White Paper "Information Security Risk Management"

Protection objectives: confidentiality, integrity, availability

Version:	1.1
Date:	March 3, 2021
Classification:	public

VDA | Verband der Automobilindustrie

Content

Introduction and Motivation

Business decisions are associated with both opportunities and risks. The assessment of which risks can be taken in a controlled manner for a company and for the company's assets must be systematically controlled. This process is called risk management.

Risk management enables companies to establish appropriate measures for the protection of corporate assets while weighing the opportunities and risks. An effective risk management system is therefore a control instrument for the company´s management and thus makes a significant contribution to the success of the company.

Risk management is an essential component of information security and forms the backbone of every effective information security management system (ISMS). Several laws (e.g. AktG, EU-DSGVO, IT security law) as well as common standards and best practices (e.g. ISO/IEC 27001, VDA ISA) require an established risk management.

The objective of this White Paper is to inform companies in the automotive industry with regard to risk-oriented information security management and to enable those to establish an effective information security risk management (ISRM). Information security risks exist in the creation and processing of information and relate to potential events that have a negative effect on the achievement of the information security protection objectives.

This White Paper focuses on the protection objectives confidentiality, integrity and availability. The terms “company” and “organization” as well as “information security risks” and “threats” are used synonymously in this document.

The explanations in this White Paper are based on the risk management standards ISO 31000 and ISO/IEC 27005, but additionally take into account specific requirements of the automotive industry.

Topical Integration in the Context of TISAX and VDA ISA

In 2017, the German Association of the Automotive Industry (VDA) has defined a uniform methodology for determining the information security level of an organization. The title of this methodology is TISAX (Trusted Information Security Assessment Exchange).

TISAX is based on the VDA's catalogue of requirements - the Information security assessment catalogue (“VDA ISA”). This catalogue contains control questions for determining the level of information security.

The requirements associated with the control questions were determined by a risk assessment carried out by the VDA Working Group on Information Security and are to be considered as minimum requirements for the protection of information processed during collaboration within the automotive industry.

In addition, the VDA ISA (current version 5.0) contains a specific control question on information security risk management (1.4.1):

"To what extent are information security risks managed?"

"The objective of information security risk management is the early identification, evaluation and treatment of risks in order to achieve the protection objectives of information security. It thus enables the organization to establish appropriate measures to protect the assets of the organization while weighing the opportunities and risks. It is advisable to make the organization’s information security risk management as simple as possible in order to operate effectively and efficiently. “

Listing 1: Control question and its objective according to VDA ISA

The following recommendations are intended to help companies to effectively implement the requirements arising from this control issue.

In the following two examples are attached to each of the process steps for illustration purposes. These are carried along throughout the entire process.

Definitions of Terms

Information Assets

Information assets represent company assets, processes or information worthy of protection. This information can be in physical (e.g. documents, prototypes) and/or digital form (e.g. as a file or in databases). The White Paper is especially dedicated to information in the automotive industry, e.g. design and construction data, development know-how or logistics information.

Threat

A threat is a circumstance or event that can impair the protection objectives of information security. The cause of a threat can originate inside or outside a company and may be intentional or unintentional.

Vulnerability

A vulnerability is a security relevant gap in processes, systems and/or organizations (e.g. employees). A vulnerability can lead to a threat becoming effective and causing damage.

Probability of Occurrence

The probability of occurrence is an estimate of the frequency with which a threat exploits a vulnerability.

Damage

Damage is caused by the occurrence of a threat by exploiting a vulnerability. This means a negative impact on the organization.

Risk

A risk describes the combination of threat and vulnerability, evaluated in terms of probability of occurrence and potential damage. The occurrence of a risk can lead to a negative deviation from operational or strategic objectives.

Organizational Framework Conditions

Definition of the Scope of Application

The risk management of information security is based on the scope of the ISMS.

Roles and Responsibilities

Different tasks, competencies and responsibilities are required for risk assessment and management. These are typically represented in roles. In principle, and especially in very small organizations, several roles can be performed by the same person. When combining several roles to one person, it should be noted that conflicts of interest may arise. These should be taken into account.

