Wie laufen TISAX®-Assessments ab?

Der Ablauf im Überblick

TISAX® ist ein unternehmensübergreifendes Prüf- und Austauschverfahren für Informationssicherheit in der Automobilindustrie. Dabei geht es um den Schutz der Daten, ihrer Vertraulichkeit, ihrer Integrität und Verfügbarkeit im Entwicklungs- und Herstellungsprozess von Fahrzeugen. Der Verband der Automobilindustrie (VDA) hat den Information Security Assessment (ISA)-Katalog in Zusammenarbeit mit renommierten Zulieferern und Prüfdienstleistern als Branchenstandard entwickelt.

Der TISAX®-Prozess umfasst im Wesentlichen die drei Phasen: Registrierung, Prüfung und Austausch. Unternehmen müssen nachweisen, dass ihr Informationssicherheitsmanagementsystem (ISMS) die erforderlichen Schutzziele ihrer Auftraggeber gemäß den Anforderungen des ISA erfüllen. Aktuell gilt für neue Audits, die auch Assessments genannt werden, der ISA-Katalog in der Version 6.

Der TISAX®-Prozess bietet Unternehmen die Möglichkeit, ihre Informationssicherheit zu verbessern, um mit den ständig neuen Bedrohungen Schritt zu halten und die Anforderungen ihrer Partner zu erfüllen.

1. Registrierung

Im kostenlos online verfügbaren TISAX®-Teilnehmerhandbuch ist eine ausführliche Beschreibung für TISAX®-Teilnehmer enthalten, wie die Registrierung der Teilnehmer, ihrer Prüfziele und ihrer betroffenen Standorte als sogenannter „Assessment Scope“ abläuft. Als Ergebnis einer erfolgreichen Registrierung wird Ihnen für jeden registrierten Assessment Scope ein sogenanntes „TISAX® Scope Excerpt“ als PDF-Datei bereitgestellt.

Diesem Scope-Excerpt entnehmen wir alle Angaben, die wir für eine seriöse Kalkulation und Angebotserstellung benötigen. Sobald TÜV NORD Ihren Auftrag erhalten hat, bekommen Sie eine Auftragsbestätigung, die Sie im Bedarfsfall Ihren Auftraggebern vorlegen können.

2. Prüfung

2.1 Kick-off-Meeting und Dokumentenprüfung

Wir weisen Ihnen einen geeigneten Auditor oder eine geeignete Auditorin aus unserem Pool zu. Diese Person wird sich dann bei Ihnen melden, um die weiteren Schritte und Termine mit Ihnen abzustimmen.

Das Kick-off-Meeting markiert den formalen Beginn des Prüfprozesses. Dabei werden neben einigen formalen Punkten, der Assessment-Ablauf, die notwendigen Vorbereitungen wie z. B. Ihr Self-Assessment, der ISA, die finalen Prüfinhalte, der Umfang und die zeitliche Abfolge abgestimmt. Bei Bedarf können wir Ihnen auch eine Zwischenbescheinigung für Ihre Auftraggeber ausstellen. Das Kick-off-Meeting kann je nach Zeitpunkt der Beauftragung und Verfügbarkeit der Beteiligten etwa drei Wochen nach Ihrer Beauftragung stattfinden und muss mindestens 14 Tage, bevor es stattfindet, bei ENX angemeldet werden.

Sobald Sie dem Auditor oder der Auditorin Ihre ISMS-Do-

kumentation und das Self-Assessment gemäß dem ISA zur Verfügung gestellt haben, kann dieser mit der Dokumentenprüfung (Plausibilitätsprüfung) beginnen. Obwohl dies effektiv nur etwa einen Arbeitstag erfordert, benötigt der Auditor oder die Auditorin etwa ein bis zwei Wochen, um sich in Ihr ISMS einzuarbeiten, Rückfragen zu klären und das Audit vorzubereiten.

2.2 Durchführung des Audits und Abschluss

Abhängig von Ihren Vorbereitungen kann das eigentliche Audit innerhalb der dann folgenden circa zwei bis vier Wochen erfolgen. Bitte beachten Sie, dass auch das Audit von uns mit zwei Wochen Vorlauf bei ENX angemeldet werden muss, damit ENX die Option nutzen kann, unsere Auditorinnen und Auditoren während des Assessments zu beobachten.

Die Ergebnisse des Audits bzw. des Initial Assessment werden am letzten Audittag im Abschlussgespräch (Closing Meeting) besprochen und im Anschluss in einem Bericht, dem Initial Assessment Report, festgehalten. Dieser wird in einer Vorab-Version im sogenannten „Report Closing Meeting“ ein paar Tage nach dem Audit – in der Regel remote – vorgestellt und besprochen. Im Anschluss daran wird der Bericht finalisiert. Die Details des finalen Initial Assessment Report werden dann vom Audit Provider in die ENX-Datenbank eingetragen. Sollte es im Initial Assessment keine Feststellungen (Findings) zu Nicht-Konformitäten geben, wird bereits zu diesem Zeitpunkt mit dem Eintrag der Ergebnisse des Initial Assessment in der ENX Datenbank das finale TISAX®-Label initiiert.

Sollte es Haupt- und/oder Nebenabweichungen geben, so sind diese im Rahmen des dann notwendigen Managements von Nichtkonformitäten mit Maßnahmen zu belegen. Bei Hauptabweichungen sind neben Sofortmaßnahmen auch die notwendigen Korrekturmaßnahmen und bei Nebenabweichungen nur die notwendigen Korrekturmaßnahmen zu planen. Diese Maßnahmen müssen dann mit Hilfe eines Korrekturmaßnahmenplanes inhaltlich und hinsichtlich ihres Umsetzungszeitpunktes mit dem Auditor oder der Auditorin abgestimmt werden. Der Auditor oder die Auditorin bewertet hierbei die von Ihnen geplanten Maßnahmen risikobasiert auf Vollständigkeit, Wirksamkeit und Angemessenheit. Dieser Schritt findet im sogenannten Corrective Action Plan Assessment statt.

