## TISAX* Readiness Checkliste (D)

Sie erhalten im Rahmen der Bearbeitung der Checkliste schnell und einfach Informationen darüber, ob Ihr Unternehmen ein integriertes Informations-Sicherheitsmanagementsystem besitzt, das bereits ausreichend für die Prüfung nach TISAX* vorbereitet ist.

Der Aufbau der Fragen orientiert sich an Managementsystemnormen. Wenn Sie eine Frage nicht sicher positiv beantworten können, dann antworten Sie mit „Nein“. Nur wenn Sie alle Fragen mit „Ja“ beantworten können, besitzt ihr Unternehmen vermutlich bereits einen ausreichenden Reifegrad. Glückwunsch!

Falls nicht, so helfen wir Ihnen im Rahmen einer detaillierten GAP-Analyse gerne dabei, herauszufinden, in welchen Bereichen Ihr Unternehmen die Anforderungen von TISAX* bereits vollumfänglich erfüllt und welchen Themen Sie sich noch zuwenden müssen.

*The Brand “TISAX” belongs to the ENX Association.

| Bereich | Frage | Ja/nein |
|---|---|---|
| IS-Richtlinien und -Organisation | Sind Richtlinien zur Informationssicherheit vorhanden? | |
| Organisation der Informationssicherheit | Wird in der Organisation Informationssicherheit gemanagt? | |
| | Sind die Verantwortlichkeiten für Informationssicherheit organisiert? | |
| | Werden Informationssicherheitsanforderungen in Projekten berücksichtigt? | |
| | Sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert? | |
| Vermögensverwaltung (Asset Management) | Werden Informationswerte (Assets) identifiziert und erfasst? | |
| | Werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt? | |
| | Wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden? | |
| IS Risk Management | Werden Informationssicherheitsrisiken gemanagt? | |
| Assessments | Wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt? | |
| | Wird das ISMS von einer unabhängigen Instanz überprüft? | |
| Incident Management | Werden Informationssicherheitsereignisse angemessen verarbeitet? | |

| Bereich | Frage | Ja/nein |
|---|---|---|
| Humanressourcen | Wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt? | |
| | Werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet? | |
| | Werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert? | |
| | Ist mobiles Arbeiten geregelt? | |
| Physische Sicherheit und Business Continuity | Werden Sicherheitszonen für den Schutz von Informationswerten gemanagt? | |
| | Ist in Ausnahmesituationen die Informationssicherheit sichergestellt? | |
| | Ist der Umgang mit Informationsträgern gemanagt? | |
| | Ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt? | |
| Identitäts- und Zugriffsmanagement | Ist der Umgang mit Identifikationsmitteln gemanagt? | |
| | Wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert? | |
| | Werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt? | |
| | **Werden Zugriffsberechtigungen vergeben und gemanagt?** | |
| IT Security / Cyber Security | Wird die Nutzung kryptografischer Verfahren gemanagt? | |
| | Werden Informationen während der Übertragung geschützt? | |
| Betriebssicherheit | Werden Änderungen gesteuert? | |
| | Sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt? | |
| | Werden IT-Systeme vor Schadsoftware geschützt? | |
| | Werden Ereignisprotokolle aufgezeichnet und analysiert? | |
| | Werden Schwachstellen erkannt und behandelt? | |
| | Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)? | |
| | Wird das Netzwerk der Organisation gemanagt? | |
| Systemakquisition, Anforderungsmanagement und -entwicklung | Wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt? | |
| | Sind Anforderungen an Netzwerkdienste definiert? | |
| | Sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt? | |
| Lieferantenbeziehungen | Wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt? | |
| | Ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart? | |

| Bereich | Frage | Ja/nein |
|---|---|---|
| Compliance | Wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt? | |
| | Wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt? | |
| Prototypenschutz, Physische und Umgebungsbezogene Sicherheit | Ist ein Sicherheitskonzept vorhanden, das Mindestanforderungen zur physischen und umgebungsbezogenen Sicherheit für den Prototypenschutz beschreibt? | |
| | Ist eine Perimetersicherung vorhanden, die einen unberechtigten Zutritt zu den zu schützenden Objekten der Liegenschaften verhindert? | |
| | Ist ein Sicht- und Einblickschutz in definierte Sicherheitsbereiche gewährleistet? | |
| | Ist der Schutz vor unbefugtem Betreten in Form einer Zugangskontrolle geregelt? | |
| | Werden die zu sichernden Räumlichkeiten auf Einbruch überwacht? | |
| | Ist ein dokumentiertes Besuchermanagement vorhanden? | |
| | Ist eine Mandantentrennung vor Ort gegeben? | |
| Organisatorische Anforderungen | Liegen vertragsrechtlich gültige Geheimhaltungsvereinbarungen/ -verpflichtungen vor? | |
| | Sind Vorgaben für die Beauftragung von Unterauftragnehmer bekannt und erfüllt? | |
| | Werden Mitarbeiter und Projektbeteiligte über den Umgang mit Prototypen nachweislich geschult und sensibilisiert? | |
| | Sind die Sicherheitseinstufungen des Projekts und die daraus resultierenden Maßnahmen zur Absicherung bekannt? | |
| | Ist ein Prozess zur Zutrittsvergabe in Sicherheitsbereiche definiert? | |
| | Snd Regelungen zur Bildaufzeichnung und Umgang mit erstelltem Bildmaterial vorhanden? | |
| | Existiert ein Prozess zur Einbringung und Nutzung von mobilen film- und fotofähigen Endgeräten in definierte Sicherheitsbereiche? | |
| Umgang mit Fahrzeugen, Komponenten und Bauteilen | Werden Transporte von als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen nach den Vorgaben des Auftraggebers abgewickelt? | |
| | Ist sichergestellt, dass als schutzbedürftig klassifizierte Fahrzeuge, Komponenten und Bauteile, den Vorgaben des Auftraggebers entsprechend abgestellt/gelagert werden? | |

| Bereich | Frage | Ja/nein |
|---|---|---|
| Anforderungen für Erprobungsfahrzeuge | Werden die vorgegebenen Regelungen zur Tarnung von den Projektbeteiligten umgesetzt? | |
| | Werden Schutzmaßnahmen freigegebener Test- und Erprobungsgelände eingehalten/umgesetzt? | |
| | Werden die Schutzmaßnahmen für freigegebene Test- und Erprobungsfahrten in der Öffentlichkeit eingehalten/umgesetzt? | |
| Anforderungen für Veranstaltungen und Shootings | Sind die Sicherheitsvorgaben für Ausstellungen und Veranstaltungen mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt? | |
| | Sind die Schutzmaßnahmen für Film- und Fotoshootings mit als schutzbedürftig klassifizierten Fahrzeugen, Komponenten oder Bauteilen bekannt? | |
| Datenschutz | Ist die Umsetzung des Datenschutzes organisiert? | |
| | Werden organisatorische Maßnahmen getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt? | |
| | Wird sichergestellt, dass die internen Prozesse bzw. Arbeitsabläufe gemäß den jeweils aktuell gültigen Datenschutzbestimmungen ablaufen und dies regelmäßig einer Qualitätsprüfung unterzogen wird? | |
| | Werden die einschlägigen Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert? | |

**TISAX* Readiness Checklist (English)**

As part of the processing of the checklist, you will receive quick and easy information about whether your company has an integrated information security management system, which is already sufficiently prepared for certification according to TISAX*

The structure of the questions is based on management system standards. If you can't answer a question positively with certainty, then answer "No". If you can answer "yes" to all questions, your organization probably already has a sufficient level of maturity. Congratulations!

As part of a detailed GAP analysis, we are happy to help you finding out in which areas your company already fully meets the requirements of TISAX* and which topics you still have to address.

