Cyberbezpieczeństwo w dobie innowacji w Automotive

GLOBALNY PARTNER
na rzecz
BEZPIECZNEGO ŚWIATA

DEKRA

THE NEW UPCOMING STANDARD FOR DATA EXCHANGE IN AUTOMOTIVE INDUSTRY

Dipl.-Ing. Wolfgang Glowatzki,
CISSP, CISM Auditor Information Management Systems
(DEKRA Austria)

TISAX® - WHAT DOES IT STAND FOR AND WHAT IS IT?

Trusted

Information

Security

Assessment

e**X**change

- Common assessment and exchange mechanism for the automobile industry
- Based on VDA Information-Security- Asessement-Questionaire catalogue for Self assessments
- Operated by ENX® Association
- Audited by TISAX® accredited audit providers who perform the assessments

ENX® - ASSOCIATION

- Communication network of the European automotive industry
- Founded in the year 2000, legally-independent union of companies and national associations
- More than 1.300 companies in more than 30 countries use globally available ENX services
- Entrusted as a neutral instance by the VDA to operate the TISAX® system
- Acts as a governance organisation of TISAX®
- Accredits TISAX® Audit Providers and monitors the quality of implementation and assessment results

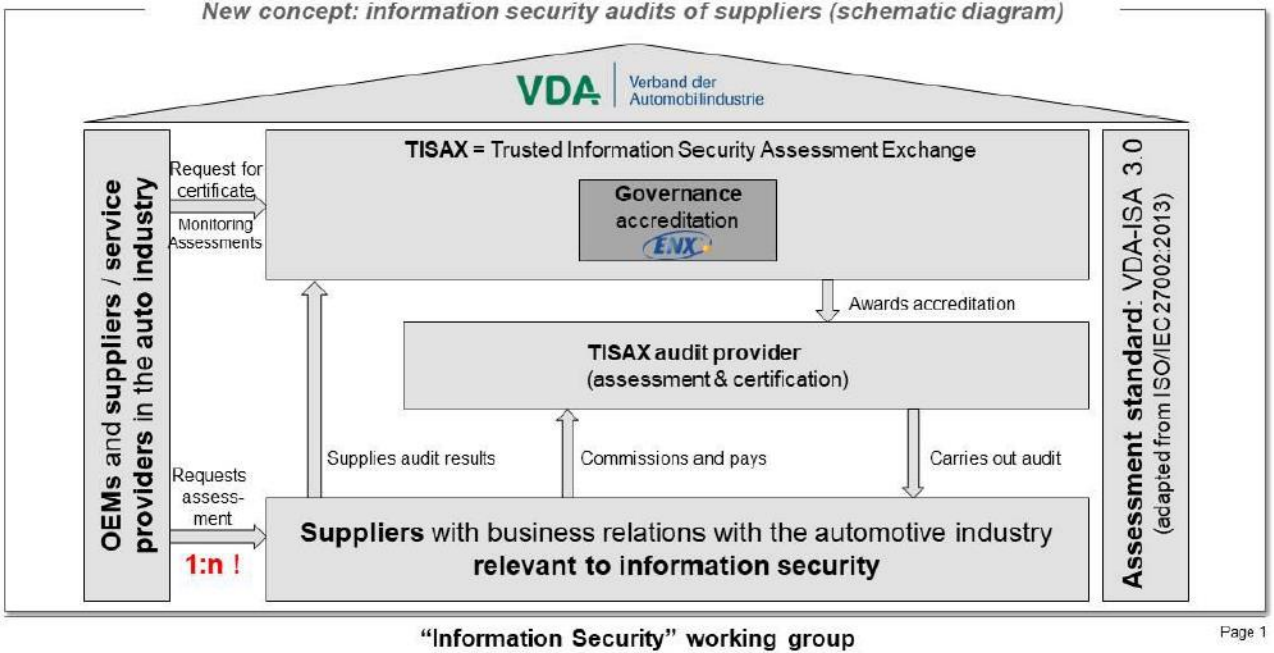
DEKRA

TISAX® - SCHEMATIC DIAGRAM

The TISAX model provides for IT security assessments by audit providers in accordance with a VDA standard, and helps avoid redundant audits.

VDA

New concept: information security audits of suppliers (schematic diagram)



"Information Security" working group

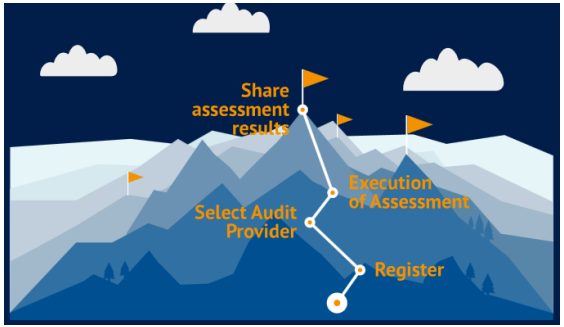
Page 1

TISAX® MAIN BENEFITS

Introduction and implementation of TISAX®…

- saves costs and efforts with manufacturers and suppliers
- establishes a common level of information security in the industry
- creates price transparency for assessments
- allows common recognition of assessment results
- creates competition between audit providers
- facilitates the renewal of existing supplier relations
- give you the chance of creating completely new business connections
- enables industry-wide recognition

TISAX® 4 BASIC STEPS TO JOIN



Source: http://enx.com/tisax/files/images/content/Grafik_Berg_EN-2.svg

1. **Register** as „ TISAX® participant“ @ TISAX® web platform
   - Define TISAX® assessment scope (Standard, Custom (Extended, Narrowed)
   - Choose TISAX® assessment level

2. Select an accredited TISAX® **audit provider** (i.e. for example **DEKRA**)

3. Execute TISAX® **assessment** based on VDA ISA questionaire

4. Upload of TISAX® **assessment results** to TISAX® web platform, **share** to TISAX® partners via platform

TISAX® ASSESSMENT OBJECTIVES

No.	Assessment objective	Abbreviation	Ass. Level
1	Information with high protection level	**Info high**	**AL 2**
2	Information with very high protection level	**Info very high**	**AL 3**
3	Connection to 3rd parties with high protection level	**Con high**	**AL 2**
4	Connection to 3rd parties with very high protection level	**Con very high**	**AL 3**
5	Handling of prototypes with high protection level	**Proto high**	**AL 2**
6	Handling of prototypes with very high protection level	**Proto very high**	**AL 3**
7	Data protection according to German §11 BDSG ("Auftragsdatenverarbeitung")	**Data**	**AL 2**
8	Data protection with special categories of personal data Special categories according to German §3 section (9) BDSG ("besondere Arten"), Data Protection according to German §11 BDSG ("Auftragsdatenverarbeitung")	**Special data**	**AL 3**

TISAX® OBJECTIVES/LABELS

- TISAX® **objectives** are the **input** to the TISAX® assessment process
- The TISAX® objectives are transformed into TISAX® labels by the assessment process
- The TISAX® **label** is the **result (output)** of the TISAX® assessment process
- Currently 8 different TISAX® Labels (list may be extended for future use):

Info High	Con High	Proto High	Data
Info Very High	Con Very High	Proto Very High	Special Data

TISAX® ASSESSMENT LEVELS

Assessment Level 1 (AL 1)

- Only for internal purposes in the sense of a self-assessment
- Auditor checks only for completeness of a self-assessment
- No access to the contents of the assessment
- No gathering of evidence

Assessment Level 2 (AL 2)

- Plausibility check of self-assessment (all locations within scope)
- Check of evidence, also by interviews with colleagues
- Generally done remotely by audio conference, only upon request in person
- In general no site-inspection, only in case of special conditions

Assessment Level 3 (AL 3)

- Includes all checks of AL 2, but more comprehensive
- Verification of self-assessment results in an in-depth on-site inspection and interviews in person

TISAX® AUDIT ASSESSMENT METHODS

Assessment Method	Ass. Level 1 (AL 1)	Ass. Level 2 (AL 2)	Ass. Level 3 (AL 3)
Self-Assessment	☑	☑	☑
Evidences	⊘	Plausibility Check	Thorough Verificiation
Interviews	⊘	By Audio Conference	In person, on-site
On-site Inspection	⊘	depends	☑

SELF ASSESSMENT QUESTIONAIRE AND RESULTS

https://vda.de/en/services/Publications/information-security-assessment.html

TOPICS | SERVICES | PRESS | ASSOCIATION | EN | VDA Verband der Automobilindustrie

