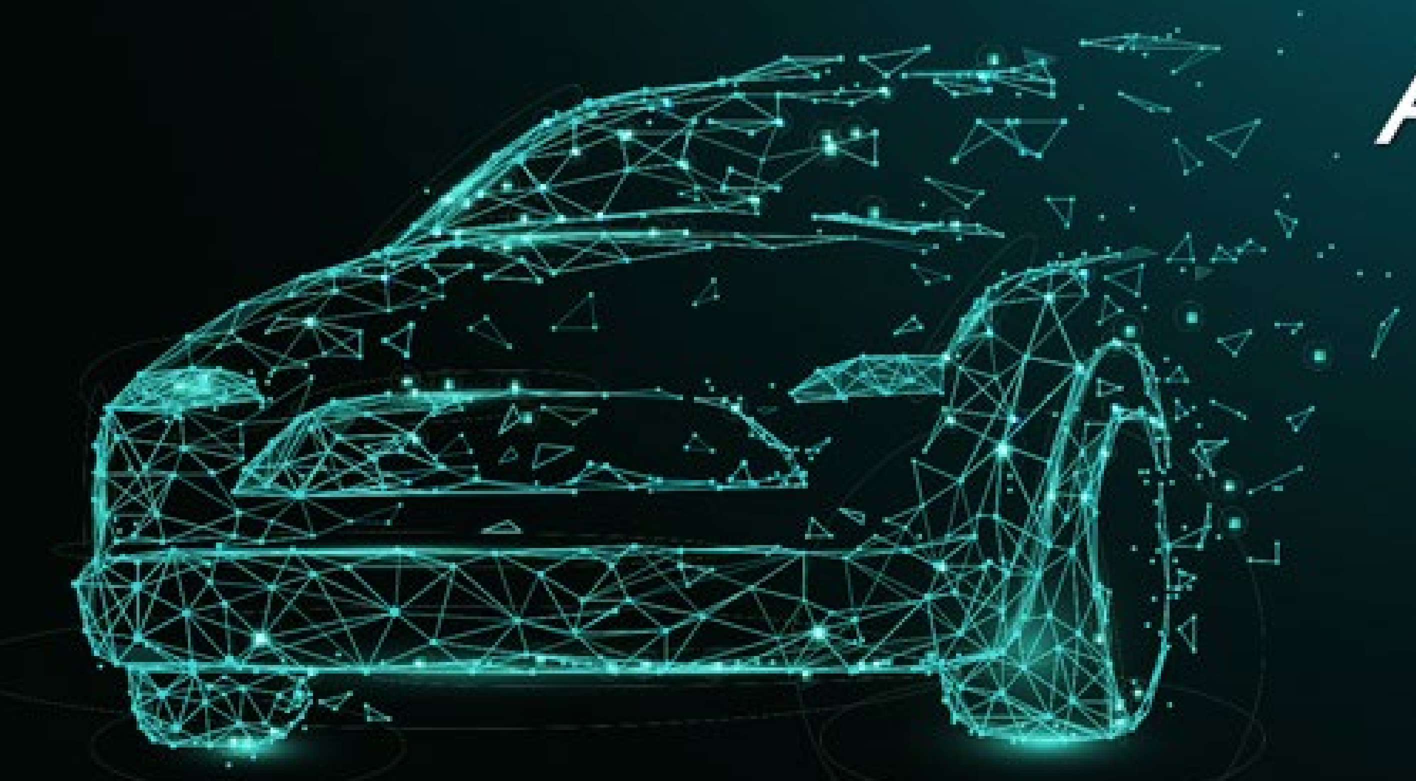
DEKRA

PERSEUS INFORMATION
SECURITY CONSULTING

Mastering TISAX®