Im „Normalfall“ werden die Korrekturmaßnahmenpläne von den Teilnehmern so lange bearbeitet, bis der Auditor oder die Auditorin sie akzeptieren und der Prozess zum Label fortgesetzt werden kann.

3. Austausch

3.1 Korrekturmaßnahmen und Label-Erteilung

Die Ergebnisse des Corrective Action Plan Assessment werden dann in die TISAX®-Datenbank der ENX eingetragen, und das temporäre Label wird initiiert.

Spätestens jetzt sollten Sie Ihr Vorhaben sichtbar machen, indem Sie Ihre Ergebnisse auf der Austauschplattform veröffentlichen und/oder mit Ihren Partnern teilen. Sie haben gemäß dem TISAX®-Regelwerk maximal neun Monate ab dem Datum des Closing Meetings Zeit, um die Korrekturmaßnahmen umzusetzen und dem Auditor oder der Auditorin nachzuweisen, dass sie auch vollständig und wirksam sind.

Diese neun Monate beziehen sich aber nur auf die maximal vom Regelwerk erlaubte Zeit für das Nichtkonformitäten-Management, da bei Überschreitung dieses Zeitrahmens das durchgeführte Assessment ungültig wird, es zu keinem finalen TISAX®-Label kommt und der gesamte Assessment-Prozess neu begonnen werden muss. Der tatsächliche Zeitrahmen für die Behebung der Nichtkonformitäten wird risikobasiert von unseren Auditorinnen und Auditoren zusammen mit Ihnen festgelegt. Dieser fällt in der Regel mit maximal drei Monaten deutlich kürzer aus als die oben genannten neun Monate.

3.2 Follow-up-Assessment und Entfristung des Labels

Das sogenannte Follow-up-Assessment ist der letzte Prüfschritt. Hier ist dem Auditor oder der Auditorin nachzuweisen, dass die beabsichtigten Korrekturmaßnahmen auch wirklich vollständig und wirksam umgesetzt wurden. In dem Fall erwirkt der Auditor oder die Auditorin dann die Entfristung Ihres Labels bei ENX auf die maximale Gültigkeitsdauer von drei Jahren ab dem Datum des Closing Meetings. Das bedeutet, die Laufzeit des temporären Labels hat keine aufschiebende Wirkung.

Ihr Weg zum TISAX®-Label:

Nr.	Name	Beschreibung	Assessment-Level
1.	Confidential	Umgang mit Informationen mit hohem Schutzbedarf im Rahmen der Vertraulichkeit (Zugriff auf vertrauliche Informationen)	AL2
2.	Strictly confidential	Umgang mit Informationen von sehr hohem Schutzbedarf im Rahmen der Vertraulichkeit (Zugriff auf streng vertrauliche Informationen)	AL3
3.	High availability	Umgang mit Informationen von hohem Schutzbedarf im Rahmen der Verfügbarkeit (hohe Verfügbarkeit der Informationen)	AL2
4.	Very high availability	Umgang mit Informationen von sehr hohem Schutzbedarf im Rahmen der Verfügbarkeit (sehr hohe Verfügbarkeit der Informationen)	AL3
5.	Proto parts	Schutz von Prototypenbauteilen und -Komponenten	AL3
6.	Proto vehicles	Schutz von Prototypenfahrzeugen	AL3
7.	Test vehicles	Umgang mit Erprobungsfahrzeugen	AL2
8.	Proto events	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings	AL2
9.	Data	Datenschutz gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz-Grundverordnung (DSGVO).	AL2
10.	Special data	Datenschutz gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz-Grundverordnung (DSGVO) mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben	AL3

Tabelle 5. Zuordnung der TISAX®-Prüfziele zu den Assessment-Leveln

Wenn Sie weitere Informationen über die Hintergründe, Abläufe und Prinzipien des TISAX® Programms benötigen, könnte das TISAX® Teilnehmerhandbuch für Sie von Interesse sein.

https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html

Inspired by Knowledge: Unser Know-How für Ihren Erfolg

In einer zunehmend komplexen Welt ist Orientierung und Transparenz gefragt. Dies leisten unabhängige, nachprüfbare Audit- und Zertifizierungsdienstleistungen von TÜV NORD. Seit vielen Jahren sind wir für die Zertifizierung von Informationssicherheits-Managementsystemen (ISMS) bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditiert. Speziell für den Automobilbereich ist TÜV NORD von der ENX Association als TISAX® Audit Provider (TISAX® AP) zugelassen und kann weltweit Assessments durchführen. Zudem bietet TÜV NORD das neue Auditprogramm ENX Vehicle Cyber Security (VCS) zur Zertifizierung von Cybersecurity-Managementsystemen (CSMS) an. Unsere Auditorinnen und Auditoren verfügen über fundiertes Wissen und unterstützen Sie sowohl mit fachlichem Know-how als auch mit objektivem Feedback.

*Hinweis: Die TÜV NORD CERT GmbH ist durch ENX autorisiert, TISAX®-Prüfdienstleistungen anzubieten. Die mit dem TISAX®-Programm verknüpften Marken und Warenzeichen sowie das damit verbundene geistige Eigentum gehören der ENX.

24-0579-07/24

Kontakt

Holger Hoffmann
M +49 201 825 2213
T hhoffmann@tuev-nord.de

TÜV NORD CERT
Am TÜV 1
45307 Essen
tuev-nord-cert.de

Weitere Informationen und Kontaktformular: