mabs4.0 Deutschland GmbH

modelling advanced business security

TISAX®

Trusted Information Security Assessment Exchange

Herausgeber

mabs4.0 Deutschland GmbH
Großenbaumer Weg 8
40472 Düsseldorf

Telefon: +49 211 205 444 80
Telefax: +49 211 205 444 81

Internet: http://mabs40.de.com

Vorwort

Liebe Interssenten,

herzlichen Dank für Ihr Interesse an unserem Portfolio.

Die **mabs4.0 Deutschland GmbH** aus Düsseldorf ist eine Unternehmensberatung mit dem spezifischen Fokus auf den drei Säulen **IT- & Informationssicherheit, Management-beratung und das Business Process Management**.

Als solches unterstützen wir erfolgreich unsere Kunden unter anderem bei der Umsetzung und Einführung von **Informationssicherheitsmanagementsystemen (ISMS) wie beispielsweise gemäß ISO27001, BSI Grundschutz oder TISAX®.**

Darüber hinaus erstreckt sich unser Portfolio in der ganzheitlichen Erhöhung des Schutzniveaus.

Auch das parallele Management verschiedenster, meist ineinandergreifender Normen („Multi-Normen-Management“) kann dabei in den Mittelpunkt rücken.

Unser erfahrenes Team unterstützt Sie beratend als auch umsetzend mit nachgewiesener Expertise und langjährige Erfahrungen bei den für Sie notwendigen Ausarbeitungen und Anpassungen.

Unser Ziel ist es, unsere Kunden als Partner in Augenhöhe nach seinem tatsächlichen Bedarf zu unterstützen.

Unsere Leistungen orientieren sich immer nach der benötigten Angemessenheit und Wirtschaftlichkeit.

Kontaktieren Sie uns gerne und unverbindlich für ein erstes kostenloses Beratungsgespräch. Gerne kommen wir auch zu Ihnen und bewerten mit Ihnen Ihre Herausforderungen.

Herzliche Grüße

Eric Schneider
Geschäftsführer der mabs4.0 Deutschland GmbH

+49211 - 205 444 80
kontakt@mabs40.com
www.mabs40.de.com

Großenbaumer Weg 8
40472 Düsseldorf
Deutschland

Inhalt

+49211 - 205 444 80
kontakt@mabs40.com
www.mabs40.de.com

Großenbaumer Weg 8
40472 Düsseldorf
Deutschland

1 Über die mabs4.0 Deutschland GmbH

Die mabs4.0 Deutschland GmbH (kurz: mabs) ist ein international agierender und unabhängiger Düsseldorfer Spezialist für

- IT & Informationssicherheit Managementsysteme,
- Integrierte Managementsysteme,
- Business Process Management und
- Interim Management.

Mit nachgewiesener Expertise und Fokussierung behandelt die mabs die gesetzlichen und normativen Anforderungen zur Informationssicherheit, wie das deutsche IT-Sicherheitsgesetz oder die EU-DSGVO genauso wie Kunden- und Normanforderungen (z.B. ISO27001 oder TISAX®) oder Maßnahmen der Digitalisierung (z.B. Cybersicherheit) und setzt diese erfolgreich gemeinsam mit Ihren Kunden um.

Die häufig hinzukommenden verschiedenen, teils bestehenden, Anforderungen aus Umweltschutz (z.B. ISO 14001), Qualitätsnormen (ISO 9001, IATF 16949), Arbeitssicherheit (ISO 45001) oder weiterer Anforderungen können zudem in einem integrierten Managementsystem (IMS) erfasst werden.

Anhängige oder betroffene Prozesse und Strukturen werden durch unsere Experten bei Bedarf analysiert und modelliert.

Die mabs unterstützt seine Kunden aus den Branchen Automotive, Industrie & Maschinenbau, Dienstleistungen, Banking, Telekommunikation, Gesundheitswesen und Pharmazie in ihren Vorhaben mit Augenmaß und schafft so transparente Projektstrukturen und echten Kundennutzen.

2 Unser USP

Wir bei mabs haben uns auf unsere Fachkompetenzen fokussiert und bauen diese stetig weiter aus. Mehr als 50 Jahre Praxis- und Projekterfahrung in unterschiedlichen Branchen haben uns gelehrt, dass stabile Organisationsprozesse das Ausfallrisiko von IT- & Informationssicherheit gestützten Wertschöpfungsketten minimiert.