Publications

Information Security Assessment

Miscellaneous, 15 February 2018

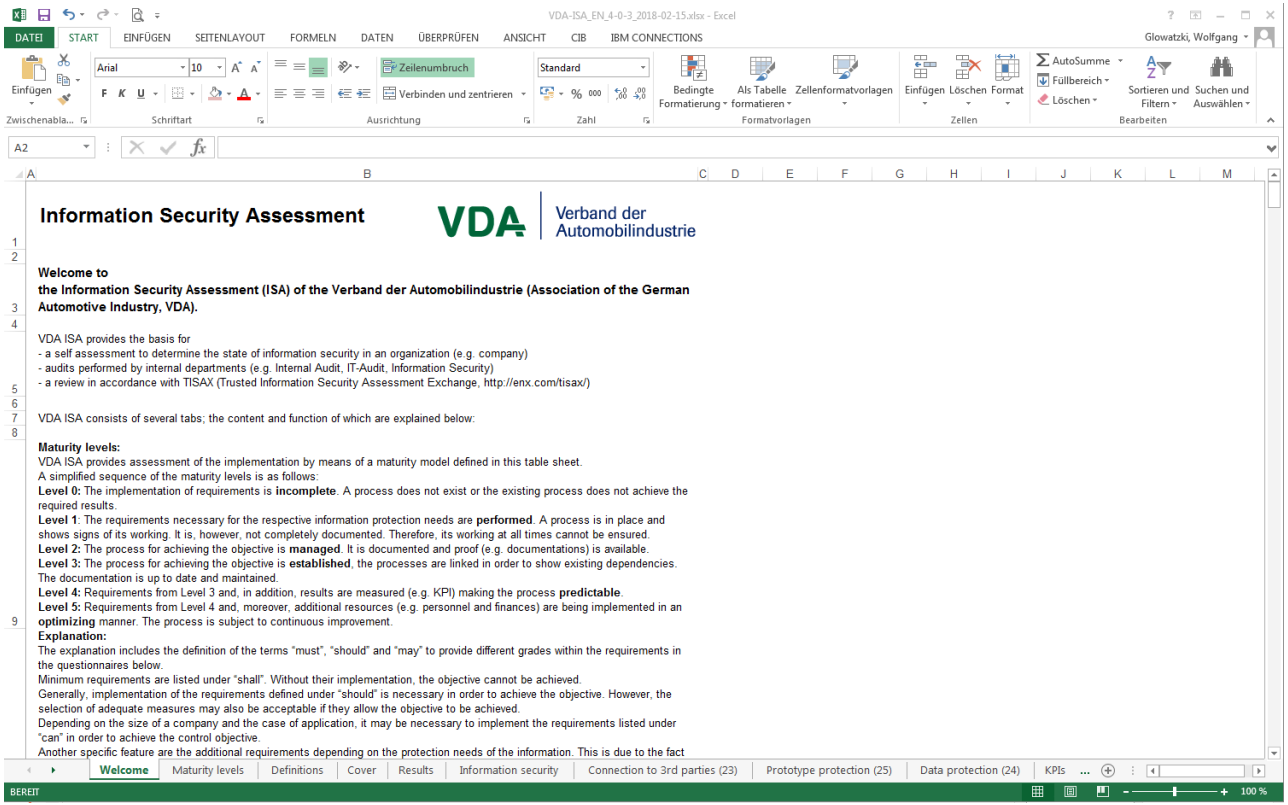
Questionnaire for checking Information Security Assessment and Information Security Management, Vers. 4

Available languages: German, English

DOWNLOAD

https://vda.de/en/services/Publications/information-security-assessment.html

SELF ASSESSMENT QUESTIONAIRE AND RESULTS



VDA-ISA_EN_4-0-3_2018-02-15.xlsx - Excel

DATEI START EINFÜGEN SEITENLAYOUT FORMELN DATEN ÜBERPRÜFEN ANSICHT CIB IBM CONNECTIONS

Glowatzki, Wolfgang

Einfügen Arial 10 Zeilenumbruch Standard Bedingte Formatierung Als Tabelle formatieren Zellenformatvorlagen Einfügen Löschen Format AutoSumme Füllbereich Löschen Sortieren und Filtern Suchen und Auswählen

Zwischenabla... Schriftart Ausrichtung Verbinden und zentrieren Zahl Formatvorlagen Zellen Bearbeiten

A2

Information Security Assessment

VDA Verband der Automobilindustrie

Welcome to
the Information Security Assessment (ISA) of the Verband der Automobilindustrie (Association of the German Automotive Industry, VDA).

VDA ISA provides the basis for
- a self assessment to determine the state of information security in an organization (e.g. company)
- audits performed by internal departments (e.g. Internal Audit, IT-Audit, Information Security)
- a review in accordance with TISAX (Trusted Information Security Assessment Exchange, http://enx.com/tisax/)

VDA ISA consists of several tabs; the content and function of which are explained below:

Maturity levels:
VDA ISA provides assessment of the implementation by means of a maturity model defined in this table sheet.
A simplified sequence of the maturity levels is as follows:
Level 0: The implementation of requirements is **incomplete**. A process does not exist or the existing process does not achieve the required results.
Level 1: The requirements necessary for the respective information protection needs are **performed**. A process is in place and shows signs of its working. It is, however, not completely documented. Therefore, its working at all times cannot be ensured.
Level 2: The process for achieving the objective is **managed**. It is documented and proof (e.g. documentations) is available.
Level 3: The process for achieving the objective is **established**, the processes are linked in order to show existing dependencies. The documentation is up to date and maintained.
Level 4: Requirements from Level 3 and, in addition, results are measured (e.g. KPI) making the process **predictable**.
Level 5: Requirements from Level 4 and, moreover, additional resources (e.g. personnel and finances) are being implemented in an **optimizing** manner. The process is subject to continuous improvement.
Explanation:
The explanation includes the definition of the terms "must", "should" and "may" to provide different grades within the requirements in the questionnaires below.
Minimum requirements are listed under "shall". Without their implementation, the objective cannot be achieved.
Generally, implementation of the requirements defined under "should" is necessary in order to achieve the objective. However, the selection of adequate measures may also be acceptable if they allow the objective to be achieved.
Depending on the size of a company and the case of application, it may be necessary to implement the requirements listed under "can" in order to achieve the control objective.
Another specific feature are the additional requirements depending on the protection needs of the information. This is due to the fact

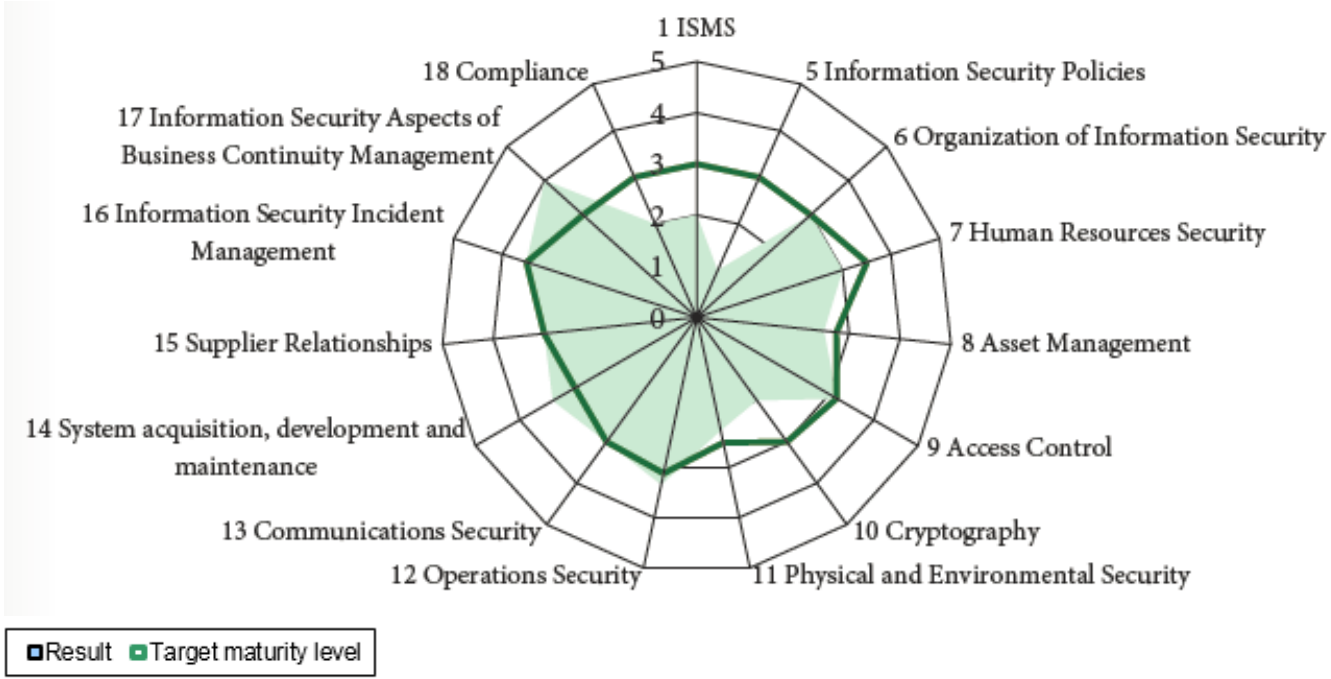
Welcome | Maturity levels | Definitions | Cover | Results | Information security | Connection to 3rd parties (23) | Prototype protection (25) | Data protection (24) | KPIs ...

