub-item: "+ System or service audits are coordinated with the operator and users of the IT systems or services")*. For critical IT systems or services and companies whose availability is essential in the supply chain, the auditor also checks that additional requirements for the assessment have been identified and taken into account *(Control 5.2.6; Requirements (additional requirements for high protection needs); first sub-item: " + For critical IT systems or services, additional system or service audit requirements have been identified and are fulfilled (e.g., service specific tests and tools and/or human penetration tests, risk-based time intervals) (A)”)*.

The assessment also includes the control of evidence of performance *(Control 5.2.6; Requirements (should); Third sub-item: "+ Within a reasonable period following completion of the audit, a report is prepared”)* as well as the storage and reporting of the results to management *(Control 5.2.6; Requirements (must); Fourth sub-item: "+ The results of system or service audits are stored in a traceable manner and reported to the relevant management")* and the derivation of appropriate measures based on the report *(Control 5.2.6; Requirements (must); Fifth sub-item: "+ Measures are derived from the results")*.

5.2.7: "To what extent is the network of the organization managed?"

In addition, the auditor checks whether the requirements for the management and control of networks are determined and fulfilled *(Control 5.2.7; Requirements (must); First sub-item: "+ Requirements for the management and control of networks are determined and fulfilled")* and whether the necessary state of the art security aspects are implemented *(Control 5.2.7; Requirements (should); Second sub-item: "+ For a risk-based network segmentation, the following aspects are considered: - Limitations for connecting IT systems to the network, - Use of security technologies, - Performance, trust, availability, security, and safety considerations - Limitation of impact in case of compromised IT systems - Detection of potential attacks and lateral movement of attackers - Separation of networks with different operational purpose (e.g. test and development networks, office network, manufacturing networks) - The increased risk due to network services accessible via the internet, - Technology-specific separation options when using external IT services, - Adequate separation between own networks and customer networks while considering customer requirements - Detection and prevention of data loss/leakage")*.

5.2.8: "To what extent is continuity planning for IT services in place?"

The auditor checks whether there is continuity planning for IT services *(Control 5.2.8; Requirements (must); First sub-item: "+ Critical IT services are identified, and business impact is considered")* and IT systems *(Control 5.2.8; Requirements (should); First sub-item: "Critical IT systems are identified- the relevant systems are classified to have the appropriate protection need- adequate and appropriate security measures are implemented)*, which is based on an assessment of the criticality of the existing services or systems and which is known to the relevant responsible parties (*Control 5.2.8; Requirements (must); Second sub-item: "+ Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled")*.

In addition, the auditor checks the existence of specifications on different scenarios *(Control 5.2.8; Requirements (should); Second sub-item: "+ Continuity planning includes at least the following scenarios affecting critical IT systems: - (Distributed) Denial of Service attacks - Successful ransomware attacks and other sabotage activities - System failure - Natural disaster)* and backup strategies *(Control 5.2.8; Requirements (should); Third sub-item: "+ Continuity planning considers the following cases - Alternative communication strategies, in case primary communication means are not available - Alternative storage strategies, in case primary storage means are not available - Alternative power and network*") whose timeliness is checked by means of review protocols *(Control 5.2.8; Requirements (should); Fourth sub-item: "+ Continuity planning is regularly reviewed and updated").*

Another part of the assessment is to ensure that backups are in a recoverable state *(Control 5.2.8; Requirements (additional requirements for high protection needs); Fifth sub-item: "+ A backup and recovery strategy for critical IT services and information is defined and implemented. The following aspects are considered: - Backups are protected against unauthorized modification or deletion by malicious software. (I, A)- Backups are protected against unauthorized access by malicious software or operators (C, I)")* and the data in the backup is not corrupt and is protected against manipulation for the entire period of storage.

5.2.9: "To what extent is the backup and recovery of data and IT services ensured?"

To ensure backups and recoverability of data and IT services, the auditor checks the existence of backup concepts for relevant systems *(Control 5.2.9; Requirements (must); first sub-item: "+ Backup concepts exist for relevant IT systems. The following aspects are considered: - Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups")* and recovery concepts for relevant IT services, *(Control 5.2.9; Requirements (must); Second sub-item: "+ Recovery concepts exist for relevant IT services.")* which consider the dependencies during recovery. *(Control 5.2.9; Requirements (should); First sub-item: "+ A backup and recovery concept exists for each relevant IT service. - Dependencies between IT services and the sequence for recovery are considered").* Furthermore, for organizations where availability is essential, the auditor checks evidence that methodical reviews of the concepts take place *(Control 5.2.9; Requirements (additional requirements for high protection needs); first sub-item: "+ Backup and recovery concepts are methodically reviewed at regular intervals. (A)"),* the general recovery capacity is taken into account and checked *(Control 5.2.9; Requirements (additional requirements for high protection needs); Second sub-item: "+ General restore capability is considered and tested (e.g., sample testing, test systems) (I, A)")* and that relevant aspects are taken into account *(Control 5.2.9; Requirements (additional requirements for high protection needs); Third sub-item: "+ Backup and recovery concepts consider the following aspects: (A) - Recovery Point Objective (RPO). - Recovery Time Objective (RTO). - Required resources for recovery (considering capacity and performance incl. personnel and hardware). - Avoidance of overload scenarios during recovery. - Appropriate spatial redundancy (e.g., separate room, separate fire section, separate datacenter, separate site))")*.

5.3.1: "To what extent is information security considered in new or further developed IT systems?"

The auditor checks the consideration of information security during planning and development of IT systems *(Control 5.3.1; requirements (must); first sub-item: "+ The information security requirements associated with the design and development of IT systems are determined and considered ")* as well as during acquisition or extension of IT systems and IT components *(Control 5.3.1; Requirements (must); second sub-item: "+ The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered")* and the further development of IT systems *(Control 5.3.1; Requirements (must); third sub-item: "+ Information security requirements associated with changes to developed IT systems are considered ")*. The auditor also checks whether requirement specifications have been created *(Control 5.3.1; Requirements (should); first sub-item: "+ Requirement specifications are prepared. The following aspects are* *considered: - The information security requirements. - Vendor recommendations and best practices for secure configuration and implementation - Best practices and security guidelines - Fail safe (designed to return to a safe condition in the event of a failure or malfunction)")* and these have been checked against information security *(Control 5.3.1; Requirements (should); Second sub-item: "+ Requirement specifications are reviewed against the information security requirements")*. The auditor also checks whether which data has been used for test purposes and, if productive data has been used, whether sufficient security mechanisms have been implemented *(Control 5.3.1; Requirements (should); fourth sub-item: "+ The use of productive data for testing purposes is avoided as far as possible (if applicable, anonymization or pseudonymization): - Where productive data are used for testing purposes, it shall be ensured that the test system is provided with protective measures comparable to those on the operational system, - Requirements for the lifecycle of test data (e.g. deletion, maximum lifetime on the IT system), - Case-related specifications for the generation of test data are defined ")*. The Assessment also includes checking evidence that audits of the IT systems were carried out prior to their productive use *(Control 5.3.1; Requirements (should); Third sub-item: "+ The IT system is reviewed for compliance with specifications prior to productive use")* and that system acceptance tests are carried out taking into account the information security requirements *(Control 5.3.1; Requirements (must); Fourth sub-item: "+ System approval tests are carried out under consideration of the information security requirements ")*.

5.3.2: "To what extent are requirements for network services defined?"

With regard to network services, the auditor checks that the information security requirements are identified and fulfilled *(Control 5.3.2; Requirements (must); first sub-item: "+ Requirements regarding the information security of network services are determined and fulfilled")* and that these are agreed in the form of SLAs *(Control 5.3.2; Requirements (should); second sub-item: "+ The requirements are agreed in the form of SLAs")*. The auditor also determines whether a procedure for protection and utilization *(Control 5.3.2; Requirements (should); First sub-item: "+ A procedure for securing and using network services is defined and implemented")* and, in the event that availability is essential, for monitoring the quality are defined and implemented *(Control 5.3.2; Requirements (additional requirements for high protection needs); First sub-item: "+ Procedures for monitoring the quality of network traffic (e.g. traffic flow analyses, availability measurements) are defined and carried out. (A)")*.

5.3.3 "To what extent is the return and secure removal of information assets from external IT services regulated?"

Furthermore, the auditor checks within the assessment that information assets located in non-organizational services are securely returned and removed *(Control 5.3.3; Requirements (must); first sub-item: "+ A procedure for the return and secure removal of information assets from each external IT service is defined and implemented")* and that the contractual basis and the scheduling process for this is in place *(Control 5.3.3; Requirements (should); first sub-item: "+ A description of the termination process is given, adapted to any changes, and contractually regulated")*.

5.3.4: "To what extent is information protected in shared external IT services?"

The auditor also checks that an effective segregation of information prevents unauthorized access to shared IT services *(Control 5.3.4; Requirements (must); first sub-item: "+ Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organization ")* and that the provider's segregation concept is documented and is subject to adjustment if necessary *(Control 5.3.4; Requirements (should); first sub-item: "+ The provider's segregation concept is documented and adapted to any changes. The following aspects are considered: - Separation of data, functions, customer-specific software, operating system, storage system and network, - Risk assessment for the operation of external software within the shared environment")*.

4.9.4 Summary:

The requirements of NIS2 Article 21 (2) h), are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor within a TISAX assessment.

4.10 Evaluation of the degree of fulfilment in accordance with NIS2 Article 21 (2) h)

4.10.1 Requirement from NIS2

NIS2 Article 21 (2) subpoint h) requires policies and procedures regarding the use of cryptography and, where appropriate, encryption.

4.10.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (2) h) is checked in accordance with the following controls:

- 5.1.1: "To what extent is the use of cryptographic procedures managed?"
- 5.1.2: "To what extent is information protected during transfer?"

4.10.3 Detailed requirements within the control questions of ISA6

5.1.1 "To what extent is the use of cryptographic procedures managed?"

