Die 10 häufigsten Stolperfallen in TISAX®-Projekten

Ausgabe 10/2024

©2024 – CISO Alliance e.V.

Hinweise:

Im gesamten Text wird zur besseren Lesbarkeit und aus Vereinfachungsgründen grundsätzlich die männliche Form verwendet. Es handelt sich um keine Einschränkung, sondern beinhaltet immer alle Formen: männlich, weiblich und divers.

In manchen Unternehmen wird der CISO (Chief Information Security Officer) auch Informationssicherheitsbeauftragter (ISB) oder Information Security Officer (ISO) genannt. Zugunsten einer besseren Lesbarkeit wird in diesem Dokument ausschließlich der Begriff CISO verwendet.

TISAX® ist eine eingetragene Marke der ENX Association1. Der Herausgeber dieses Dokuments, die CISO Alliance e.V., steht in keiner Verbindung zur ENX Association.

©2024 – CISO Alliance e.V.

Die 10 häufigsten Stolperfallen in TISAX-Projekten

Einleitung

Wer Kunden im Bereich der Automobilindustrie hat, kennt vermutlich auch den Begriff TISAX. Mit einem TISAX-Label können Lieferanten und Dienstleister gegenüber ihren Kunden nachweisen, dass sie sich um das Thema Informationssicherheit gekümmert und gewisse Informationssicherheitsstandards etabliert haben. Dabei basiert TISAX auf dem kostenfrei zugänglichen VDA Information Security Assessment Katalog (VDA ISA)2. Ebenfalls kostenfrei zugänglich ist das TISAX-Teilnehmerhandbuch3, in dem der Gesamtablauf zum Erwerb eines TISAX-Labels detailliert beschrieben ist.

Wer bereits ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 betreibt, für den hält sich der zusätzliche Aufwand für TISAX meist in Grenzen. Doch TISAX unterscheidet sich in mehreren Punkten sowohl bei der Systematik als auch bei spezifischen Anforderungen von klassischen Informationssicherheitszertifizierungen, wie der ISO 27001 oder dem IT-Grundschutz. Manche dieser Unterschiede werden zu spät wahrgenommen und können dann zur Stolperfalle in Projekten werden.

Wer sich mit dem Thema TISAX beschäftigt und noch kein ISMS betreibt, der sollte zunächst einen Verantwortlichen für die Informationssicherheit (nicht nur für die IT-Sicherheit) benennen: Wir nennen ihn in diesem Dokument den „Chief Information Security Officer (CISO)“. Der CISO kann ein externer oder ein interner Mitarbeiter sein.

Um die typischen Stolperfallen zu umschiffen, lohnt es sich, vor Projektbeginn das oben angesprochene TISAX-Teilnehmerhandbuch und unsere Broschüre zu den 10 häufigsten Stolperfallen in TISAX-Projekten zu lesen.

Viel Freude dabei.

©2024 – CISO Alliance e.V.

Die häufigsten 10 Stolperfallen im Einzelnen

1. TISAX wird als reines IT-Projekt betrachtet

Warum ist das eine Stolperfalle?

In vielen Unternehmen, die noch keinen CISO haben, landet die Anforderung für die Umsetzung von TISAX auf dem Schreibtisch des IT-Leiters. Da viele der Anforderungen im VDA ISA-Katalog direkt oder indirekt mit der Sicherheit der IT zusammenhängen, ist das auch naheliegend. Bei näherer Betrachtung wird jedoch deutlich, dass es nicht nur um IT geht, sondern auch um Personal (HR), Facility Management, Unternehmensführung, Compliance, Datenschutz, internes Projektmanagement sowie Projektmanagement bei Kunden, Risikomanagement und vieles mehr. Daher ist ein TISAX-Projekt kein Thema, das die Geschäftsleitung einfach bei der IT abladen und sich dann zurücklehnen kann.

