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

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

TÜV NORD
Zertifizierung

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 seiner Kunden („passive participant“) die Wirksamkeit ihres ISMS mit einem TISAX-Label darlegen muss (auch: Auftraggeber).

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

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

Simplified Group Assessments (SGA):
Sitchprobenverfahren 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 ISMS und die Standorte,
- die relevanten ISA-Kataloge (z.B. Einbeziehung Dritter, Prototypenschutz und Datenschutz),
- die erforderlichen Objectives (Protection Level Normal, High oder Very High);
  TISAX Label sowie ggfs. die entsprechenden Zielreifegrade.

Als Ergebnis erhält der Teilnehmer eine Participant-ID und eine Scope-ID erteilen.

Der Teilnehmer teilt der beauftragten XAP spätestens mit Auftragserteilung seine Participant-ID und seine Scope-ID mit.

In Absprache mit dem Teilnehmer legt der XAP aus den oben genannten Festlegungen zwischen Teilnehmer und Kunde fest, welche Bewertungen an welchen Standorten stattzufinden haben.
Während die Selbsteinschätzung (Self-Assessment) für Protection-Level 1 (Normal) durch den Teilnehmer selbst erfolgt, sind die Bewertungen für Protection Level 2 (High) oder Protection Level 3 (Very High) ausschließlich durch den XAP durchzuführen. Dabei gilt, dass eine Bewertung nach Level 2 oder Level 3 eine vorhergehende Selbsteinschätzung nach Level 1 voraussetzt.

Assessment Level (AL)	Kurze Beschreibung	Protection Level
AL1 (durch Teilnehmer)	Selbsteinschätzung zur Erfüllung der Controls des VDA-ISA-Katalogs samt Nachweisführung.	Normal (Normal)
AL2 (durch XAP)	Plausibilitäts-Check der Selbsteinschätzung; und die Bewertung der Nachweise; und ein telefonisches Experten-Interview (bei Bedarf auch Vor-Ort[1]). Bedingung: AL1 muss vorliegen.	Hoch (High)
AL3 (durch XAP)	Vollumfängliche Prüfung des VDA-ISA-Kataloges sowie der Selbsteinschätzung inklusive der Bewertung von Nachweisen durch Audits und Experten-Interviews Vor-Ort. Bedingung: AL1 muss vorliegen.	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 dessen besonderen Reifegrades und Wirksamkeit. 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 bestehenden ISO 27001 Zertifizierungen auf TISAX-Bewertungen 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.*

[1] *Hinweis: Bewertungen nach Level 2 von Standorten in Ländern der Activation List sind Vor-Ort durchzuführen. Gleiches gilt für das Assessment der VDA-ISA-Kataloge Anbindung Dritter und Prototypenschutz.*

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 XAP (im folgenden Auftragnehmer) durch den Teilnehmer (im folgenden Auftraggeber) wird ein formales Eröffnungsgespräch (Kick-Off-Meeting) durchgeführt, um folgendes festzulegen bzw. zu bestätigen:

- den Scope (die Standorte),
- die relevanten ISA-Kataloge (z.B. Einbeziehung Dritter, Prototypenschutz und Datenschutz),
- die erforderlichen Objectives (Protection Level: High oder Very High) und ggfs. die entsprechenden Zielreifegrade sowie
- den Ablauf, die Termine und die Beteiligten auf beiden Seiten: Experten des Auftraggebers und Mitglieder des Bewertungsteams des Auftragnehmers.

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

b. Anschließend stellt der Auftraggeber dem Auftragnehmer die erforderlichen Dokumente zur Selbsteinschätzung (Assessment Level 1) sowie zum ISMS zur Verfügung.

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

- erstellt einen inhaltlichen Bewertungsplan auf Basis der Dokumentenprüfung (Risikobetrachtung),
- koordiniert den Teilnehmerkreis der Beteiligten für die Bewertung und
- stimmt die Bewertungstermine und den Bewertungsblauf mit allen Beteiligten ab.

d. Anschließend erfolgt die eigentliche Bewertung:

- bei Assessment Level 2 vorzugsweise als telefonisches Experten-Interview zur Selbsteinschätzung und der jeweiligen Nachweise (optional auch als Web- oder Video-Konferenz oder Vor-Ort (in jedem Fall bei Ländern der Activation-List, Anbindung Dritter und Prototypenschutz)),
- 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.
- bei Simplified Group Assessments erfolgt in der Zentrale eine intensive Vorbewertung auf Level 3
  a) des Reifegrades und der Wirksamkeit des ISMS
  b) des Durchgriffs auf die anderen Standorte und
  sowie die Bewertung der Standorte gemäß der vereinbarten 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 anschließend erläutert. Der Auftraggeber hat grundsätzlich die Möglichkeit evtl. Schwächen durch entsprechende Nachweise oder Maßnahmenpläne (Corrective Action Plans) noch während des Initial Assessments zu beheben, so das zusätzliche Aufwände reduziert oder gar vermieden werden können.

II. Corrective Action Plan Assessment

Sofern nach Abschluss des Initial Assessments offene Nichtkonformitäten bestehen, muss der Auftraggeber innerhalb der durch ENX vorgegebenen Fristen Maßnahmenpläne (Corrective Action Plans) zur Beseitigung dieser Nichtkonformitäten erstellen.
Auf Wunsch des Auftraggebers führt der Auftragnehmer die Prüfung und Bewertung dieser Maßnahmepläne durch (Corrective Action Plan Assessment), schreibt den Bewertungsbericht vom Initial Assessment fort (Update) und erläutert dem Auftraggeber die Ergebnisse und den Bericht in einem Abschlussgespräch (Closing Meeting).

III. Follow-Up Assessment

Sofern nach Abschluss des Initial Assessments offene Nichtkonformitäten bestehen, muss der Auftraggeber innerhalb der durch ENX festgelegten Fristen wirksame Maßnahmen zur Beseitigung dieser Nichtkonformitäten umgesetzt haben (Implementation / Follow-Up).
Auf Wunsch des Auftraggebers führt der Auftragnehmer eine Prüfung und Bewertung der Umsetzung der Korrekturmaßnahmen durch (Follow-Up Assessment, je nach Art bzw. Umfang der Nichtkonformitäten: vor Ort, telefonisch, Web-/Video-Konferenz), erstellt den finalen Bericht (als Fortschreibung/Update der vorliegenden Fassung) und erläutert dem Auftraggeber die Ergebnisse und den Bericht in einem Abschlussgespräch (Closing Meeting).

Der Auftragnehmer lädt den finalen Bericht auf die TISAX-Plattform hoch, wo ihn der Auftraggeber nach eigenem Ermessen freigibt. Die Erteilung der entsprechenden TISAX-Label erfolgt durch ENX.
Diese Entscheidung markiert das Ende des TISAX-Verfahrens.

5. Weitere Hinweise

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

Der Auftragnehmer führt zur Qualitätssicherung nach jeder Stufe eine sogenannte Vetoprüfung durch, in der die erstellten Berichte und Unterlagen durch eine unabhängige Person auf Fehler oder Inkonsistenzen geprüft und ggf. korrigiert/modifiziert werden.