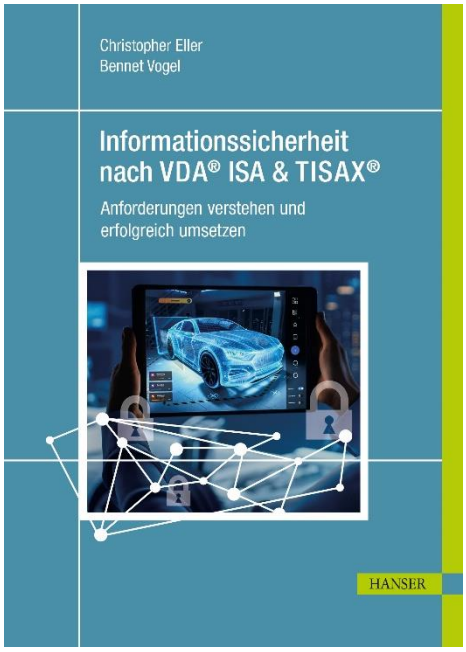
HANSER



Leseprobe

zu

Informationssicherheit nach VDA® ISA & TISAX®

von Christopher Eller und Bennet Vogel

Print-ISBN: 978-3-446-47669-1
E-Book-ISBN: 978-3-446-47751-3

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446476691
sowie im Buchhandel

Inhalt

Vorwort

TISAX® ist ein Label zum Nachweis der Erfüllung von Sicherheitsanforderungen großer deutscher Automotive-Unternehmen und betrifft nicht nur „typische Zulieferer“ im Automotive-Bereich.

Die Anforderungen der Automobilhersteller werden normenähnlich als „VDA®-ISA-Katalog“ (VDA: Verband der Automobilindustrie; ISA: Information Security Assessment) veröffentlicht, betreffen die Informationssicherheit und sind damit – abgesehen vom Sonderfall Prototypenschutz – für nahezu jedes Unternehmen sinnvoll. Unternehmen mit TISAX®-Label erreichen im Allgemeinen ein mit der ISO 27001 vergleichbar hohes und in vielen Fällen sogar höheres Niveau an Informationssicherheit.

So gut wie jedes Unternehmen, welches einen OEM (Original Equipment Manufacturer) oder größeren Zulieferer beliefert, ist bereits heute auf die Anforderungen der OEMs verpflichtet oder wird dies in naher Zukunft werden. Dies betrifft Unternehmen unterschiedlichster Art: neben den Zulieferern von Automobilteilen auch Werbeagenturen, Unternehmensberatungen, Fotografen, Softwarehäuser und viele mehr.

Der VDA®-ISA-Katalog ist inhaltlich aus der ISO-Norm 27001 hervorgegangen. Ältere Ausgaben des VDA® ISA bis Versionsnummer 4 weisen daher eine ähnliche Kapitelstruktur auf. Mit der Version 5 des VDA®-ISA-Kataloges wurde eine vollkommen neue Kapitelstruktur eingeführt. Die Verbindung zur ISO 27001 ist nicht mehr auf den ersten Blick erkennbar. Diese „Abnabelung“ von der ISO 27001 spricht für das gestiegene Selbstbewusstsein der ENX® und des VDA®, mit TISAX® eine Erfolgsgeschichte begründet zu haben.

Wenn Sie bereits mit ISO-Normen und den üblichen Auditverfahren vertraut sind, wird Ihnen auch in der „TISAX®-Welt“ vieles vertraut vorkommen. Auch hier gibt es eine Norm, allerdings in Form einer Excel-Tabelle, in der Sie direkt Angaben zur Umsetzung der Normforderungen eintragen. Auch Audits gibt es – hier heißen sie Prüfungen –, allerdings nur einmal alle drei Jahre. Statt einer DAkkS hat die ENX® die Oberaufsicht über die zugelassenen Zertifizierungsstellen – die bei TISAX® Prüfdienstleister heißen. Nur auf das geliebte Zertifikat an der Wand müssen Sie

verzichten – die *TISAX®-Label* sind ausschließlich elektronisch im Portal der ENX® einsehbar.

Zur Verwendung dieses Buches einige Hinweise: Wenn wir verkürzend von „der Norm“ oder „TISAX®-Anforderungen“ schreiben, meinen wir die Anforderungen des VDA®-ISA-Kataloges, welche dann im TISAX®-Verfahren geprüft und deren Ergebnisse mit anderen Unternehmen geteilt werden. Die Prüfung zur Erreichung des TISAX®-Labels ist vergleichbar mit einem Zertifizierungsaudit, wir bezeichnen diese Prüfung deshalb synonym auch als Audit.

