BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF BUSINESS AND MANAGEMENT

FAKULTA PODNIKATELSKÁ

INSTITUTE OF INFORMATICS

ÚSTAV INFORMATIKY

INTRODUCING COMPLIANCE WITH THE TISAX STANDARD INTO THE COMPANY

ZAVEDENÍ SHODY SE STANDARDEM TISAX DO SPOLEČNOSTI

MASTER'S THESIS

DIPLOMOVÁ PRÁCE

AUTHOR AUTOR PRÁCE	Ing. Tereza Tesařová
SUPERVISOR VEDOUCÍ PRÁCE	Ing. Petr Sedlák

BRNO 2024

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF BUSINESS AND MANAGEMENT

Assignment Master's Thesis

Department:	Institute of Informatics
Student:	**Ing. Tereza Tesařová**
Supervisor:	**Ing. Petr Sedlák**
Academic year:	2023/24
Study programme:	Information Management

Pursuant to Act no. 111/1998 Coll. concerning universities as amended and to the BUT Study Rules, the degree programme supervisor has assigned to you a Master's Thesis entitled:

Introducing compliance with the TISAX standard into the company

Characteristics of thesis dilemmas:

Introduction
Theoretical background of the work
Analysis of the current state of the art
Own proposals for solutions
Conclusion

Objectives which should be achieve:

The aim of the diploma thesis is to implement the TISAX standard in a company operating in the automotive industry and to provide a comprehensive view of the process of its implementation. It will also deal with the essence of TISAX certification, the impact of its implementation and the final evaluation of the benefits.

Basic sources of information:

ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky, 2023. [Praha]: Česká agentura pro standardizaci.

ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti, 2023. [Praha]: Česká agentura pro standardizaci.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing. ISBN isbn978-80-88260-39-4.

SEDLÁK, Petr a KONEČNÝ, Martin, 2023. Přeměna ISMS v manažerské informatice. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-110-8.

SEDLÁK, Petr a KONEČNÝ, Martin, 2021. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství. ISBN isbn978-80-7623-068-2.

Deadline for submission Master's Thesis is given by the Schedule of the Academic year 2023/24

In Brno dated 4.2.2024

L. S.

doc. Ing. Miloš Koch, CSc. Branch supervisor	doc. Ing. Vojtěch Bartoš, Ph.D. Dean

ABSTRACT

The thesis focuses on the implementation of compliance with the TISAX standard in a company operating in the automotive industry. The first part presents the theoretical basis for the issue, the second part analyses the current state of the art. This is followed by the design part, where the actual implementation as well as the financial evaluation using the ROSI model is included.

KEYWORDS

TISAX, ISMS, automotive industry, information security, audit.

ABSTRAKT

Diplomová práce se věnuje implementaci shody se standardem TISAX ve společnosti působící v automobilovém průmyslu. Její první část uvádí teoretický podklad pro danou problematiku, druhá potom analyzuje současný stav. Následuje návrhová část, kde je zahrnuta samotná implementace i finanční zhodnocení pomocí ROSI modelu.

KLÍČOVÁ SLOVA

TISAX, ISMS, automobilový průmysl, bezpečnost informací, audit.

ROZŠÍŘENÝ ABSTRAKT

ÚVOD

V dnešní digitální době, kdy má bezpečnost informací klíčový význam, se společnosti v automobilovém průmyslu stále více zaměřují na zavádění standardů a certifikací, které zaručují bezpečnost a důvěrnost výměny informací. Jedním z těchto standardů je TISAX (Trusted Information Security Assessment Exchange), který představuje základní pilíř pro zajištění bezpečnosti informací v dodavatelském řetězci automobilového průmyslu.

Rozvoj informační bezpečnosti v automobilovém průmyslu odráží technologický pokrok v oboru. S tím, jak se vozidla a výrobní procesy stávají chytřejšími a propojenějšími, se zaměření průmyslu na kybernetickou bezpečnost stále zintenzivňuje, což vyžaduje neustálé inovace a přizpůsobování, aby byla zajištěna ochrana před vyvíjející se řadou kybernetických hrozeb.

Tato diplomová práce se zaměřuje na implementaci certifikace TISAX ve vybrané společnosti, která je již certifikována dle standardu IATF (International Automotive Task Force) a čelí potřebě zlepšit svou informační bezpečnost v souladu s aktuálními oborovými standardy a požadavky zákazníků. Společnost se zavázala k neustálému zlepšování a zvyšování kvality svých produktů, což zahrnuje dodržování přísných norem a standardů souvisejících s informační bezpečností.

POPIS ŘEŠENÍ A ZÁVĚR

Implementace TISAX standardu do společnosti může být nezbytným krokem z důvodu rostoucích požadavků zákazníků na zajištění bezpečnosti informací v automobilovém průmyslu. Zavedením standardu lze dosáhnout vysoké úrovně bezpečnosti informací a posílit postavení společnosti jako důvěryhodného partnera v automobilovém průmyslu.

Dipolmová práce poskytuje ucelený pohled na proces zavádění TISAX standardu v praxi s důrazem na klíčovou roli řízení rizik a bezpečnosti dodavatelského řetězce. Poznatky získané z této práce mohou sloužit jako cenná doporučení pro organizace, které také chtějí projít procesem certifikace.

V teoretické části je nastíněna stručná historie bezpečnosti informací v automotive průmyslu, základní terminologie a standardy, jejichž pochopení je v rámci TISAX klíčové. V rámci teoretické části této práce je důležité zmínit také zásadní oblasti jako je řízení rizik a dodavatelský řetězec.

Analytická část je zaměřena na popis organizace a její charakteristiky. Zavedení robustního systému ISMS a účinné strategie řízení rizik byly zdůrazněny jako základní prvky, které jsou klíčové pro sladění s požadavky TISAX.

Praktická část práce zahrnuje process implementace TISAX ve vybrané společnosti. Tento proces začíná přípravou a pokračuje registrací na ENX portále, jejíž součástí je zvážení počtu lokací a rozsahu posouzení. Následně je provedena Gap analýza jako první posouzení, která odhalila tři malé nedostatky v současných postupech, kvůli kterým společnost dočasně obdržela temporary label na 9 měsíců. Během této doby musí společnost zavést nápravná opatření stanovená v plánu nápravných opatření. Navrhované opatření v rámci tohoto plánu byly vyvozeny na základě Gap analýzy a konzultací s odborníky. Zahrnují například dodatek NDA ke smlouvám zaměstnanců nebo odstranění přístupu neoprávněných osob do serverovny společnosti. Úspěšné zavedení těchto opatření představuje pro společnost krok směrem k úspěšnému a efektivnímu zavedení TISAX standardu do praxe.

V poslední části práce jsou srhnuty výsledky posouzení a výhody zavedení standardu TISAX do společnosti. V návaznosti na to bylo provedeno finanční zhodnocení pomocí modelu ROSI, ve kterém byly stanoveny přímé a nepřímé náklady společně s vyčíslenými ušetřenými náklady. Vyhodnocení poskytuje pochopení potenciálních finančních úspor. Výsledek zhodnocení implementace TISAX do popisované společnosti se pravděpodobně nebude shodovat s výsledkem u jiných společností, jelikož náklady se liší v závislosti na vyspělosti zavedeného systému dané společnosti, počtu lokalit nebo výběru certifikačního orgánu, který provádí audit. Ve výsledku ROSI modelu lze vidět, že investovat do zavedení bezpečnostních standardů jako je TISAX se vyplatí, jelikož jeho výsledek návratnosti je velmi pozitivní.

Mezi výhody zavedení systému TISAX do společnosti patří posílení strategické hodnoty tím, že snižuje bezpečnostní rizika a posiluje důvěru mezi partnery. Dále se k nim řadí vysoká úroveň zabezpečení dat, vyhnutí se vysokým nákladům na možné odstávky výroby a pokutám za porušení předpisů na ochranu dat, předcházení možné ztrátě zákazníka či nutnosti zákaznických auditů (jak ze strany organizace, tak ze strany zákazníka).

Nakonec je vhodné zmínit, že úspěšná implementace TISAX standardu závisí na podpoře vedení společnosti, zapojení zaměstnanců a udržování otevřené komunikace s externími partnery a zákazníky. Další důležitou částí je komplexní řízení rizik a dobře zavedený rámec ISMS, jež jsou nezbytné pro úspěšné splnění standardů TISAX, zajištění účinné ochrany informačních aktiv a zároveň budování důvěry v celém dodavatelském řetězci.

BIBLIOGRAPHIC CITATION

TESAŘOVÁ, Tereza. Zavedení shody se standardem TISAX do společnosti [online]. Brno, 2024 [visited on 2024-05-13]. Available from: https://www.vut.cz/studenti/zav-prace/detail/158749. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

DECLARATION

I declare that the present master project is an original work that I have written myself. I declare that the citations of the sources used are complete, that I have not infringed upon any copyright (pursuant to Act. no 121/2000 Coll.).

In Brno, 13 May 2024

……………………….

Ing. Tereza Tesařová

ACKNOWLEDGEMENTS

I would like to thank to my thesis advisor Ing. Petr Sedlák, for his invaluable and inspiring guidance that helped me to expand my knowledge in the field of cyber security. Furthermore, I would like to thank Mr. Marek Chlup for his valuable advice and willingness to help me during consultations. His helpfulness and practical advice were crucial to me during the writing of this thesis. Finally, I want to thank my significant other and my family for supporting me during my study.

CONTENT

INTRODUCTION

In today's digital era, where information security is of key importance, companies in the automotive industry are increasingly focusing on implementing standards and certifications that guarantee the security and confidentiality of information exchange. One of these standards is TISAX (Trusted Information Security Assessment Exchange), which represents a basic pillar for ensuring information security in the supply chain of the automotive industry.

The development of information security in the automotive industry mirrors the technological advancements within the field. As vehicles and manufacturing processes become smarter and more connected, the industry’s focus on cybersecurity continues to intensify, requiring ongoing innovation and adaptation to safeguard against an evolving array of cyber threats.

This diploma thesis focuses on the implementation of TISAX certification in a selected company, which is already certified according to the IATF (International Automotive Task Force) standard and faces the need to improve its information security in accordance with current industry standards and customer requirements. The company is committed to continuous improvement and enhancement of the quality of its products, which includes compliance with strict norms and standards related to information security.

1 PURPOSE OF THESIS

1.1 Goals of Thesis

The aim of this work is to provide a comprehensive view of the process of implementing TISAX certification in practice, including overcoming challenges, identifying key areas, and developing strategies to ensure information security in accordance with TISAX requirements. The work also examines the impact of TISAX certification implementation on the company's position in the commercial vehicle manufacturing industry and its reputation as a trusted partner.

1.2 Reason for Introducing TISAX

As a company operating within the automotive industry, you might find yourself in a scenario where your business partner requests TISAX certification to ensure the secure exchange of confidential information they hold. It's understandable that no manufacturing company would want its confidential information to be accessed by competitors. TISAX certification serves as both a guarantee and validation that the information is sufficiently protected.

As part of this work, individual steps and procedures leading to the successful introduction of TISAX certification are evaluated and recommendations are proposed for other companies in the automotive industry that decide on a similar certification process and improvement of information security in their operations.

2 THEORETICAL BASIS

2.1 Information Security in Automotive Industry

The automotive industry has undergone a profound transformation over the past few decades, not just in terms of technological innovations but also in the critical area of information security. This transformation reflects the broader digital revolution that has influenced across industries worldwide. As vehicles evolve from purely mechanical devices to complex integrated systems that combine hardware, software, and connectivity, the imperative for robust information security measures has become increasingly urgent. [1] [2]

The history and development of Information Security in the automotive industry is a critical area, particularly as vehicles and manufacturing processes become increasingly connected and digitized. This progression can be outlined through several key phases, reflecting the industry's response to emerging challenges and the integration of advanced technologies. [1] [2]

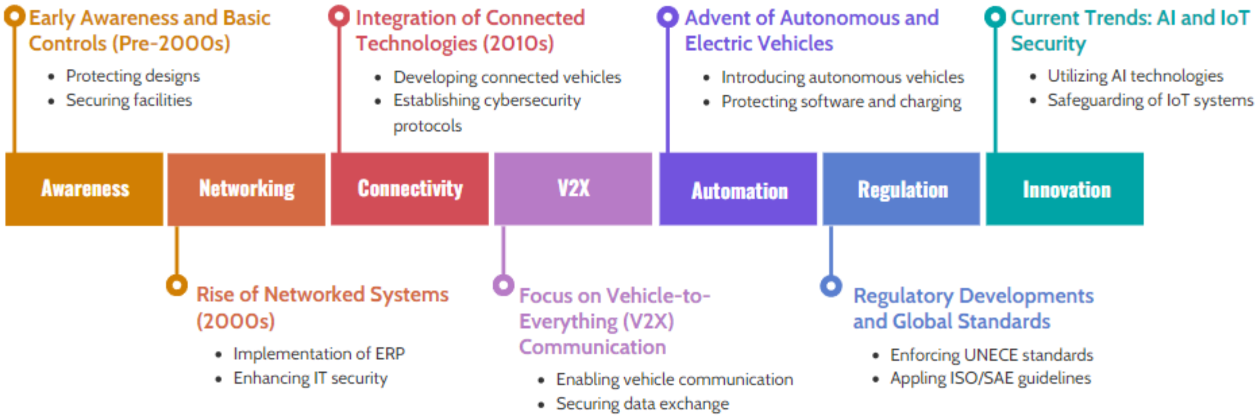

Early Awareness and Basic Controls (Pre-2000s)
• Protecting designs
• Securing facilities
Integration of Connected Technologies (2010s)
• Developing connected vehicles
• Establishing cybersecurity protocols
Advent of Autonomous and Electric Vehicles
• Introducing autonomous vehicles
• Protecting software and charging
Current Trends: AI and IoT Security
• Utilizing AI technologies
• Safeguarding of IoT systems
Awareness
Networking
Connectivity
V2X
Automation
Regulation
Innovation
Rise of Networked Systems (2000s)
• Implementation of ERP
• Enhancing IT security
Focus on Vehicle-to-Everything (V2X) Communication
• Enabling vehicle communication
• Securing data exchange
Regulatory Developments and Global Standards
• Enforcing UNECE standards
• Appling ISO/SAE guidelines

Figure 1 Evolution of Information Security in Automotive Industry [own elaboration]

2.1.1 Early Awareness and Basic Controls (Pre-2000s)

Initially, information security in the automotive industry was mostly concerned with safeguarding proprietary design and manufacturing data from industrial espionage. Security measures during this period were elementary, generally focusing on physical security and basic IT controls. The industry's reliance on isolated systems meant that cybersecurity has not yet a significant focus. [3] [4]

2.1.2 Rise of Networked Systems (2000s)

As automotive manufacturers began to incorporate networked computers extensively into their operations for design, manufacturing, and supply chain management, the need for more sophisticated cybersecurity measures increased. The adoption of technologies such as Enterprise Resource Planning (ERP) systems and the introduction of more comprehensive IT networks necessitated stronger access controls, data encryption, and incident response strategies. [5] [6]

2.1.3 Integration of Connected Technologies (2010s)

The introduction of connected cars marked a pivotal shift in information security needs. Vehicles began to feature built-in connectivity for navigation, in-car entertainment, and system diagnostics, which opened new avenues for potential cyber threats. This period manufacturers started to implement more advanced cybersecurity measures, focusing on securing both the vehicles and the networks they connected to. [7]

2.1.4 Focus on Vehicle-to-Everything (V2X) Communication

With the advancement of Vehicle-to-Everything (V2X) communication, cars started to interact with other vehicles, infrastructure, and pedestrian devices. This broader connectivity required an integrated approach to security, including not only the vehicles themselves but also the infrastructures they interact with. Automotive cybersecurity standards began to evolve, with organizations like SAE International (Society of Automotive Engineers) developing guidelines such as SAE J3061, the first automotive-specific cybersecurity standard. [3] [8]

2.1.5 Advent of Autonomous and Electric Vehicles

The development of autonomous and electric vehicles brought new complexities to automotive cybersecurity. Autonomous vehicles, relying heavily on sensors and real-time data for navigation and decision-making, posed unique security challenges that required robust protections against tampering and hacking. Electric vehicles also introduced new considerations, such as securing charging infrastructure and protecting battery management systems from cyberattacks. [7] [9] [10]

2.1.6 Regulatory Developments and Global Standards

As threats have evolved, so too have the regulatory frameworks governing automotive cybersecurity. Organizations and governments worldwide have started to implement more stringent regulations. For example, the UN Economic Commission for Europe (UNECE) WP.29 regulation mandates cybersecurity and software update management systems for new vehicle types. Similarly, the ISO/SAE 21434 standard was established to provide a global benchmark for automotive cybersecurity risk management. [11] [12]

2.1.7 Current Trends: AI and IoT Security

Today, the integration of Artificial Intelligence (AI) and the Internet of Things (IoT) in automotive technologies further complicates the cybersecurity landscape. The automotive industry is increasingly using AI to enhance vehicle functionalities and IoT devices to improve the interconnectedness of vehicle systems. These advancements necessitate cutting-edge cybersecurity solutions, including AI-driven threat detection systems and comprehensive IoT security strategies. [13]

2.2 Terminology and Fundamental Topics

2.2.1 Information, data, knowledge

Data, information, and knowledge are closely related concepts, but they have distinct meanings.

