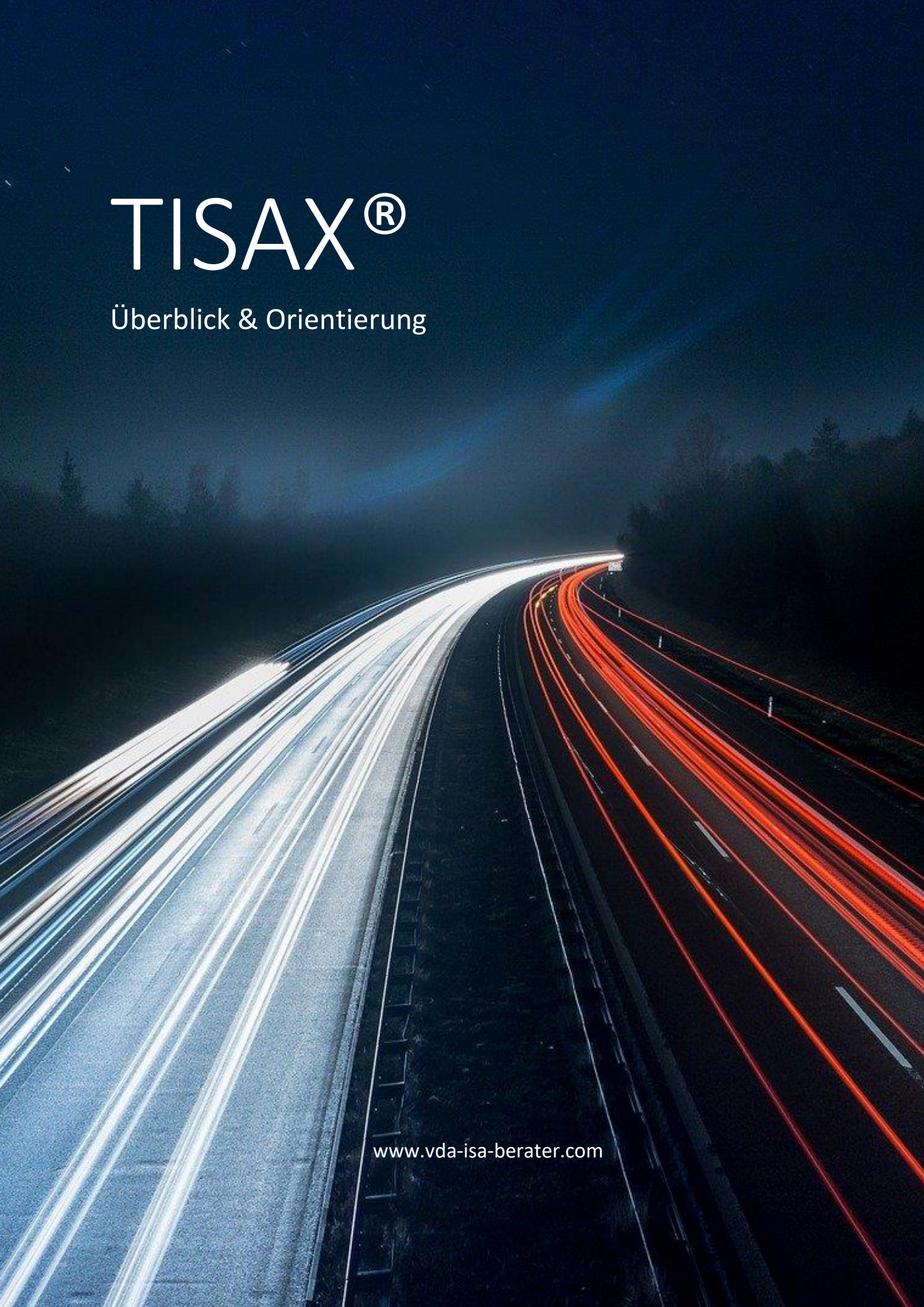
# TISAX®

## Überblick & Orientierung



www.vda-isa-berater.com

# Sicherung von schützenswerten Informationen innerhalb der Automotive-Supply-Chain

## Die Ausgangssituation

Informationssicherheit hat in den letzten Jahren eine immer stärkere Bedeutung in der Zusammenarbeit mit Kunden und Lieferanten erlangt. Somit ist auch die Herausforderung, ein hohes Sicherheitsniveau in Unternehmen zu etablieren, innerhalb der Automobilbranche deutlich gestiegen.

Zu diesem Zwecke wurde 2017 von der ENX und dem VDA einen TISAX® genannter Prüf- und Austauschmechanismus etabliert, der als Testat zum Nachweis der Erfüllung von Informations-Sicherheitsstandards dient.

Automobil Zulieferer (die Teile, Komponenten, Dienstleistungen etc. anbieten) müssen – falls noch nicht vorhanden - ein Informationssicherheitsmanagementsystem (ISMS) implementieren und aufrechterhalten, und nachfolgend die TISAX-Prüfung bestehen, um weiterhin entweder den Kundenanforderungen zu entsprechen oder generell von einem OEM unter Vertrag genommen zu werden.

## Das Vorgehen

In der Vergangenheit haben wir von OPTIQUM erfolgreich Unternehmen der verschiedensten Branchen auf ihrem Weg zum erfolgreichen TISAX®-Testat begleitet und aus diesen Erfahrungen eine Best Practice erarbeitet.

**One Size fits all? Warum Pauschalen bei TISAX® nicht funktionieren!**

Zunächst wird der der Reifegrad Ihres Managementsystems und der Aufbau Ihrer IT-Infrastruktur inkl. der IT-Dokumentation benötigt. Wir wissen, dass viele Anbieter pauschal ein Angebot über die Erstellung eines Informationssicherheitsmanagementsystem (ISMS) abgeben. Das ist aus unserer Sicht unseriös und hat meistens zur Folge das im Laufe des Projektes Nachforderungen gestellt werden. Warum genau?

Unternehmen sind in jeglicher Hinsicht äußerst unterschiedlich: Zum Beispiel existieren manchen Organisationen als Dienstleister praktisch nur in der Cloud, andere wiederum haben mehrere hundert Mitarbeiter an verschiedenen Standorten mit unterschiedlicher Vernetzung. Manche Unternehmen haben perfekt aufgestellte und gelebte Informationssicherheitsmanagementsysteme mit optimaler Dokumentation, bei anderen wiederum steckt dies noch in den Kinderschuhen und ist nur rudimentär entwickelt. Wie Sie sehen, sind die Anforderungen, mittels derer das TISAX®-Label erreicht wird derart unterschiedlich, dass eine einfache pauschale Einschätzung den individuellen Gegebenheiten innerhalb Ihres Unternehmens gar nicht gerecht werden kann.

***Was ist Tisax?***

*Der Trusted Information Security Assessment EXchange, kurz TISAX®, ist ein von der Automobilindustrie definierter Standard für Informationssicherheit.*

*Die Mitgliedsunternehmen des Verbandes der Automobilindustrie e.V. (VDA) haben hierzu einen Katalog erstellt, der, von der internationalen Industrie-Norm ISO 27001 abgeleitet, an die spezifischen Anforderungen der Automobil-Branche angepasst wurde.*

*Betrieben wird TISAX® von der rechtlich-selbstständigen Organisation ENX Association mit Sitz in Frankreich, welche die Prüfdienstleister akkreditiert und die Qualität der Durchführung sowie die Assessment-Ergebnisse überwacht.*

*Jedes Unternehmen, das für Kunden aus der Automobil-Branche arbeitet, kann seit 2017 aufgefordert werden ein TISAX®-Label nach VDA-ISA vorzulegen. Zulieferer in der Branche brauchen sie, um auch weiterhin Aufträge zu erhalten. Und um einer drohenden Auslistung zu entgehen, muss das Label möglichst zeitnah und garantiert erfolgen.*

**Ist und Soll vergleichen**

Unser Vorgehen besteht üblicherweise aus einer GAP Analyse, in der eine Dokumentensichtung und ein internes Vor-Ort/Remote Audit an Ihrem Unternehmensstandort erfolgt. Das Ergebnis ist ein VDA-ISA Self-Assessment, welches Sie auch für die eigentliche TISAX®-Prüfung benötigen und ein Bericht, in dem die aus unserer Sicht noch zu erledigenden Punkte ausführlich dargestellt werden. Das Ergebnis können Sie nachfolgend auch mit anderen Unternehmen umsetzen.

Auf dieser Basis kann nun der Gesamtaufwand für Ihr Projekt abgeschätzt werden und Sie können wählen:

- Was möchten Sie intern erarbeiten?
- Wobei bedürfen Sie externer Unterstützung?

**Unterstützungsphase**

Die Unterstützungsphase besteht üblicherweise aus mehreren Workshops zu den im Bericht aufgeführten Themen. Auf die Workshops folgt jeweils eine Umsetzungsphase der im Workshop erarbeiteten Aufgaben.

Im folgenden Workshop werden die Ergebnisse überprüft und das nächste Thema angegangen. Das Self-Assessment wird dann entsprechend angepasst. In jeder Workshoprunde kann der Aufgabenbereich neu gemäß ihren verfügbaren Ressourcen verteilt werden (Was erledigen Sie/geben Sie an Extern ab).

Nach Abarbeitung der Berichtsthemen, führen wir nun ein internes Audit durch inklusive der entsprechenden Dokumentation.

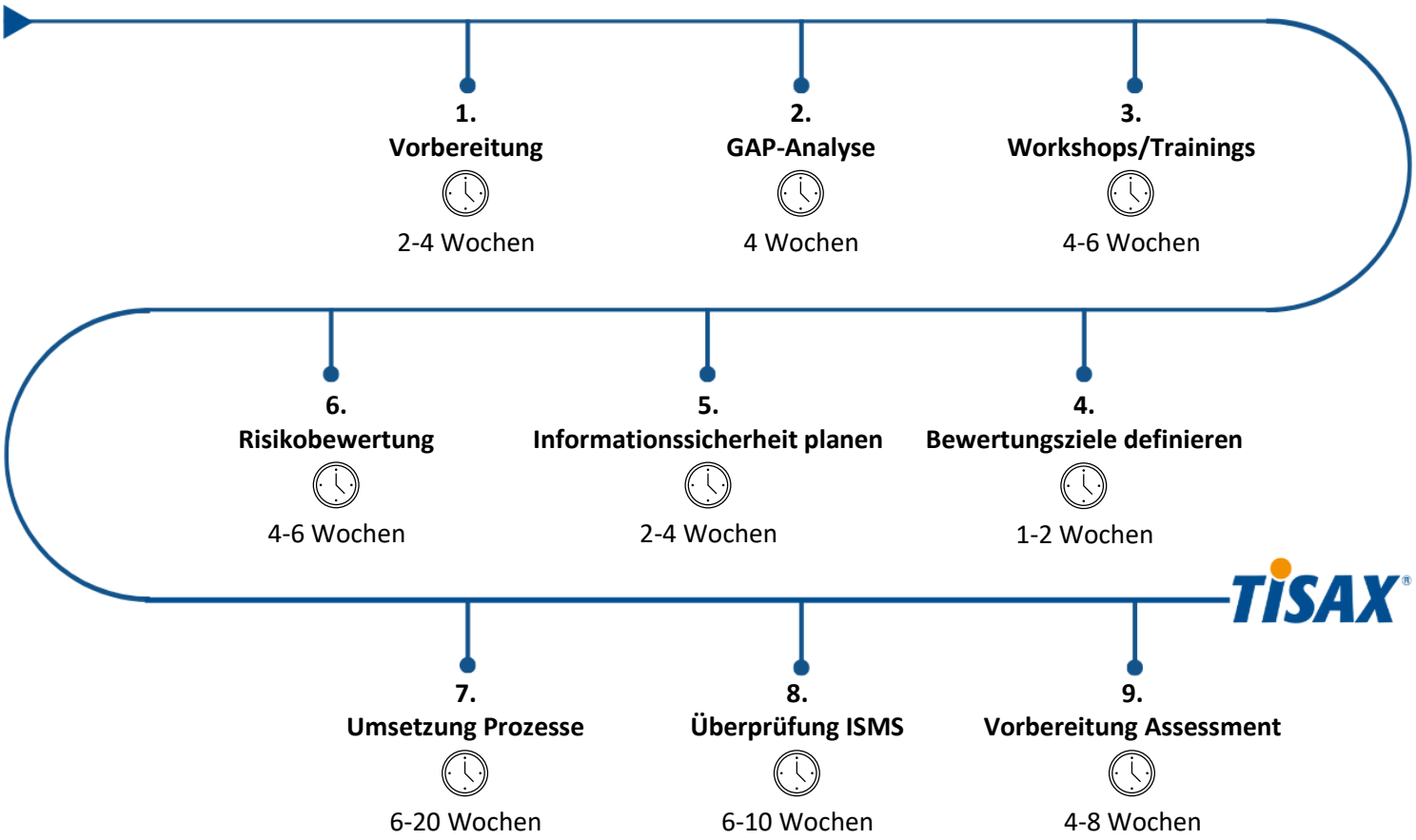
Außerdem können wir Sie bei der Auswahl und Beauftragung der Prüforganisation, sowie als Begleitung bei der offiziellen TISAX Prüfung unterstützen.