For the use of cryptographic procedures, the auditor checks that these comply with the recognized industry standard and take into account the laws and regulations affecting the company *(Control 5.1.1; Requirements (must); first sub-item: "+ All cryptographic procedures used (e.g. encryption, signature, and hash algorithms, protocols) provide the security required by the respective application field according to the recognized industry standard, - to the extent legally feasible")*. The auditor checks that a technical set of rules has been created *(Control 5.1.1; Requirements (should); first sub-item: "+ Preparation of technical rules containing requirements for encryption in order to protect information according to its classification")* and a utilization concept has been defined *(Control 5.1.1; Requirements (should); second sub-item: ""+ A concept for the application of cryptography is defined and implemented. The following aspects are considered: - Cryptographic procedures, - Key strengths, - Procedures for the complete lifecycle of cryptographic keys, including generation, storage, archiving, retrieval, distribution, deactivation, renewal, and deletion)*. It is also part of the assessment to check that the requirements for key sovereignty have been determined and fulfilled *(Control 5.1.1; Requirements (additional requirements for high protection needs); first sub-item: "+ Key sovereignty requirements (particularly in case of external processing) are determined and fulfilled. (C, I) ")* and an emergency process for restoring key material is established *(Control 5.1.1; Requirements (should); Third sub-item: + An emergency process for restoring key material is established ")*.

5.1.2 "To what extent is information protected during transfer?"

To ensure the protection of information during transmission, the auditor verifies that network services used for transmission are identified and documented *(Control 5.1.2; Requirements (must); First sub-item: "+ The network services used to transfer information are identified and documented ")*, that policies and procedures for the use of network services are defined and implemented *(Control 5.1.2; Requirements (must); Second sub-item: "+ Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented")* and that measures to protect transmitted content are implemented *(Control 5.1.2; Requirements (must); Third sub-item: "+ Measures for the protection of transferred contents against unauthorized access are implemented ")*. In addition, for organizations for which confidentiality is essential, information must be transported or transmitted in encrypted form *(Control 5.1.2; Requirements (additional requirements for high protection needs); First sub-item: + Information is transported or transferred in encrypted form: (C) - Where encryption is not feasible, information must be protected by similarly effective measures. ") (Control 5.1.2; Requirements (should); second sub-item: "+ Electronic data exchange is conducted using content or transport encryption according to the respective classification ")* and it has to be ensured that the addresses used are correct *(Control 5.1.2; Requirements (should); first sub-item: "+ Measures for ensuring correct addressing and correct transfer of information are implemented")*. The auditor also checks that remote access connections have appropriate security features and capabilities *(Control 5.1.2; Requirements (should); Third sub-item: "+ Remote access connections are verified to possess adequate security features (e.g., encryption, granting and termination of access) and capabilities ")*.

4.10.4 Summary:

The requirements of NIS2 Article 21 (2) h) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor during a TISAX assessment.

4.11 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) i)

4.11.1 Requirement from NIS2

NIS2 Article 21 (2) sub-item i) requires human resources security, access control policies and asset management.

4.11.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (2) i) is checked in accordance with the following controls:

- 1.3.1 " To what extent are information assets identified and recorded? "
- 1.3.2 "To what extent are information assets classified and managed in terms of their protection needs?"
- 1.3.3 " To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets? "
- 2.1.1: " To what extent is the qualification of employees for sensitive work fields ensured? "
- 2.1.2: "To what extent is all staff contractually bound to comply with information security policies?"

- 2.1.3: "To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?"
- 2.1.4: "To what extent is mobile work regulated?"
- 3.1.3 " To what extent is the handling of supporting assets managed?"
- 3.1.4 " To what extent is the handling of mobile IT devices and mobile data storage devices managed?"
- 4.1.1: " To what extent is the use of identification means managed?"
- 4.1.2: "To what extent is the user access to IT services and IT systems secured?"
- 4.1.3: " To what extent are user accounts and login information securely managed and applied?"
- 4.2.1: "To what extent are access rights assigned and managed?"
- 5.2.1: "To what extent are changes managed? "
- 5.2.2: "To what extent are development and testing environments separated from operational environments?"
- 5.2.3: "To what extent are IT systems protected against malware?"
- 5.2.4: "To what extent are event logs recorded and analysed?"
- 5.2.5: "To what extent are vulnerabilities identified and addressed?"
- 5.2.6: "To what extent are IT systems and services technically checked (system and service assessment)?"
- 5.2.7: "To what extent is the network of the organization managed?"
- 5.2.8: "To what extent is continuity planning for IT services in place?"
- 5.2.9: "To what extent is the backup and recovery of data and IT services ensured?"

4.11.3 Detailed requirements within the control questions of ISA6

1.3.1 "To what extent are information assets identified and recognized?"

In the TISAX assessment, the auditor checks that the information assets and assets that represent value for the company are identified and recorded *(Control 1.3.1 Requirement Must; first sub-item: "+ Information assets and other assets where security is relevant to the organization are identified and recorded. - A person responsible for these information assets is assigned")* and assigned to the responsible person. In addition, the auditor checks that the associated information carriers are identified *(Control 1.3.1; Requirements (must); Second sub-item: " + The supporting assets processing the information assets are identified and recorded: - A person responsible for these supporting assets is assigned")* and the collected information has been collected in an up-to-date directory *(Control 1.3.1; Requirements (should); First sub-item: " +A catalogue of the relevant information assets exists: - The corresponding supporting assets are assigned to each relevant information asset, - The catalogue is subject to regular review")*.

1.3.2 "To what extent are information assets classified and managed in terms of their protection needs?"

The auditor also checks that a standardized classification scheme is available *(Control 1.3.2; Requirements (must); First sub-item: " + A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available")*, that the information assets have been assessed in accordance with the scheme *(Control 1.3.2; Requirements (must); Second sub-item: " + Evaluation of the identified information assets is carried out according to the defined criteria and assigned to the existing classification scheme")* and that appropriate measures are derived from the classification and complied with *(Control 1.3.2; Requirements (must); Third sub-item: " + Specifications for the handling of supporting assets (e.g. identification,* *correct handling, transport, storage, return, deletion/disposal) depending on the classification of information assets are in place and implemented")*. For a full assessment beyond confidentiality, the auditor checks the extension of the assessment to integrity and availability *(Control 1.3.2; Requirements (should); first sub-item: " + The protection goals of integrity and availability are taken into consideration")*.

1.3.3 " To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets? "

With regard to the use of non-organizational IT services, the auditor checks that these are not used without assessment and implementation of the measures resulting from the assessment *(Control 1.3.3; Requirements (must); First sub-item: "+ External IT services are not used without explicit assessment and implementation of the information security requirements: - A risk assessment of the external IT services is available,- Legal, regulatory, and contractual requirements are considered")* and that the requirements for the services are appropriate to the protection needs of the information to be processed *(Control 1.3.3; Requirements (must); Second sub-item: "+ The external IT services have been harmonized with the protection need of the processed information assets ")*.

2.1.1: " To what extent is the qualification of employees for sensitive work fields ensured? "

To ensure the suitability of employees who access sensitive information, the auditor checks that the sensitive positions are known *(Control 2.1.1; Requirements (must); First sub-item: " + Sensitive work fields and jobs are determined")*, that the requirements for the employees in these positions are known *(Control 2.1.1; Requirements (must); Second sub-item: " + The requirements for employees with respect to their job profiles are determined and fulfilled"* and that a check of the employees' identity *(Control 2.1.1; Requirements (must); Third sub-item: " + The identity of potential employees is verified (e.g. checking identity documents)* and suitability is done *(Control 2.1.1; Requirements (should); First sub-item: " + The personal suitability of potential employees is verified by means of simple methods (e.g. job interview)"* which is extended as required *(Control 2.1.1; Requirements (should); Second sub-item: " + An extended suitability verification depending on the respective work field and job is conducted. (e.g. assessment centre, psychological analysis, checking of references, certificates and diploma, checking of certificates of conduct, checking of professional and private background))"*.

2.1.2: "To what extent is all staff contractually bound to comply with information security policies?"

The auditor also checks whether the employees are obliged to comply with the information security guidelines *(Control 2.1.2; Requirements (must); Second sub-item: "+ An obligation to comply with the information security policies is in effect")* and to maintain confidentiality *(Control 2.1.2; Requirements (must); First sub-item: "+ A non-disclosure obligation is in effect")* beyond the duration of the employment relationship or assignment *(Control 2.1.2; Requirements (should); First sub-item: "+ A non-disclosure obligation beyond the employment contract or order is in effect")*. The auditor also checks that information security is taken into account in employment contracts *(Control 2.1.2; Requirements (should); Second sub-item: "+ Information security aspects are considered in the employment contracts of the staff")* and that a procedure is described in the event of violations *(Control 2.1.2; Requirements (should); Third sub-item: "+ A procedure for handling violations of said obligations is described")*.

2.1.3: "To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?"

The auditor checks whether the company's employees are comprehensively trained and sensitized regarding the risks involved in handling information *(Control 2.1.3; Requirements (must); first sub-item: + Employees are trained and made aware)*. It is also checked that a training concept exists that covers areas relevant to information security *(Control 2.1.3; Requirements (should); first sub-item: + A concept for awareness and training of employees is prepared. As a minimum, the following aspects are considered: - Information security policy, - Reports of information security events, - Reaction to occurrence of malware, - Policies regarding user* *accounts and login information (e.g. password policy), - Compliance issues of information security, - Requirements and procedures regarding the use of non-disclosure agreements when sharing information requiring protection, - Use of external IT services)*, which takes into account the target groups for training concepts and *that* the training measures are appropriate according to the criticality of the information processed *(Control 2.1.3; Requirements (should); second sub-item: Target groups for training and awareness measures (i.e., people working in specific risk environments such as administrators, employees having access to customer networks, personnel in areas of manufacturing) are identified and considered in a training concept)* *and which has* been *approved by management* *(Control 2.1.3; Requirements (should); third sub-item: + The concept has been approved by the responsible management)*. The auditor will also check whether the training and awareness-raising measures are carried out at regular intervals and in response to events *(Control 2.1.3; Requirements (should); fourth sub-item: + Training and awareness measures are carried out both at regular intervals and in response to events)* and whether corresponding documentation is available *(Control 2.1.3; Requirements (should); fifth sub-item: + Participation in training and awareness measures is documented)*. To check that the assessment is effective, the auditor checks that the contact persons for information security are known to employees *(Control 2.1.3; Requirements (should); sixth sub-item: + Contact persons for information security are known to employees)*.

