Der TISAX® 6 Standard in der Automobilindustrie

Neue Anforderungen, neue Sprache und geänderte Rahmenbedingungen - was sich durch den neuen VDA ISA Katalog 6 für Ihr Unternehmen ändert

INHALT

0 Einführung: Trusted Information Security Assessment Exchange (TISAX®)

TISAX® (Trusted Information Security Assessment Exchange) hat sich in den vergangenen Jahren als zentraler Standard für Informationssicherheit in der Automobilindustrie etabliert. Entwickelt vom Verband der Automobilindustrie e.V. (VDA) in Zusammenarbeit mit dessen Mitgliedsunternehmen, ermöglicht TISAX® eine objektive Bewertung von Informationssicherheitsmaßnahmen von Unternehmen der Automobilbranche sowie die unternehmensübergreifende Anerkennung der zugehörigen Informationssicherheits-Assessments und TISAX®-Labels.

Das Hauptziel des bereits 2017 eingeführten TISAX®-Standards ist die Schaffung eines gemeinsamen Sicherheitsstandards in der gesamten Branche, um den Schutz sensibler und vertraulicher Informationen innerhalb der Lieferkette der Automobilindustrie zu gewährleisten. Dadurch sollen Redundanzen bei den Sicherheitsbewertungen verringert werden, indem ein einmal durchgeführtes Audit von allen teilnehmenden Unternehmen anerkannt wird. Daraus resultiert eine erhebliche Kosten-, Aufwands- und Komplexitätsreduktion für Hersteller und Zulieferer. Diese Vorgehensweise soll die Praxis von Assessments in Eigenregie ablösen und für deutlich reduzierten Ressourceneinsatz bei der Sicherstellung von Informationssicherheit sorgen. Dies spart Zeit und Ressourcen sowohl für die Zulieferer als auch für die Automobilhersteller. Neben der Vergleichbarkeit der implementierten Informationssicherheits-Standards sollen zudem Best Practices und Erfahrungen rund um Cyber Security zwischen den Unternehmen ausgetauscht werden

Zentrale TISAX®-Grundlage ist das Information Security Assessment des VDA (genannt VDA ISA Katalog), der wiederum auf dem branchenübergreifenden Goldstandard der Cyber Security, der DIN EN ISO/IEC 27001, basiert. TISAX® umfasst dabei verschiedene Sicherheitsaspekte rund um die zentralen Themen Informationssicherheit, Datenschutz und Prototypenschutz, die anhand verschiedener Anforderungen (Controls) sowie dem jeweiligen Grad der Anforderung – dem sogenannten Assessment Level – bewertet werden.

Nach erfolgreich abgeschlossenem Assessment wird das Prüfergebnis auf der Plattform der ENX Association für andere TISAX®-Teilnehmer zur Verfügung gestellt; gleichzeitig wird der bilaterale Austausch mit einem ausgewählten Teilnehmer auf der Plattform forciert, um die Weitergabe von Best Practices und Erfahrungen sicherzustellen. Ein TISAX®-Label weist grundsätzlich eine Gültigkeit von 3 Jahren auf, bevor das nächste verpflichtende Assessment zu durchlaufen ist.

1 TISAX® nach VDA ISA 6 – Neue Rahmenbedingungen

Die Entwicklungen rund um eine immer komplexere Cyberbedrohungslage in einer globalisierten Wirtschaft führen über alle Branchen hinweg zu neuen und umfangreicheren Herausforderungen bei der Cybersicherheit von Unternehmen und deren Lieferketten – so auch und insbesondere in der Automobilindustrie, die sich durch die tiefe Integration von Lieferanten in Entwicklungsprozesse seit jeher der Open Innovation verschrieben hat. Um diesen hohen Anforderungen im Umgang mit sensiblen Daten zu begegnen und auch weiterhin eine starke Resilienz der Automobilindustrie in Bezug auf Informationssicherheit sowie Lieferfähigkeit sicherzustellen, wurde der dem Branchenstandard TISAX® zugrundeliegende VDA ISA Katalog zum Jahresende 2023 revisioniert, dessen neue Version 6 die Grundlage für zukünftige TISAX®-Assessments darstellt. Durch die erhöhten Anforderungen des VDA ISA 6 werden zukünftig ausgestellte TISAX®-Labels einen noch höheres Vertrauen als bisher genießen und generell einen höheren Cyber Security Standard gewährleisten. Weitere Audits, die von bestehenden Assessments abhängen (Corrective-Action-Plan Assessments, Follow-Ups, Scope-Extension Assessments, Simplified Group Assessments etc.), werden allerdings auch zukünftig auf Basis des ursprünglichen Prüfung durchgeführt.

Diese Neuerungen in der VDA ISA Version 6 sind ein entscheidender Schritt zur Stärkung der Cybersicherheitsinfrastruktur in der Automobilindustrie. Sie betonen die Notwendigkeit strategischer Planung sowie Inanspruchnahme automatisierter Tools sowie professioneller Beratungsdienste, um die neuen Anforderungen zu verstehen, die Implementierung zu planen und das TISAX®-Label erfolgreich zu erlangen bzw. zu erneuern.

In diesem Zuhammenhang haben sich nun einige Rahmenbedingungen zum TISAX®-Prozess geändert:

- Ab dem 01. April 2024 werden TISAX®-Prüfungen standardisiert nach VDA ISA 6 durchgeführt
- Ab dem 01. April 2024 sind separate Prüfungen zum Prototypenschutz möglich
- Anmeldungen nach altem Stand (VDA ISA 5.1) sind bis zum 31. März 2024 möglich; Assessments nach VDA ISA 5.1 können bis zum Jahresende durchgeführt werden
- Um der Globalisierung der automobilen Wertschöpfung Rechnung zu tragen, wurde Englisch als führende Originalsprache (statt bisher Deutsch) festgelegt – Übersetzungen in weitere Sprachen folgen

Ebenfalls wichtig für zukünftige ISMS-Anforderungen an Unternehmen: Die meisten Anforderungen aus der vieldiskutierten NIS-2-Richtlinie sind ebenfalls im aktuellen VDA ISA Katalog abgebildet. Um die gesetzlichen Anforderungen aus dem nationalen NIS-2-Gesetz, welches im Laufe des Jahres verabschiedet werden soll, zu erfüllen, sind bei Unternehmen mit gültigem TISAX®-Label nur wenige Erweiterungen des ISMS notwendig.

2 TISAX® nach VDA ISA 6 – Neue Anforderungen

TISAX® 6 führt eine Reihe neuer Anforderungen ein, die auf die steigenden Bedrohungen in der Informationssicherheit reagieren und die Sicherheitsmaßnahmen in der Automobilindustrie weiter verstärken sollen. Der VDA ISA 6 referenziert nun neben der DIN EN ISO/IEC 27001 (nach aktueller Normversion ISO 27001:2022) zudem auf den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik sowie das NIST Cybersecurity Framework und orientiert sich damit vollständig an den höchsten Standards der Informationssicherheit. Die wesentlichen Neuerungen für zukünftige Assessments lauten dabei:

- Einführung der neuen Labels Verfügbarkeit (Ausweitung des Scopes auf Operational Technology) und Vertraulichkeit (Schutz sensibler Daten)
- Produzierende Unternehmen müssen folglich Kapitel 5 (IT Security / Cyber Security) sowohl für IT als auch OT (Operational Technology) prüfen lassen
- Einführung neuer Anforderungen (Controls) auf Basis der geänderten Cyberbedrohungslage
- Zusätzliche Spalten im TISAX®-Prüfungsfragebogen zur Bereitstellung weiterführender Informationen
- Integration von Implementierungsleitfäden

Das bisherige Label "Informationssicherheit" wird in VDA ISA 6 durch spezifischere Labels für "Verfügbarkeit" und "Vertraulichkeit" ersetzt. Diese Neuerung soll zukünftige Audits präziser auf die Rolle eines Lieferanten in der Lieferkette ausrichten und ermöglicht eine differenziertere Bewertung der Sicherheitsmaßnahmen nach Zuverlässigkeit des Lieferanten und Schutzbedarf sensibler Informationen.

In Bezug auf das Prüfziel „Verfügbarkeit" differenziert TISAX® nun in die Kategorien hoch (Availability high) und sehr hoch (Availability very high). Dieses neue Prüfziel legt einen deutlich stärkeren Fokus auf die Auditierung der Produktions-IT (Operational Technology - OT) im Unternehmen. Basis für diese neue Anforderung sind die Standards der IEC 62443 (s. Teilbereich 2 – 1), die sich auf die Sicherheit industrieller Automatisierungs- und Steuerungssysteme (IACS) konzentrieren und nun in die TISAX®-Bewertungen einfließen. Ziel ist hierbei, den spezifischen Herausforderungen von OT-Umgebungen effektiv zu begegnen:

- Lange Lebenszyklen
- Angst vor Veränderungen bei OT-Verantwortlichen
- Hohe Bedeutung für die Wertschöpfung
- Veraltete Legacy-Systeme, Kommunikationsprotokolle
- Physische Zugangspunkte, zu denen zahlreiche Mitarbeitende Zugriff haben
- Unklare Zuständigkeiten / Verantwortlichkeiten IT – OT

Diese oft komplexen und hochvernetzen Produktionsumgebungen sorgen nun für neue Herausforderungen im Hinblick auf Informationssicherheit – zu selten wurden OT-Updates automatisiert durchgeführt, um dem Produktionsprozess möglichst keine potenziellen Unterbrechungen zuzumuten und damit massive Umsatzeinbußen zu riskieren. Zusätzlich entstehen durch notwendige Vernetzungen mit IT-Systemen, Netzwerken, Fernzugriffen, Predictive Maintenance und weitere Anforderungen verschiedene Risiken im Kontext der Cyber Security.

Insgesamt müssen bei der OT-Bewertung folgende Aspekte für TISAX® 6 umgesetzt werden:

- Bei der Gewährleistung der Verfügbarkeit der OT-Systeme geht es nicht nur um Produktivität und Informationssicherheit, sondern auch um Safety. Fehlfunktionen bei OT-Komponenten können Menschen oder wertvolle Anlagenkomponenten gefährden und sind dementsprechend dringend zu vermeiden.
- Das Risikomanagement wird auf die vorhandenen OT-Systeme ausgeweitet; damit müssen diese Assets klassifiziert, überwacht und verwaltet sowie verantwortliche Teams / Rollen festgelegt und neben der IT ebenfalls im Risikomanagement behandelt werden.
- Sichere Zugangskontrollen für Dienstleister – nach aktuellem Stand der Informationstechnik umgesetzt – und detaillierte Protokollierung sind für die Aufrechterhaltung der Sicherheit und Integrität der nun zu begutachteten OT-Systeme dringend erforderlich.
- Mitarbeiter müssen wie bisher angemessen geschult, kompetent und über die potenziellen Risiken des Betriebs informiert sein – dies gilt nun auch für die Verantwortlichen der OT-Systeme.
- Ein effektives Management von OT-Systemen während ihres gesamten Lebenszyklus (inkl. Reparatur, Transport und Entsorgung) im Kontext Verfügbarkeit und Cyber Security, ist von entscheidender Bedeutung, um die mit lokalen Gerätedaten und -zugriffen verbundenen Risiken zu minimieren.
- OT muss durch robuste und angemessene Maßnahmen vor potenziellen Angriffen geschützt werden.
- Die regelmäßige Durchführung technischer Systemaudits liefert die Grundlage für den notwendigen PDCA-Zyklus, um die OT-Resilienz zu überprüfen und bekannte Schwachstellen zu ermitteln.
- Vorhandene Netze müssen je nach Zweck und Risiko angemessen segmentiert werden – sowohl an der Schnittstelle IT-OT als auch in OT-OT-Umgebungen.
- Umfassende Sicherungs- und Wiederherstellungspläne inkl. regelmäßig durchzuführender Notfall- und Recovery Tests für die OT-Systeme.
- Definition und Überwachung von Service-Levels und Verfügbarkeitsdefinitionen für OT-Systeme
- Externe Anbieter: Regelung und zugehörige Dokumentation von Informationssicherheitsstandards für externe Dienstleister, die OT-Geräte nutzen.

Neben der Umsetzung von TISAX®-Anforderungen im OT-Kontext und zugehöriger Verfügbarkeit spielt auch der Nachweis der Schutzfähigkeit sensibler Informationen eine zentrale Rolle im TISAX®-Assessment. Das nun konkret benannte Prüfziel „Vertraulichkeit" kann jeweils in hoch (Confidentiality high) oder strikt (Confidentiality strict) unterteilt werden – je nach Schutzbedarf der im Unternehmen verarbeiteten Daten.

Neben diesen neu eingeführten Prüfzielen stellen insbesondere die überarbeiteten sowie zusätzlich formulierten Anforderungen große Aktualisierungen des VDA ISA Kataloges dar. Dabei wurde insbesondere das Kapitel zum Datenschutz erweitert – statt bisher 4 sind nun 12 Controls definiert, die u. a. die Widerstandsfähigkeit gegen Ransomware-Angriffe, die Erkennung und Reaktion auf Sicherheitsvorfälle sowie die Wiederherstellung nach einem Angriff thematisieren.

Insgesamt liefert der neue VDA ISA 6 Katalog sowohl im Bereich der zu erfüllenden Anforderungen als auch in Zusammenhang mit der Struktur des Fragenkatalogs einige spannende Neuerungen. Die folgende Tabelle liefert dabei einen anschaulichen Überblick über die Aktualisierungen von TISAX® 6:

Zusätzliche Spalte N: "Additional Requirements for Simplified Group Assessments (SGA)"	Erweiterung
"Reference to other Standards"	ISO27001:2022, ISA/IEC62443, NIST
Zusätzliche Spalte Q: "Reference to Implementation Guidance"	BSI, NIST
"Support" (Spalten X-Y-Z)	Erweiterungen
"Further Information" (Spalte W)	Erweiterungen
"Possible Questions"	Erweiterungen
"Possible Evidence"	Erweiterungen
1.3.4 To what extent is it ensured that only evaluated … SW is used ….?	neues Control
1.6.1 To what extent are information security relevant events … reported?	neues Control
1.6.2 To what extent are reported security events managed?	neues Control
1.6.3 To what extent is the organization to handle crisis situations?	neues Control
5.2.8 To what extent is continuity planning for IT services in place?	neues Control
5.2.9 To what extent is the backup and recovery of data and IT services guaranteed?	neues Control
3.1.2 (IS in Ausnahmesituationen)	ersetzt durch 1.6.3., 5.2.8 & 5.2.9
Reifegrade und Definitionen ("Maturity Levels and Definitions")	Ergänzungen bei Definitionen und Glossar
"Examples KPI"	Ergänzungen für Kapitel 1.6.1 / 1.6.2
Kapitel 3.1.2	zurückgezogen

Tabelle 1: Change History aus VDA_ISA_6_EN

Interessant dabei: Neben den genannten inhaltlichen Änderungen liefert der neue VDA ISA Katalog zugleich konkrete Hilfestellungen, um die gestiegenen Anforderungen zu bewältigen. Die neue Version enthält Ergänzungen bei den Definitionen im Glossar sowie praktische Leitfäden mit konkreten Beispielen und Ratschlägen zur Implementierung der Sicherheitskontrollen, um Unternehmen bei Erlangung und Umstellung nach TISAX® hilfreiche Informationen und Best Practices bereitzustellen.

Der neue Anforderungskatalog wird in der zukünftigen Audit-Praxis spezifischere TISAX®-Labels ermöglichen – für Lieferketten besonders kritische Lieferanten können beispielsweise über das Prüfziel „Verfügbarkeit" ensprechende Zuverlässigkeit nachweisen, während eine besonders hohe Vertraulichkeit als Kompetenznachweis für die Nutzung hochsensibler Daten dient. Diese neuen Labels werden nun auch in die TISAX®-Datenbank – das ENX-Portal – integriert und sorgen hier für eine größere Transparenz und einen höheren Detailgrad der geleisteten Informationssicherheit. Gleichzeitig müssen Unternehmen zukünftig nur die Anforderungen nachweisen, die sie aufgrund ihrer Rolle in der Lieferkette auch wirklich erfüllen müssen.

Die nun aktualisierten Anforderungen stellen Automobilzulieferer nun vor zusätzliche Herausforderungen. Während bereits bestehende TISAX®-konforme Informationssicherheits-Managementsysteme (ISMS) nun zusätzliche bzw. neu formulierte Controls erfüllen und insbesondere die OT in ihren ISMS-Scope implementieren müssen, stehen zahlreiche Unternehmen auf dem Weg zu ihrem ersten TISAX®-Label vor noch größeren Aufgaben als ohnehin bereits durch die – mittlerweile auch zeitkritische – Kundenanforderung, ein ISMS aufzubauen und aufrechtzuerhalten.

In der Unternehmenspraxis wurden in der Vergangenheit insbesondere zwei Methoden kombiniert, um TISAX®-konform zu agieren: Eine individuelle Dokumentablage wurde gemeinsam mit einem der zahlreichen Berater angelegt und gefüllt, in der Hoffnung auf eine TISAX®-Konformität, jedoch ohne jede Garantie auf das entsprechende Label und massive Kosten für Beratung auf Tagessatz-Basis. Gleichzeitig hatten solche Lösungen oftmals keine automatisierten und vollumfänglich richtlinienkonformen Workflows (Dokumentlenkung und -freigabe, Rollenmanagement etc.) vorzuweisen und konnten aufgrund der Notwendigkeit weiterer Tools (Risikomanagement, Maßnahmenmanagement, Kompetenzmanagement etc.) den angestrebten Anspruch einer Single-Source-of-Truth nicht ansatzweise erfüllen.

Insbesondere aufgrund fehlender Alternativen hatte sich dieses wenig effiziente und insgesamt kostenintensive Modell in der Praxis etabliert und hat in diesem Zusammenhang für einen immensen Bürokratieaufwand und unzählige Stunden nicht wertschöpfender Tätigkeiten gesorgt.

3 Vorteile eines richtlinienkonformen SaaS-ISMS

Ein leistungsfähiges Informationssicherheits-Managementsystem muss einige grundlegenden Eigenschaften aufweisen, um dem Anspruch an Funktionsfähigkeit und Ressourceneffizienz gerecht zu werden. Ein vollständig auf Basis der TISAX®-Anforderungen aufgebautes richtlinienkonformes ISMS inkl. Integriertem Dokumentenmanagement und Freigabeworkflows, welches als Software-as-a-Service-Lösung unter höchsten Standards der Informationssicherheit betrieben wird, erfüllt diese zentralen Anforderungen vollständig.

Im Hinblick auf Funktionsfähigkeit steht insbesondere die Verfügbarkeit des Systems im Vordergrund. Lokal abgespeicherte Managementsysteme, die bei einem Cyber-Security-Vorfall nicht zugänglich sind, können im Notfall ihren Zweck nicht erfüllen und haben in solchen Szenarien schlicht keinen Nutzen. Dementsprechend sind ISMS generell in der Cloud zu administrieren, um bei einem Ausfall handlungsfähig zu bleiben.

Entsprechende Software-Tools sollten selbstverständlich selbst unter höchsten Standards der Informationssicherheit betrieben werden – entsprechende Anbieter sollten dementsprechend ebenso zwingend eine gültige ISO27001-Zertifizerung aufweisen wie die für die jeweilige Instanz genutzten Rechenzentrumsbetreiber.

Abseits dessen sollte ein ISMS-Framework nicht erst umständlich aufgebaut, sondern direkt ab dem ersten Projekttag verfügbar sein. Individuell gebaute Frameworks benötigen ein hohes Maß an internem Personalaufwand ohne inhaltliche Fortschritte zu realisieren – was der eigentliche Kern des ISMS-Aufbaus sein muss. Parallel dazu lassen sich Investitionskosten bereits im Vorfeld transparent und valide abschätzen.

Neben der Funktionalität liefert ein standardisiertes TISAX®-Framework insbesondere massive Effizienzgewinne gegenüber konventionellen Lösungen. Bereits integrierte und durch erfolgreiche Assessments validierte Dokumentationsvorlagen sorgen für einen schnellen Projektfortschritt beim Aufbau eines ISMS bzw. für hochwertige Optimierung bestehender Managementsysteme. Diese Vorlagen werden auf Basis von TISAX®-Revisionen – wie nun im Rahmen des neuen VDA ISA 6 Kataloges – umfassend aktualisiert und den Nutzern bereitgestellt.

Das genutzte System-Framework enthält weiterhin die notwendigen TISAX®-Workflows (u. a. für Dokumentlenkung, Freigabe- und periodisch Prüfprozesse, Risiko- und Maßnahmenmanagement, Abarbeitung von Nichtkonformitäten und Abweichungen, Kompetenz- und Rollenmanagement, Asset Guidelines uvm.) und dient dadurch als Single-Source-of-Truth für das ISMS – das Management zahlreicher Tools, um als Informationssicherheits-Beauftragter (ISB) den Überblick zu behalten, gehört hierbei der Vergangenheit an.

Neben dem hohen Aufwand für den Aufbau eines individuellen ISMS-Frameworks bedeuten zudem die Software-Wartung und -Aktualisierung solcher Tools einen hohen Ressourceneinsatz – im Falle eines SaaS-ISMS werden sinnvolle (und ggf. normativ geforderte) Updates automatisch eingespielt, entsprechende Wartungsarbeiten werden ebenfalls automatisiert durchgeführt.

Die eigenen Mitarbeitenden können sich folglich wertschöpfenden Tätigkeiten zuwenden – das eigene TISAX®-Label kann mit maximaler Ressourceneffizienz und minimalen Kosten für die Zertifizierung erlangt und aufrechterhalten werden.

4 TISAX® nach VDA ISA 6 – Effizienter Aufbau eines ISMS

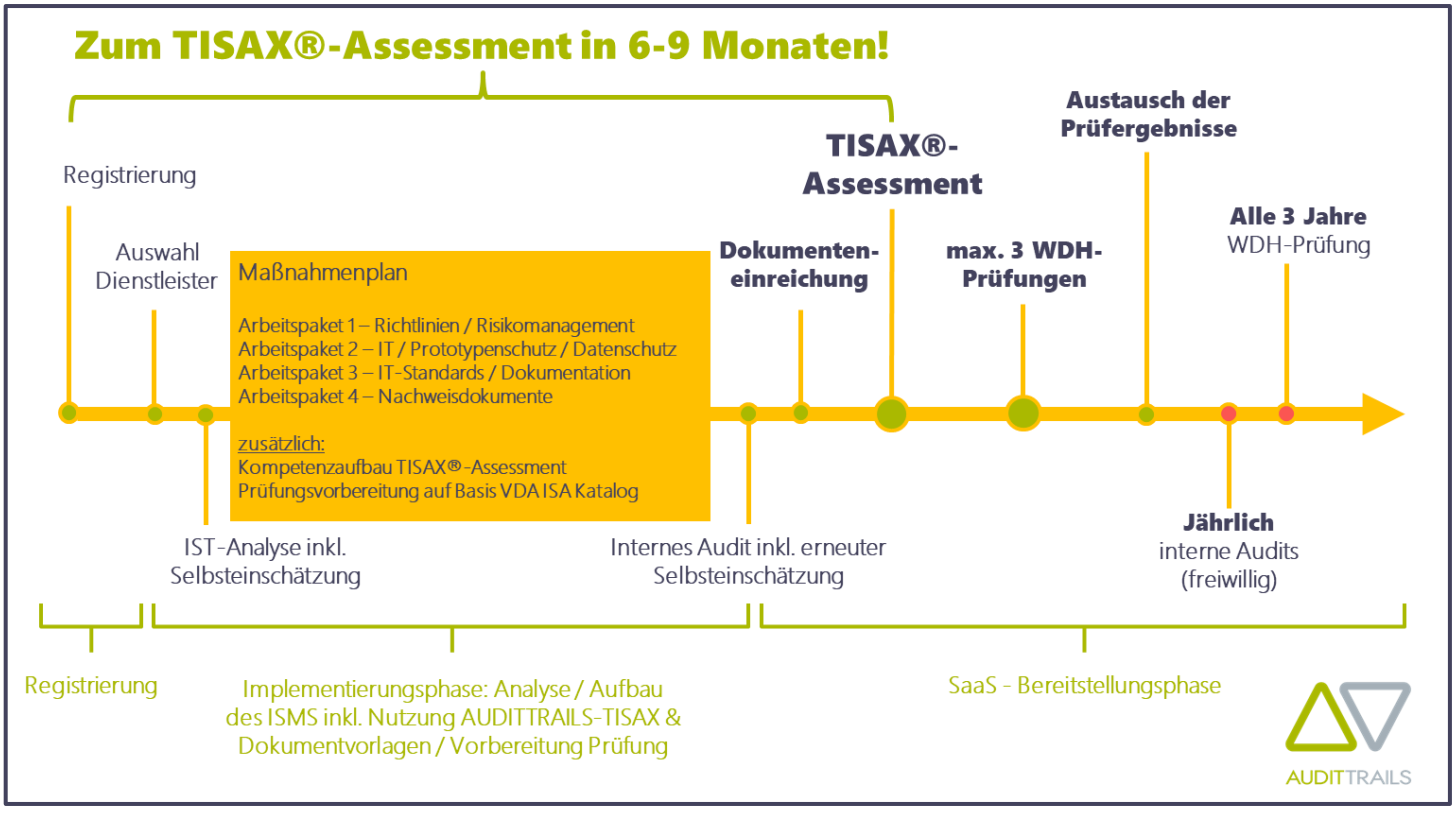

Abbildung 1: Effizienter Prozess zum TISAX®-Label

Für einen zügigen und effizienten Aufbau eines TISAX®-konformen ISMS empfiehlt sich zunächst eine rasche Registrierung und Festlegung des Scopes beim ENX-Portal – hierfür steht ein entsprechender ENX-Guide bereit. Für den Start der anschließenden Implementierungsphase empfehlen wir – abweichend von den Empfehlungen des VDA – direkt eine IST-Analyse inkl. Selbsteinschätzung auf Basis der TISAX®-Controls entlang des jeweils

notwendigen Assessment Levels vorzunehmen. Diese Bestandsaufnahme soll direkt innerhalb eines vollständig richtlinienkonformen Software-Tools erfolgen, indem die nicht erfüllten Anforderungen standardisiert als Nichtkonformitäten dokumentiert werden können. Gleichzeitig werden im Rahmen der IST-Analyse Maßnahmen zur Erfüllung angelegt und mit der betreffenden Nichtkonformität verknüpft. Selbstverständlich erhalten die Beteiligten Key-User eine umfassende Software-Schulung, um das richtlinienkonforme Tool in vollem Umfang als Single-Source-of-Truth nutzen zu können.

Der daraus innerhalb kürzester Zeit resultierende vollständige Maßnahmenplan dient in Kombination mit einem umfangreichen Dokumentvorlagen-Set – ab dem ersten Tag bereits in das Managementsystem-Framework integriert, durch TISAX®-Label-Erlangung umfassend validiert und bereits auf VDA ISA 6 aktualisiert – sowie den systemseitigen automatisierten Workflows einem enorm zügigen Projektfortschritt, da schon zu diesem frühen Zeitpunkt eine umfassende Roadmap auf dem Weg zu einem erfolgreichen Assessment bereitgestellt werden kann. Die definierten Maßnahmen – sowohl zur Dokumentation als auch zur jeweiligen (technischen) Umsetzung werden in Zusammenarbeit mit erfahrenen Consultants umgesetzt und auf Basis eines umfassenden Feedbacks aktualisiert.

Nach Abarbeitung des Maßnahmenplans und entsprechender Prüfung erfolgt zur Validierung des aufgebauten ISMS ein vollständiges internes Audit mit einem erfahrenen ISMS-Auditor, um letzte Details zu optimieren und eine hohe ISMS-Qualität für das anstehende Assessment sicherzustellen. Während der Implementierung wird durch eine entsprechende Prüfungsvorbereitung auf typische Fragen und den generellen Ablauf eines Assessments eingegangen, sodass neben dem Managementsystem selbst auch alle Beteiligten hervorragend auf die Prüfung vorbereitet sind.

Nach erfolgreichem Assessment und der zugehörigen Erlangung des TISAX®-Labels steht das Managementsystem-Framework als SaaS-Lösung inkl. Updates (z. B. im Rahmen von Richtlinienrevisionen wie dem VDA ISA 6) und einem umfassenden Service Level Agreement zur Verfügung. Die effizienten Workflows auf Basis der TISAX®-Anforderungen ermöglichen nun eine effiziente Pflege und Aufrechterhaltung des Systems bei minimalen Personalkosten und State-of-the-Art Informationssicherheit dank Erfüllung der neuesten Anforderungen.

5 TISAX® nach VDA ISA 6 – Modernisierung und Aktualisierung bestehender ISMS

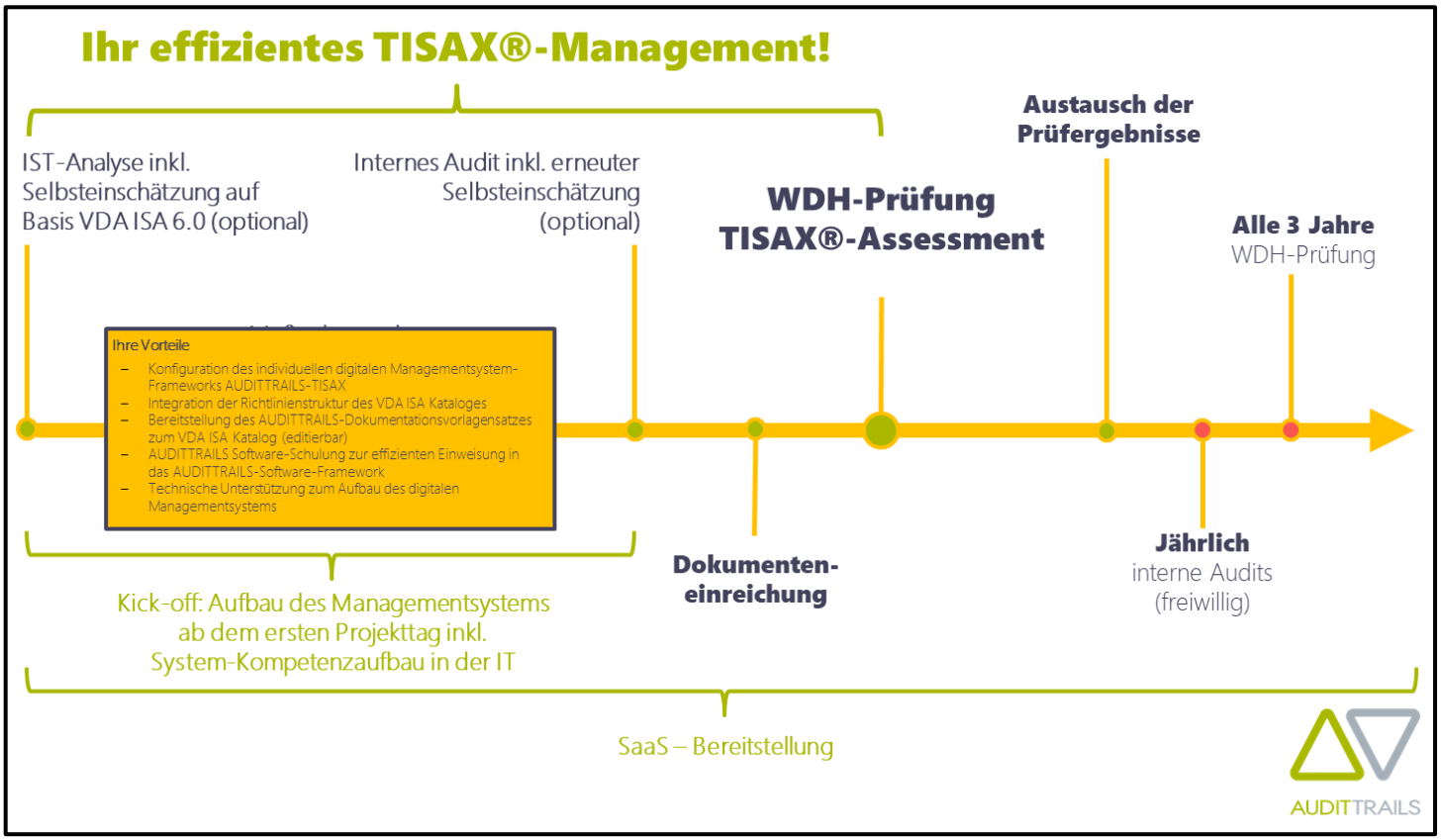

Abbildung 2: Effizientes TISAX®-Management

Die Umstellung auf ein dank automatisierter Workflows maximal effizientes ISMS-Framework bietet neben dem enormen Einsparungspotenzial von Ressourcen bei der Aufrechterhaltung gleichzeitig die Möglichkeit, das Managementsystem effizient auf die neuen Anforderungen nach TISAX® umzustellen. Auf Wunsch kann hierfür vor der selbstständigen Implementierung eine IST-Analyse auf Basis des VDA ISA Kataloges 6 absolviert werden. Hierbei werden die noch nicht erfüllten Anforderungen eines TISAX®-5.1-konformen ISMS als Nichtkonformitäten definiert und mit zugehörigen Maßnahmen verknüpft, die bei IST-Analyse definiert werden.

Im Auslieferungszustand des neuen Managementsystem-Frameworks befindet sich zur weiteren Optimierung der Dokumentation das vollständige AUDITTRAILS-Dokumentvorlagen-Set auf Basis des neuen VDA ISA 6 Kataloges, um neben der Optimierung bestehender Dokumentation gleichzeitig die neuen Anforderungen erfüllen zu können.

Nach einer umfassenden Software-Schulung zu Beginn des Projektes wird das bestehende Managementsystem in das deutlich effizientere Framework implementiert, was durch die automatisierten Workflows des Systems sowie Schnittstellen zu Azure AD etc. mit zügigem Fortschritt verläuft. Automatisierte Verknüpfungen – beispielsweise zwischen definierten Risiken und zugehörigen Maßnahmen sowie Wirksamkeitskontrollen entlang des PDCA-Zyklus oder Mitarbeitenden, ihren zugeteilten Rollen und zugehörigen Qualifikationen und Befugnissen – erleichtern sowohl die Migration bestehender Daten als auch die zukünftige Pflege enorm.

Das erfolgreich transformierte ISMS kann zudem gemäß der TISAX® 6 Anforderungen mit einem umfassenden internen Audit validiert werden, um die Konformität inkl. der neuen Anforderungen sicherzustellen. Das aktualisierte Managementsystem setzt seine zentrale Aufgabe des TISAX®-Managements nun mit höchster Effizienz und niedrigem Personaleinsatz sowie nach neuestem ISMS-Standard der Automobilindustrie um.

6 Fazit

Die neuen Anforderungen nach VDA ISA 6 – u. a. durch zusätzliche Prüfziele definiert – stellen Automobilzulieferer im Hinblick auf Maßnahmen zur Informationssicherheit vor zusätzliche Herausforderungen – insbesondere produzierende Unternehmen werden im Hinblick auf die nun notwendige OT-Integration in den TISAX®-Scope einen signifikanten Mehraufwand zu meistern haben. Die neu definierten Controls und die deutliche Orientierung an der ISO 27001:2022 als Goldstandard der Informationssicherheit heben TISAX® auf einen nochmals höheren Cyber Security Level.

Durch diese – grundsätzlich im Hinblick auf den Grad der Informationssicherheit in der Automobilindustrie zu begrüßende – Entwicklung hin zu höheren Anforderungen treten die Potenziale zur Effizienzgewinnung bei Aufbau und Aufrechterhaltung des jeweiligen Informationssicherheits-Managementsystems noch weiter in den Fokus als ohnehin schon. Die zügige flächendeckende Umsetzung von TISAX® in der Automobilindustrie ist im Hinblick auf Sicherheit und Resilienz der Branche notwendig, sie darf aber nicht unverhältnismäßig hohe (Personal-) Ressourcen beanspruchen. Das TISAX®-Management muss daher grundsätzlich auf Effizienz ausgerichtet werden, um den Fokus im Unternehmen auf die wertschöpfenden Tätigkeiten des Kerngeschäftes legen zu können; entsprechende Tools müssen dabei richtlinienkonform aufgebaut sein, relevante Workflows automatisiert im System abbilden, hochwertige Dokumentvorlagen enthalten und dank eigener Zertifizierung selbst unter höchsten Standards der Informationssicherheit bereitgestellt werden. Dies gilt sowohl für die Erlangung als auch für die Aufrechterhaltung eines TISAX®-konformen ISMS – für ressourcensparende und gleichzeitig gelebte Cyber Security.

Anhang 1: Disclaimer

TISAX® ist eine eingetragene Marke der ENX Association. Die AUDITTRAILS Networks GmbH steht in keiner geschäftlichen Verbindung zur ENX Association und bietet lediglich Beratung und Software-basierte Unterstützung zur Vorbereitung auf das Assessment nach TISAX® an. Die ENX Association übernimmt keine Verantwortung für die innerhalb dieses Whitepapers dargestellten Inhalte. Detaillierte sowie weiterführende technische Informationen zu den Änderungen im VDA ISA 6, den TISAX®-Labels und den konkreten Auswirkungen auf TISAX®-Prüfungen finden Sie auf der Website der ENX Association. Alle genannten Empfehlungen sind als Hilfestellung für Ihr Unternehmen zu verstehen. Die Entscheidung zur Erteilung eines gültigen TISAX®-Labels liegt ausschließlich bei den ENX Certified Service Providers (CSP).

Anhang 2: Kontakt / Die Autoren

Sie interessieren sich für effizientes TISAX®-Management nach aktuellem VDA ISA 6 und unter höchsten Standards der Informationssicherheit? Wir sind gerne für Sie da:

Dr. Nicholas Derra fokussiert sich nach erfolgreichem Abschluss seiner Promotion rund um praktische Anwendungen von KI und maschinellem Lernen auf seine Vision einer maximal effizienten digitalen Transformation der deutschen Wirtschaft. Nachdem er einige Jahre lang die Weiterentwicklung innovativer digitaler Geschäftsmodelle in führender Position vorangetrieben hat, liegt sein Schwerpunkt mittlerweile auf der flächendeckenden Bereitstellung effizienter Managementsystem-Frameworks zur Erfüllung der umfangreichen Anforderungen an deutsche Unternehmen, die aus den „Big 4" Normen sowie insbesondere der Informationssicherheit nach DIN EN ISO/IEC 27001 und TISAX® resultieren.

Dr. Nicholas Derra
Sales Coordinator
AUDITTRAILS Networks GmbH
nd@audittrails.com
+49 (0) 162 9258732

Thomas Schott lebt Informationssicherheit. Seit 40 Jahren von den Chancen und dem Nutzen leistungsfähiger IT begeistert, entwickelte er maßgeblich die weltweite IT-Infrastruktur und zugehörige Netzwerke in einem weltweit agierenden Konzern mit mehreren Milliarden Euro Umsatz und baute dabei eines der ersten zertifizierten ISMS in Deutschland auf. Den Green IT CIO Award (2008) gewann er ebenfalls als Erster, auch bei der Wahl zum CIO des Jahres stand er auf dem Siegerpodium. Seit 2016 agiert er als Fractional CIO und CISO, als Senior Consultant und Auditor für ISO 27001 / TISAX® definiert er zudem sein zentrales Ziel: Mehr gelebte Informationssicherheit in deutschen Unternehmen.

Thomas Schott
Senior Consultant | ISMS
AUDITTRAILS Networks GmbH
ts@audittrails.com
+49 (0) 171 8659616