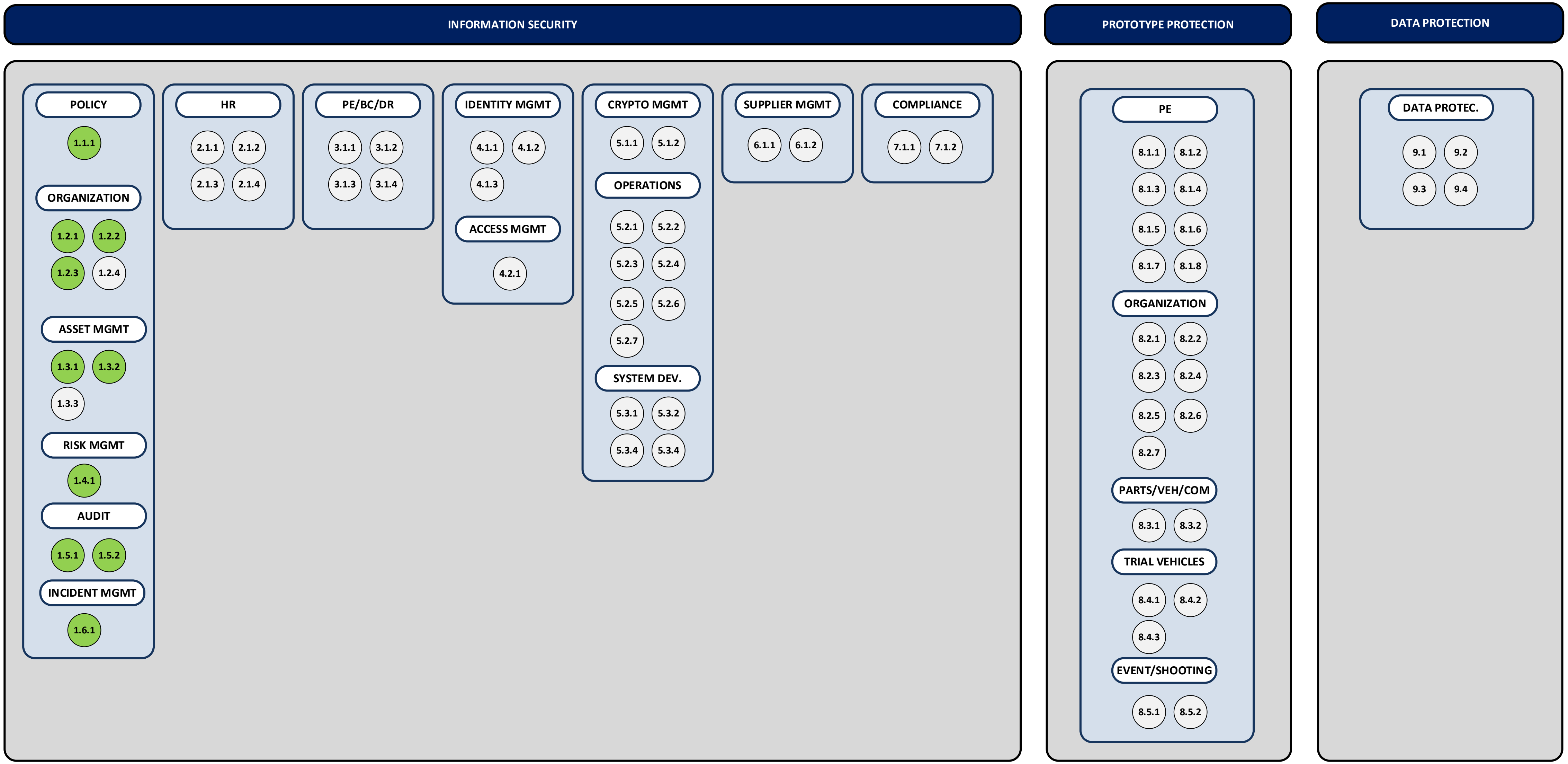
A Free Five-Part Webinar Series

May 15-19
12pm-1pm Eastern

PART TWO:

KEY PROCESSES

in an Information Security Management System



INFORMATION SECURITY

POLICY
1.1.1

ORGANIZATION
1.2.1 1.2.2 1.2.3 1.2.4

ASSET MGMT
1.3.1 1.3.2 1.3.3

RISK MGMT
1.4.1

AUDIT
1.5.1 1.5.2

INCIDENT MGMT
1.6.1

HR
2.1.1 2.1.2 2.1.3 2.1.4

PE/BC/DR
3.1.1 3.1.2 3.1.3 3.1.4

IDENTITY MGMT
4.1.1 4.1.2 4.1.3

ACCESS MGMT
4.2.1

CRYPTO MGMT
5.1.1 5.1.2

OPERATIONS
5.2.1 5.2.2 5.2.3 5.2.4 5.2.5 5.2.6 5.2.7

SYSTEM DEV.
5.3.1 5.3.2 5.3.4 5.3.4

SUPPLIER MGMT
6.1.1 6.1.2

COMPLIANCE
7.1.1 7.1.2

PROTOTYPE PROTECTION

PE
8.1.1 8.1.2 8.1.3 8.1.4 8.1.5 8.1.6 8.1.7 8.1.8

ORGANIZATION
8.2.1 8.2.2 8.2.3 8.2.4 8.2.5 8.2.6 8.2.7

PARTS/VEH/COM
8.3.1 8.3.2

TRIAL VEHICLES
8.4.1 8.4.2 8.4.3

EVENT/SHOOTING
8.5.1 8.5.2

DATA PROTECTION

DATA PROTEC.
9.1 9.2 9.3 9.4

PERSEUS INFORMATION
SECURITY CONSULTING

DEKRA

To what extent are information security policies available?

1.1.1

The organization needs at least one information security policy. This reflects the importance and significance of information security and is adapted to the organization. Additional policies may be appropriate depending on the size and structure of the organization.

- The requirements for information security have been determined and documented:
    - The requirements are adapted to the organization’s goals,
    - A policy is prepared and is released by the organization.
- The policy includes objectives and the significance of information security within the organization.
- The information security requirements based on the strategy of the organization, legislation and contracts are taken into account in the policy.
- The policy indicates consequences in case of non-conformance.
- Further relevant information security policies are prepared.
- Periodic review and, if required, revision of the policies are established.
- The policies are made available to employees in a suitable form (e.g. intranet).
- These policies (or extracts thereof) are provided to external business partners depending on the respective case.
- Employees and external business partners are informed of any changes relevant to them.

To what extent is information security managed within the organization?

1.2.1

Only if information security is part of the **strategic goals of an organization**, information security can be implemented in an organization in a sustainable manner. The information security management system **(ISMS) is a control mechanism used by the organization's management** to ensure that information security is the result of sustainable management rather than that of mere coincidence and individual effort.

- The scope of the ISMS (the organization managed by the ISMS) is defined.
- The organization's requirements for the ISMS are determined.
- The organizational management has commissioned and approved the ISMS.
- The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review).
- Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed VDA ISA catalog).
- The effectiveness of the ISMS is regularly reviewed by the management.

To what extent are information security responsibilities organized?

1.2.2

A successful ISMS requires clear responsibilities within the organization. All information security responsibilities should be defined and allocated.

- Responsibilities for information security within the organization are defined, documented and assigned.
- The responsible employees are defined and qualified for their task.
- The required resources are available.
- The contact persons are known within the organization and to relevant business partners.
- There is a definition and documentation of an adequate information security structure within the organization.
- An appropriate organizational separation of responsibilities should be established in order to avoid conflict of interests (separation of duties). (C, I, A)

To what extent are information security requirements taken into account in projects?

1.2.3

For project implementation, it is important to consider the information security requirements. This applies to projects within the organization **regardless of their type.** By appropriately establishing the information security process in the project management procedures of the organization, any overlooking of requirements is prevented.

- Projects are classified while taking into account the information security requirements.
- The procedure and criteria for the classification of projects are documented.
- During an early stage of the project, risk assessment is conducted based on the defined procedure and repeated in case of changes to the project.
- For identified information security risks, measures are derived and taken into account in the project.
- The measures thus derived are reviewed regularly during the project and reassessed in case of changes to the assessment criteria. (C, I, A)
- Projects can be classified as follows
  - CIAA (Confidentiality, Integrity, Availability, Authenticity)
  - CIA (Confidentiality, Integrity, Availability)

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent are information assets identified and recorded?

1.3.1

It is important for each organization to know the information constituting **its essential assets** (e.g. business secrets, critical business processes, know-how, patents). They are referred to as **information assets.** An inventory ensures that the organization obtains an overview of its information assets.

Moreover, it is important to know the **supporting assets** (e.g. IT systems, services/IT services, employees) processing these information assets.

- The information assets being of relevance to the organization are identified and recorded.
  - A person responsible for these information assets is assigned.
- The supporting assets processing the information assets are identified and recorded:
  - A person responsible for these supporting assets is assigned.
- A catalog of the relevant information assets exists:
  - The corresponding supporting assets are assigned to each relevant information asset,
  - The catalog is subject to regular review.

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

1.3.2

The objective of classifying information assets is the **consistent determination of their protection needs.** For this purpose, the value the information has for the organization is determined based on the protection goals of information security (confidentiality, integrity and availability) and classified according to a classification scheme. This enables the organization to implement **adequate protective measures**

- A consistent scheme for the classification of information assets with regard to the protection goal of confidentiality is available.
- Evaluation of the **identified information assets** is carried out according to the defined criteria and assigned to the existing classification scheme.
- Specifications for **the handling of supporting assets** (e.g. identification, correct handling, transport, storage, return, deletion/disposal) **depending on the classification of information assets** are in place and implemented.
- The protection goals of integrity and availability are taken into consideration.
- Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

PERSEUS INFORMATION
SECURITY CONSULTING

DEKRA

To what extent are information security risks managed?

1.4.1

Information security risk management aims at the timely detection, assessment and addressing of risks in order to achieve the protection goals of information security. It thus enables the organization to establish adequate measures for **protecting its information assets** under consideration of the associated prospects and risks. It is recommended to keep the information security risk management of an organization as simple as possible such as to enable its effective and efficient operation.

- Risk assessments are carried out both **at regular intervals and in response to events.**
- Information security risks are appropriately assessed (e.g**. probability of occurrence and potential damage**).
- Information security risks are **documented**.
- A responsible person (**risk owner**) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.
- **A procedure** is in place defining how to identify, assess and address information security risks within the organization.
- **Criteria** for the assessment and handling of information security risks exist.
- **Measures** for handling information security risks and the persons responsible for these are specified and documented:
    - A plan of measures or an overview of their state of implementation exists.
- In case of changes to the environment (e.g. organizational structure, location, changes to regulations), **reassessment** is carried out in a timely manner.

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

1.5.1

It is not sufficient to define information security requirements and to prepare and publish policies. It is important to regularly review their effectiveness.

- Observation of policies is verified throughout the organization.
- Information security policies and procedures are reviewed at regular intervals.
- Measures for correcting potential non-conformities (deviations) are initiated and pursued.
- Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals.
- The results of the conducted reviews are recorded and retained.
- A plan for content and framework conditions (time schedule, scope, controls) of the reviews to be conducted is provided.

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

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

1.5.2

As an essential control mechanism, assessing the effectiveness of the ISMS from merely an internal point of view is insufficient. Additionally, an independent and therefore objective assessment shall be obtained at regular intervals and in case of significant changes.

- Information security reviews are carried out by an independent and competent body at regular intervals and in case of significant changes.
- Measures for correcting potential deviations are initiated and pursued.
- The results of conducted reviews are documented and reported to the management of the organization.

PERSEUS INFORMATION
SECURITY CONSULTING

DEKRA

To what extent are information security events processed?

1.6.1

Organized processing of information security events aims at **limiting potential damage** and **preventing recurrence.**

- A definition of information security events and vulnerabilities exists.
- A **procedure for reporting and recording** information security events/vulnerabilities is defined and implemented.
- The following aspects are considered:
  - Reaction to information security events/vulnerabilities,
  - Report form and channel,
  - Processing body,
  - Feedback procedure
  - Indications regarding technical and organizational measures
- Procedures for **ensuring traceability** in case of information security events/vulnerabilities are established and documented.
- Information security events are assessed and documented in order to ensure traceability.
- Adequate reaction to information security events
- A strategy for an adequate reaction to events of information security violations, including **escalation procedures, remedial actions and communication to relevant internal and external bodies,** as well as a procedure for deciding whether a cybercriminal attack will be prosecuted.
- Information security events/vulnerabilities (problem management) are analyzed.
- Measures to prevent reoccurrence of similar events are defined and implemented.
- Requirements resulting from business relations (e.g. obligations of reporting to customers) are determined and implemented. (C, I, A)

Learn more

www.dekra.us/audit

www.perseusis.com

Dennis Chen
Director of Sales, DEKRA North America
dennis.chen@dekra.com

Deniz Kaya
CEO, Perseus
dkaya@perseusis.com

Bill Nelson
Director of Business Development, Perseus
bnelson@perseusis.com