Data are basic facts that may be in the form of numbers, texts, or measurements, and which may not have direct meaning in themselves, but may be processed or analyzed to obtain information. [14] [15]

Information is interpreted data about any object that provides meaning and context to enable decision-making or provide a deeper understanding of a situation or phenomenon. [14] [15]

Knowledge is the highest level in this hierarchy defined as the use of examining available information through experiences and other already acquired knowledge. Thanks to this, it is possible to draw useful insights from the information analyzed in this way, which can be applied in further decision-making processes. [15]

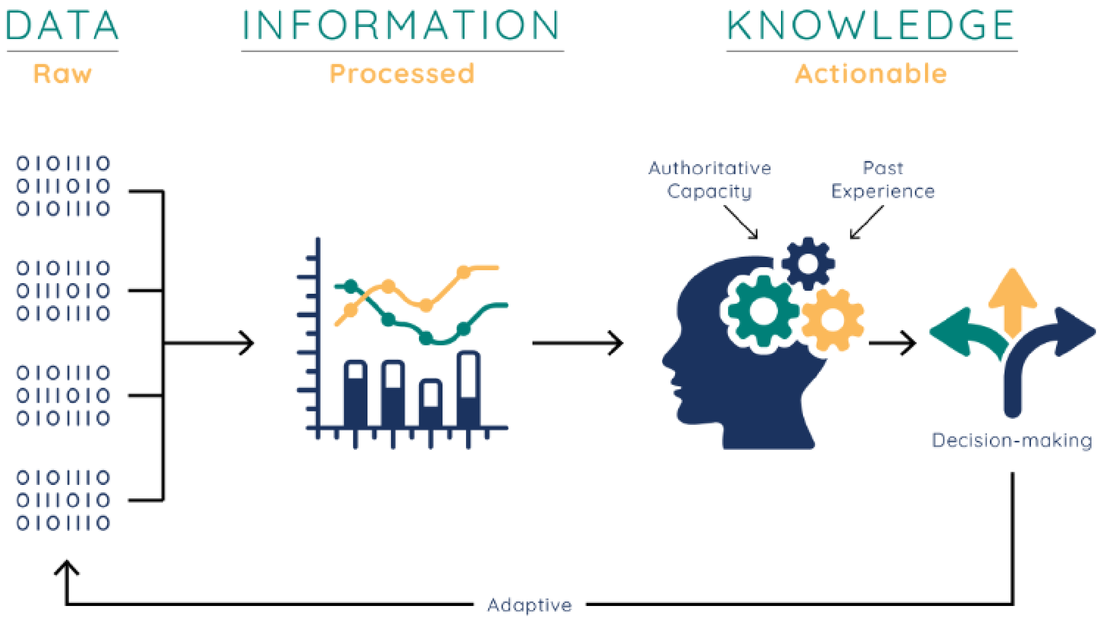


Figure 2 Data, Information and Knowledge Relation [16]

2.2.2 Information Security

It is a set of measures and methodologies aimed at protecting data and information systems against unauthorized access, misuse, loss or damage and ensuring the integrity, confidentiality and availability of information. An appropriate set of measures are selected through the risk management process and managed through the ISMS. These measures include policies, processes, procedures, organizational structures, software and hardware to ensure the protection of identified information assets. It is essential that these measures are specified, implemented, monitored, reviewed and refined where necessary to meet specific information security objectives as well as the organization's business objectives. [16] [17]

2.2.3 Information Security Management System (ISMS)

An ISMS is a strategic framework based on the principle of continuous improvement that provides organizations with a structured approach to protecting their information. It includes policies, procedures and controls designed to minimize risks to information assets and ensure compliance with legal and business requirements, as well as internal standards and policies. This framework is based on a plan-do-check-act (PDCA) approach that ensures adaptability and accountability at all levels of the organization. Its goal is not only to protect information, but also to increase the trust of customers and partners in the protection mechanisms of the organization. [16]

2.2.4 Information Security Triad

The information security triad comprises three core principles: confidentiality, integrity, and availability (CIA), which form the cornerstone of effective information security practices, aiming to secure assets from various threats and risks. [18] [19]

C
Confidentiality
The Information Security Triad
I
Integrity
A
Availability

Figure 3 Cyber Security Triad [39]

Confidentiality is a fundamental principle that ensures sensitive information is protected from unauthorized access, use, or disclosure. Only authorized users and processes should have access to data, ensuring that sensitive information remains private and secure. [19] [20]

Integrity refers to the trustworthiness and completeness of data. Data should be maintained in a correct state, preventing unauthorized modifications, and ensuring that it is accurate, authentic, and reliable. [19] [20]

Availability refers to the ability of authorized users to access data and systems when needed. This means that data and systems should be available to authorized users without interruption. [19] [20]

2.2.5 Asset, Threat and Vulnerability

Asset is a resource of value that an organization aims to protect and has value. Tangible assets are physical assets that can be seen and touched, while intangible assets are non-physical and cannot be touched. Examples of tangible assets include computers or buildings, while intangible assets include a company's strategy, customer records or financial records. [14] [21]

Threats are anything that can exploit a vulnerability to obtain, damage, or destroy an asset. They can be natural, unintentional, or intentional, and include burglars, hackers, malware, and human error. [14] [22] [23]

Vulnerabilities are weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. They can be intrinsic (within the asset) or extrinsic (outside the asset), and include software bugs, malfunctioning hardware, and user actions that make a device susceptible to malware infection. [14] [23]

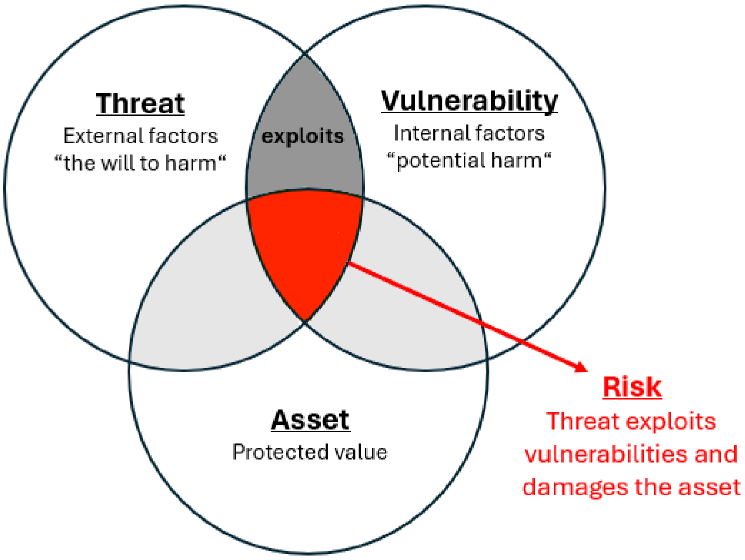


Figure 4 Threat, Vulnerability and Asset Relation [14][own elaboration]

2.2.6 Risk

Risk according to the standards of information security is the possibility of a threat exploiting a vulnerability to cause harm to an asset. It is a combination of the likelihood of an event occurring and the impact it would have on the asset if it did occur. [14] [20]

2.2.7 Audit

An audit is a systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine whether the procedures or requirements are fulfilled. [14] [20]

2.2.8 Compliance

Compliance in the context of information security refers to the process of adhering to industry-specific laws, rules, and standards to ensure the confidentiality, integrity, and availability of information. [24] [25]

2.3 Risk Management

Risk management is a process that involves the identification, analysis and application of strategies to reduce and control potential risks that could affect the organization. [14]

Risk assessment and risk management in the context of ISMS can be divided into several key stages (figure 5). This entire process is supported by relevant standards such as ISO/IEC 27005 and ISO 31000, which provide a framework and guidelines for effective risk management in the area of information security. However, the organization may also use its own methodology, this way is commonly used in practice.

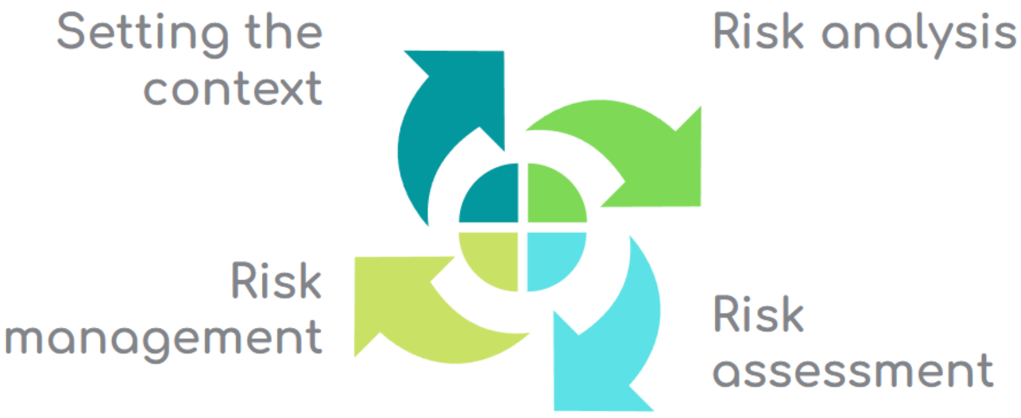


Figure 5 Risk Management Phases [14][own elaboration]

[14]

The risk management process is iterative and requires regular reviews and updates of risk analysis and risk management. This includes evaluating the effectiveness of implemented security measures and any adjustments to security policy or emergency plans. [14]

2.3.1 Risk Assessment

Risk assessment is a critical component of an ISMS. In this subchapter are described the main phases of risk assessment. ISMS risk management is defined in the ISO/IEC 27005 standard, in which the ISMS risk assessment process is described as following picture (figure 6). Risk identification and risk estimation together form the risk analysis. Each of these phases is essential for effective and systematic risk management within an ISMS. [14] [26]

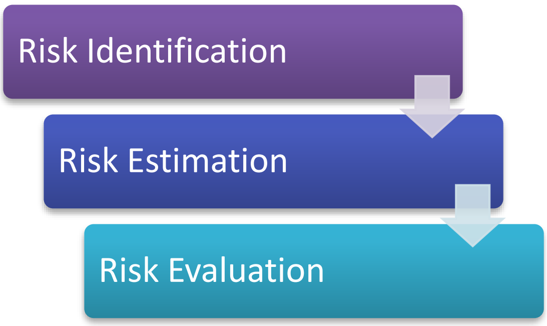


Figure 6 Risk Assessment Process [30][own elaboration]

2.3.1.1 Risk Analysis

The risk analysis process begins with identifying vulnerabilities and assessing threats. This results in an estimate of the risk level for each combination of asset and threat.

There are different approaches to risk analysis, including rough, informal (pragmatic), combined and detailed analysis, which allow organizations to choose the method best suited to their specific needs. [14]

Risk analysis is a key element of the information security management process and consists of several important phases.

Stage 1: Asset Assessment

This phase includes the identification and classification of all assets that are important to the organization. Assets are evaluated based on their importance to the organization's information systems and may include hardware devices, software products, information data, and services provided through information systems. [14] [26]

Each asset is rated for its confidentiality, integrity and availability. Asset rating involves assigning a value on a scale of 1 to 5 for each of the criteria, which allows the total weight of the asset to be calculated. [14] [26]

Stage 2: Threat and Vulnerability Assessment

In this phase, the potential threats to each asset and the vulnerabilities that the threats can exploit are identified.

Threats can include technical failure, malware attacks, physical damage or human error and are categorized by how they affect different aspects of assets such as operating systems, applications, databases and network infrastructure. Vulnerability refers to weaknesses in asset protection that can be exploited. [14] [26]

Assessment for both threat and vulnerability again use the scale of 1 to 5 (5 is the most likelihood of threat). [14]

Stage 3: Risk Rate Calculation

Based on the assessment of assets, threats and vulnerabilities, the risk level is calculated. The level of risk is expressed as the following formula (2.1.1). This calculation makes it possible to quantify the risk and makes it easier to decide on priorities in risk management. [14] [26]

$$Risk = Threat\ x\ Asset\ x\ Vulnerability \tag{2.1.1}$$

Phase 4: Selection and Implementation of Security Measures

Based on the calculation of the risk level, suitable measures for risk management are subsequently determined. These measures may involve technical, organizational or personnel changes and could be divided into different areas of security, including IT security, communication security, personnel security, administrative security and physical security. [14] [26]

The choice of measures depends on the effectiveness of risk reduction options and the economic aspects of their implementation. The goal is to achieve an acceptable level of risk for the organization. [14] [26]

2.3.1.2 Evaluation of Risk Impact

After analyzing the risks, it's important to identify which ones could cause the most damage. Considering the likelihood of the event and the impact it could have on the organization's information assets, this process allows to determine the hazards that require immediate attention and control to avert potential security breaches. [14] [26]

A risk evaluation matrix is often used to visualize the risk assessment results, which helps to prioritize risks, enabling organizations to focus on the most critical risks that require treatment. [14] [26]

2.3.1.3 Creation a Risk Treatment Plan

After identification of risks, it is important to manage them. For that purpose, serves a Risk Treatment Plan, which specifies the controls to be implemented, responsible persons, planned deadlines and required resources. [14] [26]

Risk can be treated by four ways:

a) Transferring – sharing risk to a third party (e.g. outsourcing).
b) Avoiding – avoiding the actions that cause the risk (e.g. not using technology or process that poses high risk).
c) Mitigation – taking actions that reduce the risk is the most common approach, typically involves implementing controls from Annex A of ISO 27001.
d) Acceptance – appropriate for low-impact risks or risks that meets the acceptable level.

2.3.1.4 Monitoring, Revision and Internal Auditing

Monitoring and reviewing risk management is essential for organizations to assess the effectiveness of risk management strategies, identify areas for improvement, ensure compliance with regulations, and mitigate emerging risks. Methods include internal audits, external audits, and risk assessments, with benefits such as early risk identification, compliance assurance, and improved risk management strategies. [26]

2.4 Information Security Standards

There are several key standards in the field of information security that define standards for protecting information and IT infrastructure. These standards are designed to help organizations protect themselves from threats and ensure compliance with legal and regulatory requirements. Here is a list of standards relevant to this thesis.

2.4.1 ISO/IEC 27001:2022

ISO/IEC 27001 is an international standard for Information Security Management Systems (ISMS), which helps organizations protect their information through adequate risk assessment and the implementation of effective security measures. It utilizes a process approach for the implementation, operation, monitoring, review, maintenance, and improvement of the information security management system. The catalog of safety measures is contained in Annex A of the standard. [14] [27] [28]

2.4.2 ISO/IEC 27002:2022

ISO 27002 serves as a supporting standard to ISO 27001 and provides guidance on how to perform information security controls. It acts as a code of practice for information security management and makes several recommendations for the implementation of the controls specified in ISO 27001. [14] [28] [29]

The latest edition of ISO 27002, released in 2022, updates the previous 2013 version and is synchronized with the latest version of ISO 27001. This updated version emphasizes a risk-based information security management strategy and highlights the critical role of identifying and managing risks associated with an organization's information assets. [14] [28] [29]

ISO 27002 contains an extensive list of security measures that organizations can take to strengthen the security of their information systems. The standard provides advice on risk management, security policies, information security organization, asset management, human resources, physical security, communications, systems access, acquisition, development, operations, incident response and compliance. [14] [28] [29]

2.4.3 ISO/IEC 27005:2022

ISO/IEC 27005 is a standard providing recommendations for managing information security risks within an organization. It aligns with the principles outlined in ISO/IEC 27001 and ISO/IEC 27002 and is structured to effectively support the implementation of information security through a risk management framework. This standard does not prescribe a specific methodology for managing information security risks but allows organizations to select an approach that best fits their needs, considering factors such as the scope of the ISMS, risk management context, and industry sector. ISO/IEC 27005 is suitable for all types of organizations, including commercial companies, government organizations, and non-profit organizations, intending to manage risks that could compromise the security of their information. [14] [30]

2.4.4 NIS 2

NIS Directive 2 is an update of the original Network and Information Security (NIS) Directive from 2016, which was adopted by the EU to increase cyber resilience across Member States. NIS 2 aims to strengthen cybersecurity across various sectors, impacting both public and private entities. The Directive emphasizes the need to raise the level of cybersecurity and introduces stricter obligations for incident reporting, risk assessment and measurement of security impacts. [31] [32]

National Cyber and Information Security Agency of Czech Republic (NÚKIB) will draft the text of the new Cybersecurity Act and eight related decrees at the end of January 2023. The NÚKIB has proposed not to go down the route of amending the current law, but a completely new law. [31] [32]

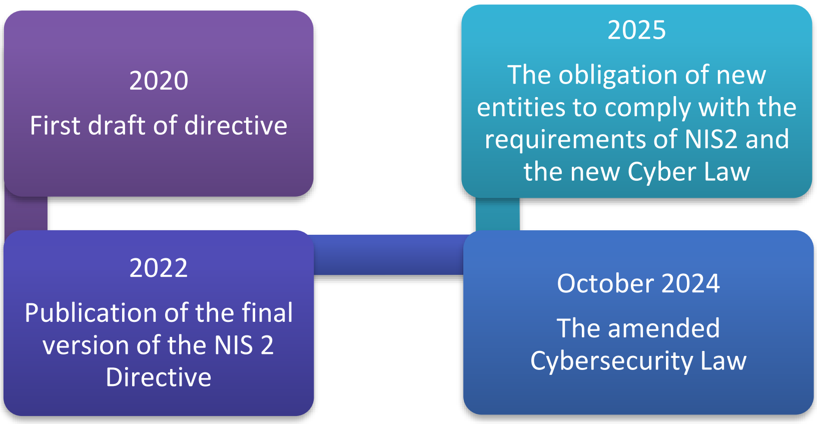

2020
First draft of directive
2022
Publication of the final version of the NIS 2 Directive
October 2024
The amended Cybersecurity Law
2025
The obligation of new entities to comply with the requirements of NIS2 and the new Cyber Law

Figure 7 NIS 2 Publication in Czech Republic [31] [32][own elaboration]

2.5 TISAX (Trusted Information Security Assessment Exchange)

TISAX is an exchange mechanism of information security assessment in automotive. It represents a unique scheme for evaluation that has been specifically developed for the automotive sector by the German Automotive Industry Association. Its main objective is to ensure that all stakeholders - from manufacturers to suppliers - adhere to uniform standards for the protection of sensitive information. Company that is TISAX certified confirms that the information security management system meets defined security levels and enables the sharing of assessment results on a specialized platform. [33] [34] [35]

Table 1 Key Terms [own elaboration]

Key terms		
ENX	European Network Exchange Association	Association of European vehicle manufacturers, suppliers and automotive organizations
TISAX®	Trusted Information Security Assessment eXchange	A standard for trusted information security assessment in the automotive industry, based on the requirements of the VDA ISA
VDA	Verband der Automobilindustrie	German Automotive Industry Association
VDA ISA	VDA Information Security Assessment	A defined set of requirements for information and physical security solutions based on ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 2717 in the area of information security

2.5.1 Origin and Meaning of TISAX

Standards created independently of a specific industry are generally conceived as a universal solution and are therefore not adapted to the specific needs of, for example, automotive companies. The automotive industry has created associations whose aim was, among other things, to improve and define standards corresponding to its specific needs. One of these associations is the "Verband der Automobilindustrie" (VDA). Within the information security working group, members of the automotive industry concluded that they share similar needs and that it is appropriate to modify existing information security management standards to better reflect the specific conditions of the automotive environment. [36]

The joint efforts of members of the automotive industry led to the creation of a questionnaire that contains the widely recognized information security requirements of the automotive industry. This process is referred to as Information Security Assessment (ISA). While some companies use the ISA only for internal purposes, others use it to assess the level of information security management of their suppliers. It can be used in a business relationship, for example, only as a self-assessment, or complete audit processes including physical on-site audits are required. [36]

With the growing awareness of the need to manage information security and the widening adoption of ISA as an information security assessment tool, more and more suppliers have encountered similar requirements from various business partners. These partners often applied different standards and had different interpretations, leading to repeated verifications and repeated audits by suppliers.