Die Kapitel sind in derselben Reihenfolge geschrieben wie im VDA®-ISA-Katalog. Auch die Kapitelnamen und die Nummerierung haben wir eins zu eins übernommen. So haben Sie als Leser den größten Nutzen, denn Sie können dieses Buch wie ein Nachschlagewerk verwenden, um sich in kurzer Zeit Klarheit über einzelne TISAX®-Anforderungen zu verschaffen.

Geschrieben haben wir das Buch in klarer Sprache, und zwar konsequent praxisorientiert und ohne Vorwissen verständlich. Unser Anspruch ist es, ein möglichst hohes Verständnis der TISAX®-Anforderungen zu ermöglichen und zugleich direkt umsetzbare Empfehlungen zur Umsetzung zu vermitteln.

Redaktionsschluss für dieses Buch war im Oktober 2022. Hierbei wurden die aktuell gültige Fassung 5.1.0 des VDA®-ISA-Kataloges und das Prüfziel Information Security zugrunde gelegt.

Darmstadt und Berlin im Frühjahr 2023 *Christopher Eller*

Bennet Vogel

Hinweise

Dieses Werk behandelt die Norm „VDA® ISA“ in der Version 5.1.0.

- Herausgeber: VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA); Behrenstr. 35; 10117 Berlin; www.vda.de © 2022 Verband der Automobilindustrie e. V., Berlin.
- Quelle: *https://www.vda.de/dam/jcr:6ea8f56e-8497-4e65-866d-d4cf98ea6e59/VDA_ISA_5_1_DE.xlsx*
- Dieses Werk ist unter der Creative Commons Namensnennung – Keine Bearbeitungen 4.0 International Public License lizenziert.

Im Text des Buches wird in den Kapitelüberschriften und den Boxen „Zitat aus der VDA® ISA 5.1.0“ aus dieser Norm zitiert. Die Gliederungsstruktur des Buches orientiert sich an der Norm.

Die Autoren des Buches sind kein Teil und auch nicht verbunden mit dem VDA® oder der ENX®. Die folgenden Warenzeichen finden Erwähnung:

- TISAX® ist ein eingetragenes Warenzeichen der ENX® Association.
- VDA® ist ein eingetragenes Warenzeichen des Verbandes der Automobilindustrie.
- ISO ist ein eingetragenes Warenzeichen der Internationalen Organisation für Normung.
- DIN ist ein eingetragenes Warenzeichen des Deutschen Instituts für Normung.

Der VDA stellt das „Information Security Assessment“ aktualisiert zum Download zur Verfügung. Abrufbar unter *https://portal.enx.com/de-de/TISAX/downloads/* bzw. unter *https://www.vda.de/de/themen/digitalisierung/daten/informationssicherheit*.

1 IS Policies and Organization

1.1 Information Security Policies

1.1.1 Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?

Zitat aus der VDA® ISA 5.1.0

Die Organisation benötigt mindestens eine Richtlinie für Informationssicherheit. Diese spiegelt die Wichtigkeit und Bedeutung der Informationssicherheit wider und ist an die Organisation angepasst. Weitere Richtlinien können je nach Organisationsgröße und -struktur sinnvoll sein.

Muss

- Die Anforderungen an die Informationssicherheit sind ermittelt und dokumentiert:
  - Die Anforderungen sind an die Ziele der Organisation angepasst.
  - Eine Richtlinie ist erstellt und von der Organisationsleitung freigegeben.
- Die Richtlinie enthält Ziele und den Stellenwert der Informationssicherheit in der Organisation.

Sollte

- Die Anforderungen an die Informationssicherheit auf der Grundlage der Organisationsstrategie, Gesetzen und Verträgen sind in der Richtlinie berücksichtigt.
- Die Richtlinie weist auf Konsequenzen bei Nichtbeachtung hin.
- Weitere relevante Richtlinien zur Informationssicherheit sind erstellt.
- Eine regelmäßige Prüfung und – falls notwendig – Überarbeitung der Richtlinien sind etabliert.
- Die Richtlinien werden Mitarbeitern in geeigneter Form (z. B. Intranet) zur Verfügung gestellt.
- Die Richtlinien werden fallbezogen (ggf. auch in Auszügen) an externe Geschäftspartner weitergegeben.
- Mitarbeiter und externe Geschäftspartner werden über für sie relevante Änderungen informiert.

In diesem Abschnitt geht es um die Erstellung mindestens einer Richtlinie für die Informationssicherheit. Die Norm zielt darauf ab, dass Richtlinien und Anforderungen an Informationssicherheit schriftlich vorgehalten werden. Es sollte mindestens eine *Richtlinie zur Informationssicherheit* erstellt werden.