Zusätzlich kann es auch zu Interessenskonflikten führen, wenn die Koordination der internen Informationssicherheit allein beim IT-Leiter liegt. Denn dann würde der IT-Leiter auch die Umsetzung der eigenen Richtlinien verantworten und sich im Anschluss selbst kontrollieren und überprüfen. Es sollte wie im Fall von Buchhaltung und Controlling sein, bei denen es selbstverständlich ist, dass die Zuständigkeiten klar getrennt sind, ohne dass darüber groß nachgedacht werden muss.

Wer ist typischerweise betroffen?

Unternehmen, die bislang noch keinen qualifizierten CISO ernannt haben.

Wie kann ich die Stolperfalle vermeiden?

Die Einführung von TISAX von Beginn an als ein Projekt planen, das das gesamte Unternehmen umfasst. Es sind Ansprechpartner aus verschiedenen Bereichen des Unternehmens mit einzubeziehen.

Unsere Empfehlung ist, den CISO außerhalb der IT anzusiedeln, da sein Wirkungskreis weit mehr als nur die IT umfasst. Idealerweise kann der CISO auf Augenhöhe mit dem CIO bzw. IT-Leiter kommunizieren und berichtet direkt an die Geschäftsleitung.

Praxistipps für die Umsetzung

Spätestens mit Projektbeginn sollte ein CISO benannt werden. Dieser kann intern oder extern sein. Ein interner CISO muss unbedingt fundiert ausgebildet sein bzw. ausgebildet werden. Nicht nur fachlich, sondern auch mit wichtigen Skills wie Verhandlungsgeschick. Der CISO sollte vorzugsweise unabhängig von der IT sein, da er ansonsten in permanente Interessenskonflikte gerät. IT-Sicherheit ist letztendlich die Summe aller Risikomitigationsmaßnahmen, die sich aus dem ISMS ergeben. Wenn CISO und IT-Leitung getrennt sind, können diese auf Augenhöhe diskutieren und zielführende IT-Maßnahmen im Sinne der Gesamtorganisation einleiten. Da der CISO und die Informationssicherheit deutlich mehr umfassen als nur die IT, werden dann weitere Maßnahmen mit anderen Bereichen erarbeitet (HR, FM, Betriebssicherheit etc.).

©2024 – CISO Alliance e.V.

2. Das ISMS wird nur für das Assessment eingeführt und nur bis zum Assessment gelebt

Warum ist das eine Stolperfalle?

Häufig passiert es, dass das Einführungsprojekt, welches für das Assessment notwendig war, nach dem Erhalt des TISAX-Labels nicht in einen kontinuierlichen Sicherheitsprozess übergeht. Zunächst scheint das kein Problem darzustellen, doch spätestens beim nächsten Assessment nach drei Jahren wird es schwierig, die dann geforderten Nachweise zu verschiedenen Themen beizubringen und es kann sogar zu sogenannten „Hauptabweichungen“ führen.

Eine Hauptabweichung führt in jedem Falle dazu, dass kein TISAX-Label zugeteilt wird und erhebliche Auflagen gemacht werden. Die Gefahr, keinen kontinuierlichen Sicherheitsprozess zu leben, wird noch dadurch unterstützt, dass es bei TISAX keine jährlichen „Überwachungsassessments“ gibt, wie sie bei anderen Sicherheitsstandards vorgeschrieben sind.

Es werden auf die Schnelle Maßnahmen definiert, Dokumentationen erstellt oder Vorlagen kopiert, ohne dass die Prozesse wirklich nachhaltig integriert und nachgehalten werden sowie zum Unternehmen passen.

Wer ist typischerweise betroffen?

Unternehmen, die das Mindset verfolgen: „Wir müssen nur das Assessment bestehen,“ ohne die Absicht, mit der Einführung eines ISMS nach TISAX auch das Sicherheitsniveau langfristig zu erhöhen, laufen Gefahr, in diese Stolperfalle zu geraten. Ebenso sind Unternehmen betroffen, die versuchen, das Projekt durch eine einzelne Person umzusetzen, ohne alle relevanten Bereiche ausreichend einzubinden.

Wie kann ich die Stolperfalle vermeiden?

