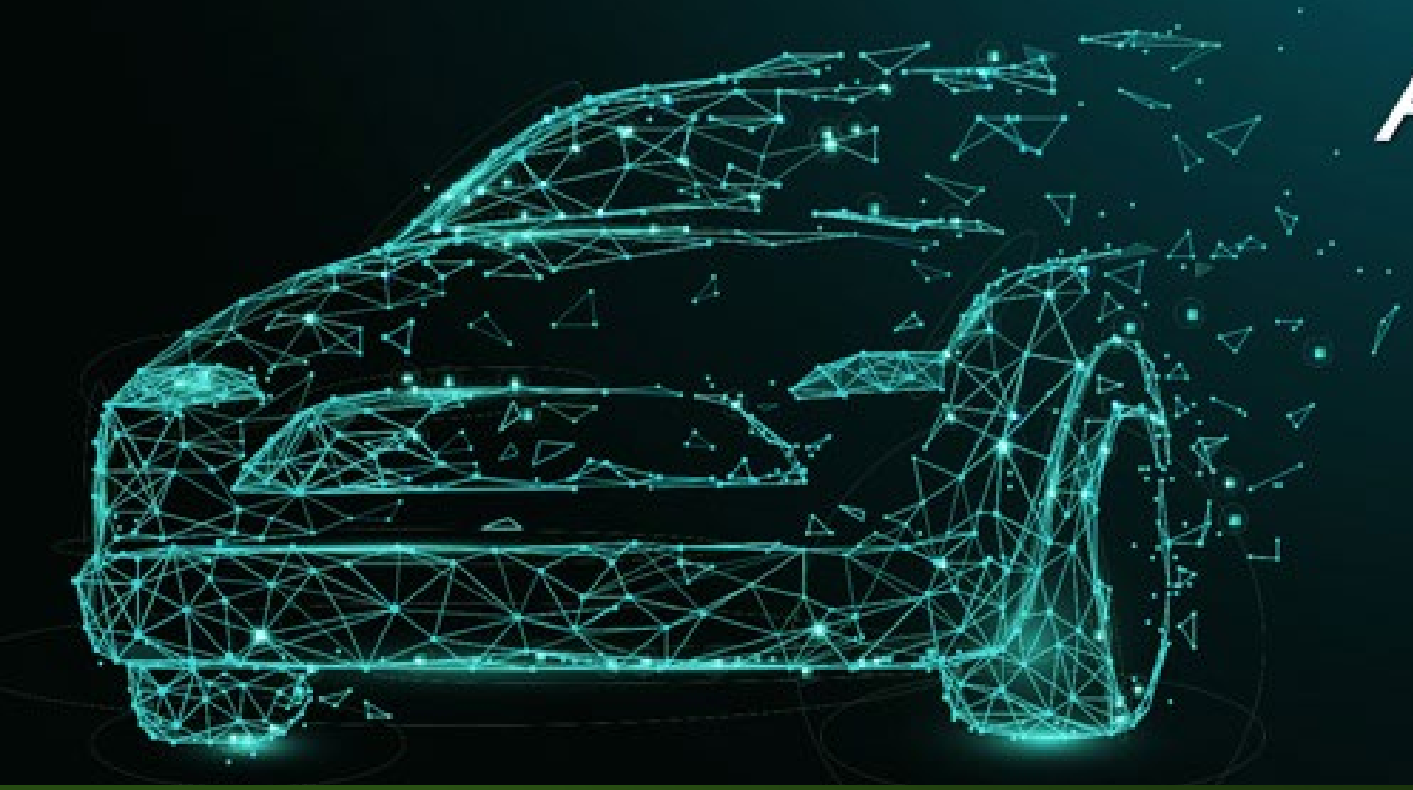
DEKRA

PERSEUS INFORMATION
SECURITY CONSULTING

Mastering TISAX®



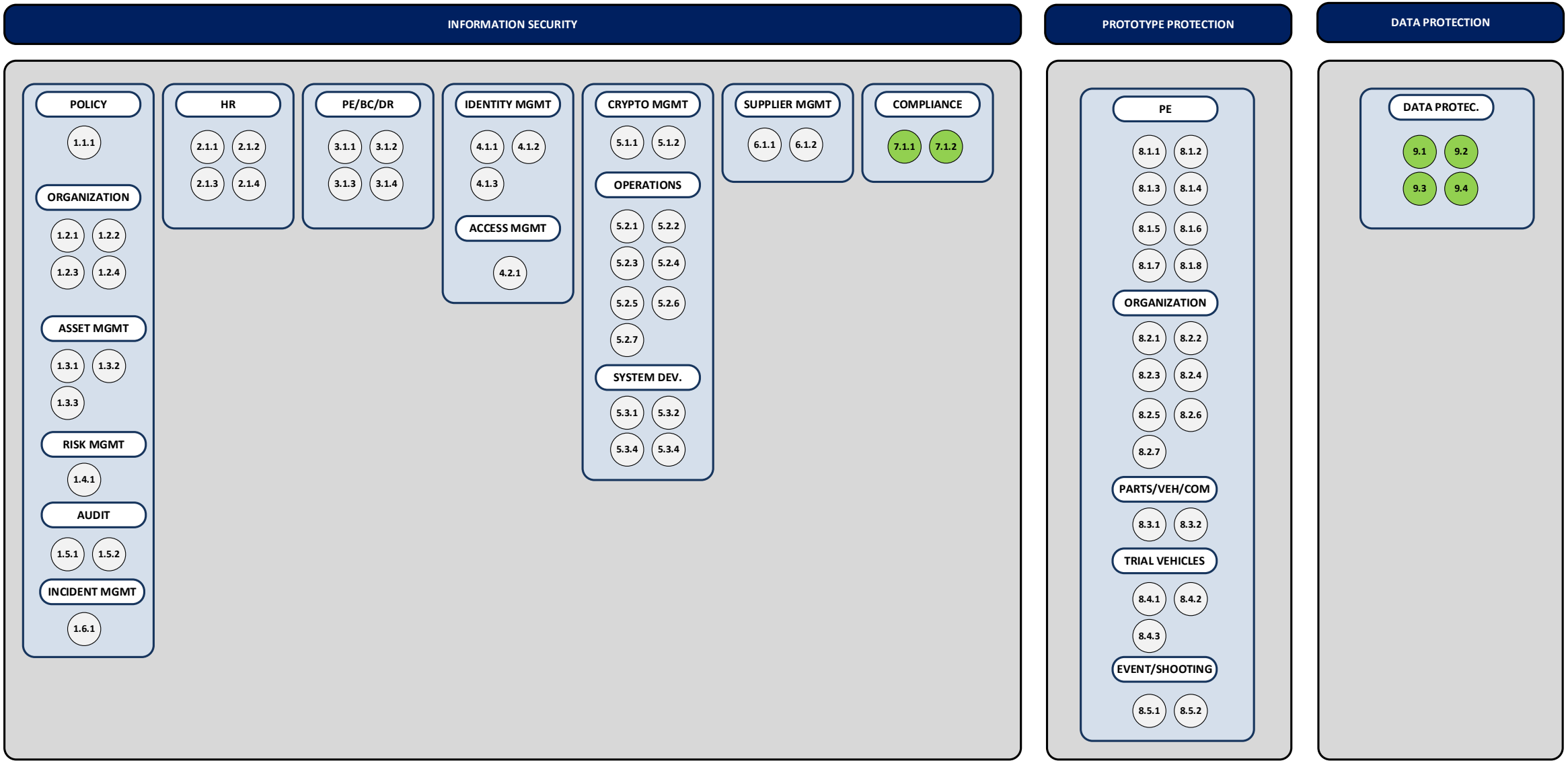
A Free Five-Part Webinar Series

May 15-19
12pm-1pm Eastern

PART FOUR:

LEGAL & COMPLIANCE CONSIDERATIONS FOR TISAX®

Data Privacy in the Automotive Supply Chain



PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

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

7.1.1

Non-compliance **with legal, regulatory, or contractual provisions** can create risks to the **information security of customers and of your organization**. Therefore, it is essential to ensure that these **provisions are known and observed**.