Wir sind hoch qualifiziert, erfahren und motiviert – unser Ziel ist es, Ihre Organisation bestmöglich ganzheitlich einzubinden, um Ihre Resilienz zu stärken. Wir sind nicht die klassischen Berater, wir sind Ihr Partner und Verbündeter zur Sicherung Ihrer Informationswerte.

Mit mabs zusammenzuarbeiten bedeutet immer effizient und mit Augenmaß gemeinsam passende Lösungen für Ihre Organisation zu finden. Fokussiert und zielgerichtet. Wir bringen best practise mit und helfen Ihnen Fehler zu vermeiden und einen Schritt voraus zu sein.

Wir sind Profis in dem was wir tun, wo wir nicht die Experten sind, arbeiten wir mit den Profis aus unserem Netzwerk zusammen.

Unsere Experten hören Ihnen zu. Nicht um zu antworten, sondern um zu verstehen.

○ Etablierte Prozesse und Verantwortlichkeiten ○ Kostenminimierung ○ Nachweise der Erfüllung von Kundenanforderungen ○ Nachweis der Erfüllung von normativen und gesetzlichen Anforderungen ○ Haftungsreduzierung ○ Wettbewerbsvorteile ○ Minimierung von Risiken und möglichen Schäden ○ Durchführung von Penetrationstests ○ Schulung und Unterweisung von Mitarbeitern

3 Rechtlicher Hinweis

TISAX® ist eine eingetragene Marke der ENX Association. mabs4.0 steht in keiner geschäftlichen Beziehung zu ENX. Mit der Nennung der Marke TISAX® ist keine Aussage des Markeninhabers zur Geeignetheit der hier benannten Leistungen verbunden.

+49211 - 205 444 80
kontakt@mabs40.com
www.mabs40.de.com

Großenbaumer Weg 8
40472 Düsseldorf
Deutschland

4 Summary

TISAX® (Trusted Information Security Exchange[1]) ist ein von der Automobilindustrie entwickelter Anforderungskatalog, welcher angemessene Schutzmaßnahmen für Informationssicherheit innerhalb der Kunden-, Lieferantenbeziehung beschreibt. Diese Anforderungen sind detailliert im VDA Information Security Assessment (ISA) Katalog beschrieben. Mit einem erfolgreich durchlaufenden TISAX®-Assessment schaffen Sie ein Informationssicherheitsmanagementsystem (ISMS) nach VDA-ISA und sichern sich darüber hinaus den Marktzugang in der Automobilindustrie.

Unternehmen in der Lieferkette der OEMs sind angehalten, ein ISMS nach VDA-ISA aufzubauen. Teilweise kommt die Aufforderung der OEMs, ein solches ISMS nachzuweisen, sehr kurzfristig und stellt Unternehmen vor großen Herausforderungen.

Seit Oktober 2020 gilt der VDA-ISA Katalog in der Version 5, der von der internationalen Norm ISO/IEC 27001 abgeleitet wurde (die vorherigen Versionen doch auch?). Er ist die Basis für Ihre Selbstauskunft und das externe TISAX®-Assessment zur Erreichung des TISAX®-Labels.

Bestandteile des VDA-ISA Katalogs sind a) Informationssicherheit, b) Prototypenschutz und c) Datenschutz. Je nachdem, wie der OEM Ihr Unternehmen eingestuft hat, müssen Sie die Anforderungen des jeweiligen Kapitels erfüllen. Hierbei legt der OEM zumeist auch den zu erfüllenden Schutzbedarf fest. Anhand der zu erfüllenden Kapitel und des Schutzbedarf wird der Scope definiert, von diesem das Assessment-Level abgeleitet wird.

Wie Sie die TISAX®-Anforderungen passgenau für Ihre Organisatin umsetzen, dazu gibt dieses Whitepaper wichtige Informationen und eine erste Orientierung.

Wir freuen uns über Ihre Rückmeldung und einen persönlichen Austausch zu Ihren Herausforderungen und Bedürfnissen zur Umsetzung des VDA-ISA Katalogs zur Erreichung des TISAX®-Labels. Unsere Experten stehen Ihnen jederzeit gerne für Ihre Fragen zur Verfügung.

Selbstverständlich ist das Erstgespräch unverbindlich und kostenlos. Buchen Sie einfach einen Termin über unsere Internetseite https://mabs40.de.com.

Mit herzlichen Grüßen,

Ihr mabs Experten Team

[1] TISAX® ist eine eingetragene Marke der ENX Association.