2.1.4: " To what extent is mobile work regulated?"

The auditor also checks that requirements for teleworking are determined and fulfilled *(Control 2.1.4; Requirements (must); first sub-item: " + The requirements for teleworking are determined and fulfilled. The following aspects are considered: - Secure handling of and access to information (in both electronic and paper form) while considering the protection needs and the contractual requirements applying to private (e.g. home office) and public surroundings (e.g. during travels), - Behavior in private surroundings, - Behavior in public surroundings, - Measures for protection from theft (e.g. in public surroundings)")* as well as separate measures for travelling activities *(Control 2.1.4; Requirements (should); first sub-item: " + The following aspects are considered: - Measures for travelling (e.g. viewing by authorities), - Measures for travelling to security-critical countries.")* are identified and fulfilled. The auditor also checks that access to the organization's network is possible via a secure connection *(Control 2.1.4; Requirements (must); Second sub-item: " + The organization's network is accessed via a secured connection (e.g. VPN) and strong authentication")* and that affected employees have been informed of all the measures mentioned *(Control 2.1.4; Requirements (should); Second sub-item: " + Employee awareness")*.

3.1.3: " To what extent is the handling of supporting assets managed?"

To ensure the security-conscious handling of data carriers, the auditor checks that requirements are defined and implemented that cover their entire life cycle *(Control 3.1.3; Requirements (must); first sub-item: " + The requirements for the handling of supporting assets (e.g. transport, storage, repair, loss, return, disposal) are determined and fulfilled")*.

3.1.4: " To what extent is the handling of mobile IT devices and mobile data storage devices managed?"

Regarding the handling of mobile IT devices, the auditor checks that requirements for mobile IT devices and mobile data carriers are determined and fulfilled *(Control 3.1.4; Requirements (must); first sub-item: " + The requirements for mobile IT devices and mobile data storage devices are determined and fulfilled. The following aspects are considered: - Encryption, - Access protection (e.g. PIN, password), - Marking (also considering requirements for use in the presence of customers)")* and that users are informed about the lack of data protection on mobile devices *(Control 3.1.4; Requirements (should); Second sub-item: " + Users are informed of missing data protection on mobile devices")*.

4.1.1: " To what extent is the use of identification means managed?"

The auditor also checks that requirements for the handling of identification means of identification over the entire life cycle are determined and fulfilled *(Control 4.1.1; Requirements (must); first sub-item: " + The* *requirements for the handling of identification means over the entire lifecycle are determined and fulfilled. The following aspects are considered: - Creation, handover, return and destruction, - Validity periods, - Traceability, - Handling of loss ")*, that production is controlled *(Control 4.1.1; Requirements (should); First sub-item: "+ Identification means can be produced under controlled conditions only")*, that validity periods are defined *(Control 4.1.1; Requirements (additional requirements for high protection needs); First sub-item: " + The validity of identification means is limited to an appropriate period. (C, I, A)"),* and that a concept for blocking or invalidation in the event of loss is defined *(Control 4.1.1; Requirements (additional requirements for high protection needs); second sub-item: "+ A strategy of blocking or invalidation of identification means in case of loss is prepared and implemented as far as possible. (C, I, A)")*.

4.1.2: "To what extent is the user access to IT services and IT systems secured?"

Part of the assessment is also that the auditor checks that the user authentication procedure has been selected based on a risk assessment that considers different attack scenarios *(Control 4.1.2; Requirements (must); first sub-item: " + The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been considered (e.g. direct accessibility via the internet)")* and that they are based on the current state of the art *(Control 4.1.2; Requirements (must); Second sub-item: " + State of the art procedures for user authentication are applied")*. It is also checked that the procedures are defined and implemented on the basis of the business-related and security-relevant requirements *(Control 4.1.2; Requirements (should); First sub-item: " + The user authentication procedures are defined and implemented based on the business-related and security-relevant requirements: - Users are authenticated at least by means of strong passwords according to the state of the art"),* that they are adapted to the criticality of the accounts *(Control 4.1.2; Requirements (should); Second sub-item: "+ Superior procedures are used for the authentication of privileged user accounts (e.g. Privileged Access Management, two-factor authentication)"),* and supplemented by additional measures as required *(Control 4.1.2; Requirements (additional requirements for high protection needs); first sub-item: "+ Depending on the risk assessment, authentication procedure and access control have been enhanced by supplementary measures (e.g. continuous access monitoring with respect to irregularities or use of strong authentication, automatic logout, disabling in case of inactivity, or brute force prevention). (C, I, A)")*.

4.1.3 "To what extent are user accounts and login information securely managed and applied?"

Part of the assessment is to check that access to information and IT systems takes place via validated user accounts and that login information is protected and the traceability of transactions and access is ensured. To this end, the auditor checks that user accounts are managed throughout their life cycle *(Control 4.1.3; Requirements (must); First sub-item: "+ The creating, changing, and deleting of user accounts is conducted")*. The auditor also checks that user accounts are blocked immediately after the user leaves the organization *(Control 4.1.3; Requirements (must); Fourth sub-item: "+ User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract)")* and that a regular check is carried out to ensure that the allocation is up to date *(Control 4.1.3; Requirements (must); Fifth sub-item: "+ User accounts are regularly reviewed")*. The auditor also checks that the accounts are personalized *(Control 4.1.3; requirements (must); second sub-item: "+ Unique and personalized user accounts are used")* or, if necessary, that the allocation of collective accounts is subject to regulation *(Control 4.1.3; requirements (must); third sub-item: "+ he use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable)")*. The secure transmission of account information *(Control 4.1.3; Requirements (must); Sixth sub-item: The login information is provided to the user in a secure manner"),* ensuring the confidentiality of the credentials *(Control 4.1.3; Requirements (must); Eighth sub-item: "+ The login information (e.g. passwords) of a personalized user account must be known to the assigned user only")* and the associated behaviors *(Control 4.1.3; Requirements (must); Seventh sub-item: "+ A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential* *compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used)*.

Regarding user profiles, the auditor checks that a standard profile exists *(Control 4.1.3; Requirements (should); first sub-item: "+ A basic user account with minimum access rights and functionalities is existent and used")*. The auditor also checks that manufacturer default accounts are deactivated *(Control 4.1.3; Requirements (should); Second sub-item: Default accounts and passwords pre-configured by manufacturers are disabled (e.g. by blocking or changing of password)")*, that there is a defined process for creating accounts *(Control 4.1.3; Requirements (should); fourth sub-item: "+ Creating user accounts is subject to an approval process (four-eyes principle)"),* and that the accounts are created by an authorized body *(Control 4.1.3; Requirements (should); third sub-item: "+ User accounts are created or authorized by the responsible body")*. The auditor also checks that blocking and deletion periods are defined *(Control 4.1.3; Requirements (should); Sixth sub-item: "+ Deadlines for disabling and deleting user accounts are defined")* and implemented for service provider accounts *(Control 4.1.3; Requirements (should); Fifth sub-item: "+ User accounts of service providers are disabled upon completion of their task")*. The auditor also checks that the use of default passwords is prevented *(Control 4.1.3; Requirements (should); Seventh sub-item: "+ The use of default passwords is technically prevented")*, that interactive login to service accounts is technically prevented *(Control 4.1.3; Requirements (should); Tenth sub-item: "+ Interactive login for service accounts (technical accounts) is technically prevented"),* that the medium is used securely when strong authentication is used *(Control 4.1.3; Requirements (should); Eighth sub-item: "+ Where strong authentication is applied, the use of the medium (e.g. ownership factor) is secure")* and finally that a regular check of the accounts takes place *(Control 4.1.3; Requirements (should); Ninth sub-item: "+ User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems")*.

4.2.1 "To what extent are access rights assigned and managed?"

To ensure that only authorized users have access to information and IT services, the auditor checks that the requirements for the management of access rights have been determined and fulfilled *(Control 4.2.1; Requirements (must); first sub-item: "+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed")*, that authorization concepts have been created *(Control 4.2.1; Requirements (should); First sub-item: "+ Strategies for authorizing access to information are prepared")*, authorization roles are used *(Control 4.2.1; Requirements (should); Second sub-item: "+ Authorization roles are used")*, that no privileged access rights are assigned to normal users *(Control 4.2.1; Requirements (should); Fourth sub-item: "+ Normal user accounts are not granted privileged access rights"),* and that the access rights have been approved by the information officer *(Control 4.2.1; Requirements (additional requirements for high protection needs); First sub-item: "+ The access rights are approved by the responsible internal Information Officer. (C, I, A)")*. The auditor also checks that the assignment of authorizations is needs-based *(Control 4.2.1; Requirements (should); Third sub-item: "+ Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility")*, that the rights are checked regularly *(Control 4.2.1; Requirements (must); second sub-item: "+ The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers"),* and that an update is also carried out in the event of changes to other areas of responsibility *(Control 4.2.1; Requirements (should); fifth sub-item: "+ The access rights of a user account are adapted after the user has changed (e.g. to another field of responsibility")*.

5.2.1: "To what extent are changes managed?"