With the increasing number of requests from partners to demonstrate the level of information security management, complaints from suppliers about constant requirements to demonstrate compliance with security standards have also increased. Manually filling in extensive tables and time-consuming teleconferences during repeated evaluations caused a significant burden on employees.

To increase the efficiency of this process, it was suggested that reports and audit findings could be shared between different partners. Along these lines, OEMs (Original Equipment Manufacturers) and members of the ENX working group, responsible for maintaining ISA, listened to their suppliers’ complaints and proposed a new approach called TISAX. [33]

2.5.2 Structure and Requirements of TISAX Certification

Every company that would like to demonstrate compliance with TISAX must follow the specific steps in process to achieve it. The TISAX process usually begins with one of the partners requesting that the other partner demonstrate a defined level of information security management according to the ISA standards. [36]

Content of following subchapters will be described in more detail in the practical part of the thesis.

2.5.2.1 Levels of Assessment

TISAX certification consists of three assessment levels: Level 1, Level 2, and Level 3, corresponding to different levels of protection - from normal to high or very high. Level 1 involves a self-assessment using a questionnaire, while Level 2 and Level 3 require involvement from an external auditor. Level 3 also includes an on-site visit by the auditor. [36]

2.5.2.2 Implementation Process

Simplified, the process of implementing TISAX includes three main steps that company should fulfill (figure 8). [36]

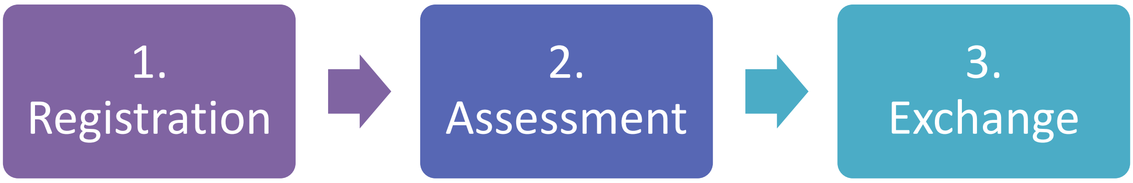


Figure 8 TISAX Implementation Process [own elaboration]

In a first step organization must register on the TISAX portal to initiate the assessment process and understand the requirements. [36]

The second step includes completing a self-assessment questionnaire, regardless of the chosen assessment level and subsequently audit performed by the auditor in case of Level 2 or 3. [36]

Final phase involves exchanging results with confirmation that an organization’s information security system complies with the security requirements outlined in TISAX VDA ISA questionnaire. [36]

2.6 Supply Chain

TISAX plays a very important role in contributing to information security within the supply chain in automotive industry. It enables mutual acceptance of information security assessments in the automotive industry, ensuring the secure sharing of sensitive information among partner companies. In the context of the supply chain, TISAX certification is essential for all organizations doing business with major players in the German automotive industry. It is a globally recognized standard that applies to automotive suppliers and service providers processing sensitive information.

Important components within the TISAX and automotive supply chain are NDAs and SLAs, which are described in following subchapters.

2.6.1 NDA

An NDA, or Non-Disclosure Agreement, is a basic contractual tool used to protect sensitive information during business relationships. This agreement specifies the information that the parties wish to keep confidential, and binds the parties involved to keep certain sensitive information confidential for a specified period of time. In the context of TISAX and supply chains in the IT and automotive industries, the NDA plays a key role in mentioning confidential information related to technology, security measures and business practices, which helps prevent the leakage of critical data and ensures compliance with relevant security standards. [20] [37]

2.6.2 SLA

An SLA defines the contractual relationship between an IT service provider and an IT service purchaser, specifying the scope, level and quality of services to be provided. It includes clauses on time availability, price, speed of problem resolution and other aspects of service. As part of TISAX and supply chain management, the SLA ensures that all components and services delivered meet specified security standards and are delivered in accordance with quality and timeliness requirements, which is essential to maintaining the integrity and security of information systems in vehicles and the wider automotive industry. [20] [37]

2.6.3 Supply Chain Attack

Supply chain attacks pose a serious threat to the security and integrity of enterprise information systems, especially in highly regulated industries such as the automotive industry. These attacks are insidious in that they exploit the trust between companies and their suppliers and can lead to a wide range of security incidents, from the leakage of sensitive information to the complete paralysis of production processes. [38]

2.6.3.1 Example of a Major Attack

In March 2022, the automotive manufacturer Toyota experienced a major disruption to its production in Japan following a cyberattack on one of its suppliers, Kojima Industries, which led to the shutdown of 28 production lines and a production outage of approximately 13 000 vehicles. [38]

2.6.3.2 Risks of Inadequate Protection

Attacks on the supply chain can have drastic consequences not only for the primarily attacked organization, but also for the entire network of connected entities. Vulnerabilities in one link in the supply chain can be exploited to attack others, often with devastating results. [38]

2.7 ROSI (Return on Security Investment) model

The Return on Security Investment (ROSI) model is a financial metric used to estimate the effectiveness and value of security investments by comparing the cost of these investments to the financial benefits derived from avoiding security incidents. ROSI is especially relevant in the context of information security, where it helps organizations justify and optimize their spending on security measures. [20]

TISAX (Trusted Information Security Assessment Exchange) provides a standardized approach to information security tailored to the automotive industry, yet the economic implications of its adoption are not immediately apparent.

2.7.1 Costs

TISAX is site-oriented and the prices of the individual components of the implementation costs vary considerably as the number of sites increases. This thesis deals with only one site, so will focus on costs for one site.

2.7.1.1 Direct Costs

This section discusses costs of preparing for TISAX assessment such as consultancy fees, staff training and internal audit. Also, it is not forgotten the cost of the certification process itself and any necessary follow-up audits.

a) **Assessment Fee:** This is a fee paid to accredited TISAX assessment providers for conducting the formal evaluation of your IT and data security practices.

b) **Consultancy Fees:** Organizations can hire external consultants to help prepare for the TISAX assessment. These consultants offer expertise in aligning the organization's practices with the required standards, which includes gap analysis, implementation guidance, and preparation for the assessment.

c) **Training Costs:** Employee training is crucial for compliance with TISAX standards. This may include training on data protection, secure data handling and understanding cybersecurity risks.

d) **Security Software and Tools:** Investments in security software, such as antivirus programs, firewalls and other cybersecurity technologies, are often necessary to meet the strict security requirements set by TISAX.

e) **Hardware Upgrades:** Implementing TISAX standards might require upgrading existing hardware or purchasing new hardware to support advanced security measures. This could include secure servers, enhanced network equipment, or specialized devices for monitoring and controlling access.

f) **Documentation and Policy Development:** Developing, updating, and maintaining documentation such as security policies, incident response plans, and compliance reports can involve significant effort.

g) **Audit and Compliance Management Costs:** Costs associated with internal audits, compliance management systems, and ongoing monitoring of compliance status are critical to ensure that the organization remains within the required standards over time.

2.7.1.2 Indirect Costs

Indirect costs include, for example time spent by internal staff in preparing and maintaining TISAX standards or possible operational disruptions during the implementation of necessary security measures.

a) **Employee Time and Productivity Loss:** Significant amounts of employee time may be required for activities related to achieving and maintaining TISAX compliance. This includes time spent in training, participating in audits, and adjusting to new security processes. The productivity loss during these activities, especially if it diverts staff from their regular duties, can be a substantial indirect cost.

b) **Opportunity Costs:** Focusing resources, including management attention and financial capital, on TISAX compliance can mean these resources are not available for other potentially profitable projects. This diversion can lead to missed opportunities elsewhere in the organization.

c) **Maintenance of Security Systems:** Beyond the initial purchase and installation of security software and hardware, ongoing maintenance and updates are required to ensure these systems continue to meet TISAX standards. While part of these costs can be considered direct, the associated time and effort to manage these updates contribute to indirect costs.

d) **Long-Term Monitoring and Compliance**: Continuous monitoring to ensure compliance with TISAX standards involves indirect costs related to the time and tools needed for ongoing evaluation and reporting. This continuous oversight is crucial but can draw resources away from other areas.

2.7.2 Benefits

2.7.2.1 Avoided Costs

In avoided costs are included estimated potential financial impact of security breaches, that TISAX certification helps to prevent. All these following points can be covered in SLE (Single Loss Expectancy) while calculating the ROSI model result.

a) **Reducing the Incidence of Loss of Confidential Information:** This means the loss or misuse of sensitive data such as production plans, vehicle designs, customer information and other confidential company information, which could lead to direct financial losses and loss of competitive advantage. TISAX compliance improves an organization's security controls and significantly reduces the risk of data breaches. Costs avoided here include legal fees, fines, remediation costs and compensation payments that would otherwise be incurred in the event of a breach.

b) **Avoiding of Regulatory Penalties:** By adhering to the strict security standards required by TISAX, an organization can avoid penalties associated with non-compliance with industry regulations, such as GDPR for data protection within the EU.

c) **Reduced Risk of Shutdown:** Increased security measures can minimize the risk of security incidents that cause production or business interruptions. Avoiding these incidents means less shutdown, which in turn avoids costs associated with lost productivity, revenue, orders or expenses for missed delivery deadlines.

d) **Avoiding Loss of Customer:** Avoiding the loss of customers is crucial for maintaining the financial stability and growth potential of a business. In the context of information security and compliance, such as with TISAX in the automotive industry, maintaining robust security measures can significantly reduce the risk of losing customers due to breaches that may damage trust and reputation. In context of this thesis, the TISAX certification was retrieved from the side of customer.

e) **Reduced incident management costs:** Better preparedness to deal with security incidents - a by-product of obtaining TISAX certification - can lead to reduced incident management costs. This may include the cost of data recovery, reinforcement of security measures, and the potential cost of training staff to better understand security threats and how to counter them.

f) **Avoiding Customer Audits:** Elimination of the probability of audits need from the customer’s or company’s side. This saves time and money by eliminating the need to complete extensive documentation in the form of Excel files or doing audit at supplier.

2.7.2.2 Operational Benefits

By benefits may be considered gaining business opportunities by being compliant with industry security standards required by potential automotive partners and suppliers or improved security posture leading to enhanced trust from clients and partners.

a) **Enhanced Market Access:** TISAX certification is often a prerequisite for doing business within the automotive industry, particularly in Europe where it is recognized by major automotive manufacturers and suppliers. Certification can therefore open doors to new business opportunities and markets.

b) **Improved Customer Trust and Satisfaction:** By demonstrating compliance with recognized security standards, an organization can enhance its reputation, thereby attracting or retaining customers who cling about data security.

c) **Increased Employee Awareness and Engagement:** The training associated with TISAX compliance increase cybersecurity awareness among employees, which can lead to better compliance with security policies and procedures across the board.

d) **Long-term Cost Savings:** Although the initial setup for TISAX certification involves some investment, the long-term benefits include continuous improvement of security practices, which can reduce costs over time associated with less efficient or outdated security measures.

2.7.3 Evaluation

The ROSI can be calculated using the following formula (2.1.2). [20]

$$ROSI = \left(\frac{Monetary\ Loss\ Reduction - Cost\ of\ Investment}{Cost\ of\ Investment}\right) \qquad (2.2.2)$$

where:

MLR (Monetary Loss Reduction)

The MLR represents the monetary loss reduction, which expresses how much the potential losses can be reduced due to the implemented safety measures. MLR is calculated as:

$$MLR = ALE \times MR \qquad (2.3)$$

where MR (Mitigation Ratio) is a reduction ratio that expresses the effectiveness of safety measures in percentage. [20]

SLE (Single Loss Expectancy)

The SLE represents the single loss expectancy and is the result of an estimate of the potential financial loss in the event of a security incident. It is calculated as:

$$SLE = asset\ value \times exposure\ factor \qquad (2.4)$$

The exposure factor is a percentage of the extent of the loss of an asset in the event of an incident. [20]

ARO (Annual Rate of Occurrence)

ARO is the annual occurrence rate, which indicates the probability with which a security incident can happen in a year. [20]

ALE (Annual Loss Expectancy)

ALE is the annual loss expectancy, which is calculated by multiplying SLE and ARO:

$$ALE = SLE \times ARO \tag{2.5}$$

This value represents the expected annual financial loss due to security incidents. [20]

3 CURRENT STATE ANALYSIS

This section essentially serves as a foundation for understanding the context in which TISAX certification is being implemented. It helps to comprehend the unique characteristics and challenges faced by the organization, providing a baseline for assessing the impact of TISAX implementation.

3.1 Characteristics of the Researched Organization

In order to grasp the meaning of the TISAX certification implementation discussed in this thesis, it is needed to describe the fundamental aspects of the organization. This includes gaining insights into its organizational structure, industry-specific standards, and its current operational landscape.

3.1.1 Identification of the Organization

The company is a development partner for European commercial vehicle manufacturers and their leading supplier, occupying a leading position in individual sectors.

The company is divided into three business units, with different product ranges:

- Business unit focused on production of pressure vessels
- Business unit focused on metal components for the automotive and utility industry
- Business unit focused on connecting rods and camshafts for passenger cars

The first business unit is focused primarily on the production of pressure vessels, which are an important element of the brake system of commercial vehicles. Compressed air that opens and closes the brakes is stored in these containers.

This unit has two production plants located in Germany and in the Czech Republic. With a market share exceeding 80%, the production plants are among the largest manufacturers of pressure vessels (air tanks) in Europe. They produce about 1000 different types of air tanks, either from steel, aluminum or stainless steel.

3.1.2 Customers

Commercial Vehicle Manufacturers: Volvo, Renault, MAN, Scania, Tatra, Iveco.

Manufacturers of Cargo Trailers: Schwarzmüller, Wielton, Schmitz, Fliegl.

Manufacturers of Brake Systems: Haldex, Knorr-Bremse, WABCO.

3.1.3 Specifics of the Industry and Production Process

The company is fulfilling the requirements outlined in the IATF 16949 standard, that is an addition of standard ISO 9001 for quality management systems within the automotive sector. The aim of this standard is to create a quality management system that will continuously improve, emphasizing defect prevention and reducing variability and losses in the supply chain.

Air tanks undergo a meticulous design, manufacturing, and assessment process in accordance with Czech legislation, specifically Law No. 90/2016 Coll., about conformity assessment of designated products for market placement, and Government Regulation No. 119/2016 Coll., on conformity assessment of simple pressure vessels when they are placed on the market. The company's production portfolio is characterized by two primary types of air tanks: simple pressure vessels and stable pressure equipment, each governed by distinct directives.

3.2 Description of the Current State in Company

This section provides an overview of company's prevailing operations and processes, focusing on its esteemed role in air tank production. While respecting the confidentiality of sensitive information, this segment encapsulates the following key aspects:

3.2.1 Market Position and Customer Relationships

Company holds a distinguished market position as a premier provider of pressure vessels within the European commercial vehicle industry. With a steadfast commitment to quality and innovation, the company has cultivated enduring relationships with key customers, including renowned European commercial vehicle manufacturers and suppliers. These relationships underscore company's role in the supply chain and its commitment to meeting the evolving needs of its clients.

3.2.2 Production Facilities Overview

The facilities' capacities and capabilities are customized to meet the various demands of the commercial vehicle industry, facilitating the production of a broad spectrum of air tank variants. This strategic infrastructure enables to uphold its reputation as a leading manufacturer in Europe's automotive landscape.

3.2.3 Quality Control Measures and Adherence to Standards

The company follows consistently to industry-leading standards, including the IATF (International Automotive Task Force) certification. For this company IATF certification means proactive stance in ensuring operational proficiency and product quality. Quality control measures are integrated into the production workflow, ensuring that each air tank meets challenging standards of performance, durability, and safety.

The organization also has an integrated management system (IMS) in place, which includes IATF 16949, ISO 14001, ISO/IEC 27001 and ISO 45001. The organization also meets many technical and product standards such as SAE J10, AD 2000, ČSN EN 286-1 and ČSN EN 286-2.

The company is dedicated to continual improvement and elevating product quality. However, amidst its commitment to progress, company faces the needs to align with evolving industry standards and customer requirements. As a certified IATF-compliant entity, the company's customers need follow also TISAX (Trusted Information Security Assessment Exchange) certification—a testament to the growing emphasis on information security within the automotive supply chain.

3.2.4 ISMS Principle

Operating in alignment with the Deming cycle principle, ISMS in this company follows the PDCA (Plan-Do-Check-Act) methodology. This system integrates standards such as TISAX and ISO, forming a unified structure wherein TISAX aligns with ISO, and ISO embodies the PDCA cycle. Following is described the PDCA cycle within ISMS in more detail.

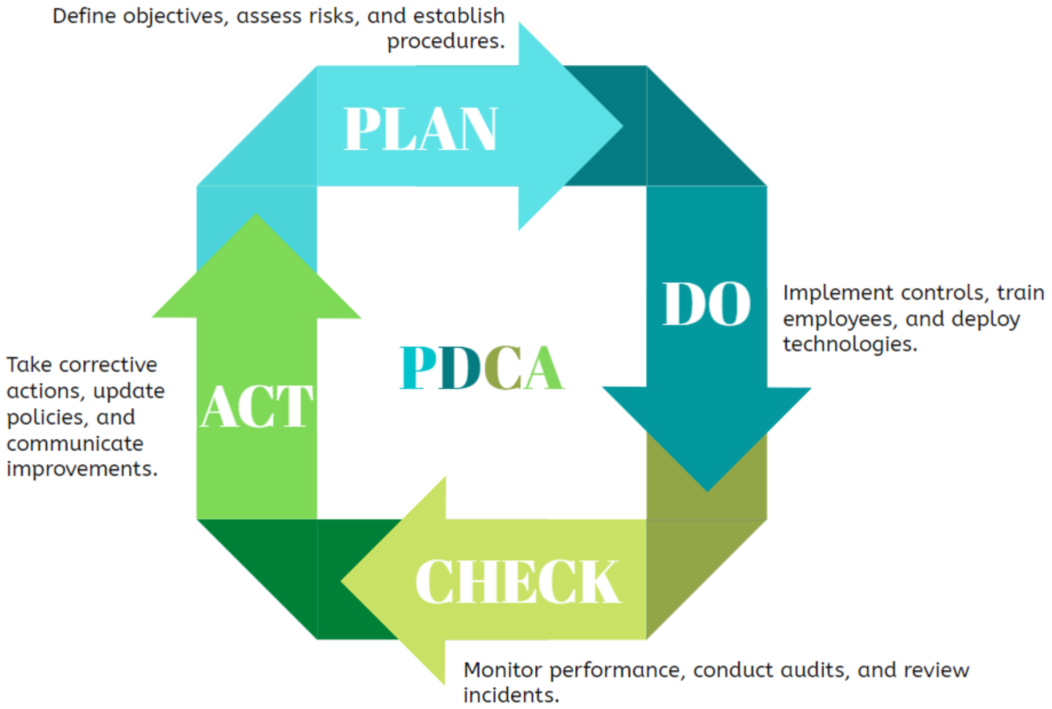

Define objectives, assess risks, and establish procedures.
PLAN
DO
Implement controls, train employees, and deploy technologies.
PDCA
Take corrective actions, update policies, and communicate improvements.
ACT
CHECK
Monitor performance, conduct audits, and review incidents.