5 Was ist TISAX®

TISAX® ist ein Informationssicherheitsmanagementsystem (ISMS) auf Basis des VDA-ISA Katalog. Ziel ist es ein ISMS anhand der spezifischen Anforderungen der Automobilindustrie umzusetzen und zu etablieren. Auch wenn der VDA-ISA Katalog von der internationalen Norm ISO/IEC 27001 abgeleitet ist, enthält dieser beispielsweise auch Anforderungen die den Prototypenschutz von Teilen/Komponenten oder Erprobungsfahrzeugen beinhalten.

6 Wer benötigt ein TISAX®-Label

Generell wird das TISAX® -Label spätestens dann benötigt, wenn die Anforderung durch den OEM an den Automobilzulieferer formuliert und kommuniziert ist. Oftmals geschieht dieses bei Neuinitiierung eines Projektes.

7 Welche Vorteile sind durch ein TISAX®-Label zu erwarten

Prinzipiell sollte jedes Unternehmen technisch organisatorische Maßnahmen umgesetzt haben, um ein bedarfsgerechtes Schutzniveau der IT- & Informationssicherheit zu gewährleisten. Zumeist orientieren sich Unternehmen hierbei an der internationalen Norm ISO/IEC 27001.

Durch TISAX® erhalten Sie zusätzlich Vorteile in der Kunden-, Lieferantenbeziehung.

- Branchenweit einheitliches Schutzniveau
- Vertrauensbasis zwischen den Geschäftspartnern
- Prüfergebnisse sind bei allen Teilnehmern vergleichbar
- Überprüfung des ISMS nur alle 3 Jahre
- Schutz Ihrer Informationswerte (Daten)
- Prozesssicherheit
- Gelebtes Risikomanagement
- Bewusstsein bei Ihren Mitarbeitenden

8 Was sind Unterschiede zwischen TISAX® und ISO/IEC 27001

Der wesentliche Unterschied besteht in der Umsetzung.

Ein normatives ISMS auf Basis der ISO/IEC 27001 passen Sie an Ihr Unternehmen an und setzen somit die normativen Anforderungen passend zu Ihrer Organisation um. Hierbei sind Sie relativ frei in der Methodik und in der Erbringung der geforderten Nachweise. Der Auditor wird zumeist Ihren Ansatz folgen, sofern sich ihm dieser erschließt und den normativen Anforderungen entspricht. Die Auditierung erfolgt nach Angemessenheit zu Ihrem Unternehmen. Somit ist ein ISMS gemäß ISO/IEC 27001 aus Ihrer Sicht umgesetzt.

TISAX® im Gegensatz stellt hingegen über den VDA-ISA Katalog Anforderungen an Ihr Unternehmen aus Sicht des OEMs. Der OEM stellt hierdurch sicher, dass sein Schutzbedarf der Informationswerte entsprechend in Ihrer Organisation umgesetzt ist. Die Anforderungen und deren Umsetzung werden unterschieden in:

- MUSS-Anforderungen
- Soll-Anforderungen
- Anforderungen für hohen Schutzbedarf
- Anforderungen für sehr hohen Schutzbedarf

Somit wird bei TISAX® die tatsächliche Umsetzung der Anforderungen geprüft. Hierbei muss sichergestellt sein, dass alle Anforderungen 1:1 umgesetzt sind. Das TISAX®-Label hängt oftmals von einigen wenigen kritischen Faktoren ab.

9 Was sind Assessment-Level

Abhängig vom geforderten Schutzniveau wird Ihr ISMS unterschiedlich intensiv geprüft. Die Prüfintensivität hängt vom Assessment-Level (AL) ab, welcher sich von dem geforderten Scope ableitet.

Sobald Sie Informationswerte mit sehr hohem Schutzbedarf prozessieren, Anforderungen des Prototypenschutzes oder des Datenschutzes bei besonderen Kategorien personenbezogener Daten erfüllen müssen, wird Ihr ISMS gemäß Assessment-Level 3 geprüft.