*The Brand “TISAX” belongs to the ENX Association.

| Area | Question | Yes/No |
|---|---|---|
| IS Policies and Organization | Are information security policies in place? | |
| Organisation of Information Security | Managed in the information security organization? | |
| | Are the responsibilities for information security organized? | |
| | Are information security requirements taken into account in projects? | |
| | Are the responsibilities between non-organizational IT service providers and your own organization defined?? | |
| Asset Management | Are information values (assets) identified and recorded? | |
| | Are information values classified and managed with regard to their protection needs? | |
| | Does the organization ensure that only evaluated and approved non-organizational IT services are used to process informational values of the organization? | |
| IS Risk Management | Are information security risks managed?? | |
| Assessments | Does the organization ensurs compliance with information security in procedures and processes? | |
| | Is the ISMS verified by an independent authority?? | |
| Incident Management | Are information security events handled appropriately? | |
| Human Ressources | Ensures the suitability of employees for sensitive areas of activity? | |
| | Are all employees obliged to comply with information security?? | |
| | Are employees trained and sensitized to the risks involved in handling information? | |
| | Is mobile working regulated? | |

| Area | Question | Yes/No |
|---|---|---|
| Physical Security and Business Continuity | Are security zones managed to protect information assets? | |
| | Is information security ensured in exceptional situations? | |
| | Is the handling of information carriers managed? | |
| | Is the handling of mobile IT devices and mobile data carriers managed? | |
| Identity and Access Management | Is the handling of means of identification managed? | |
| | Ensures users' access to network services, IT systems and IT applications? | |
| | User accounts and credentials are securely managed and applied? | |
| | Are access authorizations assigned and managed? | |
| IT Security / Cyber Security | Is the use of cryptographic methods managed?? | |
| | Is information protected during transmission? | |
| Operations Security | Are Changes controlled? | |
| | Are the development and test environments separate from the production environments? | |
| | Do your protect IT systems from malware? | |
| | Are event logs recorded and analyzed? | |
| | Are vulnerabilities detected and treated? | |
| | Are IT systems technically checked? (Systemaudit)? | |
| | Is the organization's network managed?? | |
| System acquisitions, requirement management and development | Is information security taken into account in new or further developed IT systems?? | |
| | Are requirements for network services defined? | |
| | Is information protected in shared NON-organizational IT services? | |
| Supplier relationships | Is information security ensured for contractors and cooperation partners? | |
| | Is secrecy contractually agreed when exchanging information? | |
| Compliance | Ensures compliance with regulatory and contractual requirements? | |
| | Is the protection of personal data taken into account in the implementation of information security?? | |

| Area | Question | Yes/No |
|---|---|---|
| Prototype Protection, Physical and Environmental Security | Is a security concept in place that describes minimum physical and environmental security requirements for prototype protection? | |
| | Is a perimeter security available that prevents unauthorized access to the objects of the properties to be protected? | |
| | Is a privacy and insight protection in defined security areas guaranteed? | |
| | Is the protection against unauthorized entry regulated in the form of an access control? | |
| | Are the premises to be secured monitored for burglary? | |
| | Is a documented visitor management available? | |
| | Is there a client separation on site? | |
| Organizational requirements | Are there contractually valid non-disclosure agreements/obligations? | |
| | Are specifications for the commissioning of subcontractors known and fulfilled? | |
| | Employees and project participants are demonstrably trained and sensitized to the handling of prototypes? | |
| | Are the security classifications of the project and the resulting measures for protection known?? | |
| | Is a process defined for assigning access to security areas? | |
| | Are there regulations for image recording and handling of created image material? | |
| | Is there a process for the introduction and use of mobile film- and photo-capable devices in defined security areas?? | |
| Handling of vehicles, components and components | Are transports of vehicles, components or components classified as in need of protection handled in accordance with the client's specifications?? | |
| | Is ensured that vehicles, components and components classified as in need of protection are parked/stored in accordance with the customer's specifications? | |
| Requirements for test vehicles | Are the specified regulations for camouflage implemented by the project participants?? | |
| | Are protective measures of approved test and test sites adhered to/implemented? | |
| | Are the protective measures for approved test and test drives observed/implemented in public?? | |
| Requirements for events and shootings | Are the safety requirements for exhibitions and events with vehicles, components or components classified as vulnerable known? | |
| | Are the protective measures for film and photo shoots with vehicles, components or components classified as vulnerable known?? | |

| Area | Question | Yes/No |
|---|---|---|
| Privacy | Is the implementation of data protection organized? | |
| | Are organizational measures taken to ensure that the processing of personal data is carried out in accordance with the law?? | |
| | Ensures that the internal processes or workflows run in accordance with the currently valid data protection regulations and that this is regularly subjected to a quality check? | |
| | Are the relevant processing operations documented with regard to data protection admissibility? | |