DEKRA

PERSEUS INFORMATION
SECURITY CONSULTING

Mastering TISAX®

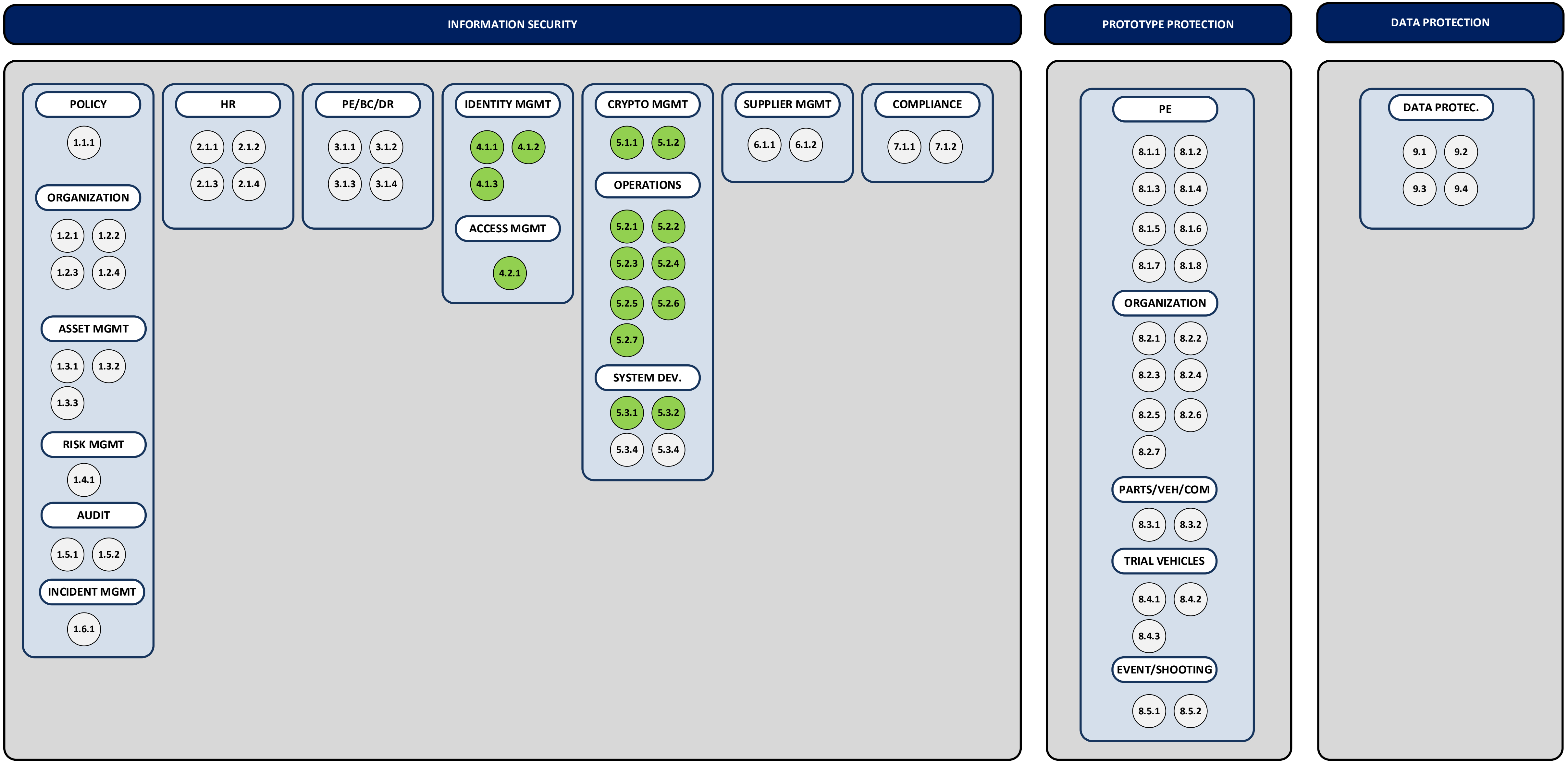
A Free Five-Part Webinar Series

May 15-19
12pm-1pm Eastern

PART FIVE:

TECHNICAL DOMAINS

Centralized vs Locally-Managed Technical Domains in TISAX®



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 the use of identification means managed?

