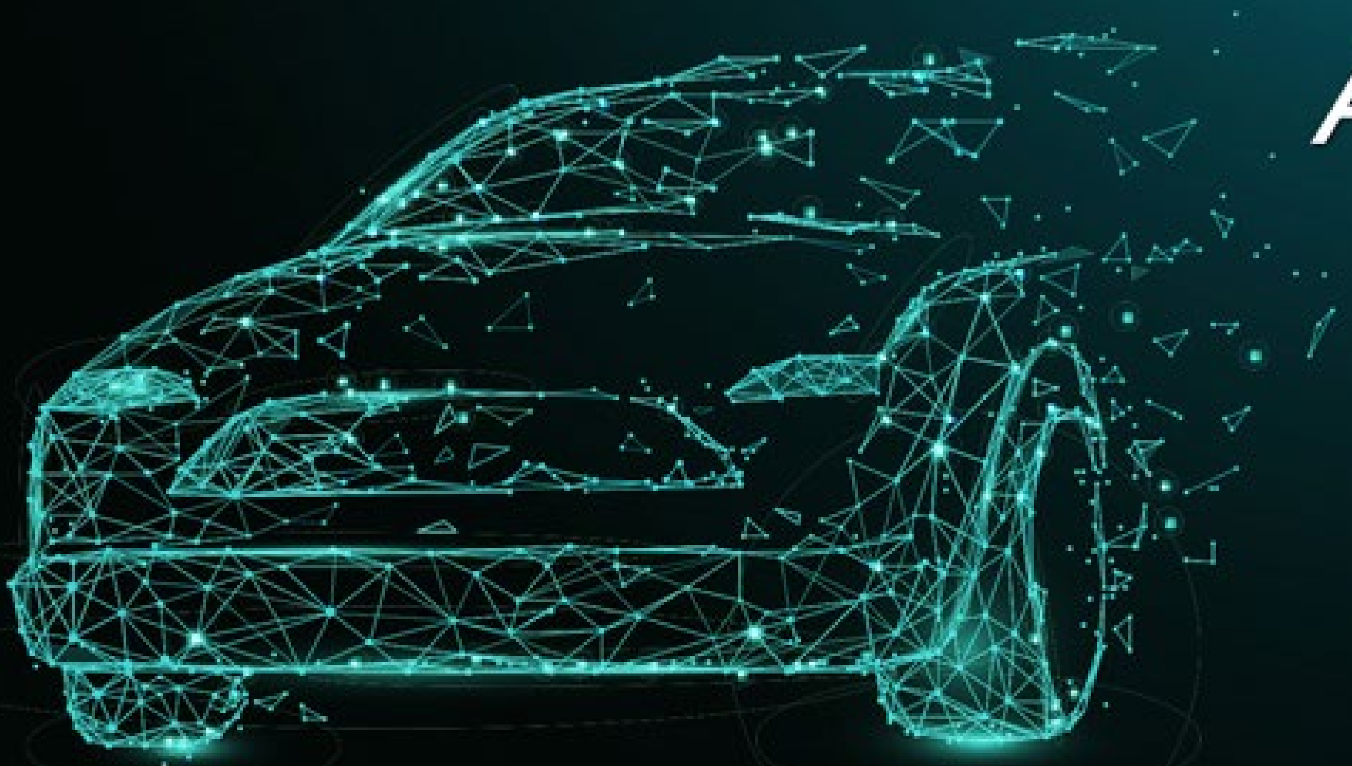
DEKRA

PERSEUS INFORMATION
SECURITY CONSULTING

Mastering TISAX®

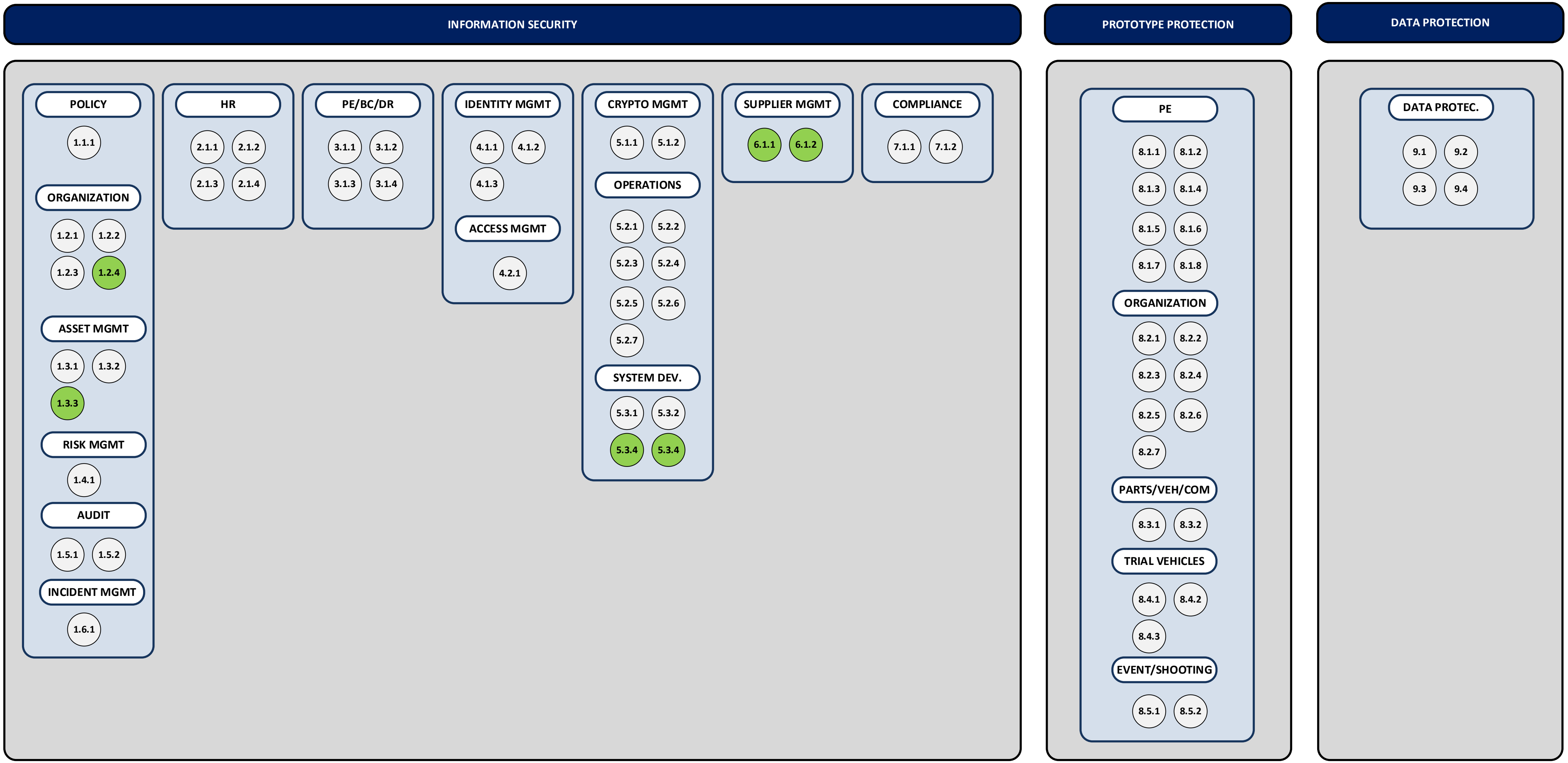
A Free Five-Part Webinar Series



May 15-19
12pm-1pm Eastern

PART THREE:
SECURING THE SUPPLY CHAIN

TISAX®-Compliant
Supplier Management



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 is information security ensured among suppliers and cooperation partners?

6.1.1

An appropriate level of information security is also maintained while collaborating with **cooperation partners and suppliers.**

- Suppliers and cooperation partners are subjected to a **risk assessment**
- An appropriate level of information security is ensured by **contractual agreements** with suppliers and cooperation partners.
- Where applicable, contractual agreements with customers are **passed on to suppliers and cooperation partners.**
- Compliance with contractual agreements is verified.
- Suppliers and cooperation partners are contractually obliged to also pass on any requirements regarding an appropriate level of information security also to their subcontractors.
- **Service reports** and documents by suppliers and cooperation partners are reviewed.
- **Evidence** that a supplier's level of information security is adequate for the protection needs of the information (e.g. certificate, attestation, audit) is provided.