Mit dem richtigen Mindset starten:

- Wir machen das für unser Unternehmen, damit es seine Geschäftsziele erreicht – und nicht für den Prüfer.
- Alle betroffenen Bereiche bei der Erarbeitung der Maßnahmen einbinden, damit die Änderungen an den Prozessen bekannt werden und auf möglichst wenig Gegenwind stoßen.

Praxistipps für die Umsetzung

Benennen Sie einen qualifizierten CISO, der das Thema ISMS auch nach dem Assessment im Auge behält und sicherstellt, dass sich alle Beteiligten weiterhin ihrer Verantwortung im Rahmen eines ISMS bewusst sind.

©2024 – CISO Alliance e.V.

3. Missverständnisse beim Scope des Assessments

Warum ist das eine Stolperfalle?

Es ist wichtig im TISAX-Umfeld den sogenannte „Scope“, also den Geltungsbereich für das TISAX-Assessment, richtig zu verstehen. TISAX kommt aus der Automobilindustrie und geht nach der Idee von „Werken“ streng standortbezogen vor. Dabei ist außerdem wichtig zu verstehen, dass es sich beim TISAX-Scope um einen oder mehrere Standorte einer juristischen Einheit handelt. Wenn ich also beispielsweise an meinem Hauptstandort die Holding als AG und drei Tochtergesellschaften als GmbHs habe und nun nur für eine der Tochtergesellschaften ein TISAX-Label für den Hauptstandort erlangt werden soll, so würde der Assessment-Scope alle Abtei-lungen und Prozesse nur dieser Tochtergesellschaft am Hauptstandort umfassen. Die Schwestergesellschaften und die Holding wären außerhalb des Scopes und treten ggf. als Dienstleister gegenüber der Tochter auf (z. B. für Personalverwaltung, Finance etc.). Allerdings sind dann auch tatsächlich alle Bereiche der Tochtergesellschaft an diesem Standort beinhaltet, selbst, wenn diese gar nichts mit Automotive zu tun haben. Ein Beispiel wäre ein Hersteller von Klebeverbindungen, der diese für Automotive, aber auch für die Elektronikindustrie macht. Wenn beide Arten in der-selben juristischen Einheit am selben Standort hergestellt oder entwickelt werden, müssen auch die Bereiche, die nur die Elektronikindustrie betreffen, TISAX-konform sein. Mehr Details dazu finden sich im TISAX-Teilnehmerhandbuch unter Punkt 4.3.24.

Berücksichtige ich diesen grundlegenden Ansatz beim Aufbau meines ISMS nach TISAX bzw. bei der Definition meines TISAX-Assessment-Scopes im Rahmen eines bestehenden und wirksamen ISMS nicht, führt dies i.d.R. im Rahmen des Assessments zu mindestens einer Hauptabweichung und damit zum Abbruch des Assessments.

Wer ist typischerweise betroffen?

Organisationen, die bereits ein bestehendes ISMS auf Grundlage von ISO/IEC 27001 oder einem anderen Informationssicherheits-Standard betreiben oder einführen. Ebenso Organisationen, die bereits andere Managementsysteme, wie z.B. in der Qualitätssicherung (ISO 9001), dem Umweltmanagement (ISO 14001) oder dem Energiemanagement (ISO 50001) erfolgreich betreiben und nun für die Informationssicherheit nur um TISAX erweitern wollen. Derartige Einrichtungen sind es gewohnt, dass sie den Zertifizierungsscope deutlich flexibler gestalten können und nur eine bestimmte Anzahl an Geschäftsprozessen oder Organisationseinheiten einbinden.

Wie kann ich die Stolperfalle vermeiden?

Es ist wichtig, das TISAX-Teilnehmerhandbuch vor Projektbeginn grundlegend zu verstehen. Zusätzlich sollte der Projektleiter und der CISO entsprechend geschult sein oder werden, wenn diese noch keine Erfahrung mit dem TISAX-Standard haben. Es ist ebenfalls wichtig, sich mit dem Automobilhersteller, der das TISAX-Label fordert, abzustimmen, für welche Produkte oder Leistungen er dieses benötigt, damit die richtigen Standorte ausgewählt werden.