4.1.1

To check the authorization for **both physical access and electronic access**, means of identification such as keys, visual IDs or cryptographic tokens are often used. The security features are only reliable if the use of such identification means is handled adequately.

- The requirements for the handling of identification means over the **entire lifecycle** are determined and fulfilled. The following aspects are considered:
    - Creation, transfer, return and destruction,
    - Validity periods,
    - Handling of loss
- Identification means can be produced under controlled conditions only.
- The **issuing** of identification means is **recorded**.
- The **returning** of identification means is **regulated**.
- The **validity** of identification means is limited to an appropriate period.
- A **concept for inactivation or invalidation** of identification means in case of loss is, as far as possible, **prepared and implemented**.

To what extent is the user access to network services, IT systems, and IT applications secured?

4.1.2

Only securely identified (authenticated) users are to gain access to IT systems. For this purpose, the identity of a user is securely determined by suitable procedures.

- The procedures for user authentication have been **selected based on a risk assessment** and potential attack scenarios have been considered (e.g. direct access via the internet)
- The procedures used for user authentication are according to the state of the art.
- The user authentication procedures are defined and applied based on the relevant business and security requirements.
- Superior procedures for the authentication of **privileged user accounts** (e.g. Privileged Access Management, two-factor authentication).
- Prior to gaining access to data of high protection needs, users are authenticated at least by means of strong passwords according to the state of the art.
- Depending on the risk assessment, authentication procedure and access control have been enhanced by supplementary measures (e.g. permanent access monitoring with respect to irregularities or use of strong authentication, automatic logout or disabling in case of inactivity).
- Prior to gaining **access to data of very high protection needs**, users are authenticated by means of strong authentication according to the state of the art (e.g. two-factor authentication).

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent are user accounts and login information securely managed and applied?

4.1.3

Access to information and IT systems is provided via validated user accounts **assigned to a person**.

It is important to protect login information and to ensure the **traceability of transactions and accesses**.

- Creation, modification, and deletion (lifecycle) of user accounts is performed.
- **Unique** and personalized user accounts are used.
- The **use of "collective accounts"** is regulated (e.g. restricted to cases where traceability of actions is dispensable).
- User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract).
- User accounts are **regularly reviewed.**
- Login info provided to users in a secure manner.
- The login information of a user account must be known only to the assigned user
- A basic user account template with minimum access rights is defined and used.
- Default accounts and passwords pre-configured by manufacturers are disabled
- User accounts are created or authorized by the responsible body, which is subject to an approval process (four-eyes principle).
- User accounts of service providers are disabled upon completion of their task.
- Deadlines are defined for disabling and deleting user accounts
- Use of default passwords is technically prevented.
- Where strong authentication is applied, the use of the medium (e.g. ownership factor) is secure.
- User accounts are reviewed at regular intervals, including user accounts in customers' IT systems.

To what extent are user accounts and login information securely managed and applied? (cont'd)

4.1.3

A policy for handling login information is defined and implemented. The following aspects are considered:

.

- No disclosure of login information to third parties – not even persons of authority – under consideration of legal restrictions
- No writing down or unencrypted storing of any login information,
- Immediate changing of login information whenever a potential compromise is suspected.
- No use of identical login information for business and non-business purposes
- Changing of temporary or initial login information following the first login
- Requirements for the quality of login information (e.g. length of password, types of characters to be used).

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent are access rights assigned and managed?

4.2.1

The management of access rights ensures that only authorized users have access to information and IT applications. For this purpose, access rights are assigned to user accounts.

- The requirements for the management of access rights (authorization) are determined and fulfilled.
- Access rights granted to user accounts and technical accounts, including those in customer IT systems, are reviewed at regular intervals.
- Strategies for authorizing access to information are prepared.
- Authorization roles are used.
- Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility.
- Normal user accounts are not granted privileged access rights.
- The access rights of a user account are adapted after the user has changed (e.g. new position)
- The access rights are approved by the person (internally) responsible for information.
- Existing access rights are regularly reviewed at shorter intervals (e.g. every three months).
- In case of external operation of the IT infrastructure (e.g. server) and/or cloud solutions, compliance with the encryption requirements according to control question 5.1.1 is ensured.
- Prevention of unauthorized persons gaining access (including privileged users)

PERSEUS INFORMATION SECURITY CONSULTING

DEKRA

To what extent is the use of cryptographic procedures managed?

5.1.1

When using cryptographic procedures, it is important to consider risks in the **field of availability** (lost key material) as well as **risks due to incorrectly applied procedures** in the fields of integrity and confidentiality (poor algorithms/protocols or insufficient key strengths).

- All **cryptographic procedures** used (e.g. encryption, signature, and hash algorithms, protocols, applications) provide the security required by the respective application according to the state of the art.
- The **legal parameters** for the use of cryptography are taken into account.
- Preparation of technical rules containing requirements for encryption in order to protect information according to its classification.
- An **emergency process** for restoring key material is established.
- Requirements regarding key control are determined and fulfilled.
- **Risks arising from external processing** (e.g. in the cloud) are taken into account.
- A concept for the application of cryptography is defined and implemented. The following aspects are considered:
  - Cryptographic procedures,
  - Key strengths,
  - Procedures for the **complete lifecycle of cryptographic keys** including generation, storage, archiving, retrieval, distribution, deactivation, renewal and deletion.

To what extent are changes managed?

5.2.1

The aim of control is to ensure that information security aspects are taken into account when changes are made to the organization, business processes and IT systems in order to prevent those changes from causing **unregulated reduction** in the level of information security.

- Information **security requirements for changes** to the organization, business processes, IT systems are **determined and applied**.
- A **formal approval procedure** is established.
- Changes are checked and evaluated for potential impacts on information security
- Changes affecting information security are **planned and tested**.
- Procedures for **fallback** in fault cases are taken into account
- Compliance with the information security requirements is **verified during and after the changes** are applied.

To what extent are development & testing environments separated from operational environments?

5.2.2

Separation of development, testing and operational environments aims at ensuring that reliability, availability, confidentiality and integrity are maintained.

- The IT systems have been subjected to **risk assessment** in order to determine the **necessity of separation** into development and productive systems.
- A separation is implemented based on the results of risk analysis.
- The requirements for development and testing environments are determined and implemented. The following aspects are considered:
  - Separation of **development, test, and productive systems**

- **No development and system tools** on productive systems (other than those necessary for operation)
- Use of **different user profiles** on test and productive systems

To what extent are event logs recorded and analyzed?

5.2.4

Event logs support the **traceability of events** in case of a security incident. This requires that events necessary to determine the causes are recorded. In addition, activity logging and analysis in accordance with applicable legislation is required to determine which user account made changes to the systems.

- **Information security requirements** regarding handling of event logs are determined and fulfilled.
- **Security-relevant requirements** regarding the logging of activities of system administrators and users are determined and fulfilled.
- The IT systems used **are assessed regarding the necessity of logging.**
- Where externally operated services (particularly cloud services) are used, information on monitoring options are obtained and considered in the evaluation.
- Event logs are **checked regularly** for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions.
- Procedures for **handling rule violations** are specified (e.g. reporting to authorized bodies).

To what extent are event logs recorded and analyzed? (cont'd)

5.2.4

- A **procedure for reporting violations** to authorized bodies (e.g. security incident report, data protection, corporate security, IT security) is defined and established.
- Event logs (contents and meta data) are **protected against alteration** (e.g. by a dedicated environment).
- Adequate monitoring and recording of any actions on the network that are relevant to information security are established.
- Information security requirements regarding the handling of event logs, e.g. contractual requirements, are **determined and applied**.
- Cases of access during connection and disconnection of external networks, **such as remote maintenance,** are logged.
- Logging of any access to data **of very high protection needs** as far as is technically feasible and as permissible according to legal and organizational provisions.