Umsetzung der Muss-Anforderungen

Eine **Muss-Anforderung** ist zwingend zu erfüllen. Die Erfüllung einer Muss-Anforderung kann nicht ausgeschlossen werden.

Anforderungen ermitteln und dokumentieren

Sie erstellen mindestens eine zentrale Richtlinie für die Informationssicherheit *(Informationssicherheitsrichtlinie)*. Eine solche Richtlinie ist üblicherweise etwa zehn bis 15 Seiten lang. Sie beschreibt insbesondere Folgendes (Auswahl):

- Eine Beschreibung aus Sicht der Unternehmensleitung, warum Informationssicherheit für Ihr Unternehmen wichtig ist und wie Sie grundsätzlich eine hohe Informationssicherheit herstellen wollen.
- Eine Beschreibung, wie Ihr Unternehmen grundsätzlich die Ziele Vertraulichkeit, Verfügbarkeit und Integrität von Informationen sicherstellen will (strategischer Ansatz).
- Sie stellen messbare Ziele *(KPI – Key Performance Indicator)* für die Informationssicherheit für einen fest definierten Zeitraum auf (z. B. Einstellung von zwei neuen Mitarbeitern in der IT, Einführung der Zwei-Faktor-Authentifizierung für System X, Anschaffung eines neuen Servers usw.). Da sich diese Ziele regelmäßig ändern, empfiehlt es sich, sie in einem getrennten Dokument (KPI) zu beschreiben und in der zentralen Richtlinie auf sie zu verweisen.
- Allgemeine Verhaltensregeln für den Umgang mit Informationen und mit bereitgestellter Hard- und Software (z. B. Verbot der lokalen Speicherung privater Dateien, Verhaltensregeln bei Verlust eines Firmen-Notebooks usw.).

Die Richtlinie muss in geeigneter Form gespeichert sein. Hier bietet sich das PDF-Format an oder ein Eintrag im Intranet. Wichtig ist, dass die Richtlinie nur durch berechtigte Personen editiert werden kann.

Wir empfehlen, in jede Richtlinie eine Versionshistorie aufzunehmen. Zwingend vorgeschrieben ist die Freigabe durch die Geschäftsleitung. Eine Unterschrift/elektronische Unterschrift der Geschäftsleitung ist von der Norm nicht vorgeschrieben. Sie können selbst regeln, wann ein Dokument als freigegeben gilt. Auf jeden Fall müssen das Datum der Freigabe und der Name der freigebenden Person aus der Geschäftsleitung erkennbar sein.

Es bietet sich an, in der zentralen Richtlinie auf weitere einzelne Richtlinien zu verweisen. So können Sie etwa das Thema Virenschutz oder Vergabe von Nutzerberechtigungen kurz in der zentralen Richtlinie beschreiben und auf die ausführlichen Beschreibungen in den jeweiligen einzelnen Richtlinien verweisen. Alternativ können Sie alles in der zentralen *Richtlinie zur Informationssicherheit* beschreiben, dann sind Sie schnell bei einem Umfang von 150 Seiten oder mehr. Dies ist unüblich, aber gemäß der Norm zulässig.

Policy ist nicht gleich Policy!

Vorsicht ist bei der englischen Version der Norm geboten. Hier wird der Begriff *Policy* für *Richtlinie* verwendet. *Policy* kann aber auch mit *Politik* übersetzt werden. Tatsächlich verlangt die Norm keine Informationssicherheitspolitik oder Information Security Policy, wie dies z. B. bei der ISO 27001 der Fall ist.

Umsetzung der Sollte-Anforderungen

Eine **Sollte-Anforderung** sollte zwar erfüllt werden, wenn es allerdings eine nachvollziehbare Begründung gibt, dass diese nicht erfüllt wird, kann sie ausgeschlossen werden.

Erweiterte Anforderungen

Sie beschreiben in der zentralen *Richtlinie zur Informationssicherheit* auch Folgendes:

- Eine Beschreibung aus Sicht der Unternehmensleitung, warum Informationssicherheit für Ihr Unternehmen wichtig ist, insbesondere die strategische Bedeutung und die Bedeutung in Hinblick auf geltende Gesetze und vertragliche Vereinbarungen.
- Verantwortlichkeiten (z. B. Information Security Officer – ISO, Datenschutzbeauftragter, System-Administratoren) werden benannt, z. B. in einer Funktionsmatrix.
- Sie weisen auf arbeitsrechtliche und mögliche strafrechtliche Konsequenzen (Angabe von einzelnen Gesetzen oder Paragrafen ist nicht erforderlich) hin für den Fall, dass Mitarbeiter gegen die Richtlinie verstoßen. Weitere Anforderungen hierzu in Abschnitt 2.1.1.