Die Umsetzung kann 3 bis 9 Monate dauern, abhängig von der Dringlichkeit und der Personalverfügbarkeit auf Ihrer Seite.

## Der zeitliche Fahrplan für ein TISAX®-Assessment

Die benötigte Vorbereitungszeit kann stark variieren, da sie von ganz unterschiedlichen Faktoren abhängt, wie beispielweise der Anzahl der Standorte, den zeitlichen und fachlichen Ressourcen innerhalb des Unternehmens sowie den vorab bereitgestellten, gesichteten Dokumenten.

Wir haben einen ungefähren zeitlichen Ablauf zur Übersicht erstellt, der auf unseren gesammelten Erfahrungen im Bereich TISAX® beruht.




→ Insgesamt ist mit einem zeitlichen Aufwand zwischen 9 und 16 Monaten zu rechnen.

Zu beachten ist, dass das unternehmerische Engagement maßgeblich zur finalen Roadmap und der zeitlichen Bewältigung der einzelnen Schritte ausschlaggebend sind. Die Vorbereitung auf Ihr TISAX® Assessment ist ein durchaus zeitaufwändiger, komplexer Prozess und erfordert gute Vorbereitung und Einsatz. Doch die Vorteile des TISAX® Labels überwiegen den Aufwand. Daher ist es ratsam, gleich zu Beginn externe Expertise zur strategischen Planung zu Rate zu ziehen.

***Ihre Supply-Chain***

*Während sich das Auto selbst weiterentwickelt, klimaeffizienter und digitaler wird, sind Unternehmen aus den Bereichen neue Energien, mobiles Internet und autonomes Fahren ein unverzichtbarer und wachsender Teil der automobilen Lieferkette, ebenso wie Dienstleister aus der Medienbranche.*

*Innerhalb dieser gesamten Lieferkette muss die Informationssicherheit im Sinne von TISAX® eingehalten und nachgewiesen werden, wen es vom Kunden eingefordert wird.*

*Beispielsweise bezieht sich dies bei einem Prototyp darauf, dass dieser sowohl auf dem Testgelände vor unerlaubter Mediendokumentation wie auch beim beauftragten Fotografen vor ungewollter Vorabveröffentlichung ausreichend geschützt ist. Denn diese Datenlecks können ungeahnte Regressionsforderungen nach sich ziehen!*

*TISAX® zieht schon jetzt weite Kreise in der Supply-Chain – sichern Sie sich daher zeitnah ab.*

**Wie beginnen?**

Da ist sie nun, die Anforderung Ihres Kunden, dass Sie das TISAX®-Label nachweisen müssen. Um gut starten zu können, hier die wichtigsten Basics:

Informieren Sie vor Projektbeginn die entsprechenden involvierten Abteilungen. Hierzu gehören neben dem Management und der IT alle Abteilungen, die mit Kunden und Lieferanten in Kontakt stehen, die schützenswerte Informationen der OEM bzw. des Kunden behandeln, die TISAX® fordern, sowie dessen relevante Daten austauschen.

Stellen Sie sicher, dass alle Dokumente, die relevant werden könnten, gesichtet und griffbereit sind. So zum Beispiel Geheimhaltungsvereinbarungen, Notfallpläne für Feuer-, Wasser- und Gebäudeschäden sowie Strom- und Serverausfälle.

Falls möglich schätzen Sie im Vorfeld die verfügbaren Ressourcen ein, die Sie für den TISAX®-Prozess bereitstellen können: Über welches Knowhow im Bereich der Informationssicherheit verfügen Sie im Unternehmen? Welche Mitarbeiter können Sie für welchen Zeitraum freistellen? Welche Qualifikationen bringen die gewählten Mitarbeiter mit? Welche Aufgabenbereiche sollten definitiv an externe Experten abgegeben werden?