To what extent are vulnerabilities identified and addressed?

5.2.5

Vulnerabilities **increase the risk** of IT systems being unable to meet the requirements for confidentiality, availability and integrity. Among other things, attackers can exploit a vulnerability in order to gain access to the IT system or jeopardize its operational stability.

- Information on technical vulnerabilities for the IT systems in use is **gathered** (e.g. information from the manufacturer, system audits, CVS database) and **evaluated** (e.g. Common Vulnerability Scoring System CVSS)
- Potentially affected IT systems and software are identified, assessed and any **vulnerabilities are addressed.**
- **Risk minimizing measures** are implemented as necessary.

- An **adequate patch management** is defined and implemented (e.g. patch testing and installation).
- Successful installation of patches is verified in an appropriate manner.

To what extent are IT systems technically checked (system audit)?

5.2.6

The technical audit aims at identifying states potentially jeopardizing the availability, confidentiality, or integrity of IT systems.

- **Requirements for auditing** of IT systems are determined.
- The scope of the system audit is specified **in a timely manner**.
- System audits are **coordinated with the operator and users** of the IT systems.
- The results of system audits are stored in a traceable manner and reported to the relevant management.
- Measures are derived from the results.
- System audits are planned taking into account **security risks** they might cause (e.g. disturbances).
- System audits are carried out by trained experts.
- Suitable tools (e.g. vulnerability scanners) are available for system audits.
- Within a reasonable period following completion of the audit, a report is prepared.

To what extent is the network of the organization managed?

5.2.7

IT systems in a network are exposed to different risks or have different protection needs. In order to detect or prevent unintended data exchange or access between these IT systems, they are **subdivided into suitable segments** and access is controlled and monitored by means of security technologies.

- Requirements for the **management and control** of networks are determined and fulfilled.
- Requirements regarding **network segmentation** are determined and fulfilled.
- Procedures for the management and control of networks are defined.
- Extended requirements for the management and control of networks are determined and implemented. The following aspects are considered:
    - Authentication of IT systems on network.
    - **Access to the management interfaces** of IT systems is restricted

- For network segmentation, the following aspects are considered:
    - Restrictions in the connection of IT systems to the network.,
    - Use of security technologies
    - The increased risk presented by network services accessible via the Internet (e.g. use of DMZ networks)
    - Technology-specific separation options (e.g. firewall) when using external services
    - Appropriate separation of own networks and customer networks taking customer requirements into account

To what extent is information security considered in new or further development of IT systems?

5.3.1

Information security is an integral part of the entire lifecycle of IT systems. This particularly includes consideration of information security requirements in the **development or acquisition of IT systems.**

- The information security requirements associated with the **design and development** of IT systems determined.
- The information security requirements associated with the acquisition or extension of IT systems and IT components are determined.
- Information security requirements associated with **changes to IT systems** are taken into account.
- **System approval tests** are carried out under consideration of the information security requirements.
- **Requirement specifications** are prepared under consideration of the information security requirements.
- Requirement specifications are reviewed against the information security requirements.
- The IT system is reviewed for compliance with specifications prior to productive use.
- The **use of productive data for testing purposes** is avoided as far as possible (e.g. anonymization or pseudonymization).

To what extent is information security considered in new or further development of IT systems?

5.3.2

Network services have different requirements for information security, **quality of data transfer**, and management. It is important to know these criteria and the scope of use of different network services.

- Requirements regarding the information **security of network services** are determined and fulfilled.
- Procedures for securing and using network services are defined and implemented.
- The requirements are agreed in the form of **SLAs.**

- Adequate **redundancy solutions** are implemented.
- **Procedures for monitoring** the quality of network traffic (e.g. traffic flow analyses, availability measurements) are defined and applied.

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