Figure 9 PDCA - ISMS Principle [own elaboration]

Plan

The first step includes defining the scope, objectives, and policies. Next, it is essential to identify the relevant legal, regulatory, and contractual requirements. Conducting a risk assessment and establishing risk treatment plans follow this step. Developing procedures for incident management, business continuity, and compliance, and assigning roles, responsibilities, and accountability are also crucial in this phase.

Do

The implementation phase involves putting ISMS policies, procedures, and controls into action. This includes providing training and awareness programs for employees and deploying security technologies and tools to protect information assets. Company also conducts testing and exercises to evaluate security controls and incident response procedures, while documenting all implementation activities for future audits.

Check

To ensure the effectiveness of the ISMS, monitoring KPIs and metrics is essential. Internal audits and assessments are conducted to ensure compliance, and security incidents and vulnerabilities are reviewed to identify areas for improvement. Evaluating the effectiveness of risk management processes and soliciting feedback from stakeholders further contributes to continuous improvement.

Act

In final phase is company taking corrective and preventive actions to address non-conformities and vulnerabilities. Based on lessons learned, ISMS policies, procedures, and controls are updated. Communicating these changes and improvements to stakeholders and allocating the necessary resources for implementation are the concluding steps in maintaining an ISMS certification.

3.2.5 Risk Management

In relation to Information Security Management Systems (ISMS) risk management involves identifying, analyzing, and evaluating risks that impact the confidentiality, integrity, and availability of information assets. Process of risk analysis is a key component of ISMS and is required by standards like ISO 27001.

Organization has established and is maintaining information security risk management that includes risk acceptance and assessment criteria, ensuring assessments are consistent and valid.

Risk analysis in this company includes assigning risks to owners, determining risk levels, assessing potential consequences, and evaluating the likelihood of risks occurring. Once risks are evaluated, they must be managed according to a documented risk management plan.

In company is defined process of managing risks according to the following (figure 10):

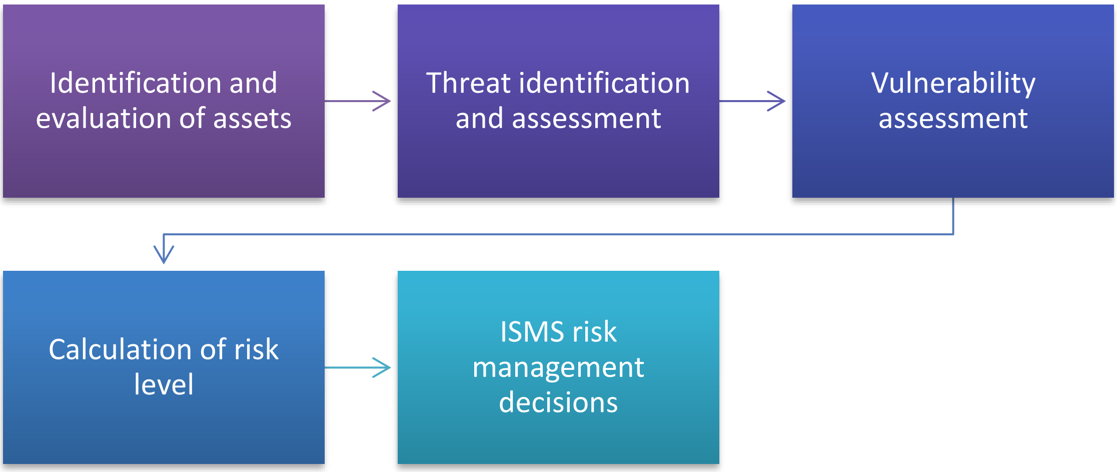

Identification and evaluation of assets
Threat identification and assessment
Vulnerability assessment
Calculation of risk level
ISMS risk management decisions

Figure 10 Risk Management Process [own elaboration]

3.2.5.1 Asset Management

Assets are both intangible and tangible, have value to the company and are therefore required to be protected. This is especially true in the combination of asset and information security. Assets are identified and described through Excel sheet tagged and named according to company’s standard. Assets are subsequently transcribed into the ISMS risk scorecard, rated and further managed.

3.2.5.2 Risk Acceptance Criteria

This chapter focuses on the risk acceptability criteria, which allows an organization to determine what risk is still acceptable and when action is needed. To simplify the decision-making process, a risk assessment table is presented that categorizes the different types of risk according to their calculated value.

The table (table 2) contains the following:

- **Risk level** identifies the likelihood of the risk occurring and its normal frequency.
- **Risk value** in numerical scale.
- **Risk impact** provides an overview of the potential consequences for the organization if the risk occurs.
- **Response** suggests strategies for mitigating or eliminating the risk.

Table 2 Risk Acceptance Criteria [own elaboration]

Risk level	Risk value	Risk level	Impact of risk	Response
I.	**91-125**	Unacceptable risk	Existential hardship to liquidation	Immediate response, elimination within 3 months
II.	**71-90**	Adverse risk	Serious inconvenience, significant financial loss	Resolution within 6 months, increased monitoring
III.	**51-70**	Moderate risk	Difficulty and financial loss	Resolution within 1 month, monitoring
IV.	**31-50**	Acceptable risk	Negligible impact, possible escalation	Included in monitoring and control system
V.	**25-30**	Negligible risk	Negligible impact	Under review as part of risk assessment
VI.	**0-24**	No significant risk	Will not happen	Under review as part of the risk assessment

3.2.5.3 Risk Assessment Criteria

This chapter focuses on the risk assessment criteria that are essential for identifying and classifying risks according to their impact on key aspects.

Asset Assessment

Asset assessment is a key process that enables an organization to fully understand the value of its underlying assets.

The table (table 3) categorizes these criteria:

- Confidentiality - highlights the potential loss of information confidentiality.
- Availability - highlights the ability to access information resources that are necessary for normal operational operations.
- Integrity - includes preserving the accuracy and completeness of data and information systems.

Table 3 Risk Assessment Criteria [own elaboration]

Value	Confidentiality	Availability	Integrity
1	Public	Unimportant	Irrelevant
2	Non-public	Occurrence of insignificant problems	Of little significance
3	Controlled access	Important – problems	Emergence of asset problems
4	Uncontrolled access	Important – emergence of problems	Disposal of asset
5	Confidential	Indispensable	Impairment of asset

The value of asset is calculated as following formula (3.1).

$$\text{Asset} = \frac{(\text{Confidentiality} + \text{Availability} + \text{Integrity})}{3} \qquad (3.1)$$

Threat Likelihood and Vulnerability Level

In this subchapter is described how company identify and categorize potential threats and vulnerabilities that could negatively impact its operations. This chapter focuses on the criteria for risk identification and presents a structured approach to assessing risks using a table (table 4), which includes:

- Value - reflects the significance of the risk to the organization in the context of potential loss or damage.
- Likelihood of the threat occurring - provides an estimate of how often the risk may be realized.
- Vulnerability level - assesses the level of susceptibility of systems or processes to the identified threats.

Table 4 Threat Criteria [own elaboration]

Value	"T" The likelihood of the threat occurring	"V" Vulnerability level
1	Less than annually	Negligible
2	Annually	Minor limitation
3	Monthly	Functional limitation
4	Weekly	Disable
5	Daily	Destruction

Risk Identification

Risk identification is an essential step in the risk management process that enables organizations to identify, analyze, and assess potential threats to their operations and assets. Here is a methodology for calculating the level of risk, where the key element is the following formula (3.1):

$$\textbf{R}\text{isk measure} = \textbf{A}\text{sset value x }\textbf{T}\text{hreat probability x }\textbf{V}\text{ulnerability measure} \qquad (3.2)$$

3.2.5.4 Risk Analysis

The organization's risk analysis process is based on reports that are the output of the identified risk assessment and, among other things, identify following.

Risk Distribution by Level of Risk Acceptance

Based on this report, the ISMS team prepares a set of measures to reduce or eliminate risks, which is presented to the company's management. Based on these, the latter will take the necessary measures to ensure information security.

Relation of Assets to the Size of the Identified Risk and the Level of Acceptance

Based on this input, recommendations are made for the management of assets in terms of their performance, protection, maintenance and monitoring system.

Comparison of the Effectiveness of the Measures Taken from the Previous Risk Assessment

Comparing the level of identified risks with previous assessments shows the effectiveness and efficiency of the measures taken and implemented. This information is important for assessing the technique of taking and implementing measures and their economic return. Another area where the findings can be implemented is the company's training and education system.

Analysis as an Input for Decision-Making by the Management of Company

The outputs and analyses following the risk assessment are used as important inputs for the decision-making of the management in the areas of building infrastructure and process management that will respect the requirements for information security and data protection.

Technical Support for Risk Analysis in Excel

The risk analysis is performed in an application processed in the MS Excel product environment, using the Excel table. The quality of the outputs is directly proportional to the quality of the assessments conducted and data captured.

3.2.5.5 System of Measures and Risk Treatment

Risk management is addressed by a whole system of measures at the level of corrective actions, preventive actions, tasks or projects.

The basic approach for risk management is following.

1) Risk mitigation - this is about reducing the possibility of risks or eliminating their impact, taking action, etc. Risk reduction measures and their action is a planned process that is documented in Risk Management Plan.
2) Conscious acceptance of the risk - the risk does not have a fatal impact if it occurs and acts, its elimination would be costly or difficult to achieve.
3) Avoidance of risk - the area of risk is removed from processes, processes are designed differently, external services are used that are not risky, etc.
4) Risk transfer (sharing) - e.g. agreement with a customer, insurance of risk damage, etc.

3.2.5.6 Risk Implementation System and Mitigation Measures

The risk implementation system and measures resulting from the identified risks ensure that risks are addressed used by following:

Corrective Actions

This is a managed process that follows the PDCA principle. A detailed description, including controlled records, is provided in internal standard Nonconformance Management and Corrective Action.

Preventive Actions

Preventive Actions follow a similar process to Corrective Actions. However, they are used to address unwanted conditions before they occur. They can be initiated by customer requests and alerts, identification of new threats in the digital space, changes in legislation, etc.

Tasks

Tasks are mainly used for partial solutions within Corrective Actions or in case of smaller required solutions that can be implemented in a short time.

Projects and Planned Actions

Projects are long-term activities that lead to large-scale changes in the company's processes and infrastructure in use. The planning of projects and actions is documented through Risk Management Plan.

3.2.5.7 Declaration of Applicability

The applicability statement is the output of an assessment of the risks and the scope of existing and future measures to address them.

The applicability statement is a controlled document that defines, whether the area is implemented and what measures are used to make the ISMS area beneficial for information risk management. The aim is to ensure continuity with the requirements of ISO 27001 and Annex "A".

3.2.5.8 Risk Management Plan

The Risk Management Plan is maintained through the document ISMS Objectives, the CA Book, the ISMS Project records, the Incident and Resolution records and the Risk Management Plan record.

3.2.5.9 Agreement of Process Owners to Identified Risks

When measures to address identified risks are defined and agreed, the personnel involved are invited to participate in the definition of the measures at the time the measures are developed. The process owners usually become the responsible person for the implementation of the measures.

3.2.5.10 Acceptance of Residual Risks

Residual risks, i.e., risk level V and VI, or risks that management has decided not to address, are identified and a banded document is made of their acceptance under Management Review of ISMS. While these risks are not addressed by an active measure or project, they must be recorded, reassessed in subsequent risk assessments, and reviewed within ISMS to provide assurance that these risks are not becoming more significant risks.

3.2.5.11 Documented Risk Management Information

The documentation of information (documented information) is addressed according to the rules set out within the ISMS. Where specified, documented and controlled records must be maintained.

3.2.5.12 Evaluation Example

For an example will be presented the evaluation process of one selected asset of the company.

Asset: MES (Manufacturing Execution System)

Table 5 Asset Assessment [own elaboration]

Evaluation aspect	Value
Confidentiality	4
Integrity	4
Availability	4
Weight of asset	4

Threat: theft of data/information/records

Table 6 Threat Assessment [own elaboration]

Evaluation aspect	Result
Threat group	unauthorized activity
The likelihood of threat	2

Vulnerability

Table 7 Vulnerability Assessment [own elaboration]

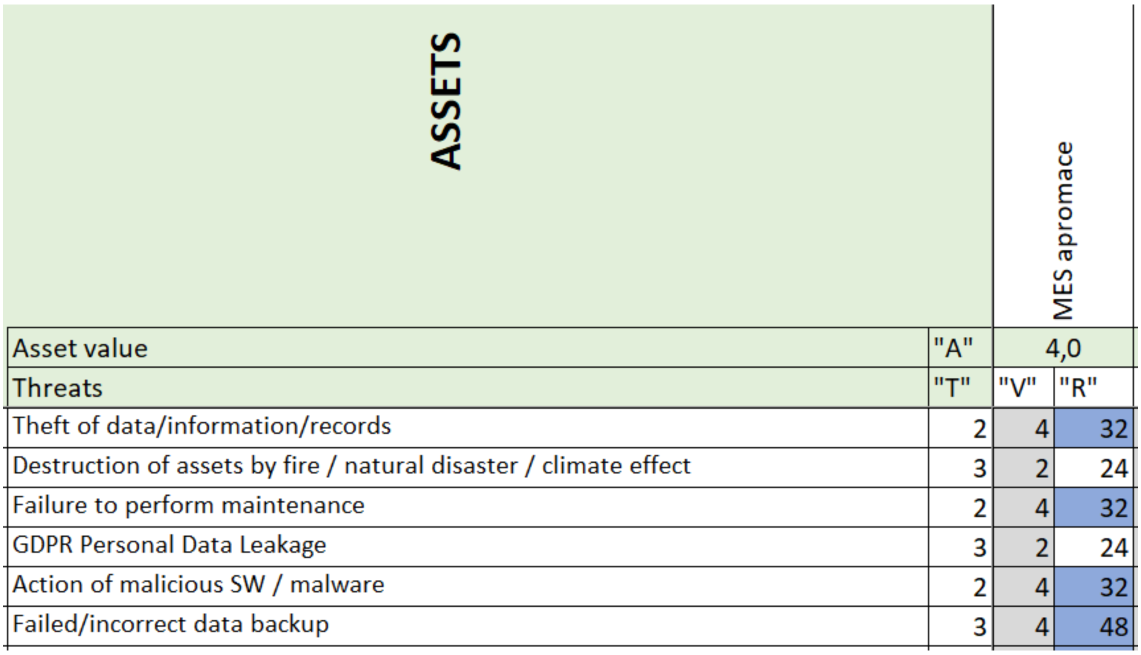
Evaluation aspect	Result
Vulnerability group	disable
Vulnerability value	4

Value of the risk

$$R = asset\ x\ threat\ x\ vulnerability = 4x2x4 = 32 \qquad (3.3)$$

The result of risk value is 32, which means acceptable risk with negligible impact and possibility of escalation.

The figure below (figure 11) shows a matrix from Excel sheet which company uses, where the MES asset is also evaluated for other threats such as failure of maintenance or data backup. In the assets line, all the remaining assets of the company are then listed and subsequently evaluated.



ASSETS		MES apromace	
Asset value	"A"	4,0	
Threats	"T"	"V"	"R"
Theft of data/information/records	2	4	32
Destruction of assets by fire / natural disaster / climate effect	3	2	24
Failure to perform maintenance	2	4	32
GDPR Personal Data Leakage	3	2	24
Action of malicious SW / malware	2	4	32
Failed/incorrect data backup	3	4	48

Figure 11 Risk Matrix - Asset Evaluation [internal]

4 IMPLEMENTATION OF TISAX

The TISAX process typically starts with request of customer or partner of the company that it should provide a defined level of information security management according to the requirements of the "Information Security Assessment" (ISA).

As was said, the process of implementing TISAX includes three main steps that company should fulfill. Nevertheless, this chapter discusses in more detail the entire process of implementing TISAX which takes more than these three main steps – as shown in picture (figure 12).

