Spezielle Bedingungen für die Durchführung von TISAX-Bewertungen der TÜV NORD CERT GmbH

TÜV NORD Zertifizierung

Inhaltsverzeichnis

Haben Sie Fragen zu der Leistungsbeschreibung? Wir helfen Ihnen gern weiter.

Sie erreichen uns per Mail info.tncert@tuev-nord.de oder persönlich von Montag bis Freitag zwischen 07:30 Uhr und 18:00 Uhr unter 0800 – 2457457.

TÜV NORD CERT GmbH

Langemarckstraße 20

45141 Essen

www.tuev-nord-cert.de

1. Bewertungsgrundlage

Grundlage für das Information Security Assessment (ISA) ist der jeweils aktuelle Prüfkatalog des VDA sowie die aktuell gültigen Rahmenbedingungen (wie z.B. das Teilnehmerhandbuch) des Trusted Information Security Assessment Exchange (TISAX) und der ENX Association.

2. Begriffe

Active Participant (Auditee) / Teilnehmer:
Organisation, die auf Anforderung eines ihrer Kunden („passive participant“) die Wirksamkeit ihres ISMS mit einem TISAX-Label darlegen muss oder dies aus strategischen Gründen will (auch: Auftraggeber).

Passive Participant / Kunde:
Organisation, die ihre relevanten Geschäftspartner („active participants“) auffordert, die Wirksamkeit ihres ISMS mit einem entsprechenden TISAX-Label darzulegen.

TISAX Assessment Provider (TISAX AP):
Von ENX zugelassene Stelle, die TISAX-Bewertungen durchführen darf (auch: Auftragnehmer).

Simplified Group Assessments (SGA):
Stichprobenverfahren für die Bewertung von Teilnehmer-Organisationen, die ihre Tätigkeiten auf mehrere Standorte verteilen.

3. Teilnahmebedingungen / Voraussetzungen

Der Teilnehmer registriert sich bei ENX für die Teilnahme am TISAX Verfahren.

Dazu stimmt der Teilnehmer (active participant) mit seinen Kunden (passive participant) folgendes ab:

- den Scope des TISAX Assessments in Bezug auf relevante Assessment Objectives, notwendige Protection Level und das daraus resultierende Assessment Level mit den notwendigen und im Scope enthaltene Standorten,

Basis für diese Abstimmung ist die Betrachtung aller Prozesse, Verfahren und beteiligten Ressourcen an den Standorten im Scope, mit denen Informationen verarbeitet werden, die Sicherheitsanforderungen von Partnern aus der Automobilindustrie unterliegen. Dies schließt sowohl die Erhebung, die Speicherung wie auch die Verarbeitung von Informationen ein.

Als Ergebnis erhält der Teilnehmer eine Participant-ID und eine Scope-ID bzw. Das sogenannte TISAX Scope Excerpt.

Der Teilnehmer stellt dem TISAX AP dieses TISAX Scope Excerpt für dessen Kalkulation und Angebotserstellung, sowie für die Auditplanung als Grundlage zur Verfügung.

In Absprache mit dem Teilnehmer legt der TISAX AP aus den oben genannten Festlegungen zwischen Teilnehmer und Kunde in einem Kickoff Meeting fest, welche Bewertungen an welchen Standorten stattzufinden haben.

Grundlage für das seitens des TISAX AP durchzuführende Assessment ist die Selbstbewertung (Self Assessment) des Teilnehmers auf Basis des für das Assessment gültigen VDA ISA. Der TISAX AP führt eine Plausibilitätsprüfung der Selbstbewertung des Teilnehmers durch und auf Basis dieser Plausibilitätsprüfung

werden die weiteren Assessment Details sowohl für Assessment Level 1, Assessment Level 2 als auch Assessment Level 3 festgelegt.

Assessment Level (AL)	**Kurze Beschreibung**	**Protection Level**
AL1 (durch TISAX AP)	Bewertung der Selbsteinschätzung des Teilnehmers zur Erfüllung der Controls des VDA-ISA-Katalogs samt Nachweisführung.	Normal (Normal)
AL2 (durch TISAX AP)	Plausibilitäts-Check der Selbsteinschätzung des Teilnehmers inkl. Bewertung der Nachweise und ein Experten-Interview via Telefonkonferenz oder Online Meeting (bei Bedarf auch Vor-Ort[1]).	Hoch (High)
AL3 (durch TISAX AP)	Vollumfängliche bzw. detaillierte Prüfung der Selbsteinschätzung inklusive der Bewertung von Nachweisen durch Audits und Experten-Interviews Vor-Ort.	Sehr hoch (Very high)
Die Anwendung des Stichprobenverfahrens bei Mehrfach-Standorten (SGA) muss bei ENX beantragt und registriert werden. Sie erfordert eine intensive Vorbewertung des zentralen ISMS (Exhaustive Precondition Check) nach AL3 und den Nachweis eines besonderen Reifegrades und einer besonderen Wirksamkeit des ISMS. Neben der Zentrale wird eine repräsentative Stichprobe an Standorten bewertet, die wie folgt ermittelt wird (bei realen Werten in immer die nächst größere Ganzzahl anzusetzen): $No_{locations} \leq 10$: $No_{samples} = 2$ $No_{locations} \leq 50$: $No_{samples} = 0{,}1*(No_{locations} - 10) + 2$ $No_{locations} > 50$: $No_{samples} = 0{,}05*(No_{locations} - 50) + 6$ Die weiteren Standorte werden dann einer vereinfachten Bewertung unterzogen.		

Anmerkung: *Nach den Regelungen der ENX sind keine formalen Anerkennungen oder Reduzierungen von TISAX Assessment Aufwänden aufgrund bestehender ISO 27001 Zertifizierungen zulässig. Kombinierte oder integrierte TISAX-Bewertungen mit ISO 27001 Auditierungen sind im Vorfeld mit dem Auftragnehmer abzustimmen.*
Simplified Group Assessments und Erweiterungen oder Reduzierungen dieser sind ebenfalls abzustimmen.

4. Bewertungsablauf – Leistungen und Pflichten der Vertragspartner (analog jeweils für Assessment Level 2 bzw. 3)

I. Initial Assessment

a. Nach Anfrage, Angebot und Beauftragung des TISAX AP (im folgenden Auftragnehmer) durch den Teilnehmer (im folgenden Auftraggeber) wird ein formales Eröffnungsgespräch (Kick-Off-Meeting) durchgeführt, um folgendes festzulegen bzw. zu bestätigen:

- den Assessment Scope (Assessment Objectives und die im Scope befindlichen Standorte),
- den relevanten VDA ISA - Katalog
- notwendige Assessment Voraussetzungen wie das Self Assessment des Auftraggebers
- den Assessment Ablauf inkl. Nicht-Konformitäten Management und Reporting
- die Termine und die Beteiligten auf beiden Seiten: Experten des Auftraggebers und Mitglieder des Bewertungsteams des Auftragnehmers.

Das Kick-Off-Meeting kann telefonisch oder per Web-/Video-Konferenz bzw. als Online Meeting erfolgen. Das Kick-Off-Meeting markiert den Beginn des TISAX-Verfahrens.

b. Anschließend stellt der Auftraggeber dem Auftragnehmer die erforderlichen Dokumente seines Self Assessments zur Verfügung.

c. Der Auftragnehmer bewertet die Dokumentation (Selbsteinschätzung und entsprechende Nachweise) auf Vollständigkeit und Plausibilität und bereitet darauf basierend die eigentliche Bewertung bzw. das Assessment vor:

- erstellt einen inhaltlichen Bewertungsplan auf Basis der Dokumentenprüfung
- koordiniert den Teilnehmerkreis der Beteiligten für die Bewertung und
- stimmt die Bewertungstermine und den Bewertungsablauf mit allen Beteiligten ab.

d. Anschließend erfolgt die eigentliche Bewertung bzw. das Assessment:

- AL1: Nur in dem Fall, dass bei einem Simplified Group Assessment (SGA) eine Selbstbewertung eines Standorts vorliegt, der nicht in der Stichprobe der SGA Bewertung enthalten ist, wird diese detaillierte Bewertung durch eine Prüfung auf Vollständigkeit und Plausibilität ersetzt

- AL2: Bei Assessment Level 2 vorzugsweise als telefonisches oder online Experten-Interview auf Basis der seitens des Auftragnehmers durchgeführten Vollständigkeits- und Plausibilitätsbewertung des Self Assessments und der zugehörigen Nachweise des Auftraggebers (optional kann dies auch Vor-Ort erfolgen).

- AL3: Bei Assessment Level 3 die vollumfängliche Bewertung zur Selbsteinschätzung und der Controls des VDA-ISA-Katalogs auf Wirksamkeit inklusive aller entsprechender Nachweise durch Audits und Experten-Interviews Vor-Ort.