With regard to changes, the auditor checks that the information security requirements are determined and applied *(Control 5.2.1; Requirements (must); first sub-item: + Information security requirements for changes to the organization, business processes, IT systems are determined and applied "), and that* an assessment is carried out with regard to the impact on information security *(Control 5.2.1; Requirements (should); second sub-*

item: "+ Changes are verified and assessed for their potential impact on the information security"). The auditor also checks that a formal approval procedure has been established for changes with an impact on information security *(Control 5.2.1; Requirements (should); first sub-item: "+ A formal approval procedure is established")*, *and that* these are planned and tested *(Control 5.2.1; Requirements (should); Third sub-item: "+ Changes affecting the information security are subjected to planning and testing")*, that they are verified during and after the changes *(Control 5.2.1; Requirements (additional requirements for high protection needs); First sub-item: "+ Compliance with the information security requirements is verified during and after the changes are applied. (C, I, A) "),* and the fallback in the event of errors is taken into account *(Control 5.2.1; Requirements (should); Fourth sub-item: "+ Procedures for fallback in fault cases are considered”).*

5.2.2: "To what extent are development and testing environments separated from operational environments?"

The auditor checks the existence of a risk assessment regarding the need to separate production and test systems *(Control 5.2.2; Requirements (must); First sub-item: + The IT systems have been subjected to risk assessment in order to determine the necessity of their separation into development, testing and operational systems ")*, the implementation of the results *(Control 5.2.2; Requirements (must); Second sub-item: + A segmentation is implemented based on the results of risk analysis "),* and that requirements for development and test environments have been determined and implemented *(Control 5.2.2; Requirements (should); First sub-item: "+ The requirements for development and testing environments are determined and implemented. The following aspects are considered: - Separation of development, testing and operational systems, - No development and system tools on operational systems (except those required for operation), - Use of different user profiles for development, testing, and operational systems ").*

5.2.3: "To what extent are IT systems protected against malware?"

In order to ensure the protection of IT systems against malware both technically and organizationally, the auditor checks that technical and organizational measures for protection against malware are defined and implemented *(Control 5.2.3; Requirements (must); second sub-item: "+ Technical and organizational measures for protection against malware are defined and implemented")* and that the requirements for protection against malware are determined *(Control 5.2.3; Requirements (must); first sub-item: "+ Requirements for protection against malware are determined*. The check also includes that unneeded network services are disabled *(Control 5.2.3; Requirements (should); First sub-item: "+ Unnecessary network services are disabled ")*, access to network services is restricted *(Control 5.2.3; Requirements (should); Second sub-item: "+ Access to network services is restricted to necessary access by means of suitable protective measures")*, software for protection against malware is installed and regularly updated *(Control 5.2.3; Requirements (should); Third sub-item: "+ Malware protection software is installed and updated automatically at regular intervals (e.g. virus scanner")*, and that received files and received software are automatically inspected for malware *(Control 5.2.3; Requirements (should); Fourth sub-item: "+ Received files and software are automatically inspected for malware prior to their execution (on-access scan)")*. The auditor also checks that regular checks for malware are carried out *(Control 5.2.3; Requirements (should); Fifth sub-item: "+ The entire data contents of all systems is regularly inspected for malware")*, that data transmitted from central gateways is automatically checked *(Control 5.2.3; Requirements (should); Sixth sub-item: "+ Data transferred by central gateways (e.g. e-mail, internet, third-party networks) is automatically inspected by means of protection software: - Encrypted connections are considered")*, and that encrypted connections are considered.

With regard to the user, the auditor checks that protection software is prevented from being deactivated or altered by users *(Control 5.2.3; Requirements (should); Seventh sub-item: "+ Measures to prevent protection software from being deactivated or altered by users are defined and implemented")* and that case-related awareness-raising measures take place *(Control 5.2.3; Requirements (should); Eighth sub-item: "+ Case-related staff awareness measures")*. For IT systems that are operated without malware protection software, the auditor checks that alternative measures have been implemented *(Control 5.2.3; Requirements (should); Ninth sub-*

item: "+ For IT systems operated without the use of malware protection software, alternative measures (e.g. special resilience measures, few services, no active users, network isolation) are implemented ").

5.2.4: "To what extent are event logs recorded and analysed?"

In order to ensure the traceability in the event of a security incident, the auditor checks that event logging takes place and that its handling takes into account the requirements of information security *(Control 5.2.4; Requirements (must); first sub-item: "+ Information security requirements regarding the handling of event logs are determined and fulfilled") and ensures appropriate monitoring and recording of all information security-relevant actions in the network (Control 5.2.4; Requirements (should); third sub-item: "+ Adequate monitoring and recording of any actions on the network that are relevant to information security are established")*. In addition, the auditor determines whether security-relevant requirements for logging the activities of system administrators and users are determined and fulfilled *(Control 5.2.4; Requirements (must); second sub-item: "+ Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled")*. The auditor also checks that the IT systems used are assessed with regard to logging *(Control 5.2.4; requirements (must); third sub-item: "+ The IT systems used are assessed regarding the necessity of logging")* and that the monitoring options are known and taken into account, especially for IT systems outside the organization *(Control 5.2.4; requirements (must); fourth sub-item: "+ When using external IT services, information on the monitoring options is obtained and considered in the assessment")*. The auditor also checks that the accesses set up when establishing and terminating network connections from outside the organization are logged *(Control 5.2.4; Requirements (additional requirements for high protection needs); second sub-item: "+ Cases of access during connection and disconnection of external networks (e.g. remote maintenance) are logged. (C, I, A)")*, the existence of evidence of regular checks of event logs *(Control 5.2.4; Requirements (must); Fifth sub-item: "+ Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions")*, and that an escalation procedure is used for relevant events *(Control 5.2.4; Requirements (should); first sub-item: "+ A procedure for the escalation of relevant events to the responsible body (e.g. security incident report, data protection, corporate security, IT security) is defined and established")*. The auditor also checks that the information security requirements relevant to security during handling are defined and implemented *(Control 5.2.4; Requirements (additional requirements for high protection needs); first sub-item: "+ Information security requirements relevant to the security during the handling of event logs, e.g. contractual requirements, are determined and implemented. (C, I, A)")*, and that the logs are protected against changes *(Control 5.2.4; Requirements (should); Second sub-item: "+ Event logs (contents and meta data) are protected against alteration. (e.g. by a dedicated environment)")*.

5.2.5: "To what extent are vulnerabilities identified and addressed?"

With regard to the vulnerability analysis, the auditor checks that information on technical vulnerabilities is gathered and evaluated *(Control 5.2.5; Requirements (must); First sub-item: "+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS)"), that the findings obtained are used to address such vulnerabilities (Control 5.2.5; Requirements (must); Second sub-item: "+ Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed ")*, and that risks are minimized *(Control 5.2.5; Requirements (should); Second sub-item: "+ Risk minimizing measures are implemented, as necessary ")*. The auditor also checks that patch management is established *(Control 5.2.5; Requirements (should); First sub-item: "+ An adequate patch management is defined and implemented (e.g. patch testing and installation)")* and that the successful installation is verified (*Control 5.2.5; Requirements (should); Third sub-item: "+ Successful installation of patches is verified in an appropriate manner")*.

5.2.6: "To what extent are IT systems and services technically checked (system and service audit)?"

To verify the technical review of IT systems and services, the auditor checks that the requirements for assessing these systems and services are defined *(Control 5.2.6; Requirements (must); First sub-item: "+ Requirements for auditing IT systems or services are determined")*, that these are performed regularly *(Control 5.2.6; Requirements (should); Second sub-item: "+ Regular system or service audits are performed - carried out by qualified personnel - suitable tools (e.g. vulnerability scanners) are used for system and service audits (if applicable) - performed from the internet and the internal network")*, that the assessments are defined in scope *(Control 5.2.6; Requirements (must); Second sub-item: "+ The scope of the system audit is specified in a timely manner")*, and evaluated with regard to the security risks that arise *(Control 5.2.6; Requirements (should); First sub-item: "+ System and service audits are planned taking into account any security risks they might cause (e.g. disturbances)")*. The auditor also checks that they are made known to the operators and users *(Control 5.2.6; Requirements (must); third sub-item: "+ System or service audits are coordinated with the operator and users of the IT systems or services")*.

The assessment also includes the control of evidence of performance *(Control 5.2.6; Requirements (should); Third sub-item: "+ Within a reasonable period following completion of the audit, a report is prepared)* as well as the storage and reporting of the results to management *(Control 5.2.6; Requirements (must); Fourth sub-item: "+ The results of system or service audits are stored in a traceable manner and reported to the relevant management")* and the derivation of appropriate measures based on the report *(Control 5.2.6; Requirements (must); Fifth sub-item: "+ Measures are derived from the results")*.

5.2.7: "To what extent is the network of the organization managed?"

In addition, the auditor checks whether the requirements for the management and control of networks are determined and fulfilled *(Control 5.2.7; Requirements (must); First sub-item: "+ Requirements for the management and control of networks are determined and fulfilled")* and whether the necessary state of the art security aspects are implemented *(Control 5.2.7; Requirements (should); Second sub-item: "+ For a risk-based network segmentation, the following aspects are considered: - Limitations for connecting IT systems to the network, - Use of security technologies, - Performance, trust, availability, security, and safety considerations - Limitation of impact in case of compromised IT systems - Detection of potential attacks and lateral movement of attackers - Separation of networks with different operational purpose (e.g. test and development networks, office network, manufacturing networks) - The increased risk due to network services accessible via the internet, - Technology-specific separation options when using external IT services, - Adequate separation between own networks and customer networks while considering customer requirements - Detection and prevention of data loss/leakage ")*.

5.2.8: "To what extent is continuity planning for IT services in place?"

The auditor checks whether there is continuity planning for IT services *(Control 5.2.8; Requirements (must); First sub-item: "+ Critical IT services are identified, and business impact is considered")* and IT systems *(Control 5.2.8; Requirements (should); First sub-item: "Critical IT systems are identified- the relevant systems are classified to have the appropriate protection need- adequate and appropriate security measures are implemented)*, which is based on an assessment of the criticality of the existing services or systems and which is known to the relevant responsible parties (*Control 5.2.8; Requirements (must); Second sub-item: "+ Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled")*.