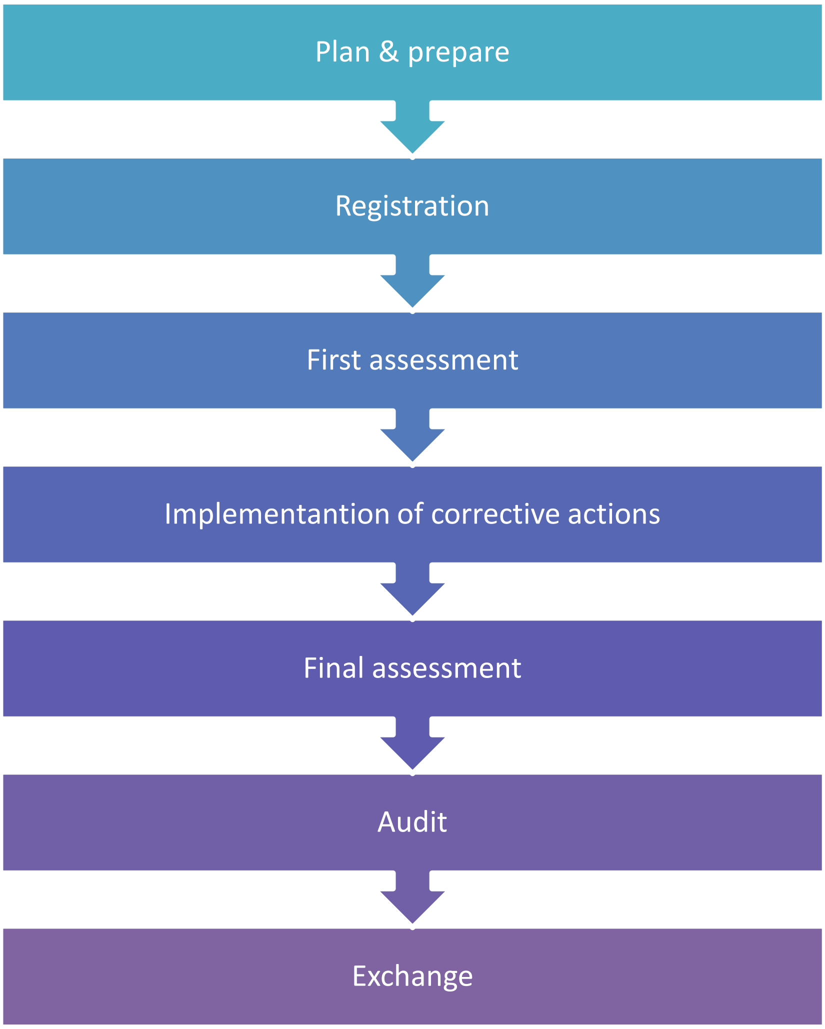


Figure 12 TISAX Implementation Process Steps [own elaboration]

4.1 Planning and Preparation for Certification

The first step in process of TISAX implementation involves thoroughly understanding the TISAX requirements and criteria. This includes reviewing the TISAX standard, understanding the scope of certification, and identifying applicable security requirements.

At this very first step should organization consider the need of contacting external company (as organization concerned in this thesis did), which provides complete guidance in process of TISAX implementation. This may help to speed up the process if it's really needed.

The other steps that should be taken are considering signing contracts with organization's TISAX audit provider and with ENX Association which covers mutual relationships between organizations and customers and defines the rights and duties for both sides. These are needed for next process step – registration.

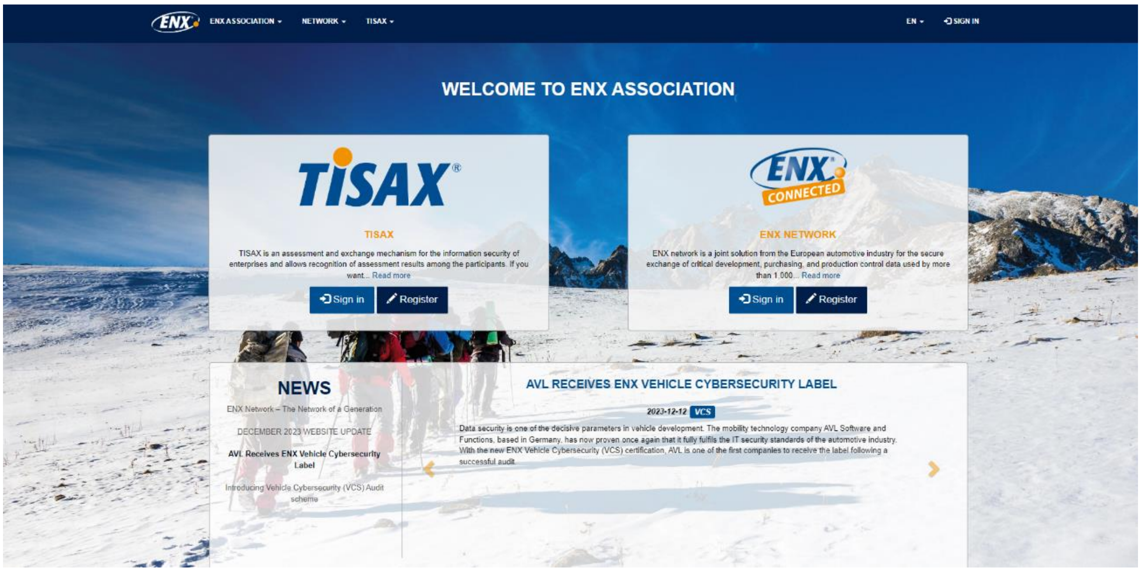
4.2 Registration

After familiarizing the process and requirements of the TISAX, company needs to initiate the registration process on the official TISAX website enx.com. There company provides essential details of organization and documentation required for registration, including company information, contact details, industry affiliations and mainly assessment level (AL).

On the main website can be found two possibilities for registration (picture below). The first one serves for registration to a TISAX exchange process and the second is network for the secure exchange of critical development, purchasing and production control data. It is recommended to do whole process (from basic registration to assessment scope) at one time. The company becomes a participant after registration. Information needed for registration are:

- name of the company, including DUNS number,
- the exact name of the location that will be mentioned in TISAX scope,
- email address,
- assessment level (AL),

- account number from which will be paid the ENX fee.



WELCOME TO ENX ASSOCIATION

TISAX

TISAX is an assessment and exchange mechanism for the information security of enterprises and allows recognition of assessment results among the participants. If you want... Read more

ENX NETWORK

ENX network is a joint solution from the European automotive industry for the secure exchange of critical development, purchasing, and production control data used by more than 1.000... Read more

NEWS

ENX Network – The Network of a Generation

DECEMBER 2023 WEBSITE UPDATE

AVL Receives ENX Vehicle Cybersecurity Label

Introducing Vehicle Cybersecurity (VCS) Audit scheme

AVL RECEIVES ENX VEHICLE CYBERSECURITY LABEL

2023-12-12

Data security is one of the decisive parameters in vehicle development. The mobility technology company AVL Software and Functions, based in Germany, has now proven once again that it fully fulfils the IT security standards of the automotive industry. With the new ENX Vehicle Cybersecurity (VCS) certification, AVL is one of the first companies to receive the label following a successful audit.

Figure 13 ENX Portal [33]

4.2.1 Location

Next task is defining location. If company operates on a smaller scale (one location), the task is relatively simple - adding location to the rating range. If company is larger, it may be considered including more than one location in the evaluation.

Here are several advantages of a single location:

- One evaluation report, one result and one expiration date.
- Evaluation costs can be reduced because the TISAX audit provider only must assess central processes, procedures and resources once.

More locations included may have these pitfalls:

- All locations must have the same assessment objectives.
- The results of the assessment will only be available after the TISAX audit provider has assessed all locations. This may be a problem if the assessment results are needed urgently.
- The outcome of the assessment depends on all sites undergoing the assessment, that means if one location fails, the assessment result will not be positive.

When filling in the site description (scope location), it is needed:

- the name of the location,
- DUNS (Data Universal Numbering System) number,
- location type (for example, leased, owned, shared space or data center),
- total number of employees at the location,
- number of IT staff,
- number of IT security employees,
- number of security employees.

4.2.2 Assessment Scope

A key phase of the first step within TISAX is defining control areas and assigning them to a certain assessment level (Assessment level - AL). It is important to note that the assessment level only describes the way in which the certification audit of organization is conducted, but not the requirements that are placed on the organization. In order to identify the appropriate requirements, it is necessary to determine the assessment objectives, which gives the information about assessment scope.

It is possible to choose one of two following options for description of assessment scope:

1. Standard scope – sufficient for most participants
2. Custom scope – possibility of standard scope extension to include additional activities that are not part of the standard scope (e.g. data center services). However, it is possible that in this case the assessment will take place without achieving the TISAX label, i.e. verifying that you meet the TISAX requirements. Also, there are next two possible ways of custom scope:
    a. Custom extended scope
    b. Full custom scope

The table below gives the specifications of each level, with three levels - AL1 to AL3. It is always recommended to consult the appropriate assessment level with the partner. The partner's purchasing or sales department is usually the authority for the correct choice.

Table 8 Assessment Level Specifics [own elaboration]

Assessment method	AL 1	AL 2	AL 3
Self-assessment	Yes	Yes	Yes
Evidence	No	Plausibility check	Thorough verification
On-site inspection	No	At your request	Yes
Interviews	No	At your request	Yes

4.2.2.1 AL 1

Level AL1 is intended for internal self-assessment only. In this level an auditor checks only for the existence of a completed self-assessment, and it is not required to have further evidence. Results of AL 1 have a low trust level, that is why it is not used in TISAX.

4.2.2.2 AL 2

AL2 rating is in place to ensure sufficient protection and availability of information. In this case an auditor checks plausibility on self-assessment by checking the evidence and conducting an interview with the person in charge information security. This may be done by personal or remote meeting.

4.2.2.3 AL 3

In contrast to assessment level 2, level 3 requirements are verified in a real environment. An auditor examines documents and evidence, observe local conditions etc. To illustrate: AL2 may include a screenshot of an antivirus program, while AL3 may include antivirus checks on an active device, including setup, verification, updates, management, etc. In the case of information processing in prototype and pre-series mode, it is necessary to choose a variant at the AL3 level.

The aforementioned assessment objectives map to these criteria catalogues (table 9). Described company has the objective number 1, so its assessment level is AL 2.

Table 9 Mapping Objectives [own elaboration]

No.	Assessment objective	ISA criteria catalogue(s)	Assessment level (AL)
1.	Information with high protection	Information Security	AL 2
2.	Information with very high protection	Information Security	AL 3
3.	Confidential	Information Security	AL 2
4.	Strictly confidential	Information Security	AL 3
5.	High availability	Information Security	AL 2
6.	Very high availability	Information Security	AL 3
7.	Prototype parts and components	Prototype Protection	AL 3
8.	Prototype vehicles	Prototype Protection	AL 3
9.	Test vehicles	Prototype Protection	AL 3
10.	Prototypes during events	Prototype Protection	AL 3
11.	Data protection	Information Security Data Protection	AL 2
12.	Special data protection	Information Security Data Protection	AL 3

4.3 GAP Analysis as First Assessment

The purpose of analysis is to consider the organization's current information security practices against the TISAX requirements. This helps identify areas where the organization needs to improve to meet the certification standards. The first evaluation and completion of the VDA ISA questionnaire are pivotal milestones in the TISAX certification journey. This chapter delineates the assessment process and the significance of the VDA ISA form in evaluating information security measures.

4.3.1 VDA ISA Form

The VDA ISA questionnaire, used to assess information security according to TISAX, includes 8 main areas in which questions are asked about different parts of the company’s ISMS. These areas are described in detail in the following sections. The VDA ISA questionnaire contains the requirements of the normative standard ISO/IEC 27001 extended by the requirements of TISAX, but also corresponds to the requirements of the ISO/IEC 27002 standard, which provides recommendations for measures in the implementation of ISMS.

The VDA ISA (Information Security Assessment) has evolved through different versions, each introducing changes and enhancements to the assessment criteria. Evolution process was addressed to changing cybersecurity threats and industry needs. Each version introduces new controls, requirements, and focuses to ensure the protection of sensitive information. Following is a summary of the last versions and their key differences.

4.3.1.1 VDA ISA Version 4

The fourth version of the VDA ISA catalog focused primarily on the "confidentiality" of information within organizations in the automotive industry. This version emphasized protecting sensitive data and trade secrets, with a strong focus on confidentiality as the main security objective.

4.3.1.2 VDA ISA Version 5

Version 5 of the VDA ISA catalog introduced significant changes, including a restructuring of controls according to subject areas and minor adjustments in numbering and assignments. Additional requirements were included, particularly related to prototype protection, and the module "Connection of third parties" was released in this version.

4.3.1.3 VDA ISA Version 6

The latest version, VDA ISA Version 6, is valid as of April 1,2024. Introduces significant changes and innovations to the assessment criteria. A major shift in ISA 6 is the addition of the "Availability" label alongside "Confidentiality" to ensure the availability of IT resources and operational technology, reflecting the increasing importance of uninterrupted production processes and system availability. The new version refers to other standards and frameworks such as ISO/IEC 27001:2022, ISA/IEC 62443-2, NIST Cyber Security Framework, and the BSI Baseline Protection to leverage synergies and enhance information security measures.

Since the company’s TISAX assessment started before first of April, this thesis will deal with the VDA ISA questionnaire Version 5.

The individual chapters of the VDA ISA questionnaire therefore focus on specific areas of the ISMS and ask questions that need to be answered in the assessment, with reference to the relevant regulations or procedures. Each of these responses is rated on a scale of 0 to 5 according to the level of maturity, where 0 means no requirements in place and 5 means full implementation of the requirement.

ISA questionnaire contains 3 main criteria (table 10):

Table 10 VDA ISA Main Criteria [own elaboration]

1.	Information security
2.	Prototype protection
3.	Data protection

Each of these criteria have own excel sheet. In each of these are fields that need to be filled when conducting a self-assessment (table 11):

Table 11 VDA ISA Mandatory Fields Filling [own elaboration]

Form field	Purpose	Mandatory?
Implementation description (Column F)	Briefly description of what was implemented to address this control question in company.	Yes
Reference documentation (Column G)	Which documents prove the implementation.	Yes
Findings/Results (Column H)	Findings where a gap exists between what should be and what is.	No

There are also more optional columns supporting self-assessment:

- Measures/Recommendations (Column R)
- Date of assessment (Column S)
- Date of completion (Column T)
- Responsible department (Column U)
- Contact (Column V)

4.3.2 Model of Maturity Level

Maturity level assessment is performed based on the maturity level model. This model distinguishes 6 basic levels (table 12).

Table 12 Maturity Levels [own elaboration]

Level	Name
0	Incomplete
1	Performed
2	Managed
3	Established
4	Predictable
5	Optimizing

During assessment, the maturity level of the process must be objectively demonstrated. This demonstration takes place through outputs from control processes, statements from process owners and involved workers, or other suitable means.

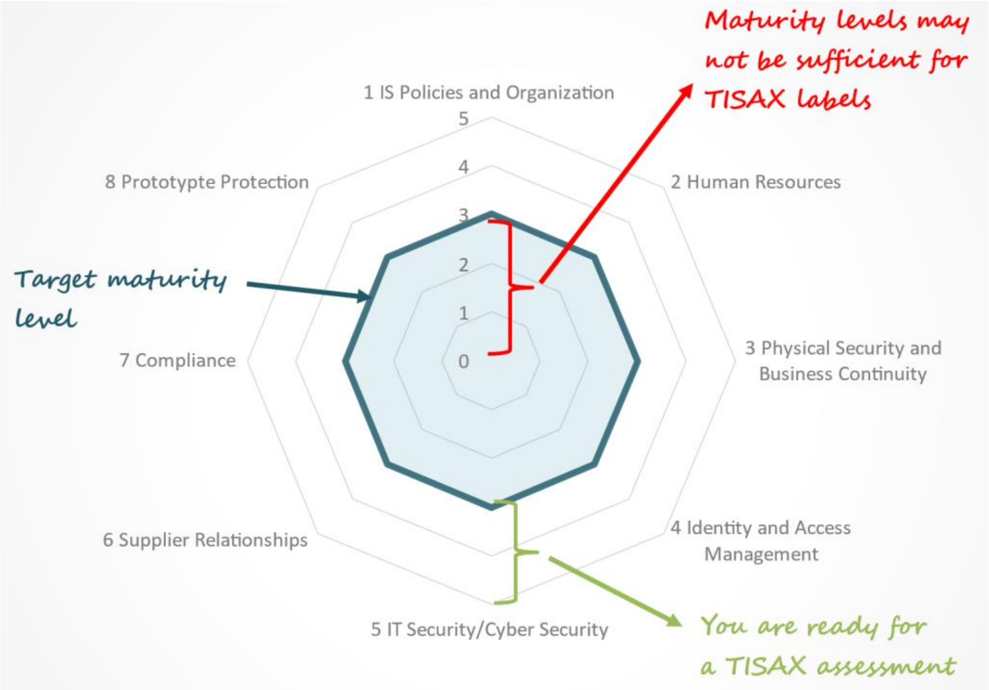


Figure 14 Radar Chart of Maturity Levels [own elaboration]

4.3.2.1 Level 0

Incomplete level means, that the questioned process doesn’t achieve the basic goals or is not at all implemented in the company. In this case of level are documented information about systematical fulfilling of process basic goals vanishing or none.

4.3.2.2 Level 1

Once the process has undergone assessment of performed level, it indicates its existence but may lack sufficient documentation.

4.3.2.3 Level 2

Process documentation and implementation evidence are available. Process performance is planned and followed.

4.3.2.4 Level 3

At maturity level 3 are evaluated routine processes. This level is considered standard within the VDA ISA questionnaire. Overall, at least 60 of the 74 assessed areas are required to reach maturity level three. Especially in the area for handling prototypes, all requirements must be at least at this level of maturity.

At the established level are dependencies documented, and evidence shows sustained use over time. Requirements for this level include:

- defined standard process,
- determined sequence and interaction with other processes,
- identified competencies and roles,
- identified infrastructure and work environment requirements,
- and determined methods for monitoring process effectiveness.

To achieve this level of maturity, it is necessary to have, among other things, described process documentation, a process plan, quality records, rules/policies and standards, as well as processed records of implementation and risk dependencies.

4.3.2.5 Level 4

This level is the maximum required level in VDA ISA questionnaire. Level 4 as a predictable level is described as follows: an established process is followed, monitored for effectiveness, and key performance indicators are defined.

Key activities at this level involve:

- establishing process information requirements,
- deriving process measurement objectives,
- setting quantitative objectives for process performance,
- identifying measurement characteristics and frequency,
- and collecting, analyzing, and reporting measurement results.

As can be seen the difference between level 4 and level 3 is mainly focused on monitoring, reporting and predicting the process behavior.

Furthermore, along with the existing documentation required for the previous maturity level, plans for active process control, measurement, and process improvement are added.

4.3.2.6 Level 5

The highest level of the maturity level is level 5 – optimizing. It makes high demands not only for a process as itself, but also to workers, who perform or manage this process. Process at his level is described as a predictable with continual improvement. Improvement is actively advanced with dedicated resources.