- SGA: Bei Simplified Group Assessments erfolgt in der Zentrale eine intensive Vorbewertung mit Prüftiefe nach Assessment Level 3
  a) des Reifegrades und der Wirksamkeit des ISMS
  b) des Durchgriffs auf die anderen Standorte
  c) sowie die Bewertung der Standorte gemäß der vereinbarten Assessment Objectives.
  Dabei werden die Standorte außerhalb der festgelegten Stichprobe einer vereinfachten Bewertung unterzogen.

e. Der Auftragnehmer erstellt Aufzeichnungen und einen vorläufigen Bewertungsbericht, den er dem Auftragnehmer im sogenannten Closing Meeting erläutert. Mit dem Closing Meeting beginnt dann die 9-Monatsfrist, innerhalb der das Verfahren abgeschlossen sein muss. Nach dem Closing Meeting erstellt der Auftragnehmer den endgültigen Bewertungsbericht (Initial Assessment Report) und sendet diesen dem Auftraggeber zu und berichtet anschließend an die ENX.

II. Corrective Action Plan Assessment

Sofern nach Abschluss des Initial Assessments Nichtkonformitäten bestehen, muss der Auftraggeber innerhalb von mit dem Auftragnehmer abzustimmenden Fristen einen Maßnahmenplan (Corrective Action Plan) zur Beseitigung dieser Nichtkonformitäten erstellen.
Auf Wunsch des Auftraggebers führt der Auftragnehmer die Prüfung und Bewertung dieses Maßnahmenplans im Rahmen des Corrective Action Plan Assessments durch, schreibt den Bewertungsbericht vom Initial Assessment fort (Update) und erzeugt dabei auf Basis des vereinbarten Corrective Action Plans den Corrective Action Plan Assessment Report. Dieser wird seitens des Auftragnehmers dem Auftraggeber zugesendet. Danach berichtet der Auftragnehmer an die ENX und falls es die Ergebnisse ermöglichen, kann seitens der ENX ein temporäres TISAX Label als Assessment Zwischenergebnis erteilt werden.

III. Follow-Up Assessment

Sofern nach Abschluss des Initial Assessments offene Nichtkonformitäten bestehen, muss ein Maßnahmenplan zur Beseitigung dieser Nichtkonformitäten mit dem Auftragnehmer abgestimmt und anschließend umgesetzt werden.
Auf Wunsch des Auftraggebers führt der Auftragnehmer danach eine Prüfung und Bewertung der wirksamen Umsetzung dieser Maßnahmen im Rahmen eines Follow-Up Assessments durch. Je nach Art bzw. Umfang der Nichtkonformitäten: vor Ort, telefonisch oder online als Web-/Video-Konferenz.
Danach erstellt der Auftragnehmer den finalen Bericht bzw. den Follow-Up Assessment Report (als Fortschreibung/Update des Corrective Action Plan Assessment Reports). Dieser wird seitens des Auftragnehmers dem Auftraggeber zugesendet. Danach berichtet der Auftragnehmer an die ENX und falls es die Ergebnisse des Follow-Up Assessments ermöglichen, also wenn alle im Initial Assessment festgestellten Nicht-Konformitäten wirksam behoben wurden, kann seitens der ENX das finale TISAX Label als finales Assessment Ergebnis erteilt werden und entsprechend auf der TISAX-Plattform der ENX abgebildet werden.
Das finale TISAX Label markiert das Ende des TISAX-Verfahrens.

Der Auftraggeber legt nach eigenem Ermessen fest, wer auf der bzw. über die TISAX-Plattform der ENX seine Assessment-Ergebnisse einsehen darf.

5. Weitere Hinweise

Ein TISAX-Verfahren muss spätestens neun Monate nach dem Closing Meeting abgeschlossen sein.

Der Auftragnehmer führt zur Qualitätssicherung nach jedem Assessment Prozessschritt eine Qualitätsprüfung der erstellten Berichte durch eine unabhängige Person durch. Fehler oder Inkonsistenzen werden hierüber festgestellt und dann entsprechend korrigiert/modifiziert.

6. Auskunftspflicht

Auf Anfrage eines passiven Teilnehmers muss ihm der Auftragnehmer entsprechend der von ENX festgelegten Regeln detaillierte Berichtsversionen in der angefragten Detailtiefe zur Verfügung stellen.