Auf das richtige Level

Das Tisax-Assessment angemessen einschätzen

TEIL 3 In den beiden vorangegangenen Beiträgen sind die ersten fünf Schritte beschrieben, die Unternehmen auf dem Weg zum Tisax-Assessment gehen müssen. Auch die drei letzten Schritte sind nicht trivial: Es geht um den Geltungsbereich und die Entscheidung für das richtige Zertifizierungslevel.

Andreas Altena, Dr. Holger Grieb und Melanie Krauß

Auf dem Weg zu Trusted Information Security Assessment Exchange (Tisax, eine eingetragene Marke der ENX-Association), dem branchenspezifischen Framework für Informationssicherheit in der Automobilindustrie, stellen sich den Unternehmen viele Fragen. Erfahrene Experten beantworten die wichtigsten und geben praktische Empfehlungen.

Was ist denn eigentlich mein Geltungsbereich?

Viele Organisationen sind mit dem Vorgehen bei den ISO- bzw. IATF-Zertifizierungen vertraut und versuchen daher, die bekannte Begrifflichkeit des Geltungsbereiches auf das Tisax-Verfahren zu übertragen. Dies trifft bei der Geltungsbereich-Definition des Tisax-Scopes allerdings so nicht zu. Die Folgen sind Unklarheiten, die ggf. zu Problemen in der Prüfung führen können. Daher ist es wesentlich, sich in dem Tisax-Teilnehmerhandbuch das Kapitel des Tisax-Prüf-Scopes genauer unter die Lupe zu nehmen. Die aktuelle Version (V2.3 vom 20.01.21) steht auf der Webseite der ENX bzw. des VDA zum Download bereit.

Größter Unterschied bei dem Tisax-Prüf-Scope ist, dass dieser vordefiniert ist und direkt so formuliert wurde, dass alle Unternehmensbereiche, die mit vertraulichen Informationen Ihrer Partner umgehen, eingeschlossen sind. Der Gedanke dahinter ist simpel: Für alle Teilnehmer auf der ENX-Plattform ist eine größtmögliche Standardisierung der Prüfung von Vorteil, da diese wenig Interpretationsspielräume bieten. Somit können sich alle Beteiligte auf ein erteiltes Label mit Standard-Scope nahezu „blind“ verlassen. Die ENX sieht zwar noch sowohl einen reduzierten als auch einen erweiterten Scope vor, empfiehlt jedoch gerade aus genannten Gründen die Nutzung des Standard-Scopes. Dieser Empfehlung folgt auch die absolute Mehrheit der registrierten Organisationen auf der ENX-Plattform.

Bei einer bestehenden ISO/IEC 27001-Zertifizierung sollte der Deckungsgrad mit dem Standard-Scope von Tisax sehr hoch sein. Wenn in der Vergangenheit versucht wurde, den Geltungsbereich der ISO-Zertifizierungen möglichst einzuschränken, wird der Tisax-Prüfstandard-Scope sicher umfassender sein und realistischer den Ansatz zur Informationssicherheit abdecken.

Unsere Empfehlung:
Die Möglichkeiten des reduzierten oder erweiterten Tisax-Prüf-Scopes sollten vor allem in größeren Unternehmen mit mehreren Standorten in die Betrachtung einbezogen werden. Da jeder Standort im ENX-Portal registriert werden muss, ergibt sich eine gute Übersicht über den gesamten Umfang einer Tisax-Prüfung. Nicht jede Leistung wird an jedem Standort erbracht, z. B. steht nicht an jedem Standort ein Rechenzentrum, sondern eher an ein, zwei zentralen Standorten, die für das gesamte Unternehmen gültig sind.

Bei solchen Ausgangssituationen ist anzuraten, präzise und ggf. unterschiedliche Tisax-Prüf-Scopes zu definieren. Das

hat einen direkten Einfluss auf den Umfang der gesamten Prüfung.

Welchen Level an Zertifizierung muss ich machen?

Zuallererst wollen wir an dieser Stelle mit einer weit verbreiteten Fehlinterpretation aufräumen. Der Begriff des Levels wird oft mit dem Umfang der eigentlichen Prüfung gleichgesetzt. Dem ist allerdings nicht so, sondern in den einzelnen Assessment-Leveln wird die Art und Weise der Prüfungsdurchführung auf Basis der Tisax-Prüfziele definiert. Während beispielsweise der Prüfaufwand zwischen Level 2 und Level 3 in der Grundprüfung annähernd identisch ist, so erfolgt bei Level 3 eben noch eine Vor-Ort-Prüfung, die es bei Level 2 nicht gibt.

Die Tisax-Prüfziele sind abhängig von dem definierten Schutzbedarf, dem die schützenswerten Informationen unterliegen. Dieser Schutzbedarf sollte aus den Vorgaben der Kunden abgeleitet werden, um sodann in entsprechende Maßnahmen zur unternehmensspezifischen Umsetzung von Tisax zu münden. Leider zeigt die Erfahrung der Autoren, dass genau das nicht immer so einfach ist. Versuchte Klarstellungen zu den Vorgaben der Kunden ergaben in der Regel Aussagen wie: „Machen Sie bitte immer die höchste Stufe, damit gehen Sie auf Nummer sicher!“ Zweifelsfrei unbefriedigend, dass hier keine Unterstützung angeboten, sondern auf Nummer sicher gegangen wird.