This level includes activities such as:

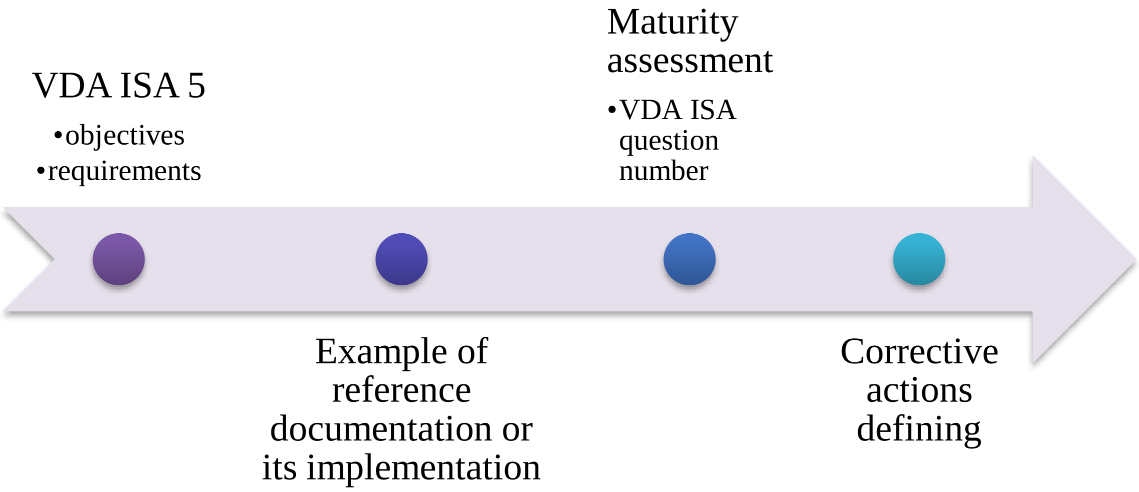
- defining process improvement objectives,
- analyzing data for process performance variations,
- identifying options for best practices and innovation,
- establishing implementation strategies for process improvement objectives,
- and assessing the impact of proposed changes on process objectives.

Added to the documentation requirements are plans for continuous improvement and measurement, which should include appropriate details for this level.

4.3.3 IS Policies and Organization (1)

The first section of the VDA ISA questionnaire is divided into 6 sections, which are further divided into subsections. In summary, the first section of the questionnaire deals with general aspects of ISMS. Subsequently, individual sections with their requirements will be described in more detail and practical examples will be given.

Following chapters are described as the structure below (figure 15):



VDA ISA 5
•objectives
•requirements
Maturity assessment
•VDA ISA question number
Example of reference documentation or its implementation
Corrective actions defining

Figure 15 Structure of First Assessment [own elaboration]

4.3.3.1 IS Policies and Organization Information Security Policies (1.1)

As an objective for the first area is stated at least one information security policy. It includes following requirements:

- Established and documented information security requirements tailored to its objectives.
- Developed and disseminated a policy outlining objectives and the importance of information security within the organization.

As an illustrative example for these requirements of IS Policies and Organization Information Security Policies, the ISMS manual can be used to document a company's ISMS in accordance with the requirements of ISO/IEC 27001 Information Security Management System and TISAX requirements. The information security management system covers all situations where information and data may be leaked, misused or lost, whether intentionally or unintentionally, internally or externally, and includes information or data internal to the company or information and data of partners, customers and other third parties that is confidential.

Evaluation

VDA ISA 1.1.1: The requirements are described in organization’s internal standards related to ISMS and Integrated Management System (IMS). Both systems are implemented across organizations departments and operations.

Table 13 VDA ISA 1.1.1 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.3.2 Organization of Information Security (1.2)

Organization of Information Security is divided into four main sections which objectives and requirements are described as following.

1. Integrating information security into organizational strategy - the role of ISMS in sustainable management:

- the ISMS is established with defined scope and requirements,
- commissioned and approved by organizational management,
- equipped with monitoring and control mechanisms,
- determined applicable controls, and subject to regular effectiveness reviews by management.

2. Clear responsibilities within the organization:
   - Information security responsibilities are clearly defined with qualified employees, necessary resources, and known contact persons established both internally and externally with relevant business partners.
3. Integrating Security Requirements Across All Projects:
   - security in projects classification,
   - documentation of classification procedures,
   - implementation of security measures,
   - early risk assessment.
4. Clarifying responsibilities in information security (collaboration with external IT service providers):
   - identified services and IT services utilized,
   - determined relevant security requirements,
   - defined responsible parties for implementation,
   - specified mechanisms for shared responsibilities,
   - ensured the fulfillment of respective responsibilities by the responsible organization.

One of the documentations that fulfils the requirements of this criteria is a guideline that describes information security standards. In this directive, the objective is to design, implement and monitor an effective set of information security measures to minimize the risks to the availability, confidentiality and integrity of the data that the company produces and processes.

Availability here means ensuring the processes and information necessary to achieve corporate objectives and meet legal requirements. The established rules are mandatory for all employees (full-time or part-time), contractors, third-party workers and other users who have access to company data and information. The standards cover information in any form, including hardware, software, business applications, support systems, data stored on computers and servers, data transmitted over a network, printed, written on paper, scanned, stored on portable media (e.g. CDs, DVDs, USB drives, tapes), spoken in conversations or transmitted over the telephone. The document is reviewed at least annually or when major process changes occur.

Evaluation

VDA ISA 1.2.2: Not all information security responsibilities are assigned and qualified for their task.

Table 14 VDA ISA 1.2.2 Evaluation [own elaboration]

Maturity level:	**2**
Corrective actions:	Qualified and assigned responsibilities for information security

4.3.3.3 Asset Management (1.3)

1. Identifying information assets (including supporting assets, such as IT systems and the employees who work with them):
   - identification of important information assets and assignment of responsible persons,
   - catalog of the relevant information assets,
   - a person responsible for information and supporting assets is assigned.
2. Introducing adequate protective measures and information assets classifying (based on security objectives - CIA) to determine protection:
   - A consistent scheme for classifying information assets according to confidentiality is available.
   - Identified information assets are evaluated and assigned to the existing scheme.
   - Specifications for the handling of support assets are established and implemented according to the classification of information assets.
3. The risks of using low-cost or free external IT services - compromising information security:

- Use of external IT services only after assessment and implementation of information security requirements.
- Risk assessment of external IT services is available.
- Consideration of legal, regulatory and contractual requirements.

As the internal standard Planning of ISMS describes, assets are identified and described via systemic document, where are also evaluated threats and risks connected to these assets.

Evaluation

VDA ISA 1.3.1: Information assets of critical value to the organization are identified and recorded in document. A person responsible for these information assets is assigned and recorded in the same document.

Table 15 VDA ISA 1.3.1 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.3.4 IS risk management (1.4)

Objective of this chapter is information security risk management focused on early detection, assessment and resolution of risks. This ensures the introduction of adequate measures to protect information assets. An organization's information security risk management should be as simple as possible for efficiency. Requirements are following:

- Regular risk assessment intervals and response to incidents.
- Information security risks are properly assessed and documented.
- Responsible person (risk owner) is assigned to each information security risk - responsible for assessing and managing information security risks.

A good example for compliance is the systemic record of the risk management plan, which contains a list of actions including associated activities and potential threats. It is recommended not to forget, for example, the nature of the measures, the date of implementation, approval and review of the status of the solution. Subsequently, it is advisable to write down the person responsible for the measures and set a deadline for their review.

Evaluation

VDA ISA 1.4.1: Risk assessments are carried out both at regular intervals (1x12 months) and in response to events (e.g. Critical Security incident). Information security risks are assessed in a suitable manner according to probability of occurrence and potential damage. Information risks are documented, and risk owner is assigned to each threat. A procedure to identify, assess and address information security risks within the organization is described in Risk Management Plan system document. Criteria for the assessment and handling of information security risks exist (internal standard Planning ISMS).

Table 16 VDA ISA 1.4.1 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.3.5 Assessments (1.5)

Assessments chapter is divided in two sections.

1. Regular review for effective information security:
    - Policy compliance is verified throughout the organization.
    - Policies and procedures are regularly revised.
    - Determination and implementation of corrective measures.
    - Regular verification of compliance with information security requirements (e.g. technical specifications).
    - Results are recorded and stored.
2. Ensuring objectivity in ISMS assessments:
    - Information security checks are carried out by an independent and competent authority at regular intervals and in case of significant changes.

- Measures to correct potential deviations are identified and implemented.

Fulfillment of the chapter evaluation requirement was ensured by the ISMS monitoring plan files and the ISMS audit minutes. The ISMS monitoring plan includes the areas or attributes to be monitored, the method and specified regular intervals for their monitoring, the responsible person, and the appropriate response to any problems. Within the internal audit minutes, it is possible to observe both the questions asked on the sub-chapters, the audit findings and the possible notation of non-conformities or recommendations, as well as the overall result of the audit with the audit team.

Evaluation

VDA ISA 1.5.1: Observation of policies is verified throughout the organization by internal audits and KPI. Information security policies and procedures are reviewed at regular intervals (1x12 months). Nonconformities are reported to management. Compliance with information security requirements is verified at regular intervals. The results of the conducted reviews are recorded (system document).

Table 17 VDA ISA 1.5.1 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.3.6 Incident management (1.6)

Incident management discusses the organized processing of information security events aims at limiting potential damage and preventing recurrence.

- Technical and organizational measures are established.
- Procedures are defined for traceability in the event of information security incidents or vulnerabilities.
- Events and vulnerabilities are assessed and documented.
- Adequate response to information security events and vulnerabilities is provided.

- The IS breach response strategy includes escalation procedures, measures and communication with internal and external authorities, and decisions to prosecute cybercriminal attacks.

While assessing this criterium, it is possible to be shown the record of security incidents in the ticketing tool or standard described before named information security standards.

Evaluation

VDA ISA 1.6.1: A definition for information security events and vulnerabilities is established, which includes both security events and security incidents. Procedures for reporting and recording these events and vulnerabilities have been defined and are implemented through email. Information security incidents are reported using both email and an Excel table.

Table 18 VDA ISA 1.6.1 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.4 Human Resources (2)

Section 2 related to human resources is further divided into four subsections.

1. Competent, reliable, and trustworthy employees:
   - Determined sensitive work fields and jobs.
   - Determined requirements for employees concerning respect to their job profiles.
   - Verified identity of potential employees.
2. Employees commit to compliance with the policies:
   - Duty of confidentiality.
   - Obligation to comply with information security principles.
3. Information security is internalized and practiced as a natural part of employee’s work:
   - Trained and made aware employees.
4. Risk of working outside of the specified security zones:

- Requirements for teleworking established. The following aspects are considered:
  - Safe handling of information and access to it (in electronic and paper form) regarding protection needs and contractual requirements applicable to private (e.g. working from home) and public environments (e.g. when traveling).
  - Behavior in privacy.
  - Behavior in public.
  - Measures to protect against theft (e.g. in a public environment).
- The organization's network is accessed through a secure connection (e.g. VPN) and strong authentication.

As an appropriate example is a concept for awarenesses and training of employees. Main themes:

- Information security Policy
- Reporting of information incidents
- Reaction of malware
- Password policy
- Compliance issues of information security
- NDA requirements
- The training is for all employees. The concept has been approved by the CEO. Training is carried out at regular intervals (1x12 months). Participation in training and awareness measures are documented.

Evaluation:

VDA ISA 2.1.2: During the assessment process was noted that most of employees haven’t signed NDAs.

Table 19 VDA ISA 2.1.2 Evaluation [own elaboration]

Maturity level:	**2**
Corrective actions:	**All employees get an NDA contract amendment.**

4.3.5 Physical Security and Business Continuity (3)

Other important aspects that the organization must manage in detail include the security of the organization's environment and premises.

This criterium is divided into four sections:

1. Security zones:
   - Security zone concept including protective measures.
   - Implemented protective measures.
   - The code of conduct for security zones is known to all persons involved.
2. Exceptional situations:
   - Identified and recorded possible exceptional situations.
   - Identified and recorded potentially endangered infrastructure components (IT systems, access points etc.).
   - Identified and implemented measures for limiting the impact of threats.
3. Handling assets:
   - Determined and fulfilled requirements for handling of supporting assets (e.g. transport, storage, loss…).
4. Mobile IT devices and mobile data storage devices:
   - Determined requirements.
   - Considered aspects of encryption, access protection (e.g. PIN, password), marking.

Interesting implementation could be setting of security zones, which are described as follows:

Security zones

For maximum data and technology protection at the organization, security features are implemented in the form of dividing individual perimeters into security zones. The principle of assigning access to individual zones is based on the need-to-know principle.

White zone

The white zone includes all areas of the organization that are not subject to any form of protection other than the security provided by the facility manager. Typically, these are public areas of the organization, such as the reception and meeting room for visitors.

Yellow Zone

The yellow zone indicates areas of the organization where secondary assets of the organization may be located. Access to these areas is only allowed to employees of the organization based on their job responsibilities and "need to know". Third party employees may only enter the Yellow Zone when accompanied by a responsible employee of the organization. The level of access is defined by keys.

Purple Zone

The purple zone is reserved for Cargo.

Red Zone

The Red Zone represents the highest level of protection and includes TPV's own premises and prototype workshops, where primary technologies and customer data are located. Access to the Red Zone is controlled by a system key. Only strictly selected employees of the organization have access to these areas, and only for the time necessary to carry out the relevant activity. Third parties may enter the red zone only on an exceptional basis, always accompanied by a responsible employee of the organization and after thorough training. This training must be recorded and the third party's visit to the red zone must be logged.

Evaluation:

VDA ISA 3.1.1: Although access to the server room is well defined, access is allowed to non-expert personnel.

Table 20 VDA ISA 3.1.1 Evaluation [own elaboration]

Maturity level:	**2**
Corrective actions:	**Access review - Removing access from all unauthorized persons and leaving access only to persons authorized by the IT department**

4.3.6 Identity and Access Management (4)

Identity management is divided into three sections which are described below.

1. Identification means:
    - Determined and fulfilled requirements for identification means over the entire lifecycle.
    - Considered aspects of creation, handover, return and destruction, validity periods, traceability and handling of loss.
2. User access to network services, IT systems and IT applications:
    - Selection based on a risk assessment.
    - Consideration of potential attack scenarios.
    - Compliance of the authentication procedure with the current state of the art.
3. Accounts and login information:
    - User accounts are uniquely created, modified, and deleted to maintain personalized access.
    - Use of collective accounts is restricted to ensure traceability of actions where necessary.
    - User accounts are promptly disabled after the user leaves the organization to secure access.
    - Specifications are set for password quality, such as minimum length and character types, to enhance security.

Shortly the Access management is described as follows.

1. Access rights:
    - Determined and fulfilled requirements.
    - Considered procedure for application, verification and approval.
    - Verification at regular intervals of access rights of accounts also within IT systems of customers.

Identity and Access management is detailed in internal standard Information Security Standards, which was described before (chapter Organization of IS 1.2). Part of this standard is for example chapter dedicated separately for Access management, which contains subchapters about organization's access control requirements, user access management and control, user responsibilities, access control to systems and applications. An appropriate example of access management is Use of secret authentication information, where the following rules are set:

- The password must not be stored on the computer in an unprotected form.
- The password must not be displayed on the computer, asterisks must be shown.
- The user must not place the written form of the password content on or near the hardware or other accessible locations.
- The user must not disclose passwords or other security access and identification data to any other person.
- The user must use passwords for software security that are no shorter than 15 characters in length, contain at least one capital letter and a number or a special character (e.g. .,*;! etc.), unless this is excluded by the operating system or application being used.
- In the case of the use of a password, the user is fully responsible for the use of the software through his/her account and password.

Evaluation

VDA ISA 4.1.2: Every user has own name and password. The procedure for users is based on principle need to know and least privileges. For standard users is valid 15 characters, contains min. one uppercase letter and a number, for privilege password is valid 15 characters, full complexity.

Table 21 VDA ISA 4.1.2 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.7 IT Security / Cyber Security (5)

IT Security/Cyber Security topic is divided into two sections.

1. Cryptographic procedures:
   - All used cryptographic methods meet the current security standards required for their applications.
   - The legal parameters for the use of cryptography are taken into account.
2. Protection of information during transfer:

- Identified and documented network services used for transferring information.
- Defined and implemented policies and procedures according to requirements for the use of network services.
- Implemented measures for the protection of transferred contents against unauthorized access.

Operations security contains seven sections, each described below.

1. Changes:
   - Determined and applied information security requirements for changes to the organization, business processes and IT systems.
2. Separation of development and testing environments:
   - Subjected IT systems to risk assessment in order to determine the necessity of their separation into development, testing and operational systems.
   - Implemented segmentation based on the results of risk analysis.
3. Protection of IT systems against malware:
   - Determined requirements for protection against malware.
   - Defined and implemented technical and organizational measures for protection against malware.
4. Event logs:
   - Information security and logging requirements are established and met for event logs, system administrators, and user activities.
   - IT systems are evaluated for necessary logging, including when using external services.
   - Event logs are regularly reviewed for compliance and anomalies within legal and organizational limits.
5. Vulnerabilities:
   - Affected systems and software are identified, evaluated, and vulnerabilities are mitigated.
   - Gathered and evaluated information on technical vulnerabilities for the IT systems.
6. Technical check of IT systems:

- Determined requirements for auditing IT systems.
- Specified scope of the system audit in a timely manner.
- Audit results are stored in a traceable manner and reported to management.
- Measures derived from the results.

7. Network:
    - Determined and fulfilled requirements for the management and control of networks.
    - Determined and fulfilled requirements regarding network segmentation.

Third and last part of IT Security / Cyber Security topic is a System acquisitions.

1. Evaluating information security in new and upgraded IT systems:
    - Identified and considered information security requirements for designing, developing, acquiring, extending, and modifying IT systems,
    - system approval tests are carried out under consideration of the information security requirements.
2. Requirements for network services:
    - Determined and fulfilled requirements regarding the information security of network services,
    - requirements are agreed in the form of SLAs,
    - adequate redundancy solutions are implemented.
3. Return and removal of information assets from external IT services:
    - Defined and implemented procedure for return and secure removal of information assets.
4. Protection of information in shared external IT services:
    - Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organizations.

The organization describes the approach and rules of IT security / Cyber security in the Information Security Standards directive. As an example, the organization describes how protection against Malware is ensured:

- Antivirus Sentinel One is used in the organization.
- Users are prohibited from using software other than that provided to them by the IT service provider.

- Users have local admin privileges disabled on their workstations; they cannot intervene in the system.
- Information assets that can be attacked by malware (typically PC, laptops, Server, PDA, etc.) must be configured so that it is not possible to install unauthorized software.
- Unnecessary network services are turned off.

Evaluation

VDA ISA 5.2.5: Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed during regularly patches for company equipment. Vulnerability management is established on manually principles. The list of keys assets for Patch management is based on Risk analysis. Organization make Penetration test once per 12 months.

Table 22 VDA ISA 5.2.5 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.8 Supplier Relationship (6)

The supplier relationship criteria are presented in two segments as follows.