Schutz-bedarf	AL	Prüfaufwand	Aufwand
Normal	1	Selbsteinschätzung ohne externe Plausibilitätsprüfung. Dient zumeist nur internen organisatorischen Zwecken und wird nicht als TISAX® Prüfergebnis verwendet.	gering
Hoch	2	Plausibilitätsprüfung der Selbstauskunft durch einen externen Prüfdienst-leister. Die Prüfung erfolgt remote per Telefon-, oder Online-Interview. Die Nachweise sind vorab an den Prüfdienstleister bereitzustellen.	mittel
Sehr hoch	3	Vor-Ort-Assessment an mindestens 2 Tagen. Der externe Prüfdienstleister prüft alle Dokumente und Nachweise bei Ihnen vor Ort. Typischerweise erfolgt auch eine Begehung und Bewertung der Betriebsstätte.	hoch

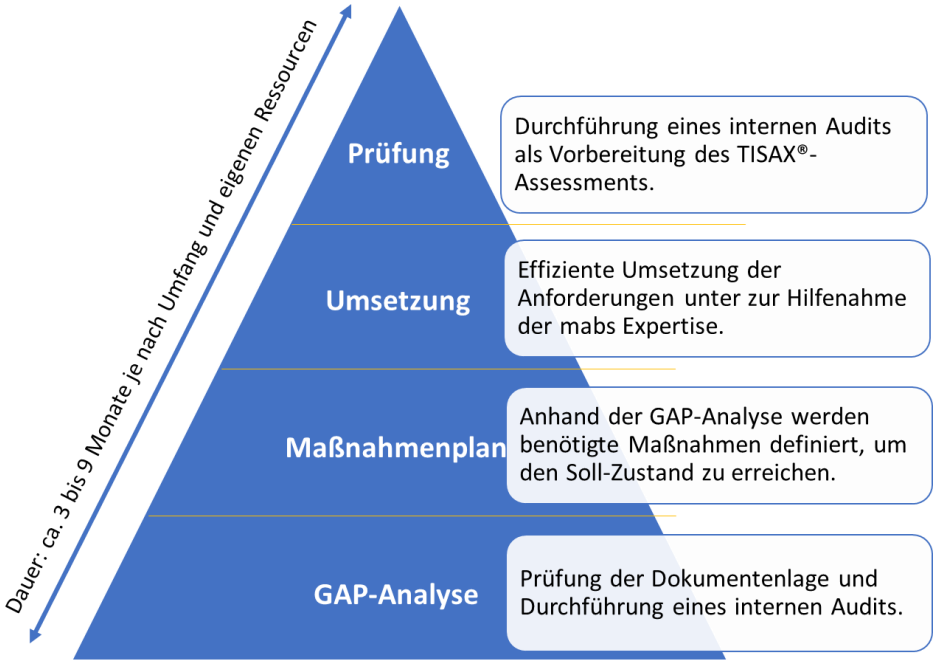
Eine Prüfung gemäß Assessment-Level 2 erscheint erst einmal recht verlockend. Allerdings haben Sie somit nur geringen“ Einfluss“ auf die Prüfung. Die Praxis hat gezeigt, dass eine Vor-Ort-Prüfung oftmals Vorteile hat und der Dialog mit dem Prüfer darüber hinaus durchaus wertvolle Informationen für das Follow-Up (Nachprüfung der erforderlichen Maßnahmen bei festgestellten Abweichungen) beinhaltet.

+49211 - 205 444 80
kontakt@mabs40.com
www.mabs40.de.com

Großenbaumer Weg 8
40472 Düsseldorf
Deutschland

10 Unser Vorgehensmodell

Unser Vorgehensmodell basiert auf 4 Eckpfeilern.



11 Unsere Leistungen

Wir haben nicht nur die Qualifikationen, sondern auch die fachliche Kompetenz und Praxiserfahrung. Unsere Kompetenz haben wir in vielen erfolgreichen Projekten unter Beweis gestellt. Alle von uns unterstützten Unternehmen sind erfolgreich unabhängig geprüft worden und verfügen über ein etabliertes Informationssicherheitsmanagementsystem (ISMS) welches TISAX® konform ist.

Wir haben das Ziel, unsere Kunden zu befähigen und bauen auf eine langfristige Partnerschaft. Durch engagiertes und verantwortungsvolles Handeln eines jeden Einzelnen erreichen wir ein Höchstmaß an Identifizierung mit unseren Kunden.

11.1 Ermittlung Ihres Reifegrades

Zuerst analysieren wir die Anforderungen Ihres Kunden und gleichen diese mit dem VDA-ISA Katalog ab. Hieraus ergibt sich der Scope. Durch die GAP-Analyse stellen wir den IST/Soll-Vergleich her; Ihren derzeitigen Reifegrad zu dem geforderten Reifegrad.

11.2 Anmeldung des Prüfungsmanagement

Bevor Sie einen externen Dienstleister zur Durchführung des TISAX®-Assessments beauftragen können, müssen Sie auf der ENX-Plattform registrieren. Hierbei unterstützen wir Sie gerne, damit Sie den notwendigen Assessment-Level definieren.