In addition, the auditor checks the existence of specifications on different scenarios *(Control 5.2.8; Requirements (should); Second sub-item: "+ Continuity planning includes at least the following scenarios affecting critical IT systems: - (Distributed) Denial of Service attacks - Successful ransomware attacks and other sabotage activities - System failure - Natural disaster)* and backup strategies *(Control 5.2.8; Requirements (should); Third sub-item: "+ Continuity planning considers the following cases - Alternative communication strategies, in case primary communication means are not available - Alternative storage strategies, in case primary storage means are not available - Alternative power and network*") whose timeliness is checked by means of review protocols *(Control 5.2.8; Requirements (should); Fourth sub-item: "+ Continuity planning is regularly reviewed and updated")*.

Another part of the assessment is to ensure that backups are in a recoverable state *(Control 5.2.8; Requirements (additional requirements for high protection needs); Fifth sub-item: "+ A backup and recovery strategy for critical IT services and information is defined and implemented. The following aspects are considered: - Backups are protected against unauthorized modification or deletion by malicious software. (I, A)- Backups are protected against unauthorized access by malicious software or operators (C, I)")* and the data in the backup is not corrupt and is protected against manipulation for the entire period of storage.

5.2.9: "To what extent is the backup and recovery of data and IT services ensured?"

To ensure backups and recoverability of data and IT services, the auditor checks the existence of backup concepts for relevant systems *(Control 5.2.9; Requirements (must); first sub-item: "+ Backup concepts exist for relevant IT systems. The following aspects are considered: - Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups")* and recovery concepts for relevant IT services, *(Control 5.2.9; Requirements (must); Second sub-item: "+ Recovery concepts exist for relevant IT services.")* which consider the dependencies during recovery. *(Control 5.2.9; Requirements (should); First sub-item: "+ A backup and recovery concept exists for each relevant IT service. - Dependencies between IT services and the sequence for recovery are considered")*. Furthermore, for organizations where availability is essential, the auditor checks evidence that methodical reviews of the concepts take place *(Control 5.2.9; Requirements (additional requirements for high protection needs); first sub-item: "+ Backup and recovery concepts are methodically reviewed at regular intervals. (A)"),* the general recovery capacity is taken into account and checked *(Control 5.2.9; Requirements (additional requirements for high protection needs); Second sub-item: "+ General restore capability is considered and tested (e.g., sample testing, test systems) (I, A)")* and that relevant aspects are taken into account *(Control 5.2.9; Requirements (additional requirements for high protection needs); Third sub-item: "+ Backup and recovery concepts consider the following aspects: (A) - Recovery Point Objective (RPO). - Recovery Time Objective (RTO). - Required resources for recovery (considering capacity and performance incl. personnel and hardware). - Avoidance of overload scenarios during recovery. - Appropriate spatial redundancy (e.g., separate room, separate fire section, separate datacenter, separate site))")*.

4.11.4 Summary:

The requirements of NIS2 Article 21 (2) i) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor during a TISAX assessment.

4.12 Evaluation of the degree of fulfilment according to NIS2 Article 21 (2) j)

4.12.1 Requirement from NIS2

NIS2 Article 21 (2) subpoint j) requires the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

4.12.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (2) j) is checked in accordance with the following controls:

- 1.6.3 / To what extent is the organization prepared to handle crisis situations?
- 4.1.2 / To what extent is the user access to IT services and IT systems secured?
- 4.1.3 / To what extent are user accounts and login information securely managed and applied?
- 5.1.2 / To what extent is information protected during transfer?
- 5.2.8 / To what extent is continuity planning for IT services in place?

4.12.3 Detailed requirements within the control questions of ISA6

1.6.3: "To what extent is the organization prepared to handle crisis situations?"

To ensure emergency communication, the auditor checks the existence of crisis planning that considers the means of communication and a fallback level *(Control 1.6.3; Requirements (should); Fifth sub-item: + Crisis policies and procedures are defined and approved. The following aspects are considered: - Exceptional authorities and decision-making processes beyond the crisis management team - Primary and backup means of communication - Emergency operating procedures - Exceptional organizational structures (e.g., reporting, information gathering, decision making) - Exceptional functions, responsibilities, and authority (including reporting) - Exceptional tools ")*.

4.1.2: "To what extent is the user access to IT services and IT systems secured?"

The auditor checks that the user authentication procedure has been selected based on a risk assessment that considers different attack scenarios *(Control 4.1.2; Requirements (must); first sub-item: " + The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been considered (e.g. direct accessibility via the internet)")* and that they are based on the current state of the art *(Control 4.1.2; Requirements (must); Second sub-item: " + State of the art procedures for user authentication are applied")*. It is also checked that the procedures are defined and implemented on the basis of the business-related and security-relevant requirements *(Control 4.1.2; Requirements (should); First sub-item: " + The user authentication procedures are defined and implemented based on the business-related and security-relevant requirements: - Users are authenticated at least by means of strong passwords according to the state of the art")*, that they are adapted to the criticality of the accounts *(Control 4.1.2; Requirements (should); Second sub-item: "+ Superior procedures are used for the authentication of privileged user accounts (e.g. Privileged Access Management, two-factor authentication)")*, and supplemented by additional measures as required *(Control 4.1.2; Requirements (additional requirements for high protection needs); first sub-item: "+ Depending on the risk assessment, authentication procedure and access control have been enhanced by supplementary measures (e.g. continuous access monitoring with respect to irregularities or use of strong authentication, automatic logout, disabling in case of inactivity, or brute force prevention). (C, I, A)")*.

4.1.3 "To what extent are user accounts and login information securely managed and applied?"

Part of the assessment is to check that access to information and IT systems takes place via validated user accounts and that login information is protected and the traceability of transactions and access is ensured. To this end, the auditor checks that user accounts are managed throughout their life cycle *(Control 4.1.3; Requirements (must); First sub-item: "+ The creating, changing, and deleting of user accounts is conducted")*. The auditor also checks that user accounts are blocked immediately after the user leaves the organization *(Control 4.1.3; Requirements (must); Fourth sub-item: "+ User accounts are disabled immediately after the user* *has resigned from or left the organization (e.g. upon termination of the employment contract)")* and that a regular check is carried out to ensure that the allocation is up to date *(Control 4.1.3; Requirements (must); Fifth sub-item: "+ User accounts are regularly reviewed")*. The auditor also checks that the accounts are personalized *(Control 4.1.3; requirements (must); second sub-item: "+ Unique and personalized user accounts are used")* or, if necessary, that the allocation of collective accounts is subject to regulation *(Control 4.1.3; requirements (must); third sub-item: "+ he use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable)")*. The secure transmission of account information *(Control 4.1.3; Requirements (must); Sixth sub-item: The login information is provided to the user in a secure manner")*, ensuring the confidentiality of the credentials *(Control 4.1.3; Requirements (must); Eighth sub-item: "+ The login information (e.g. passwords) of a personalized user account must be known to the assigned user only")* and the associated behaviours *(Control 4.1.3; Requirements (must); Seventh sub-item: "+ A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used)*.

With regard to user profiles, the auditor checks that a standard profile exists *(Control 4.1.3; Requirements (should); first sub-item: "+ A basic user account with minimum access rights and functionalities is existent and used")*, that manufacturer default accounts are deactivated *(Control 4.1.3; Requirements (should); Second sub-item: Default accounts and passwords pre-configured by manufacturers are disabled (e.g. by blocking or changing of password)")*, that there is a defined process for creating accounts *(Control 4.1.3; Requirements (should); fourth sub-item: "+ Creating user accounts is subject to an approval process (four-eyes principle)")*, and that the accounts are created by an authorized body *(Control 4.1.3; Requirements (should); third sub-item: "+ User accounts are created or authorized by the responsible body")*. The auditor also checks that blocking and deletion periods are defined *(Control 4.1.3; Requirements (should); Sixth sub-item: "+ Deadlines for disabling and deleting user accounts are defined")* and implemented for service provider accounts *(Control 4.1.3; Requirements (should); Fifth sub-item: "+ User accounts of service providers are disabled upon completion of their task")*. The auditor also checks that the use of default passwords is prevented *(Control 4.1.3; Requirements (should); Seventh sub-item: "+ The use of default passwords is technically prevented")*, that interactive login to service accounts is technically prevented *(Control 4.1.3; Requirements (should); Tenth sub-item: "+ Interactive login for service accounts (technical accounts) is technically prevented")*, that the medium is used securely when strong authentication is used *(Control 4.1.3; Requirements (should); Eighth sub-item: "+ Where strong authentication is applied, the use of the medium (e.g. ownership factor) is secure")*, and finally that a regular check of the accounts takes place *(Control 4.1.3; Requirements (should); Ninth sub-item: "+ User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems")*.

5.1.2 "To what extent is information protected during transfer?"

To ensure the protection of information during transmission, the auditor verifies that network services used for transmission are identified and documented *(Control 5.1.2; Requirements (must); First sub-item: "+ The network services used to transfer information are identified and documented ")*, that policies and procedures for the use of network services are defined and implemented *(Control 5.1.2; Requirements (must); Second sub-item: "+ Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented")*, and that measures to protect transmitted content are implemented *(Control 5.1.2; Requirements (must); Third sub-item: "+ Measures for the protection of transferred contents against unauthorized access are implemented ")*. In addition, for organizations for which confidentiality is essential, information must be transported or transmitted in encrypted form *(Control 5.1.2; Requirements (additional requirements for high protection needs); First sub-item: + Information is transported or transferred in encrypted* *form: (C) - Where encryption is not feasible, information must be protected by similarly effective measures. ") (Control 5.1.2; Requirements (should); second sub-item: "+ Electronic data exchange is conducted using content or transport encryption according to the respective classification ")* and it has to be ensured that the addresses used are correct *(Control 5.1.2; Requirements (should); first sub-item: "+ Measures for ensuring correct addressing and correct transfer of information are implemented")*. The auditor also checks that remote access connections have appropriate security features and capabilities *(Control 5.1.2; Requirements (should); Third sub-item: "+ Remote access connections are verified to possess adequate security features (e.g., encryption, granting and termination of access) and capabilities ")*.