---

## Sie haben Fragen?

TISAX® - der Standard für Informationssicherheit in der Automobilindustrie!

Unsere Experten verbinden diese beiden Aspekte optimal miteinander, denn sie verfügen über mehr als 10jährige Erfahrung sowohl seitens der **Automobilbranche** über IATF und VDA 6.x als auch im Bereich der **IT und des Informationssicherheitsmanagement**.
Kompetent und komplett deckt unser Team daher alle Anforderungen rund um TISAX® / VDA-ISA ab, um den Weg zu Ihrem TISAX®-Label leicht und unkompliziert zu gestalten.

Wir von OPTIQUM sind für Sie da, um Sie zu Ihren Anliegen in Bezug auf TISAX®, Informationssicherheit und Datenschutz zu beraten.

Telefon: +49 221 82 95 91 0
info@vda-isa-berater.com

# Dürfen wir vorstellen?
# Unsere Experten für den Bereich TISAX®:

**David Zinzius**, ist zertifizierter Auditor ISO 27001 und Datenschutzbeauftragter. Er besitzt eine Zusatzqualifikation EC Council Certified Hacking Forensic Investigator und ist Ansprechpartner für die Umsetzung branchenspezifischer Standards wie VDA ISA / TISAX® und Implementierung von Maßnahmen gemäß ISO 27000 bzw. BSI Grundschutz sowie KRITIS und Fragen rund um Datenschutz und Informationssicherheit (ISO 27001, DSGVO, ITIL, B3S u.a.)

**Marc Mietz**, Zertifizierter 3rd Party Auditor für IATF 16949, ISO 9001:2015 und besitzt eine Zusatzqualifikation nach VDA 6.3 und Automotive Prozessmanager. Auf Grund seiner fundierten, langjährigen Erfahrung im Bereich der Automobilzuliefererindustrie kennt er sich bestens mit den Anforderungen der Branche aus und unterstützt mit seinem Knowhow Kunden effektiv und zielorientiert auf dem Weg zum TISAX®-Label.

**Bernt Böhmer**, Mehr als 30 Jahren ist Bernt Böhmer als Mitarbeiter im Bereich Qualität für verschiedene 1st und 2nd tier Automotive Unternehmen im In- und Ausland tätig gewesen und heute als zertifizierter 1st und 2nd Party Auditor für IATF 16949 und Auditor für ISO 27001 tätig, mit einer Zusatzqualifikation in den Bereichen Lieferantenqualitätsmanagement / Projektmanagement (Reifegrad VDA) und Qualitätsmanagement.

**Phillipp Mühle**, ist TÜV-zertifizierter ISO/IEC 27001 Information Security Officer und Lead Auditor. Bei seinem früheren Arbeitgeber -einem mittelständischen Automobilzulieferer- war er als Global Information Security Officer tätig und hat erfolgreich ein ISMS nach TISAX® eingeführt. Darüber hinaus hat er Erfahrungen als Datenschutzkoordinator (DSGVO).

**Erich Lange**, ist zugelassener 3rd party IATF 16949 Leadauditor und hat als TISAX-Auditor im Zulassungsverfahren einer Zertifizierungsstelle mitgewirkt. Zusätzlich ist er als ISO 27001 Leadauditor und im Bereich KRITIS (BSIG §8a) qualifiziert. Durch seine vorherige festangestellte Tätigkeit in Zertifizierungsstellen kann er Ihnen wertvolle Einblicke zu Zertifizierungsverfahren vermitteln.

**Christoph Holighaus**, ist TÜV-zertifizierter IT-Security-Beauftragter sowie TÜV-zertifizierter Informationssicherheitsbeauftragter für TISAX® und ISTQB Vertified Tester. In seiner Berufspraxis hat er als IT-Verantwortlicher, sowie als Team Coordinator Embedded Quality Assurance fundierte Erfahrung in entsprechenden Projekten gesammelt und ist versiert in den Bereichen Prozessgestaltung und Prozessoptimierung

OPTIQUM GmbH
Siegburger Straße 223
D-50679 Köln

+49 221 82 95 91 0
info@vda-isa-berater.com