Da dieser Weg also in der Regel nicht zu dem gewünschten Erfolg führt, beziehen Sie Informationen aus den bestehenden Verträgen und auch aus dem Tisax-Teilnehmerhandbuch ein. Hierüber kann eine realistische Einstufung erfolgen, denn die Kapitel der Tisax-Prüfziele, Schutzbedarfe und Assessment-Level geben hierzu durchaus Aufschluss. Beispielhaft seien Informationen mit „hohem“ (d.h. nicht „sehr hohem“) Schutzbedarf genannt, welche somit auch nur die Informationsklassifizierung „vertraulich“ (d.h. nicht „geheim“) aufweisen. Hier kann der Assessment-Level 2 mit der „Aktenprüfung/Remote“ vollkommen ausreichen und auf die Vor-Ort-Prüfung des Assessment-Level-3 verzichtet werden.

Unsere Empfehlung:

Bestimmen Sie die Schutzbedarfe der Informationswerte und die sich ableitenden Informationsklassifizierung vor dem Hintergrund Ihrer Anforderungen und nicht mit dem Blick auf ein vermeintlich einfacheres Prüfungsverfahren. Am Ende gilt das, was sehr oft hilft: Sprechen Sie so früh wie möglich mit Ihrem Prüfdienstleister. Nur so kann die für Sie richtige Kalkulation zum Prüfumfang ermittelt werden.

Schüttle ich das aus dem Ärmel oder ist das doch etwas aufwändiger?

Abhängig von dem Stellenwert, welche bereits heute die Informationssicherheit in Ihrem Unternehmen genießt, werden Sie in dem Rennen des Hasen gegen den Igel entweder glauben der Schnellste zu sein oder erleichtert feststellen können: „Ich bin schon da!“ In jedem Fall befinden Sie sich auf dem Weg, da auf Bestehendem aufgesetzt werden kann. Diesem Bild folgend ist zunächst festzustellen, dass ein Abbrechen auf halber Strecke erheblichen Schaden verursachen wird, kommt dieser Abbruch doch dem Eingeständnis gleich, der Bedeutung der Informationssicherheit nicht gerecht geworden zu sein. Auch dem Schein vor dem Sein den Vorrang zu geben, wird über kurz oder lang erkennbar und Ihrer Organisation auf die Füße fallen.

Indem wir den olympischen Gedanken dem genannten Rennen zur Seite stellen, wird deutlich, dass Sie keinesfalls schon beim ersten Rennen (sprich Assessment) herausragende Ergebnisse erreichen müssen. Die kontinuierliche Verbesserung auf einer stabilen, die Anforderungen erfüllenden Grundlage entspricht durchaus bekannten Managementprinzipien.

Unsere Empfehlung

Unterschätzen Sie den Aufwand (sowohl an erforderlichen kompetenten Mitwissern als auch an Zeit und Geld) in der Umsetzung der geforderten Maßnahmen in keinem Falle. Auf der Basis einer Analyse des Status ist die Erarbeitung der angemessenen Maßnahmen einem breit aufgestellten Team zuzuordnen. In der operativen Umsetzung ist der aktive Beitrag aller im Unternehmen einzufordern. ■

TISAX® Assessments

Schutzbedarf	Grundprüfung	Optionale Prüfung	
	Informationssicherheit	Prototypenschutz	Datenschutz
Assessment Level 1 (normal)	Selbstauskunft	Selbstauskunft	Selbstauskunft
Assessment Level 2 (hoch)	Akten Prüfung/Remote	Vor Ort	Akten Prüfung/Remote
Assessment Level 3 (sehr hoch)	Vor Ort	Vor Ort	Vor Ort
	VDA Information Security Assessment		

Bild 1. Module und die resultierenden Freigaben in der Tisax-Version 5.0 Quelle: ENX Association, © Hanser

INFORMATION & SERVICE

BEITRAGSREIHE

In der Beitragsserie zu Trusted Information Security Assessment Exchange (Tisax), dem branchenspezifischen Framework für Informationssicherheit in der Automobilindustrie sind bereits erschienen:
Teil 1 „Schritt für Schritt zum Assessment - Informationssicherheit in der Automobilindustrie: Der Blick aufs Ganze“ in QZ 7/2021.
Teil 2 „Gut vorbereitet für die Prüfung - Verantwortliche und Beteiligte im Tisax-Verfahren“ in QZ 8/2021.

AUTOREN

Andreas Altena ist Geschäftsführer der Sollence GmbH, Krefeld, Berater, Trainer und DQS-Excellence-Auditor mit den Kernkompetenzen Organisationsentwicklung und integrierte Managementsysteme, Qualitäts-, Informationssicherheits-, Risiko und (IT-)Servicemanagement.
Dr. Holger Grieb ist Lead-Consultant im Schwerpunkt Management & IT der Ksi Consult Ltd. & Co. KG, Düsseldorf, DQS-Auditor, DGQ-Prüfer, Lehrbeauftragter für „internationale Managementsysteme“ an der Hochschule Fresenius, Düsseldorf.
Melanie Krauß ist Qualitätsmanagerin und leitende Auditmanagerin bei der Continental AG, Ingolstadt, Auditorin für Prozessaudits nach VDA 6.3 und Systemaudits nach IATF 16949, Sprecherin des DGQ-Fachkreises Audit und Assessment und DGQ-Regionalkreisleiterin Mittelbayern.

KONTAKT

André Säckel
DQS-Produktmanager u.a. für ISO 27001 und Tisax
T 069 95427–8117
andre.saeckel@dqs.de