5.2.8: "To what extent is continuity planning for IT services in place?"

The auditor checks whether continuity planning exists for IT services *(Control 5.2.8; Requirements (must); First sub-item: "+ Critical IT services are identified, and business impact is considered")* and IT systems *(Control 5.2.8; Requirements (should); First sub-item: "Critical IT systems are identified - the relevant systems are classified to have the appropriate protection need - adequate and appropriate security measures are implemented)*, which takes backup strategies into account *(Control 5.2.8; Requirements (should); Third sub-item: "+ Continuity planning considers the following cases - Alternative communication strategies, in case primary communication means are not available - Alternative storage strategies, in case primary storage means are not available - Alternative power and network*").

4.12.4 Summary:

The requirements of NIS2 Article 21 (2) j) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation within a TISAX assessment by the responsible auditor.

4.13 Evaluation of the degree of fulfilment in accordance with NIS2 Article 21 (4)

4.13.1 Requirement from NIS2

NIS2 Article 21 (4) requires that an organization that becomes aware that it is not complying with the measures referred to in Article 21; paragraph 2; a to j (Chapter 4.3 to 4.12 above) shall immediately take all necessary, appropriate and proportionate corrective measures.

4.13.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 21 (4) is checked in accordance with the following controls:

- 1.5.1 "To what extent is compliance with information security ensured in procedures and processes?"
- 1.5.2 "To what extent is the ISMS reviewed by an independent authority?"

4.13.3 Detailed requirements within the control questions of ISA6

1.5.1 "To what extent is compliance with information security ensured in procedures and processes?"

In the TISAX assessment, the auditor checks compliance with information security in procedures and processes *(Control 1.5.1; Requirements (must); First sub-item: + Observation of policies is verified throughout the organization)*. The auditor also checks that compliance with information security in procedures and processes is checked at regular intervals *(Control 1.5.1; Requirements (must); Second sub-item: + Information security policies and procedures are reviewed at regular intervals)* according to a defined plan *(Control 1.5.1; Requirements (should); First sub-item: + A plan for content and framework conditions (time schedule, scope, controls) of the reviews to be conducted is provided)* and is documented in a comprehensible manner *(Control 1.5.1; Requirements (must); Fifth sub-item: + The results of the conducted reviews are recorded and retained)*. The auditor also verifies that compliance with information security requirements is regularly checked *(Control 1.5.1; Requirements (must); Fourth sub-item: "+ Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals")* and that corrective measures are initiated and followed up in the event of non-conformities *(Control 1.5.1; Requirements (must); Third sub-item: "+ Measures for correcting potential non-conformities (deviations) are initiated and pursued")*.

1.5.2 "To what extent is the ISMS reviewed by an independent authority?"

The auditor also checks that an assessment is carried out by an independent body at regular intervals and in the event of significant changes *(Control 1.5.2; Requirements (must); First sub-item: + Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes)* and that the results are documented and reported to the organization's management *(Control 1.5.2; Requirements (should); First sub-item: + The results of conducted reviews are documented and reported to the management of the organization)*. Part of his assessment is also to ensure that corrective actions for possible deviations are initiated and followed up *(Control 1.5.2; Requirements (must); Second sub-item: + Measures for correcting potential deviations are initiated and pursued)*.

4.13.4 Summary:

The requirements of NIS2 Article 21 (4) are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation within a TISAX assessment by the responsible auditor.

Considering the obligation for operators of critical infrastructures within the meaning of the IT Security Act in accordance with the German BSI Act (BSIG) and the German BSI-Kritisverordnung to submit proof of fulfilment of the requirements every two years and the risk-based approach of the NIS2 Directive, a three-year cycle is considered appropriate.

5 NIS2 Article 23

5.1 Evaluation of the degree of fulfilment according to NIS2 Article 23 (1)

5.1.1 Requirement from NIS2

NIS2 Article 23 (1) requires essential and important entities to notify their CSIRT or, where applicable, their competent authority without undue delay of any security incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant security incident). Where applicable, the organizations concerned shall immediately inform the recipients of their services of such significant security incidents that could affect the provision of the service concerned. It shall also require that, inter alia, any information is provided that allows the CSIRT or, where appropriate, the competent authority to determine whether the security incident has a cross-border impact.

5.1.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 23 (1) is checked in accordance with the following controls:

- 1.6.1: "To what extent are information security relevant events or observations reported?"
- 1.6.2: "To what extent are reported security events managed?"

5.1.3 Detailed requirements within the control questions of ISA6

1.6.1: "To what extent are information security relevant events or observations reported?"

The auditor checks whether the parameters by which a reportable event can be measured are defined *(Control 1.6.1; Requirements (must); first sub-item: " + A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders. The following aspects are considered: - Events and observations related to personnel (e.g., misconduct / misbehaviour) - Events and observations related to physical security (e.g., intrusion, theft, unauthorized access to security zones, vulnerabilities in the security zones) - Events and observations related to IT and Cybersecurity (e.g., vulnerable IT-systems, detected successful or unsuccessful attacks) - Events and observations related to suppliers and other business partners (e.g., any incidents that can have negative effect on the security of own organization)")* and that the reporting mechanisms adapted to the severity of the incident are known *(Control 1.6.1; Requirements (must); second sub-item: + Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters")*. The auditor also checks that the necessary reporting channels are available *(Control 1.6.1; Requirements (must); Third sub-item: "+ Adequate channels for communication with event reporters exist".* Another part of the assessment is to ensure that reporting channels are available that are based on the severity of the incident *(Control 1.6.1; Requirements (should); second sub-item: "+ Different reporting channels according to perceived severity exist (i.e., real time communication for significant events / emergencies in addition to asynchronous mechanisms such as tickets or email) are available")* and that the reporting procedures and types are accessible to all relevant reporters *(Control 1.6.1; Requirements (should);*

Fifth sub-item: "+ Mechanism to - and information how to - report incidents is accessible by all relevant reporters").

1.6.2: "To what extent are reported security events managed?"

The assessment includes consideration of handling of events based on their category are defined and assigned *(Control 1.6.2; Requirements (should); Second sub-item: "+Responsibilities for handling of events based on their category are defined and assigned. The following aspects are considered: - Coordination of incidents and vulnerabilities across multiple categories - Qualification and resources - Contact mechanisms based on type and priority (e.g., non-time-critical communication, time-critical communication, emergency communication) - Absence-management")*.

It is also checked that the reporting obligations and the associated contact information are known *(Control 1.6.2; Requirements (additional requirements for high protection needs); third sub-item: "+ Lawful, regulatory, and contractual reporting obligations and respective contact information are known. (C, I, A)")* and a communication strategy is in place that takes into account the target recipients, reporting periods and reporting form *(Control 1.6.2; Requirements (additional requirements for high protection needs); Fourth sub-item: "+ A communication strategy for security related events exist. The following aspects are considered: (C, I, A) - To whom to communicate (e.g., shareholders, affected business partners and customers, other shareholders, general public) - When to communicate - Responsibilities for communication - Authorization and approval of communication - Legal and regulatory restrictions of communication - What to communicate (e.g. prepared templates and building blocks for specific scenarios) - How to communicate (e.g., communication channels)").*

5.1.4 Summary

The requirements of NIS2 Article 23 (1) regarding immediate notification of any security incident that has a significant impact on the provision of its services (significant security incident) and the immediate notification of the recipients of their services of these significant security incidents that could affect the provision of the respective service, if required as well as the requirement that, among other things, all information is transmitted that enables the CSIRT or, if applicable, the competent authority to determine whether the security incident has cross-border implications, are almost fully met by the ISA 6 assessment standard and the controls tested therein.
One exception here is the disclosure of cross-border effects, which is not explicitly required within the ISA. It has already been defined here that emergency communication must be expanded to include the specifications from NIS2. Once this extension has been considered, the requirements are fully met.

5.2 Evaluation of the degree of fulfilment according to NIS2 Article 23 (2)

5.2.1 Requirement from NIS2

NIS2 Article 23 (2) requires that essential and important entities shall promptly communicate to the recipients of their services potentially affected by a significant cyber threat any measures or remedial actions that those recipients may take in response to that threat. The entities shall also inform those recipients, where appropriate, of the significant cyber threat itself.

5.2.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 23 (2) is checked in accordance with the following controls:

- 1.6.2: "To what extent are reported security events managed?"

5.2.3 Detailed requirements within the control questions of ISA6

1.6.2: "To what extent are reported security events managed?"

The review of the handling of reports includes categorization, qualification and prioritization *(Control 1.6.2; Requirements (should); First sub-item: "+ During processing, reported events are categorized (e.g. by responsibility into personnel, physical and cyber), qualified (e.g. not security relevant, observation, suggested security improvement, security vulnerability, security incident) and prioritized (e.g. low, moderate, severe, critical)")* and the response assigned to the class within a defined timeframe *(Control 1.6.2; Requirements (must); First two sub-items: "+ Reported events are processed without undue delay. + An adequate reaction to reported security events is ensured")* as well as involving the necessary responsible parties *(Control 1.6.2; Requirements (should); Second sub-item: "+ Responsibilities for handling of events based on their category are defined and assigned. The following aspects are considered: - Coordination of incidents and vulnerabilities across multiple categories - Qualification and resources - Contact mechanisms based on type and priority (e.g., non-time-critical communication, time-critical communication, emergency communication) - Absence-management*"). It is also checked that the reporting obligations and the associated contact information are known *(Control 1.6.2; Requirements (additional requirements for high protection needs); third sub-item: "+ Lawful, regulatory, and contractual reporting obligations and respective contact information are known. (C, I, A)")* and a communication strategy is in place that takes into account the target recipients, reporting periods and reporting form *(Control 1.6.2; Requirements (additional requirements for high protection needs); Fourth sub-item: "+ A communication strategy for security related events exist. The following aspects are considered: (C, I, A) - To whom to communicate (e.g., shareholders, affected business partners and customers, other shareholders, general public) - When to communicate - Responsibilities for communication - Authorization and approval of communication - Legal and regulatory restrictions of communication - What to communicate (e.g. prepared templates and building blocks for specific scenarios) - How to communicate (e.g., communication channels)").*

5.2.4 Summary

The requirements of NIS2 Article 23 (2), that essential and critical entities immediately notify the recipients of their services potentially affected by a significant cyber threat of any measures or remedial actions that these recipients may take in response to this threat and that the entities also inform these recipients of the significant cyber threat itself, if applicable, are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the responsible auditor within a TISAX assessment. The auditor's review of the ISA requirements catalogue also includes checking compliance with reporting times and reporting channels. The explicit contact information, reporting channels and languages must be included in the Business Continuity Management (BCM) by the companies following their publication by the EU member states. The auditor cannot guarantee that this information is available, as the information to be included is company-specific and can therefore take a variety of forms.

5.3 Evaluation of the degree of fulfilment according to NIS2 Article 23 (3)

5.3.1 Requirement from NIS2

NIS2 Article 23 (3) describes a security incident as significant if:

- it has caused or may cause serious disruption to the operation of services or financial loss to the organization concerned
- he has caused or may cause considerable material or immaterial damage to other natural or legal persons

5.3.2 Summary

The requirements of NIS2 Article 23 (3) are purely informative for the specification of a significant security incident and therefore do not constitute content which can be assessed.

5.4 Evaluation of the degree of fulfilment according to NIS2 Article 23 (4)

5.4.1 Requirement from NIS2

NIS2 Article 23 (4) requires that relevant organizations submit the following to the CSIRT or, where applicable, to the competent authority for the purposes of the notification referred to in paragraph 1:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

By way of derogation from point (b) of the first subparagraph, a Trust Service Provider shall notify the CSIRT or, where applicable, the competent authority of a significant security incident affecting the provision of its trust services without undue delay and in any event within 24 hours of becoming aware of the significant security incident.

5.4.2 Applicable control questions of ISA6

In the TISAX assessment in accordance with the current ISA6 standard, fulfilment of the requirement of NIS2 Article 23 (4) is checked in accordance with the following controls:

- 1.6.1: "To what extent are information security relevant events or observations reported?"
- 1.6.2: "To what extent are reported security events managed?"
- 1.6.3: "To what extent is the organization prepared to handle crisis situations?"

5.4.3 Detailed requirements within the control questions of ISA6

1.6.1: "To what extent are information security relevant events or observations reported?"

The auditor checks whether the parameters by which a reportable event can be measured are defined *(Control 1.6.1; Requirements (must); first sub-item: "+ + A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders. The following aspects are considered: - Events and observations related to personnel (e.g., misconduct / misbehaviour) - Events and observations related to physical security (e.g., intrusion, theft, unauthorized access to security zones, vulnerabilities in the security zones) - Events and observations related to IT and Cybersecurity (e.g., vulnerable IT-systems, detected successful or unsuccessful attacks) - Events and observations related to suppliers and other business partners (e.g., any incidents that can have negative effect on the security of own organization)")* and that the reporting mechanisms adapted to the severity of the incident are known *(Control 1.6.1; Requirements (must); Second sub-item: + Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters")*. Another part of the assessment is to ensure that reporting channels are available based on the severity of the incident *(Control 1.6.1; Requirements (should); Second sub-item: "+ Different reporting channels according to perceived severity exist (i.e., real time communication for significant events / emergencies in addition to asynchronous mechanisms such as tickets or email) are available")*, that the reporting procedures and types are accessible to all relevant reporters *(Control 1.6.1; Requirements (should); Fifth sub-item: "+ Mechanism to - and information how to - report incidents is accessible by all relevant reporters")* and that there is an obligation to report such incidents *(Control 1.6.1; Requirements (should); Third sub-item: "+ Employees are obliged and trained to report relevant events")*. It is also checked that a procedure for feedback is established *(Control 1.6.1; Requirements (should); Sixth sub-item: "+ A feedback procedure to reporters is established".*

1.6.2: "To what extent are reported security events managed?"

The review of the handling of reports includes categorization by class, category and severity *(Control 1.6.2; Requirements (should); First sub-item: "+ During processing, reported events are categorized (e.g. by responsibility into personnel, physical and cyber), qualified (e.g. not security relevant, observation, suggested security improvement, security vulnerability, security incident) and prioritized (e.g. low, moderate, severe, critical)")* and the response assigned to the class within a defined timeframe *(Control 1.6.2; Requirements (must); First two sub-items: "+ Reported events are processed without undue delay. + An adequate reaction to reported security events is ensured")* as well as involving the necessary responsible parties *(Control 1.6.2;*

Requirements (should); Second sub-item: "+ Responsibilities for handling of events based on their category are defined and assigned. The following aspects are considered: - Coordination of incidents and vulnerabilities across multiple categories - Qualification and resources - Contact mechanisms based on type and priority (e.g., non-time-critical communication, time-critical communication, emergency communication) - Absence-management").

It is also checked that the reporting obligations and the associated contact information are known *(Control 1.6.2; Requirements (additional requirements for high protection needs); third sub-item: "+ Lawful, regulatory, and contractual reporting obligations and respective contact information are known. (C, I, A)")* and a communication strategy is in place that takes into account the target recipients, reporting periods and reporting form *(Control 1.6.2; Requirements (additional requirements for high protection needs); Fourth sub-item: "+ A communication strategy for security related events exist. The following aspects are considered: (C, I, A) - To whom to communicate (e.g., shareholders, affected business partners and customers, other shareholders, general public) - When to communicate - Responsibilities for communication - Authorization and approval of communication - Legal and regulatory restrictions of communication - What to communicate (e.g. prepared templates and building blocks for specific scenarios) - How to communicate (e.g., communication channels)")*. It is also checked that maximum response times are defined *(Control 1.6.2; Requirements (additional requirements for high protection needs); first sub-item: "+ Maximum response times based on class, category and severity are defined. (C, I, A)")* and their compliance is monitored and escalated if necessary *(Control 1.6.2; Requirements (additional requirements for high protection needs); Second sub-item: "+ Event not processed appropriately according to their priority are escalated. (C, I, A) - Conditions and thresholds such as maximum reaction times before escalation are defined - Mechanisms, processes, and contacts for escalation are defined - Escalation paths up to the organization's top management is defined")*.

1.6.3: "To what extent is the organization prepared to handle crisis situations?"

Regarding crisis situations, organizations for which availability is essential check that necessary resources for communication are identified *(Control 1.6.3; Requirements (additional requirements for high protection needs); second sub-item: "+ Necessary resources and information to handle crisis (e.g. communication infrastructure, availability of necessary information such as contact information and relevant risks in different crisis situations) are identified. (A) - Appropriate measures to ensure availability of infrastructure or fallback planning and information considering different crisis scenarios are in place")* and a communication strategy is in place *(Control 1.6.3; Requirements (additional requirements for high protection needs); third sub-item: "+ A communication strategy for crisis situations exist. The following aspects are considered: (A) - To whom to communicate (e.g., shareholders, affected business partners and customers, other shareholders, general public) - When to communicate - Responsibilities for communication - Authorization and approval of communication - Legal and regulatory restrictions of communication (e.g., stock corporation regulations) - What to communicate (e.g. prepared templates for statements, contact information and building blocks for specific scenarios) - Communication channels (e.g., Media channels, social media) - Instruments to monitor communication - Instruction and procedures for employees (in case of direct communication approaches such as direct contact of employees by business partners) ")*.

5.4.4 Summary

The requirements of NIS2 Article 23 (4) that relevant entities comply with and are aware of the reporting channels and deadlines to the CSIRT or, where applicable, the competent authority for the purpose of reporting significant security incidents are described by the controls defined in the ISA6 assessment standard and are checked for existence and implementation by the auditor within a TISAX assessment. In addition to the knowledge and existence of the necessary reporting channels and deadlines, the ISA standard also requires the establishment of crisis-proof communication. At this point, the requirements of the ISA go beyond the requirements of NIS2.

The explicit contact information, reporting channels and languages must be included in the Business Continuity Management (BCM) by the companies once they have been published by the EU member states. The existence of this information is not checked during the TISAX assessment, as the information to be included is company-specific and can therefore take a variety of forms.

5.5 Evaluation of the degree of fulfilment according to NIS2 Article 23 (5 - 11)

5.5.1 Requirement from NIS2

NIS2 Article 23 (5- 11) does not make any explicit demands on affected companies that require them to take preparatory measures.

5.5.2 Summary

The requirements of NIS2 Article 23 (5 - 11) do not result in any measures to be assessed and are therefore not included in the ISA 6 requirements catalogue.

6 NIS2 Article 24

6.1 Evaluation of the degree of fulfilment in accordance with NIS2 Article 24 (1)

6.1.1 Requirement from NIS2

NIS2 Article 24 (1) does not make any explicit demands on affected companies that require them to take preparatory measures.

6.1.2 Summary

The requirements of NIS2 Article 24 (1) do not result in any measures to be assessed and are therefore not included in the ISA 6 requirements catalogue.

7 NIS2 Article 25

7.1.1 Requirement from NIS2

NIS2 Article 25 deals with the application of European and international standards and technical specifications for the security of network and information systems.

No explicit demands are made on affected companies that require preparatory measures.