Prüfung und weitere Richtlinien ermitteln und dokumentieren

Weitere Richtlinien – wie beschrieben – müssen ebenfalls in geeigneter Form gespeichert und freigegeben sein. Hier gilt jedoch ein Unterschied: Nur die zentrale *Richtlinie zur Informationssicherheit* muss von der Geschäftsleitung freigegeben

sein. Alle weiteren Richtlinien können z. B. auch vom Information Security Officer freigegeben werden.

Die Richtlinien müssen allen Personen, die sie betreffen, zugänglich sein, am besten durch Ablage in einer geeigneten Ordnerstruktur. Bei Änderungen an den Richtlinien sind die betroffenen Personen zu informieren. Bei Bedarf können einzelne Inhalte auch an Geschäftspartner weitergegeben werden. Dieser Punkt spielt in der Praxis zunehmend eine Rolle, da Unternehmen immer häufiger im Rahmen von Self-Assessments aufgefordert werden, einzelne Richtlinien ihren Auftraggebern zur Verfügung zu stellen.

Sämtliche Richtlinien prüfen Sie regelmäßig – mindestens einmal jährlich – auf Aktualität und Vollständigkeit. Diese Prüfung(en) planen Sie am besten in Ihrer zentralen Maßnahmenliste *(Maßnahmenplan)* oder als Serientermin in Ihrem Kalender. Die durchgeführte Prüfung muss immer dokumentiert werden, auch wenn Sie inhaltlich keine Veränderungen an den Dokumenten vornehmen. Tabelle 1.1 zeigt beispielhaft, wie ein Maßnahmenplan aufgebaut sein könnte.

Tabelle 1.1 Maßnahmenplan (Beispiel)

ID	Anforderung	Maßnahme	Verantwortlich	Termin	Prüfung
…	…	…	…	…	…
…	…	…	…	…	…

1.2 Organization of Information Security

Die Normforderung beschreibt die Anforderungen an die organisatorischen Strukturen und Maßnahmen zur Umsetzung von Informationssicherheit. Hieraus leitet sich zentral das Erfordernis zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) ab.

1.2.1 Inwieweit wird in der Organisation Informationssicherheit gemanagt?

Zitat aus der VDA® ISA 5.1.0

Nur wenn Informationssicherheit in den strategischen Zielen einer Organisation verankert ist, kann Informationssicherheit nachhaltig in einer Organisation umgesetzt werden. Das Informationssicherheitsmanagementsystem (ISMS) ist ein Steuerungsinstrument für die Organisationsleitung, mit dem sie sicherstellt, dass Informationssicherheit nicht nur ein Ergebnis von Zufällen und individuellem Engagement, sondern von nachhaltigem Management ist.

Muss

- Der Geltungsbereich (Scope) des ISMS (die vom ISMS gemanagte Organisation) ist festgelegt.
- Die Anforderungen der Organisation an das ISMS sind ermittelt.
- Die Organisationsleitung hat das ISMS beauftragt und freigegeben.
- Das ISMS stellt der Organisationsleitung geeignete Kontroll- und Steuerungsmittel zur Verfügung (z. B. Management-Review).
- Anwendbare Kontrollen wurden ermittelt (z. B. ISO 27001 Statement of Applicability, ausgefüllter ISA-Katalog).
- Die Wirksamkeit des ISMS wird regelmäßig durch das Management überprüft.

Grundsätzlich muss Ihre Organisation die Struktur, Verantwortlichkeiten und Mittel zur Einhaltung der Informationssicherheit definieren, um sicherzustellen, dass „Informationssicherheit“ im beabsichtigten Rahmen umgesetzt wird und die gewünschten Ergebnisse erzielt werden.

Umsetzung der Muss-Anforderungen

Festlegen des Scopes

Um darzulegen, welchen Scope Ihr Unternehmen für das ISMS anstrebt, sollte ein Dokument (Erklärung der Anwendbarkeit oder *Scope*) erstellt werden, in dem Sie darlegen:

- Welche Norm inklusive Versionsnummer berücksichtigt das Unternehmen zur Umsetzung des ISMS?
- Welches Assessment-Level und welche Prüfziele sind gewählt?
- Welche Standorte umfasst das ISMS (einschließlich Nennung der Adressen)?
- Welche spezifischen Ein- oder Ausschlüsse gelten?

Das Dokument sollte durch die Geschäftsführung freigegeben werden.

Index

N

O

P

R

S

T

V

W

Z