Risk Manager

The risk manager controls the risk management in the company and "keeps the overview" of the risks. He[1] consolidates the individual risks and reports them to the organization's management. He defines processes, methods, tools / templates and is responsible for the quality assurance of reported risks.

Risk Owners

The risk owner is responsible for assessing and handling the risks assigned to him. The risk owner must therefore be determined at a hierarchical level within the organization that is empowered to make appropriate decisions in dealing with those risks. In practice, the risk owner usually works in a “business department“ and is the information owner. To assess and deal with risks, the risk owner should draw on professional expertise from the business. The risk owner can delegate the implementation of risk assessment and handling, but never the responsibility.

All Employees and Third Parties

Any employee or third party who has access to information or to the organization's IT systems is responsible for identifying threats that may jeopardize the information security objectives and communicating them to the risk owner (if known), risk manager or security officer of the organization. Risk management essentially consists of the steps risk assessment, risk treatment and monitoring.

[1] In this White Paper the male gender is used only for convenience, but refers to all genders equally.

Risk Assessment

This chapter explains how the requirements of VDA ISA control question 1.4.1 can be implemented with regard to the first step - risk assessment.

+ *Risk assessments are carried out both regularly and on an ad hoc basis*

+ *If the environment changes (e.g. organizational structure, location, change of rules and regulations), a prompt reassessment is carried out*

+ *Information security risks are assessed according to the probability of occurrence and potential damage*

+ *A procedure exists for identifying, assessing and dealing with information security risks within the organization*

+ *Information security risks are documented*

+ *Each information security risk is assigned to a responsible person (risk owner). This person is responsible for the assessment and handling of information security risks.*

Listing 2: Measures according to VDA ISA for risk assessment

In addition to the systematic recording of risks as part of a regular process, it is also necessary that risks identified at short notice are considered in risk management and documented as required.

The result of the risk assessment is an overview ("risk register") of all identified risks, the clustering into "very high", "high", "medium" and "low" risks and the allocation of risks to the risk owners. This overview is the basis for the next step - risk treatment.

The sub-steps for identifying, analyzing and assessing risks are explained in the following and can be seen as a process description, supplemented by the respective responsibilities for the individual steps.

The risk assessment consists of the following activities:

1) Risk identification
2) Risk analysis (and evaluation)

Risk Identification

The purpose of risk identification is to systematically record the risks affecting an organization. Possible tools for identifying risks are workshops (with technical experts) or assessments (e.g. a TISAX self-assessment using the VDA ISA).

The requirements described in the VDA ISA already represent risk-reducing measures (if effectively implemented) and reflect an accepted level of risk by the members of the VDA. A TISAX assessment is therefore well suited to identify possible deviations from the requirements and thus potential vulnerabilities in the organization.

The following aspects should be considered in the context of risk identification:

- information assets to be protected
- relevant threats
- potential weaknesses/vulnerabilities

1) Starting point: identification of the information assets to be protected

Possible risks should be recorded based on the identified critical information assets and assigned to the respective responsible persons (VDA ISA control question 1.3.1). In accordance with control question 1.3.2, the identified information assets are then categorized during the process of information classification with regard to their respective protection requirements (see VDA "White Paper "Harmonization of Classification Levels").

Examples:

- *Information asset 1: Immobilizer-relevant data transmitted from an automobile manufacturer to a supplier - very high protection requirement.*
- *Information asset 2: Research and development information in physical and digital form - high protection requirements.*

2) Identification of relevant threats

To identify threats, opinions of internal experts should be obtained, experience from past information security incidents or information from IT security companies or authorities should be taken into account. Standardized threat catalogs (e.g. “Elementary threats” in the IT-Grundschutz Compendium of the German Federal Office for Information Security (BSI) or Annex of ISO/IEC 27005) can be used to support this process.

Examples:

- *Threat 1: Attack by hackers*
- *Threat 2: Unauthorized access to development offices with criminal intent*

3) Identification of potential vulnerabilities

The third aspect of risk identification is the identification of potential vulnerabilities.

In control question 5.2.6, the VDA ISA requires the timely sourcing of information (e.g. information from IT security companies) regarding potential vulnerabilities and, in addition, in 5.2.7, the testing of IT systems for vulnerabilities. In addition, the opinion of internal technical experts should be obtained or taken into account in order to identify concrete potential vulnerabilities (depending on the information asset).