7.1.2 Summary

The requirements of NIS2 Article 25 to use European and international standards and technical specifications for the security of network and information systems to ensure the implementation of the requirements for companies resulting from NIS2 are met by an audit of an organization's ISMS carried out in accordance with TISAX, as this report demonstrates.

8 NIS2 Articles 22, 26-29

8.1 Evaluation of the degree of fulfilment in accordance with NIS2 Article 22, 26 - 29

8.1.1 Requirement from the NIS2

NIS2 Article 22 deals with coordinated risk assessments in relation to the security of critical supply chains at Union level.

NIS2 Articles 26 to 28, which are summarized in Chapter V, deal with jurisdiction and territoriality (Article 26), the register of entities (Article 27) and the database of domain name registration data (Article 28).

No explicit demands are made on the companies concerned that require preparatory measures.

NIS2 Article 29 requires the exchange of information on cybersecurity information.

8.1.2 Summary

NIS2 Article 22 does not contain any specific requirements for companies. Therefore, this article is not considered further in this report.

The requirements of NIS2 Articles 26 to 28 do not result in any measures to be examined and are therefore not considered in this document.

The requirements of NIS2 Article 29 are not assessed within the TISAX assessment.

9 Overall summary

In the automotive industry, the need for industry-wide information- and cybersecurity has been recognized for years and is being addressed in a structured manner, including through the establishment of the TISAX assessment standard in 2017 and the ISA requirements catalogue on which it is based, on the basis of which over 17,500 locations have already been assessed

According to the experts in the automotive industry for information- and cybersecurity, the ISA and TISAX standard represent the state of the art according to the specification of the Manual of Legal Formality[4] :

"The state of the art is the state of development of advanced processes, equipment and operating methods which, according to the prevailing opinion of leading experts, appears to ensure the achievement of the legally prescribed objective. Procedures, equipment and operating methods or comparable procedures, equipment and operating methods must have proven themselves in practice or - if this is not yet the case - should have been successfully tested in practice as far as possible"

This is achieved through the application of TISAX by hundreds of auditors at thousands of companies, the resulting gain in knowledge and the continuous further development and integration of the latest findings from the field of Cybersecurity by the expert panel.

According to the experts of the automotive industry for information- and cybersecurity, the TISAX label is proof that the management of a TISAX-assessed company fulfils the responsibility required in NIS2 Article 20 and has implemented all state-of-the-art risk management measures required in Article 21 within the company, provided that the assessment objectives reflect the overall risk to which the assessed company is exposed and all company locations affected by the requirements of the NIS2 Directive were part of the assessment.

The proof required for this is confirmed by an independent auditor in a three-year cycle. Taking into account the obligation for operators of critical infrastructures within the meaning of the IT Security Act in accordance with the German BSI Act (BSIG) and the German BSI Criticism Ordinance to submit proof of compliance with the requirements every two years and the risk-based approach of the NIS2 Directive, the three-year cycle of the TISAX audit is considered appropriate according to the experts in the automotive industry for information- and cybersecurity.

Within the three-year cycle, the assessed company is obliged to follow up on the measures specified in the assessment and to document their implementation. The company must also carry out regular internal audits of information security policies and procedures and record and retain the results of the audits carried out. These documents are used as proof of active implementation in the next assessment or during interim assessments.

This means that companies that already have a valid TISAX label or will be assessed in the future are well positioned to meet the requirements of the NIS2 directive in these areas.

In addition, NIS2 requirements for the fulfilment of mandatory reporting to authorities and customers must be anchored at the appropriate points in incident management. TISAX provides proof that mechanisms have been established for the fulfilment of such requirements. Due to the direct reference of the document to the requirements of the NIS2 directive, it remains the responsibility of the audited companies to inform themselves about country-specific additional requirements and to check these against the implemented measures.

[4] Federal Ministry of Justice / 3.4.1 General clauses > 122 "State of the art" general clause
https://www.bmj.de/SharedDocs/Publikationen/DE/Fachpublikationen/Handbuch_der_Rechtsfoermlichkeit.pdf

10 Acknowledgements

The German automotive industry was intrinsically motivated and showed the necessary urgency to deal with the holistic establishment of information- and cybersecurity in the industry's organizations. This resulted in the ISA requirements catalogue that has been maintained and published by the ENX Association's ISA working group and the German Association of the Automotive Industry (VDA) respectively. Moreover, it has also resulted in the global application of the TISAX assessment standard.

The way we are positioned as an industry today is due to the great commitment of the experts in the participating companies, the German Association of the Automotive Industry (VDA) and the ENX Association. We would like to express our sincere thanks for this commitment, which is reflected not least in the work on this analysis.

11 Definition of process maturity levels according to ISA

	Maturity level 0
Name	**Incomplete**
Brief description	There is no process, no process is followed or the process is not suitable for achieving the goal.
Definition of	A process is not implemented or the process purpose is not achieved. There is little or no evidence that the purpose of the process is being systematically achieved.

Table 1 Description of the maturity level 0

	Maturity level 1
Name	**Carried out**
Brief description	An undocumented or incompletely documented process is followed ("informal process") and there are signs that it is achieving its goal.
Definition of	- The realised process fulfils its (process) purpose. - The intended basic practices are demonstrably carried out.
Possible proofs (GWP)	+ Work results that provide proof of process results.

Table 2 Description of the maturity level 1

	Maturity level 2
Name	**Controlled**
Brief description	A process is followed that achieves its objectives. Process documentation and proof of process implementation are available.
Definition of	Control of the process implementation (PA 2.1): - The performance targets of the process are identified. - The implementation of the process is planned and monitored. - The implementation of the process is adapted to fulfil the plans. - Responsibilities and authorizations for implementing the process are defined, assigned and communicated. - Resources and information required for the implementation of the process are identified, provided, allocated and utilised. - Interfaces between the units involved are managed to ensure effective communication and clear assignment of responsibilities. Management of work results (PA 2.2): - Requirements for the work results of the process are defined - Requirements for the documentation and management of work results are defined. - Work results are appropriately identified, documented and controlled. - Work results are reviewed in accordance with planned actions and adjusted if necessary to fulfil requirements.
Possible proofs (GWP)	+ Process documentation + Process plan + Quality plan, records + Process implementation records

Table 3 Description of the maturity level 2

	Maturity level 3
Name	**Established**
Brief description	A standard process is followed that is integrated into the overall system. Dependencies on other processes are documented and suitable interfaces created. There is evidence that the process has been used sustainably and actively over a longer period of time.
Definition of	Process definition (PA 3.1): - A standard process, including suitably customised specifications, is defined that describes the basic elements that a defined process must contain. - The sequence and interaction of the standard process with other processes are determined. - Competences and roles required to carry out the process are identified as part of the standard process. - The infrastructure and working environment required to carry out a process are identified as part of the standard process. - Appropriate methods are determined to monitor the effectiveness and appropriateness of the process. Output/dissemination/distribution of the process (PA 3.2): - A defined process based on a suitably selected and/or customised standard process has been rolled out/distributed. - The roles, responsibilities and authorizations required to carry out the defined process are assigned and communicated. - The personnel who carry out the defined process are competent or specialised, which is based on appropriate education, training and experience. - Resources and information required to carry out the defined process are available, allocated and utilised. - The necessary infrastructure and working environment required to carry out the defined process are available, managed and maintained. - Appropriate data is collected and analysed to gain a baseline understanding of the behaviour of the process, demonstrate its appropriateness and effectiveness and assess where continuous process improvement (CIP) can be made.
Possible proofs (GWP)	+ Process documentation + Process plan + Quality records + Guidelines and standards + Process implementation records

Table 4 Description of the maturity level 3

	Maturity level 4
Name	**Predictable**
Brief description	An established process is followed. The effectiveness of the process is continuously monitored by collecting key figures. Threshold values are defined at which the process is considered insufficiently effective and must be adjusted. (Key Performance Indicators)
Definition of	Process measurement (PA 4.1): - Requirements for process information to support relevant, defined business objectives are established. - Process measurement objectives are derived from the process information requirements. - Quantitative objectives regarding process performance to support relevant, defined business objectives are established. - Metrics and frequency of measurements are identified and defined in accordance with process measurement objectives and quantitative process performance objectives. - Measurement results are collected, analysed and reported to monitor the degree of achievement of quantitative process performance objectives. - Measurement results are used to characterise the performance of the process. Process control (PA 4.2): - Analysis and control techniques are determined and applied as applicable. - Variable control limits are established for the normal performance of the process. - Measurement data for specific variants are analysed. - Corrective actions are taken to account for special variants. - Control limits are re-established (if necessary) following corrective actions.
Possible proofs (GWP)	+ Process documentation + Process control plan + Process improvement plan + Process measurement plan + Process implementation records

Table 5 Description of the maturity level 4

	Maturity level 5
Name	**Optimising**
Brief description	A predictable process is followed in which continuous improvement is a key objective. Improvement is actively driven by dedicated resources.
Definition of	Process innovation (PA 5.1) - Process improvement objectives are defined for the specific process that supports the relevant business objectives. - Appropriate data is analysed to identify common causes of variation in process performance. - Appropriate data is analysed to identify opportunities for the application of best practice and innovation. - Opportunities for improvement derived from new technologies and new process concepts are identified. - An implementation strategy is established to achieve the goals of process improvement. - Continuous optimisation (PA 5.2): - The impact of all proposed changes is assessed in relation to the objectives of the defined and standard process. - The implementation of all agreed changes is managed to ensure that any disruption to the performance of a process is understood and acted upon. - The effectiveness of a process change is assessed based on actual performance against defined process requirements and process objectives to determine whether results are consistent with general or specific cases.
Possible proofs (GWP)	+ Process improvement plan + Process measurement plan + Process performance records

Table 6 Description of the maturity level 5

ENX Association
Bockenheimer Landstr. 97-99
60325 Frankfurt am Main
Germany
+49 69 9866927-0
info@enx.com

ENX Association
20 rue Barthélémy Danjou
92100 Boulogne-Billancourt
France