1. Information security among contractors and cooperation partners:
    - Risk assessments and contractual agreements ensure an appropriate level of information security with contractors and partners.
    - Compliance with these contracts is verified, and client agreements are extended to these parties where relevant.
2. Assessing contractual agreements on non-disclosure in information exchange:
    - Non-disclosure requirements are established and met.
    - All relevant parties are informed about non-disclosure agreement (NDA) procedures before sharing sensitive information.
    - NDAs are signed prior to information disclosure, and their use and procedures are regularly reviewed.

As part of the implementation, the company has created a list of suppliers, which is recorded in an Excel table. The evaluation of these suppliers is based on four criteria:

- compliance with NDA (non-disclosure agreement),
- ISMS/TISAX (Information Security Management Systems),
- terms and conditions,
- complaints.

For the first three criteria, it is assessed whether confirmation has been received from suppliers that they meet information security requirements. If a supplier fails to provide the necessary confirmation, the Cybersecurity Committee must decide on further action with that supplier.

In terms of complaint ratings, the organization applies a scale of 1 (best) to 5 (worst) to assess the level of satisfaction with the services provided. If a supplier is rated lowest, the Cybersecurity Committee shall analyze the reasons for the low score.

Evaluation

VDA ISA 6.1.1: Suppliers and cooperation partners are subjected to a risk assessment regarding information security. An appropriate level of information security is ensured by contractual agreements with suppliers and cooperation partners. Suppliers and cooperation partners are contractually obliged to also pass on any requirements regarding an appropriate level of information security also to their subcontractors.

Table 23 VDA ISA 6.1.1 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.9 Compliance (7)

The Compliance criteria categorization follows structure below.

1. Compliance with regulatory and contractual provisions:

- Legal, regulatory, and contractual provisions relevant to information security are regularly reviewed.
- Policies to ensure compliance are defined, implemented, and communicated to responsible parties.

2. Personal data protection:
   - Legal and contractual requirements for handling personally identifiable data are established and known to relevant personnel.
   - These are incorporated into the information security management system along with defined compliance regulations.

The organization has implemented several key measures to ensure compliance and security. A comprehensive register of legal requirements and planning measures has been prepared to guide operations. Intellectual property protection is systematically addressed through contractual agreements in each employment and supply contract. Additionally, records are securely stored on internal servers and backed up regularly; access to these records is strictly controlled by access rights. The organization also follows a detailed shredding and archiving procedure, which clearly defines the storage duration for all documentation.

Evaluation

VSA ISA 7.1.2: The organization has implemented a personal data protection policy, which is in accordance with Regulation No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals.

Table 24 VDA ISA 7.1.2 Evaluation [own elaboration]

Maturity level:	**3**
Corrective actions:	**None**

4.3.10 Prototype Protection (8)

The company has not implemented these criteria because it is not working with prototypes but is preparing to do so in the future. Therefore, only a description of the content, requirements and an example implementation will be given below without subsequent evaluation.

Prototype protection covers vehicles, components, and parts that are deemed to require protection but have not yet been publicly disclosed or adequately published by the original equipment manufacturer (OEM). The OEM department in charge of commissioning is responsible for determining the need for protection for these vehicles, components, and parts. The minimum standards for prototype protection for the high and very high protection classes must adhere to the VDA ISA guidelines.

4.3.10.1 Physical and Environmental Security

1. Necessary prototype protection measures must be applied and implemented at the properties and facilities of suppliers, development partners, and service providers.
2. Prevented unauthorized access to properties where protected vehicles, components, or parts are manufactured, processed, or stored.
3. Unauthorized access to buildings and security areas where protected vehicles, components, or parts are manufactured, processed, or stored must be prevented.
4. Ensure that unauthorized viewing of protected vehicles, components, or parts is prevented.
5. Securing access points to protected manufacturing areas.
6. Monitoring and alarm processing for secure manufacturing premises.
7. Ensuring documented security for protected manufacturing areas.
8. Ensuring client-specific know-how protection through segregation.

4.3.10.2 Organizational Requirements

1. Ensured secure information transmission with external organizations.
2. Ensured subcontractors meet minimum requirements for prototype protection.
3. Employees must gain the necessary skills in trainings and awareness seminars to securely handle protected prototypes.
4. Ensured all project members are aware of and adhere to security classifications and requirements as the project progresses.

5. A process is established to prevent unauthorized access to areas where protected vehicles, components, or parts are manufactured, processed, or stored.
6. Defined regulations for recording images of protected vehicles, components, or parts to prevent unauthorized creation or transmission of such images.
7. Defined a process for using mobile video and photography devices in security areas where protected vehicles, components, or parts are handled, ensuring prevention of unauthorized image creation or transmission.

4.3.10.3 Handling of Vehicles, Components and Parts

1. Protected transported vehicles, components, and parts from unauthorized viewing, image recording, and access.
2. Ensured vehicles, components, and parts requiring protection are secured against unauthorized viewing, photography, and access when parked/stored.

4.3.10.4 Requirements for Trial Vehicles

1. Ensured all project members know and follow camouflage regulations to adequately protect trial vehicle visibility.
2. Observed customer-defined protective measures to maintain secure operations on test and trial grounds.
3. Ensured knowledge and adherence to customer requirements for operating protected trial vehicles on public roads.

4.3.10.5 Requirements for Events and Shootings

1. Ensured knowledge of customer-specific security requirements for presentations and events involving protected vehicles, components, or parts.
2. Ensured awareness of customer-specific security requirements for film and photo shoots involving protected vehicles, components, or parts.

Prototype protection includes vehicles, parts and components that are classified as requiring protection that have not yet been presented to the public and/or disclosed in an appropriate form by the manufacturer.

The Business Office is responsible for classifying the protection needs of vehicles, components and parts. The minimum protection requirements for prototypes for the

High and Very High protection classes shall be applied in accordance with the VDA ISA.

The VDA ISA catalogue defines the following general protection classes for companies depending on the potential damage:

Table 25 General Protection Classes [internal]

Class of protection	Description
Normal	The potential for harm is low, limited in time and affects one company.
High	Potential for harm is high, long term, even unlimited, affecting one company.
Very high	Potential for damage is very high, threatens the existence of the company, affects multiple companies.

During the development process, special protection of the innovative design is required. As regards these processes, special attention should be paid to risk analysis, the implementation of effective safeguards and the monitoring of the effectiveness of the safeguards. Appropriate procedures must be used and documented to ensure that everything is done in compliance.

4.3.11 Summary of Evaluation

Summary of evaluation contains table with all the evaluation made in this thesis. It can be seen that 3 minor nonconformities were found (table 26). For each is also stated corresponding corrective action which are also stated in CAP (Corrective Action Plan).

Table 26 Summary Evaluation Table [own elaboration]

Chapter	VDA ISA	Maturity level	Corrective actions
IS Policies and Organization Information Security policies (1.1)	1.1.1	3	None
Organization of IS (1.2)	1.2.2	2	Trained and assigned responsibilities for information security
Asset management (1.3)	1.3.1	3	None
IS risk management (1.4)	1.4.1	3	None
Assessments (1.5)	1.5.1	3	None
Incident management (1.6)	1.6.1	3	None
Human resources (2)	2.1.2	2	All employees get an NDA contract amendment.
Physical Security and Business Continuity (3)	3.1.1	2	Access review - Removing access from all unauthorized persons and leaving access only to persons authorized by the IT department
Identity and Access Management (4)	4.1.2	3	None
IT Security / Cyber Security (5)	5.2.5	3	None
Supplier Relationship (6)	6.1.1	3	None
Compliance (7)	7.1.2	3	None
Prototype protection (8)	-	-	-

4.4 Implementation of Corrective Actions

During the assessment were identified 3 minor nonconformities that led to an insufficient level of maturity, which prevented the successful completion of the TISAX audit. After the Corrective Action Plan (CAP) with chosen measures was drafted. The period allowed for completing corrective actions after a TISAX assessment is nine months from the Closing Meeting, which is the final meeting of the Initial Assessment. During this period, the organization obtains the so-called temporary label which lasts 9 months. The temporary label is possible to get only in case of minimum 2,7 maturity score and on the base of elaborated CAP, without any principal nonconformities which would mean maturity level 0 or 1. If the corrective actions are not completed within this timeframe, the assessment process must start again from the beginning.

Table 27 Suggested Corrective Actions [own elaboration]

Requirement	Noncompliance	Corrective action
1.2.2 **Clear responsibilities within the organization**	Not all information security responsibilities are assigned and qualified for their task.	Assigned and trained responsibilities for information security.
2.1.2 **Staff contractually bound to comply with information security policies**	During the assessment process was noted that most of employees haven't signed NDAs.	All employees get an NDA contract amendment.
3.1.1 **Managing security zones to protect information assets**	Although access to the server room is well defined, access is allowed to non-expert personnel	Access review - Removing access from all unauthorized persons and leaving access only to persons authorized by the IT department

4.5 Final Assessment

After identification of the weaknesses and implementing all the corrective actions, is coming up the final assessment. At this stage of assessment are reviewed only sections that did not reach the required level of maturity during the first evaluation. Since this company has the temporary label, the final assessment should be done within the 9-month period, but it is recommended not to leave it to the last minute and to arrange the final evaluation in advance.

The table below (table 28) shows the requirements which haven't been fulfilled and proof of corrective actions implementation.

Table 28 Evidence of Corrective Actions [own elaboration]

Requirement	Proof of corrective actions implementation
1.2.2 **Clear responsibilities within the organization**	Assigned documentation, job description and proof of training (certification)
2.1.3 **Staff contractually bound to comply with information security policies**	Proof of NDAs – signed NDAs
3.1.1 **Managing security zones to protect information assets**	Proof of removed access from all unauthorized persons and access only of IT department

4.6 Audit

While for the ISO framework are inherent annual audits, conversely TISAX audits occur on a triennial basis, maintaining synchronization with ISMS objectives. Despite not being a normative document itself, ISMS encompasses ISO and TISAX as integral subsets within its overarching framework.

Audit TISAX is carried out by an external company (certifying authority), which is approved by both VDA and ENX. Participant can choose from the list of audit providers, which is available at official ENX website. Participant had an option for example from certifying authorities such as TÜV SÜD Management Service GmbH, TÜV NORD CER GmbH, or Bureau Veritas Services. After choosing the subject, who is going to carry out an audit, the company arranges the date of the audit and sends VDA ISA questionary for assessment to auditor from selected certified authority.

There are two options how the audit would be done, distributed by AL 2 and AL3. The main difference between the audit of AL 2 and AL 3 is that the AL 2 is held via teleconference meeting and the evidence is sent forward (e.g. print screen of Active Directory, picture of the door with knob etc.). In case of AL 3 the audit is done physically on site during which is all the evidence checked (e.g. physical control of physical security).

Basically, the auditor studies the VDA ISA questionnaire and verify its findings with the selected organization. The organization must also provide evidence of implementation the corrective actions in the form of documented information.

If auditor identifies that the selected organization’s approach to the requirement under review is not in compliance, two types of non-compliance are distinguished:

1) Minor non-conformance.

This type of non-compliance doesn't undermine the overall effectiveness of the existing information security management system and doesn't pose a significant security risk. These are accidental errors or minor flaws in implementation.

2) Major non-conformance.

This type of finding is more serious and raises concerns about the overall effectiveness of the existing information security management system or poses a significant security risk. These could involve systemic non-conformities or substantial implementation deficiencies that lead to critical data and information security risks.

If one major non-conformance is identified, the audit conclusion is that organization is not in compliance with TISAX requirements and is not obtaining the TISAX label. Changing such a rating is only possible by setting appropriate corrective actions that are approved by the audit service provider. Thereafter, the overall audit conclusion may be changed, and company can get a so-called TISAX temporary mark.

After the non-conformities have been settled, the auditor prepares a final report containing the result of the TISAX assessment, which can take three states:

1) In compliance with TISAX requirements (organization obtains TISAX label).

2) In compliance with TISAX requirements with minor deviations (organization obtains temporary TISAX label).

3) Non-compliance with TISAX requirements (the process of TISAX implementation needs to start from the beginning again).

4.7 Implementation and Results Sharing

The main purpose of the TISAX assessment is to disclose the results of the assessment to other TISAX participants and to share the outcome of the assessment with partner(s). The decision to disclose and share the result of assessment can be made either during the registration process or any time afterwards. The company can also decide for itself whether the results reveal to all partners and in what detail.

If it is needed to reassure partner about the ongoing registration or preparation for the audit, it is possible to contact the TISAX Certification Body - Audit Provider who can issue a confirmation (after signing the contract) when the actual audit will take place. This certificate can then be sent to the partner as proof that the company has already received the audit date and is in the process of preparing for the audit.

5 EVALUATION AND BENEFIT OF THESIS

This chapter aims to critically evaluate the findings and outcomes of implementing the TISAX framework within the context of the organization described in this thesis.

The benefits that the implementation of TISAX has brought to the organization include:

- Specialization in the Automotive Industry - includes the ability to securely handle prototypes.
- Free Choice of Audit Provider - TISAX creates competition among audit providers and allows a joint recognition of assessment results between TISAX participants.
- Standardization of Security Requirements - companies in the automotive industry apply uniform security standards across their supply chain.
- Simplifying Assessment and Certification - suppliers can demonstrate their ability to protect sensitive information through a recognized certification that is acceptable to all major automotive manufacturers.
- Improving Trust and Transparency - implementation strengthens trust between car manufacturers and their suppliers. Suppliers that are TISAX certified are perceived as more reliable and safer partners.
- Mitigation of Security Risks - Systematic assessments and regular reviews ensure that all stakeholders continuously update and improve their security protocols.
- High Level of Data Security - which is key to protecting sensitive information.
- Avoiding Possible Customer Loss - in case customer requires TISAX certification.
- Elimination of the Need for Customer Audits - both from side of organization and customer, leading to savings in both financial and time resources.
- New Automotive Contracts - expanding the company's business opportunities.

5.1 Results

This chapter clearly illustrates the partial results of the practical part of this thesis. The thesis follows the whole implementation process, and its most comprehensive part was the GAP analysis or the first assessment of the currently implemented metrics and guidelines related to ISMS in the company. This part is based on the principle of the VDA ISA questionnaire and shows the most practical approach to proceeding with self-assessment. Each criterion of this questionnaire is described with its objectives and requirements, then an example of reference document or its implementation is given and finally the current state is evaluated using the maturity model. The evaluation consists of a brief description of the implementation and corrective actions are then identified in case of non-compliance.

This analysis resulted in three minor non-conformities and the corrective actions identified in the CAP. From the chart below (figure 16), it can be seen in which parts has the company gaps. In order to meet the requirements and obtain TISAX certification these gaps had to be effectively addressed. Despite these challenges, the organization obtained temporary TISAX label, because the final score of assessment was 2,93 and organization has submitted a CAP.

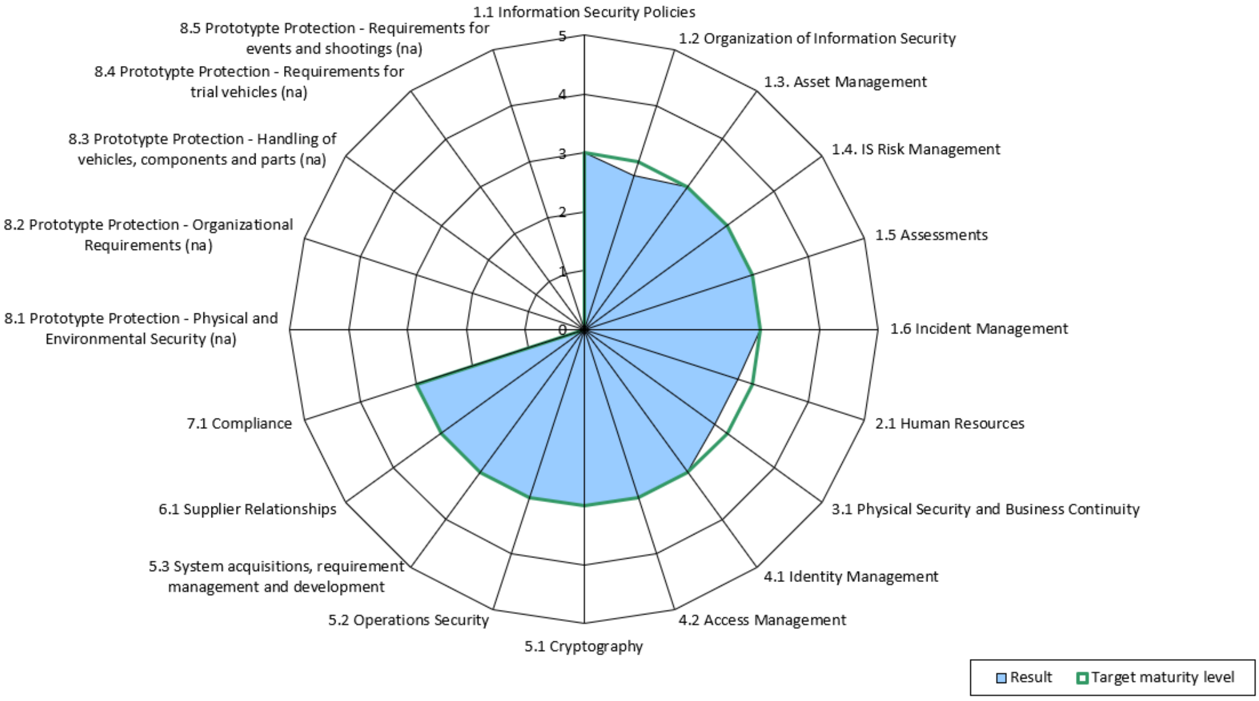


Figure 16 Weak Areas - Radar Chart [internal]

5.2 Economic Cost Analysis

This chapter presents a detailed economic evaluation of implementing TISAX certification within the automotive sector, utilizing the Return on Security Investment (ROSI) model as the analytical framework, because it is one of the elements of the basic managerial perception of security issues. The commitment to enhance an organization’s security posture through TISAX certification necessitates financial investments, that's why it is important to quantify the potential financial returns relative to these investments. This model not only aids in justifying the economic feasibility of TISAX certification but also enhances the understanding of its strategic value within the realm of information security investments in the automotive industry.

5.2.1 Evaluation

The following tables lists the direct costs, indirect costs and avoided costs that were associated with the implementation of TISAX in the company related to this diploma thesis. Some of the items have only estimated amounts and the rest were applied in this company but may vary depending on various factors such as the size of the company or the choice of external entities.