Examples:

- *Vulnerability 1: Lack of security patches in IT systems*
- *Vulnerability 2: Lack of encryption of stored data*
- *Vulnerability 3: Issued access authorizations are not regularly checked and are not automatically withdrawn*

Finally, the results of the individual steps of risk identification are combined. These results can be presented in the form of damage/risk scenarios.

Examples:

- *Risk scenario 1: An attack by hackers (Threat 1) on IT systems with missing security patches (vulnerability 1) can steal immobilizer-relevant data (information asset 1). The damage occurs because the data is not stored in encrypted form (vulnerability 2).*

- *Risk scenario 2: Unauthorized access to the development offices (threat 2) can lead to the theft of research and development information in physical and digital form (information asset 2), as authorizations once granted are not regularly checked or automatically revoked (vulnerability 3), e.g. when employees leave the company.*

The risks described in this way form the result of the risk identification process and represent the input for the risk analysis.

Risk Analysis

During risk analysis, the risks identified in risk identification are further examined. The objective is to assess the existing risk in the form of risk classes. For example, the calculation can be done as follows:

Risk class = probability of occurrence x potential damage

In a pragmatic way, the potential damage is taken directly from the information classification according to the protection classes defined in the VDA ISA ("normal", "high" and "very high"), supplemented by the protection class "low" (recommendation of the BSI).

The probability of occurrence indicates how likely the vulnerability will be exploited. Again, a four-step scheme (e.g. "unlikely", "possible", "likely" and "very likely") can be used.

With regard to the probabilities of occurrence, the use of relative frequencies of occurrence in relation to years has become common practice:

Probability of occurrence	Frequency of occurrence	Asset
most likely	Annually or more frequently	100%
probably	About every 2 years	50%
Possible	About every 5 years	20%
unlikely	About every 10 years	10%

Table 1: Examples of the probabilities of occurrence

Risk Evaluation

The risk evaluation enables the identified risks to be weighted and thus a risk-oriented approach: Risks threatening the continued existence of the company require different treatment and control measures than insignificant risks. In the course of the evaluation, all identified risks are analyzed and their probability of occurrence and extent of damage are assessed.

The combination probability of occurrence and protection class results in a 4 x 4 matrix from which the resulting risk class can be taken. The rating of the individual fields as "low", "medium", "high", "very high" and their coloring depends on the individual organization and its willingness to take risks ("risk appetite").

Protection class / Probability of occurrence	low	normal	high	very high
most likely	low	medium	high	very high
probably	low	medium	high	high
possible	low	low	medium	medium
unlikely	low	low	low	low

Table 2: Example of a 4 x 4 risk matrix (basis: BSI)

The classification of the risk in the corresponding risk class ("low", "medium", "high" or "very high") concludes the risk assessment. The risk assessment represents a conscious decision process by the risk owner.

The results of identification, analysis and evaluation of risks are documented in the risk register with the risks prioritized according to risk classes. Subsequently, it must be decided how the risks are to be dealt with. This risk treatment is documented in the risk treatment plan.

Examples

- *Risk scenario 1: The probability of an attack on IT systems with missing security patches is assessed as "very probable" by technical experts. A "very high" need for protection has already been identified in the information classification for the immobilizer-relevant data, so the risk category is to be assessed as "very high".*
- *Risk scenario 2: The probability of unauthorized access to development offices was assessed as "probable". Access to the offices is via a key card reader controlled door or a key/lock cylinder. Evaluations have shown that several employees, who have already left the company, still have access authorizations and the whereabouts of two keys could not be clarified. For research and development information in physical and digital form, a "high" need for protection was identified in the information classification; therefore the risk class is to be rated as "high".*

As the risk class of risk scenario 1 ("very high") is higher than the risk class of risk scenario 2 ("high"), risk scenario 1 has to be prioritized with regards to risk treatment. The prioritized risks are entered in the risk register.

Risk scenario	Risk class	Prio	Risk owners
Theft of immobilizer-relevant data	very high	1	Person A
Unauthorized access to development offices	high	2	Person B

Table 3: Example representation of a risk register

A risk owner must be determined and documented for each risk. This is usually the information owner.