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is non-disclosure regarding the exchange of information contractually agreed?

6.1.2

Non-disclosure agreements provide legal protection of an organization’s information, particularly where information is **exchanged beyond the boundaries of the organization**.

- The non-disclosure requirements are determined and fulfilled.
- Requirements and procedures for applying non-disclosure agreements are **known to all persons passing on information** in need of protection.
- Valid non-disclosure agreements are concluded **prior to forwarding sensitive information**.
- The requirements and procedures for applying non-disclosure agreements and handling sensitive information are regularly reviewed.
- Non-disclosure agreement templates are available and checked for legal applicability.
- Options of demonstrating compliance with specifications (e.g. review by an independent third party or **audit rights**) are defined.
- Non-disclosure agreements include the following information:
  - The persons/organizations involved,
  - The nature of the information covered by the agreement,
  - The subject of the agreement,
  - The validity period of the agreement (temporary or permanent),
  - The responsibilities of the obligor(s).
- Non-disclosure agreements include provisions for the handling of sensitive information **beyond the contractual relationship.**
- A process for **monitoring the validity period** of temporary non-disclosure agreements and initiating their extension in due time is defined and implemented.

To what extent are responsibilities between external service providers and the own organization defined?

1.2.4

It is important, that a common understanding of the **division of responsibilities** exists and that the implementation of all security requirements is ensured. Therefore, when using external IT service providers and services, the responsibilities regarding the implementation of information security measures are to be **defined and verifiably documented**.

- The concerned **services used are identified**.
- The **security requirements** relevant to the IT service are determined:
- The organization responsible for implementing the requirement is defined and aware of its responsibility.
- Mechanisms for **shared responsibilities** are specified and implemented.
- Organizations fulfil their respective responsibilities.
- In case of IT services, configuration has been conceived, implemented and documented based on the necessary security requirements.
- The responsible staff is adequately trained.

- **A list exists** indicating the concerned IT services and the respective responsible IT service providers. (C, I, A)
- The applicability of the VDA ISA controls has been verified and documented. (C, I, A)
- The service configuration is included in the regular security assessments. (C, I, A)
- **Proof** is provided that the IT service providers fulfil their responsibility. (C, I, A)
- Integration into local protective measures (such as secure authentication mechanisms) is established and documented. (C, I, A)

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is it ensured that only evaluated and approved external IT services are used?

1.3.3

Particularly in the case of external IT services that are relatively low cost or free, there is an increased risk that procurement and commissioning will be carried out **without appropriate consideration** of the information security requirements and that security therefore is not ensured.

- External IT services are not used without explicit assessment and implementation of the information security requirements:
  - A **risk assessment** of the external service is available,
  - **Legal, regulatory, and contractual requirements** are considered.
- The external IT services have been harmonized with the protection need of the **processed information assets.**
- Requirements regarding the procurement, commissioning and release associated with the use of external IT services are determined and fulfilled.
- A **procedure for release** in consideration of the protection need is established.
- External IT services and their **approval are documented.**
- It is **verified at regular intervals** that only approved external IT services are used.

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is information protected in shared external IT services?

5.3.4

Clear segregation between individual clients must be ensured to protect information in external IT services at all times and to prevent it from **being accessed by other organizations.**

- Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organizations.
- The provider’s segregation concept is documented and adapted to any changes. The following aspects are considered:
    - Separation of data, functions, applications, operating system, storage system and network,
    - Risk assessment for the operation of external software within the shared environment.

To what extent is the return and removal of information assets from external IT services regulated?

5.3.3

In order to ensure control over the information assets as the information owner, it is necessary that the information assets can be **safely removed or are returned**, if required, when terminating the IT service.

- A **procedure for returning and securely removing** information assets from any external IT service is defined and implemented.
- The fulfilment of the provider's responsibilities is **regulated by contract**.
- A description of the **termination process** is available and adapted to any changes.
- The responsibilities intended in the procedure are **documented and accepted by the provider.**

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