5.2.1.1 Investment Costs

Not all items from the list in the theoretical part of the thesis were included in the investment costs for the ROSI calculation, as the company had already implemented most of the possible changes needed to comply with the TISAX standard. This means, for example, software or hardware upgrades. Therefore, these items will no longer be counted. Only costs that are known or that the author has estimated from own experience in implementing TISAX in the company under consideration are quantified. Other items in the table (training, maintenance of security systems, etc.) are based on this fact and therefore represent a lower value than would be expected.

Direct Costs

Registration fee includes payment required to initiate the TISAX assessment process. Company paid 405 € for registration on the ENX portal.

Consultancy may be needed in some companies. As the company decided to hire external expert to advise and ensure all standards are met before the audit, paid also this service for 2 000 €.

Certification audit (AL 2) fee includes conducting the Level 2 audit, which is necessary for compliance verification by the certifying body. Company paid 4 000 € for certification audit.

Annual audit cost includes maintenance of the system and ensuring ongoing compliance with the TISAX standards. Company hired external auditor for this task and is paying 600 € per year.

Training expenses are related to training staff on compliance and security procedures. Also contain cost of specific training for responsibilities in Cybersecurity Committee, who don’t yet have sufficient knowledge to carry out their tasks.

Indirect Costs

Documentation and policy development includes time and resources spent by creating and updating documentation and policies to meet TISAX requirements. Due to hiring external advisor for consultancy, this task took a lot less time. This time was estimated as 3 man-days, while 1 man-day in this case has 7,5 working hours.

Employee time means the hours that employees dedicate to implementing and maintaining TISAX standards, which are not billed directly but represent a significant part of the compliance cost. This time was estimated as 15 man-days per one year.

Maintenance of security systems includes ongoing costs involved in keeping security systems up to date to prevent breaches and ensure compliance. Estimated time for this task are 10 man-days.

Long term monitoring and compliance includes resources allocated to continually monitor the compliance status and adapt to new regulatory changes or updates in TISAX standards. Estimated duration of this task was 7 man-days per year.

Table 29 Direct and Indirect Costs [own elaboration]

Type of costs	Activity/Item	Amount [€]	Sum [€]	
Direct costs	Registration fee (ENX portal)	405	8 605	13 925
	Consultancy (implementation of TISAX)	2 000		
	Certification audit (AL 2)	4 000		
	Annual audit - system maintenance (external auditor)	600		
	Training	1 600		
Indirect costs	Documentation and policy development (3 MD)	456	5 320	
	Employee time (15 MD)	2 280		
	Maintenance of security systems (10 MD)	1 520		
	Long term monitoring and compliance (7 MD)	1 064		

5.2.1.2 Avoided Costs

As it is very difficult to express the monetary value of the benefits (listed in chapter 2.7.1.2 Benefits) in the company covered by the thesis, these components will not be taken into account in the following calculations.

Avoided costs include three main examples that a company can avoid by implementing the TISAX standard.

1. Loss of confidential information and incident costs are quantified for 2 million euros based on the fact, that for small businesses (under 500 employees), the average cost of a data breach was 2,742 million euros in 2021. The company discussed in this thesis has no experience with such an incident, so the amount has been rounded to 2 million euros in table below.
2. The General Data Protection Regulation (GDPR) imposes fines for violations to ensure data protection. The fines can be substantial, with the maximum fine being up to 20 million euros or 4% of the company's worldwide annual turnover from the preceding financial year. In specific cases, fines can reach up to 1,2

billion euros, as could be seen in the case of Meta (formerly Facebook), which was fined by the Irish Data Protection Commission (DPC) for continuous and large-scale violations of GDPR regulations. Violations of data protection regulations fine was set up in this example as 10 million euros.

3. As the thesis addresses a manufacturing company in automotive industry, the shutdown is a very important component of following table. In case of incident there would be a substantial loss of revenue. One minute of shutdown in this company costs approximately 120 euros, so as it is three-shift operation with 7,5 hours working time, it would be 162 000 euros per one day of shutdown.

Table 30 Avoided Costs [own elaboration]

	Activity/item	**Amount [€]**
Avoided costs	Violations of data protection regulations fine	10 000 000
	Loss of confidential information and incident costs	2 000 000
	Shutdown (1 day)	162 000

5.2.1.3 ROSI model

The table below illustrates the Return on Security Investment (ROSI) percentages based on varying Mitigation Ratios (MR) between 10% and 50% and Annual Rate of Occurrence (ARO) expressing one incident in one year. For the evaluation and calculation of the ROSI model were used amounts mentioned in the previous tables (the total investment costs 13 925 € from table 29 and SLE from table 30).

Table 31 ROSI [own elaboration]

SLE	**10 000 000 €**	**2 000 000 €**	**162 000 €**
MR/ARO	1	1	1
10 %	7 081 %	1 336 %	16 %
20 %	14 263 %	2 773 %	133 %
30 %	21 444 %	4 209 %	249 %
40 %	28 625 %	5 645 %	365 %
50 %	35 807 %	7 081 %	482 %

As Mitigation Ratio rises (table 31) so do the percentage of ROSI from 7 081% at ARO 1 to 35 807% in case of violations of data protection regulations fine (10 000 000 € SLE), indicating substantial returns even at the lowest mitigation ratio, due to reduced potential losses. Even in case of shutdown (162 000 € SLE) is the percentage raising from 16 % to 482 %.

This table demonstrates that increasing the mitigation ratio directly correlates with significantly higher returns. Therefore, investing in measures that reduce the impact of potential security breaches results in exponential returns on investment, justifying the costs associated with compliance and security upgrades.

CONSLUSION

The implementation of the TISAX standard in the company may be a necessary step due to the increasing demands of customers to ensure the security of information in the automotive industry. The introduction of the standard can achieve a high level of information security and ensure the company's position as a trusted partner in the automotive industry.

The diploma thesis provides a comprehensive view of the process of implementing TISAX in practice with an emphasis on the key role of risk management and supply chain security. The findings gained from this work can serve as valuable recommendations for an organization that needs to go through the certification process.

The theoretical part outlined a brief history of information security in the automotive industry, basic terminology and standards, which are key within TISAX. Within the theoretical part of this work, it was also important to mention a fundamental area such as risk and supply chain management.

The analytical part is focused on the description of the organization and its characteristics. The implementation of a robust ISMS system and an effective risk management strategy were highlighted as essential elements that are key to align with TISAX requirements.

The practical part of the work includes the process implementation of TISAX in the selected company. This process begins with preparation and continues with registration on the ENX portals, which includes consideration of the number of locations and the scope of the assessment. Subsequently, a Gap Analysis was carried out as a first assessment and revealed three small nonconformities in the current procedures, due to which the company temporarily received a temporary label for nine months. During this time, the company must implement the corrective measures set out in the CAP. The proposed measures within the Corrective Action Plan were developed on the basis of this analysis and consultations with experts. They include, for example, adding NDAs to employee contracts or removing unauthorized access to the company's server room. The successful implementation of these measures represents for the company a step towards the successful and effective implementation of the TISAX standard in practice.

The last part of the work summarizes the results of the assessment and the benefits of introducing the TISAX standard into the company. Following this, a financial evaluation was carried out using the ROSI model, in which direct and indirect costs were determined together with calculated avoided costs. The evaluation provides an understanding of the potential financial savings. The result of evaluating the implementation of TISAX in the described company is unlikely to match with the result of other companies, since the costs differ depending on the maturity of the established system of the company, on the number of locations or on the certification body that performs the audit. In the result of the ROSI model can be seen that investing in the implementation of security standards such as TISAX is worthwhile, because its return result is very positive.

The benefits of introducing the TISAX system to a company include enhancing strategic value by reducing security risks and strengthening trust between partners. Furthermore, the benefits include a high level of data security, avoiding high costs for possible production shutdowns and fines for violating data protection regulations, preventing possible customer losses or lower customer audits (both from the organization and from the customer).

Finally, it important to mention that the successful implementation of the TISAX standard depends on the appropriate support of the company's management, the involvement of employees and the maintenance of open communication with external partners and customers. Other important components are comprehensive risk management and a well-established ISMS framework, which are necessary to successfully meet TISAX standards, ensure effective protection of information assets while building trust throughout the supply chain.

BIBLIOGRAPHY

[1] Cybersecurity in the Automotive Industry: New Challenges for Automotive Developers. In: *Magna* [online]. 2023 [visited on 2024-05-12]. Available from: https://www.magna.com/stories/inside-automotive/2023/cybersecurity-in-the-automotive-industry

[2] The Evolution of Cybersecurity in the Automotive Industry. In: *Cyberautox* [online]. 2023 [visited on 2024-05-12]. Available from: https://cyberautox.com/cybersecurity-in-the-automotive-industry/

[3] SAE J3061: Cybersecurity Risk Management for Automotive. In: *Visure* [online]. [visited on 2024-05-12]. Available from: https://visuresolutions.com/blog/automotive/sae-j3061/

[4] Cyber security in the automotive sector: the scenario, risks and future challenges. In: *Safecore* [online]. [visited on 2024-05-12]. Available from: https://safecore.io/en/industry/cyber-security-in-the-automotive-sector-the-scenario-future-risks-and-challenges/

[5] *The challenge of digital transformation in the automotive industry Jobs, upgrading and the prospects for development* [online]. ETUI aisbl, Brussels, 2020 [visited on 2024-05-12]. ISBN 978-2-87452-570-4. Available from: https://www.etui.org/sites/default/files/2020-09/The%20challenge%20of%20digital%20transformation%20in%20the%20automotive%20industry-2020.pdf

[6] The History of ERP. In: *Blue link* [online]. [visited on 2024-05-12]. Available from: https://www.bluelinkerp.com/blog/the-history-of-erp/

[7] A Simple Guide to Automotive Software. In: *AutoPi* [online]. 2022 [visited on 2024-05-12]. Available from: https://www.autopi.io/blog/what-is-automotive-software-and-its-benefits/

[8] What Is Vehicle-to-Everything (V2X) Technology?. In: *Builtin* [online]. 2023 [visited on 2024-05-12]. Available from: https://builtin.com/articles/v2x-vehicle-to-everything

[9] Electric Vehicles: How Much Should We Worry About Cyber Security?. In: *RUSI* [online]. 2023 [visited on 2024-05-12]. Available from: https://www.rusi.org/explore-our-research/publications/commentary/electric-vehicles-how-much-should-we-worry-about-cyber-security

[10] Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *Journal of Cybersecurity and Privacy* [online]. 2023, **2023** [visited on 2024-05-12]. Available from: https://www.mdpi.com/2624-800X/3/3/25

[11] Connected, safe, and secure: the future of connected vehicles. In: *Giesecke+Devrient* [online]. [visited on 2024-05-12]. Available from: https://www.gi-de.com/en/digital-security/connectivity-iot/automotive

[12] Cybersecurity in automotive: Mastering the challenge. In: *McKinsey and Company* [online]. 2020 [visited on 2024-05-12]. Available from: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/cybersecurity-in-automotive-mastering-the-challenge

[13] AI-IOT-Based Adaptive Control Techniques for Electric Vehicles. *Electric Power Components and Systems* [online]. 2024, 1-19 [visited on 2024-05-12]. Available from: https://doi.org/10.1080/15325008.2024.2304685

[14] SEDLÁK, Petr a Martin KONEČNÝ. *Přeměna ISMS v manažerské informatice*. Vydání: první. Brno: CERM, akademické nakladatelství, 2023. ISBN 978-807-6231-108.

[15] Data vs Information vs Knowledge: What Are The Differences?. In: *Tettra* [online]. 2023 [visited on 2024-05-12]. Available from: https://tettra.com/article/data-information-knowledge/

[16] What are Data, Information, and Knowledge. In: *Internet of Water* [online]. [visited on 2024-05-12]. Available from: https://internetofwater.org/valuing-data/what-are-data-information-and-knowledge/

[17] ISO/IEC. *ISO/IEC 27000 Information technology*. 5th. 2018.

[18] What is the CIA Triad? Definition & Examples in Cybersecurity. In: *Coretelligent* [online]. 2022 [visited on 2024-05-12]. Available from: https://coretelligent.com/insights/what-is-the-cia-triad-and-why-does-your-cybersecurity-position-depend-on-it/

[19] The CIA triad: Definition, components and examples. In: *CSO* [online]. 2020 [visited on 2024-05-12]. Available from: https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

[20] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Vydání: první. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-807-6230-682.

[21] What Is the Difference Between a Threat, a Vulnerability, and a Risk?. In: *Sectigo* [online]. 2020 [visited on 2024-05-12]. Available from: https://www.sectigo.com/resource-library/what-is-the-difference-between-a-threat-a-vulnerability-and-a-risk

[22] Hrozba. In: *Ministestvo vnitra České Repubilky* [online]. 2003 [visited on 2024-05-12]. Available from: https://www.mvcr.cz/clanek/hrozba

[23] Threat, vulnerability, risk – commonly mixed up terms. In: *Threat Analysis Group* [online]. https://www.threatanalysis.com [visited on 2024-05-12]. Available from: https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

[24] What is Information Security Compliance and why is it important. In: *Sprinto* [online]. 2024 [visited on 2024-05-12]. Available from: https://sprinto.com/blog/information-security-compliance/

[25] What is information security compliance?. In: *Onetrust* [online]. 2023 [visited on 2024-05-12]. Available from: https://www.onetrust.com/blog/what-is-information-security-compliance/

[26] 8 critical steps to successful risk management. In: *DataGuard* [online]. 2024 [visited on 2024-05-12]. Available from: https://www.dataguard.co.uk/blog/critical-steps-for-risk-management/

[27] ISO/IEC. *ISO/IEC 27001 Information security, cybersecurity and privacy protection*. 3rd. 2022.

[28] Jaké změny přinesla nová norma ISO 27002:2022? Jaký má vliv na certifikaci systémů informační bezpečnosti? Jaký je rozdíl mezi ISO/IEC 27001 a ISO/IEC 27002?. In: *EUCERT* [online]. 2022 [visited on 2024-05-12]. Available from: https://eucert.cz/jake-zmeny-prinesla-nova-norma-iso-270022022-jaky-ma-vliv-na-certifikaci-systemu-informacni-bezpecnosti-jaky-je-rozdil-mezi-iso-iec 27001-a-iso-iec-27002/

[29] ISO/IEC. *ISO/IEC 27002 Information security, cybersecurity and privacy protection*. 3rd. 2022.

[30] ISO/IEC. *ISO/IEC 27005 Information security, cybersecurity and privacy protection*. 4th. 2022.

[31] Nová směrnice EU o kybernetické bezpečnosti "NIS 2". In: *NÚKIB* [online]. [visited on 2024-05-12]. Available from: https://osveta.nukib.gov.cz/course/view.php?id=145

[32] Směrnice NIS2 a nový Zákon o kybernetické bezpečnosti. In: *Pwc* [online]. https://www.pwc.com [visited on 2024-05-12]. Available from: https://www.pwc.com/cz/cs/temata/smernice-nis2.html

[33] About TISAX. In: *ENX* [online]. [visited on 2024-05-12]. Available from: https://enx.com/en-US/TISAX/

[34] CO JE TO TISAX®, PRO KOHO JE DŮLEŽITÝ A JAK SE PŘIPRAVIT NA CERTIFIKACI?. In: *Bureau Veritas* [online]. 2021 [visited on 2024-05-12]. Available from: https://www.bureauveritas.cz/newsroom/co-je-tisaxr-pro-koho-je-dulezity-jak-se-pripravit-na-certifikaci

[35] Posouzení zabezpečení výměny důvěrných informací: Trusted Information Security Assessment Exchange - TISAX. In: *Česká společnost pro jakost* [online]. 2021 [visited on 2024-05-12]. Available from:

https://www.csq.cz/infocentrum/odborne-clanky/detail/posouzeni-zabezpeceni-vymeny-duvernych-informaci-trusted-information-security-assessment-exchange-tisax

[36] *TISAX Participant Handbook* [online]. 2.7.2. ENX Association, 2024 [visited on 2024-05-12]. Available from: https://www.enx.com/handbook/tisax-participant-handbook.html

[37] SEDLÁK, Petr Ing. *Řízení dodavatelů* [PDF]. VUT, 2022.

[38] SEDLÁK, Petr Ing. *Útoky na dodavatelský řetězec* [PDF]. 2021.

[39] Requirements for cybersecurity in agricultural communication networks. In: *ResearchGate* [online]. 2020 [visited on 2024-05-12]. Available from: https://www.researchgate.net/figure/The-Confidentiality-Integrity-Availability-CIA-triad_fig1_346192126

GLOSSARY

Acronym	Meaning
AI	Artificial Intelligence
AL	Assessment Level
ALE	Annualized Loss Expectancy
ARO	Annual Rate of Occurrence
CAP	Corrective Action Plan
CCTA	Central Computer and Telecommunications Agency (UK)
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, Availability
Coll.	Collection of Law
CRAMM	CCTA Risk Analysis and Management Method
ČSN	Česká státní norma (Czech National Standards)
DUNS	Data Universal Numbering System
e.g.	Exempli Gratia (Latin for "for example")
EN	European Norm
ENX	European Network Exchange
ERP	Enterprise Resource Planning
etc.	Et Cetera (Latin for "and other things")
EU	European Union
GmbH	Gesellschaft mit beschränkter Haftung (German for "Company with limited liability")
IATF	International Automotive Task Force
IEC	International Electrotechnical Commission
i.e.	Id Est (Latin for "that is" or "in other words")

IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KPI	Key Performance Indicator
MES	Manufacturing Execution System
MLR	Monetary Loss Reduction
MR	Mitigation Ratio
NA or N/A	Not Applicable
NDA	Non-Disclosure Agreement
NIS	National Institute of Standards
NIST	National Institute of Standards and Technology
No.	Number
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost (Czech National Cyber and Information Security Agency)
OEM	Original Equipment Manufacturer
PC	Personal Computer
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PIN	Personal Identification Number
ROSI	Return on Security Investment
SAE	Society of Automotive Engineers
SLA	Service-Level Agreement
SLE	Single Loss Expectancy
TISAX	Trusted Information Security Assessment Exchange
TPV	Third-Party Verification
TUV	Technischer Überwachungsverein (Technical Inspection Association - Northern

NORD	Germany)
TUV SUD	Technischer Überwachungsverein (Technical Inspection Association - Southern Germany)
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)
VDA ISA	VDA Information Security Assessment
VPN	Virtual Private Network

LIST OF TABLES

LIST OF FIGURES