BEREIT 100 %

DEKRA

SELF ASSESSMENT RESULTS

Total result: 2,49
Max. achievable: 3,0



TISAX® REFERENCES

ENX®:

- https://www.enx.com/tisax/files/downloads/TISAX-Participant-Handbook-current.pdf
- https://portal.enx.com/en-en/TISAX/faqs/

VDA:

- https://vda.de/en/services/Publications/information-security-assessment.html

DEKRA:

- https://www.dekra-certification.de/informationssicherheitsmanagement/tisax.html

CZYNNIK LUDZKI W BEZPIECZEŃSTWA DANYCH ORAZ INFORMACJI

Piotr Ubych,
Menedżer ds. Usług Ochrony Danych
(Grupa DEKRA w Polsce)

UWARUNKOWANIA WZMACNIAJĄCE BEZPIECZEŃSTWO INFORMACJI

- Opracowano programy szkoleń, uwzględniające mechanizmy bezpieczeństwa adekwatnie do ryzyk (np. reagowanie na próby wyłudzenia informacji, korzystanie z publicznych sieci WIFI etc.)
- Programy rozwojowe umożliwiają nabycie praktycznych umiejętności w zakresie stosowania zasad ochrony danych (np. umiejętność budowania haseł, umiejętność szyfrowania dokumentów, umiejętność bezpiecznego niszczenia danych etc.)
- Budowana jest świadomość konsekwencji niewłaściwego postępowania w zakresie ochrony danych

UWARUNKOWANIA WZMACNIAJĄCE BEZPIECZEŃSTWO INFORMACJI

- Pracownicy uczestniczą w pracach związanych z doskonaleniem ochrony danych
- Pracownicy rozumieją swój wpływ na poziom bezpieczeństwa ochrony danych
- Pracownicy podczas codziennej pracy stosują zasady bezpiecznej pracy w zakresie ochrony danych (np. złożoność haseł, przechowanie danych etc).
- Pracownicy rozpoznają i reagują na zagrożenia ochrony danych