- Legal, regulatory and contractual requirements and specifications of relevance to information security are **regularly determined**.
- Policies regarding compliance with the requirements are **defined, implemented, and communicated** to the responsible persons.
- Measures for fulfilling the requirements regarding **intellectual property rights** and the use of **software protected by copyright** (acquisition and license management) are defined and implemented.
- **Staff awareness measures** with respect to compliance topics associated with information security are carried out regularly.
- The **integrity of records** in compliance with contractual, regulatory or legal obligations and business requirements are taken into account.

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is the protection of personal data considered when implementing information security?

Privacy and protection of personal data is taken into account in the implementation of information security as required by relevant national legislation and regulations, where applicable.

- Legal and contractual information security requirements regarding the **procedures in the processing of personal data** are determined.
- Regulations regarding the compliance with **legal and contractual requirements** for the protection of personal data are defined and known to the entrusted persons.
- Processes and procedures for the protection of personal data are taken into account in the information security management system.

7.1.2

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is the implementation of data protection organized?

- **Appointment of a data protection officer** where legally required, otherwise appointment of a person responsible for data protection
- Organizational implementation of data protection
  - Integration of the data protection officer into the **corporate structure**
  - Voluntary or obligatory appointment of a data protection officer
  - Full-time or part-time data protection officer
  - Internal or external data protection officer
  - Support of the data protection officer by directly assigned employees **(department "Data Protection")** depending on the company size
  - Support of the data protection officer by **data protection coordinators** in the company departments depending on the size of the company (e.g. Marketing, Sales, Human Resources, Logistics, Development, etc.)

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

Are organizational measures taken to ensure personally identifiable data is processed in compliance with legislation?

- Specification of data protection principles **(processing of personally identifiable data)** in a documented company-internal data protection strategy (e.g. **company-internal policy**).
- Implementation of **company-internal steering committees** or responsibilities - in collaboration with the data protection officer - addressing topics relevant to data protection.
- Implementation of a process which ensures the **involvement of the data protection officer** in any topics relevant to data protection (e.g. in the context of a data protection impact assessment).
- **Documentation of work processes** when processing personally identifiable data.
- Documentation of **statements and comments of the data protection officer** regarding data protection **law assessments.**
- Implementation of a process by means of which - in case a **subcontracting processor** is commissioned - the processor is contractually or otherwise legally obliged to comply with the same data protection requirements as specified by contract between the controller and the processor.
- Company-internal **work instructions or manuals** in specific task fields concerning the processing of personally identifiable data.

9.2

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

Are organizational measures taken to ensure personally identifiable data is processed in compliance with legislation? (cont'd)

- Employees' (and, if applicable, subcontractors') confidentiality obligation.
- Implementation of technical and organizational measures for supporting the controller in handling data subject rights as far as feasible and appropriate for processing.
- Implementation of **reporting processes** for immediately informing the customer, under consideration of any subcontractors, so the legal reporting deadlines for data protection incidents can be observed.
- Implementation of a process **for documenting data protection provisions**.
- **Documentation of subcontracting relationships** including contractual regulations with relevant subcontractors, where any right to inspect the contractual regulation is in any case limited to the subcontractor's obligations concerning data protection.
- Ability to implement **data clearing concepts**.
- Implementation of a procedure of **regularly checking, assessing, and evaluating TOMs.**

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

Are internal processes regularly checked to ensure they are carried out according to current data protection regulations?

- Demonstration of **regular checks and optimizations** of the data protection management system (e.g. certification).
- Measures for maintaining confidentiality and integrity **when transferring personally identifiable data**.
- Adequate protection mechanisms for **reducing unauthorized access** to personally identifiable data.
- **Obligatory training** of employees entrusted with the processing of personally identifiable data of the customer (e.g. classroom training, WBT).
- Ensuring implementation of contracts and provisions of the customer.

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is admissibility under data protection laws of the relevant processing procedures documented?

- **Documentation of essential tasks** regarding the processing of personally identifiable data in compliance with legal requirements.
- Supporting customers in conducting **data protection impact assessments** and documenting the results thereof.
- **Informing the customer** when detecting unlawful data processing, where applicable, under consideration of different national legislations.

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

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