11.3 Umsetzung der Anforderungen

Wir unterstützen Sie die VDA-ISA Anforderungen auf Ihr Unternehmen passend umzusetzen und ggf. in bestehende Managementsysteme zu integrieren. Somit erhalten Sie ein TISAX® konformes Informationssicherheitsmanagementsystem (ISMS).

11.4 Einbindung der Mitarbeiter

Informationssicherheit ist kein Projekt, sondern ein fortlaufender Prozess, der sich kontinuierlich weiterentwickelt. Daher ist es notwendig Ihre Mitarbeiter durch Unterweisungen einzubinden und das Kernteam zu coachen. Wir unterstützen Sie durch Workshops, Vorträge und passende Schulungen.

11.5 Herstellung des Assessmentfähigkeit

Das TISAX®-Assessment beginnt bereits mit Ihrer Selbstauskunft auf Basis des VDA-ISA Katalogs. Die Anforderungen können hier je nach zu erfüllenden Assessment-Level unterschiedlich sein. Wir unterstützen Sie dabei den VDA-ISA Katalog ordnungsgemäß und aussagekräftig auszufüllen. Selbstverständlich können wir auch ein internes Assessment zur Vorbereitung mit Ihnen durchführen. Darüber hinaus können wir Sie auch bei dem eigentlichen externen Assessment begleiten.

11.6 Follow-Up

Der Assessor wird Nebenabweichungen feststellen. Wir unterstützen Sie dabei diese im relevanten Zeitraum abzustellen und die Notwendigen Nachweise zu erbringen.

12 Fazit

Informationssicherheit ist ein Prozess und kein Projekt. Es gibt nicht das TISAX®-Einführungs-, oder Umsetzungs-Projekt. Informationssicherheit ist vielschichtig und oftmals auch komplex in der Umsetzung. Wesentliche Bestandteile sind etablierte Prozesse, formulierte Verfahrensanweisungen und ein funktionierendes Risikomanagement.

Unternehmen sind unterschiedlich in ihren Strukturen, Abläufen und Abhängigkeiten. Auch variiert der Reifegrad der Informationssicherheit von Organisationen. Darüber hinaus spielen Unternehmensgröße, Standorte, Art der Vernetzung, Prozessierung von Daten, sowie Schutzbedarf der Informationswerte eine wichtige Rolle bei der Umsetzung der Anforderungen.

Das ISMS kann seine Wirksamkeit nur entfalten, wenn a) das Managementsystem von der Geschäftsführung getragen wird, b) alle Mitarbeitenden geschult und involviert sind, d) das Know-how ganzheitlich vorhanden ist, c) kontinuierlich das Schutzniveau angehoben wird und d) fest in die Wertschöpfungskette integriert ist.

13 Nützliche Links

https://mabs40.de.com/

https://portal.enx.com/de-de/

https://portal.enx.com/de-de/TISAX/downloads/

14 Zusätzliche Informationen

14.1 Schutzziele der Informationssicherheit

Die Informationssicherheit verfolgt drei Schutzziele:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

auch bekannt als C-I-A-Criteria (Confidentiality – Integrity - Availability).

Bei der Vertraulichkeit dürfen Daten lediglich von autorisierten und befugten Benutzern verarbeitet werden. Durch die Integrität soll verhindert werden, dass Daten unbemerkt verändert und manipuliert werden können. Die Verfügbarkeit dient der Verhinderung von Systemausfällen.

14.2 Ihr Nutzen

Ein ISMS schafft eine ganzheitliche Informationssicherheit. Sie müssen hierfür kein „Tekki“ sein. Neben den technisch relevanten Maßnahmen sind die organisatorischen Maßnahmen ein wesentlicher Aspekt der ganzheitlichen Informationssicherheit.

Machen Sie Ihre Mitarbeiter zur „Human Firwall“ und minimieren Sie Ihre Risiken durch ein durchgängiges Rahmenwerk mit entsprechender Prozesssicherheit.

Durch entsprechende Unterweisungen werden Ihre Mitarbeiter den Mehrwert sehr schnell erkennen und die Informationssicherheit auch in ihrem privaten Umfeld als festen Bestandteil etablieren.

Ihr Sicherheitsniveau wird sich in kürzester Zeit nachhaltig erhöhen und die Geschäftsrisiken werden geringer.

+49211 - 205 444 80
kontakt@mabs40.com
www.mabs40.de.com

Großenbaumer Weg 8
40472 Düsseldorf
Deutschland