Risk Treatment

This chapter explains how the requirements of the VDA ISA control question 1.4.1 can be implemented with regard to the second process - risk treatment.

+ Criteria for the assessment and treatment as well as acceptance of information security risks are available.
+ Measures for dealing with information security risks and their responsible parties are defined and documented.
- A measure plan or status overview of the measure implementation exists.

Listing 3: Measures in accordance with VDA ISA for risk treatment

Risks must be adequately addressed according to their individual assessment result. The basis for this is the risk register.

There are different ways of dealing with risks. A basic distinction is made between four types of risk treatment:

- Risk Avoidance
- Risk Mitigation
- Risk Transfer
- Risk Acceptance

In order to achieve an acceptable residual risk level (risk class after effective treatment), a risk can be treated in one or more ways. The risk owner decides on the type of risk treatment.

Risk Avoidance

The risk is eliminated or completely avoided if activities or processes that cause the risk (e.g. a project to establish a new production site, a new product variant or performance of business trips to a certain region) are completely stopped or eliminated. This implies that a threat no longer leads to a risk.

Risk Mitigation

Risk mitigation is the most common type of risk treatment. A mitigation of risk can, for example, be achieved by one or more complementary measures that counteract the risk. In this case, the probability of occurrence and/or the extent of damage is reduced by security measures. Risk-reducing measures can be of a technical or organizational/process-related nature (e.g. implementation of security training, restructuring of processes/procedures, construction measures).

Risk Transfer

In the case of a risk transfer, the potential loss is borne by another area of responsibility or another institution. This can be done, for example, by outsourcing or - as a prevention against financial risks - by taking out insurance (e.g. contingency insurance, cyber security insurance). Responsibility for the risk remains with the risk owner within the organization.

Risk Acceptance (Assumption)

In the context of risk acceptance, risks are accepted in their present risk class.

Risk acceptance can be a suitable approach if the business opportunities are greater than the risks or if measures are lacking that can reduce the risk in a financial efficient manner. Violations of laws (e.g. with possible consequences under criminal or civil law) must generally not be accepted by means of risk acceptance.

Risks may only be accepted by risk owners whose financial responsibility at least corresponds to the respective risk category.

Since risk acceptance can have consequences beyond the area under consideration, organization-wide regulations and requirements (e.g. thresholds for the acceptance of risks, materiality limits) must be defined. Among other things, this is intended to prevent a risk owner from accepting a risk that could become critical for the entire organization.

In this case, the management of the organization (e.g. executive management/board of directors) must be informed and involved in the decision or ideally take the decision themselves.

The acceptance of a risk, whose risk class exceeds a defined threshold, must be documented in the form of a risk acceptance form.

For risks resulting from a deviation from the agreed requirements of the automotive industry (VDA ISA), risk acceptance by an organization is not possible.

Risk Treatment Plan

The handling of each individual information security risk is defined in a Risk Treatment Plan. It specifies how the respective assessed risk is to be handled, who is responsible for implementation and by when implementation is to take place.

Examples:

- *Risk scenario 1: The risk owner decides to reduce the risk by patching all affected IT systems (measure 1) and installing encryption mechanisms on relevant IT systems and data carriers (measure 2) used for processing immobilizer-relevant data.*
- *Risk scenario 2: The risk owner would gladly accept the risk and would not take any further measures to deal with the risk. However, since customer data could be affected on the premises of research and development within the scope of projects, risk acceptance is not possible and the risk must be reduced. The risk owner then decides to replace the locking cylinder and all keys (Measure 3) and to withdraw all outdated access authorizations (Measure 4).*

Responsibilities for all measures are defined and time frames for implementation are agreed. The measures are documented in the risk treatment plan.

Risk scenario	Risk class	Risk owners	Measure	Person responsible, Implementation period
Theft of immobilizer-relevant data	very high	Person A	Patching the IT systems	Person 1 2 weeks
Theft of immobilizer-relevant data	very high	Person A	Encryption of the data	Person 2 2 weeks
Unauthorized access to development offices	high	Person B	Exchange of key and locking cylinder	Person 3 4 weeks
Unauthorized access to development offices	high	Person B	Withdrawal of obsolete access authorizations	Person 4 2 weeks

Table 4: Example of a risk treatment plan

Risk Monitoring and Communication

Follow-up of risks and implementation of treatment plans

A functioning risk management requires the effective handling of risks.

For this reason, a process must be established to track measures to be implemented and provide opportunities for countermeasures in the event of delay or failure to address risks. This includes at least the following points:

- Management and control of treatment plans as uniformly and centrally as possible (e.g. via database or collaboration platform)
- Define clear responsibilities (who is responsible for the implementation of which measure in which period)
- Regular tracking of progress
- Defined communication and escalation paths
- Consequences of non-implementation (e.g. escalation to the next higher management level, possibly risk acceptance)
- Measures tracking as integral part of internal and external audits

This is where the risk awareness of the management comes into effect. If treatment plans are not implemented properly, management must react as soon as it becomes aware of the problem.

Documentation and Reporting

The approaches and measures described in this White Paper (e.g. roles and responsibilities, scope, risk management process) must be documented. In this context, it may be useful to connect to or merge with any existing risk management approaches or systems (e.g. environmental management, quality management, compliance). The main results of risk management should be reported regularly to the organization's management.

Examples

- *Risk scenario 1: Measures 1 (patching) and 2 (encryption) are reported back in time by the persons responsible for implementation. The risk class is reduced to "low" (probability of occurrence "unlikely" and protection class "very high") due to the effectiveness of the implemented measures.*
- *Risk scenario 2: Measure 4 (withdrawal of old access authorizations) is reported back in time by the person responsible for implementation. Measure 3 (replacement of the locking cylinder and all keys) is not implemented on time. After an escalation by the risk manager via the organizational management, the measure is completed with an extended implementation period. After implementation of all measures, the risk class is reduced to "low" (probability of occurrence "unlikely" and protection class "high"). The measures will continue to be monitored.*

Risk scenario	Risk class	Risk Owner	Description
Theft of immobilizer-relevant data	low	Person A	Measures 1 and 2 were implemented on xx.xx.xxxx. The risk class is thus reduced to "low
Unauthorized access to Development offices	low	Person B	Measure 4 was implemented on xx.xx.xxxx. Implementation period Measure 3 extended after release/risk acceptance by organizational management until xx.xx.xxxx

Table 5: Example of the adjusted risk register

Conclusion and recommendation

This White Paper is intended to support organizations in preparing or conducting a TISAX assessment to meet the requirements of the VDA ISA control question 1.4.1. It´s content it is to be considered as implementation recommendations, not as a mandatory requirements.

The ISRM of an organization should be designed as simple as possible in order to operate effectively and efficiently. The employees of an organization also play a decisive role here. They must know how to identify and report risks.

It is also important that the ISRM process is geared to the specific needs of the respective organization and is integrated into any existing risk management system, even if most of the risks identified in information security do not exceed the threshold assets of corporate risk management.

The definition of clear responsibilities is another crucial success factor of ISRM. For each documented risk, one risk owner should be determined so that no discussions arise regarding responsibilities in risk handling. In conclusion the correct and controlled treatment of information security risks is important in order to limit the resulting effects of an occurrence of a risk.

The VDA recommends its members to use this White Paper as a guide.

List of Authors

Name	Company	E-mail address
Jens Frölich	AUDI AG	jens.froelich@audi.de
Thomas Donner	BMW AG	thomas.donner@bmwgroup.com
Oliver Schmitt	Robert Bosch GmbH	oliver.schmitt@de.bosch.com
Jürgen Rilling	Daimler AG	juergen.rilling@daimler.com
Thomas Harich	MAHLE Ltd.	thomas.harich@mahle.com
Matthias Teuscher	Rheinmetall AG	matthias.teuscher@de.rheinmetall.com
Burkhard Kesting	ZF Friedrichshafen AG	burkhard.kesting@zf.com

Document and Version History

Version	Date	Status, remarks
1.0	July 31, 2020	Final
1.1	March 3, 2021	Page 9: Change of *threat catalog* in *“Elementary threats” in the IT-Grundschutz Compendium*