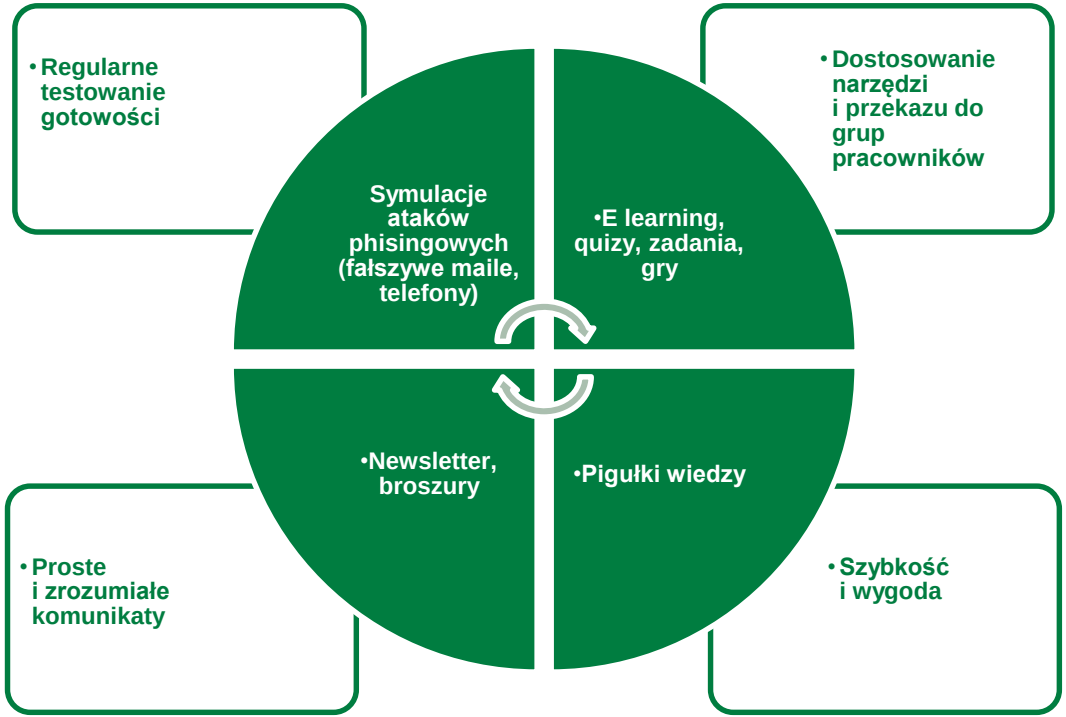
UWARUNKOWANIA WZMACNIAJĄCE BEZPIECZEŃSTWO INFORMACJI

- W organizacji wzmacnia się potrzebę współuczestniczenia w budowaniu pożądanych zachowań
- Organizacja nie faworyzuje wybranych pracowników kosztem pozostałych
- Pracownicy mają możliwość zgłoszenia w wygodnej formie problemów związanych z ochroną danych
- Badane jest wśród pracowników stosowanie zasad ochrony danych w praktyce (rozmowy, ankiety, warsztaty, audyty, kontrole)

UWARUNKOWANIA WZMACNIAJĄCE BEZPIECZEŃSTWO INFORMACJI

- Organizacja przewiduje nagrody dla pracowników którzy wyróżniają się postawą w zakresie właściwej ochrony danych
- Organizacja ma ustanowione procesy analizowania zaistniałych incydentów pod kątem ich unikania w przyszłości
- Stan bezpieczeństwa danych w organizacji jest oceniany na podstawie analiz (ustrukturyzowane raporty, zestawienia)
- Dostawcy posiadają i stosują procedury w zakresie raportowania przez swój personel potencjalnych zagrożeń

DZIAŁANIA UŚWIADAMIAJĄCE



WSKAZÓWKI

Udostępnianie informacji	• Zasady udzielania informacji przez telefon
Ochrona informacji w miejscach publicznych	• Zasady prowadzenia rozmów • Używanie filtrów prywatyzujących • Zasady korzystania z publicznych sieci WIFI
Ochrona haseł	• Reagowanie na żądanie ujawnienia haseł (prośba administratora, email) • Reagowanie na podejrzenie wycieku hasła • Bezpieczne przechowywanie haseł
Korzystanie z poczty email	• Postępowanie z emailami z załącznikiem lub linkiem od nieznanego nadawcy
Urządzenia mobilne i nośniki danych	• Zasady użycia BYOD
Ochrona fizyczna informacji	• Zasady przechowywania i niszczenia dokumentów / urządzeń mobilnych

LOTERIA WIZYTÓWKOWA DEKRA
WYGRAJ PODWÓJNY BILET NA WYŚCIG DTM

ZAPRASZAMY NA STOISKO

DEKRA

W HOLU PRZED SALĄ KONFERENCYJNĄ

ZOSTAW WIZYTÓWKĘ

DO WYGRANIA 2-OSOBOWY BILET NA WYŚCIG DTM NA TORZE NÜRBURGRING WRAZ Z NOCLEGIEM W HOTELU I WSTĘPEM DO STREFY DEKRA HOSPITALITY

LOSOWANIE NAGRODY PODCZAS WIECZORNEJ GALI (20.06)

ZAPRASZAMY!

THANK YOU!
DZIĘKUJEMY!

MISSION

SAFETY

ZAPEWNIAMY

BEZPIECZEŃSTWO

DEKRA