Praxistipps für die Umsetzung

Ein erfahrener Berater oder externer CISO, der schon mehrfach erfolgreich TISAX-Assessments begleitet hat, ist ein Garant dafür, dass auch Ihr TISAX-Assessment maximal mit wenigen Nebenabweichungen mit einem TISAX-Label belohnt wird.

©2024 – CISO Alliance e.V.

4. Fehler bei der zeitlichen Planung sowie den Abgabefristen

Warum ist das eine Stolperfalle?

Häufig wird die Dauer von Projekten zur Einführung eines ISMS unterschätzt. Selbst in kleineren Organisationen sollten dafür mehr als 6 Monate eingeplant werden. Bei großen und komplexeren Organisationen mit viel Abstimmungsbedarf auch gerne weit über 12 Monate. Daher kann es sich auch lohnen, schon einmal vorsorglich mit den Vorbereitungen zu starten, statt zu warten, bis eine Organisation wirklich ein TISAX-Label sehen möchte.

Hinzu kommt, dass TISAX-Prüfer leider knapp gesät sind und daher oft kurzfristig keine passenden Termine frei haben. Insbesondere, wenn man einen bestimmten Prüfer oder einen bestimmten Prüfdienstleister bevorzugt oder mehrere Vor-Ort-Assessments anstehen, ist auch hier ein Vorlauf von mindestens 6 bis 12 Monaten einzuplanen. Sprich: Wenden Sie sich am besten bereits zu Beginn des TISAX-Projektes an einen Prüfdienstleister, um einen Termin für das Assessment festzulegen. In diesem Rahmen kann Ihnen der Prüfdienstleister auch die ein oder andere Frage zum TISAX-Assessment beantworten.

Auch vor und nach dem TISAX-Assessment gibt es verschiedene feste Fristen zu beachten. Werden sie nicht eingehalten, führt das im besten Fall zu Verzögerungen und schlimmsten Fall muss das Assessment nochmal von vorne begonnen werden.

Daher hier ein Überblick über die wichtigsten Fristen:

- Die Dokumentationen müssen spätestens zwei Wochen vor Beginn des Assessments zu dem mit dem Prüfer vereinbarten Termin eingereicht wer-den, damit der Prüfer ausreichend Zeit hat, sich vorab ein Bild zu machen.
- Bei Haupt- oder Nebenabweichungen muss innerhalb einer vom Prüf-dienstleister festgelegten Zeit ein sogenannter „Corrective Action Plan“ (Korrekturmaßnahmenplan) vorgelegt und genehmigt werden.
- Nach der Genehmigung des Corrective Action Plans durch den Prüf-dienstleister müssen die darin beschriebenen Maßnahmen innerhalb von 3 Monaten umgesetzt werden. Dauert es länger als 3 Monate, wird eine Be-gründung benötigt. Dauert es länger als 6 Monate, wird zusätzlich ein Nachweis benötigt, warum es nicht schneller gehen kann. Nach spätestens 9 Monaten müssen die beschriebenen Maßnahmen umgesetzt sein. Damit sollte jedoch nicht bis auf den letzten Drücker gewartet werden, denn es muss auch ein Follow-Up-Assessmenttermin mit dem Prüfer gefunden werden und das Ergebnis muss anschließend noch durch interne Qualitätssicherungsmaßnahmen des Prüfdienstleisters laufen. Daher empfehlen wir das Follow-Up-Assessment spätestens 8 Monate nach dem Erstassessment anzupeilen. Sollte das Follow-Up-Assessment nicht nach spätestens 9 Monaten durchgeführt sein, muss der gesamte Assessment-Prozess von vorne gestartet werden.

Wer ist typischerweise betroffen?

Unternehmen, die dringend ein TISAX-Label benötigen oder die sich nach dem Assessment mit der Umsetzung der vereinbarten Maßnahmen lange Zeit lassen möchten, da schon ein temporäres TISAX-Label zugeteilt wurde.

Lösungsansätze und Praxistipps für die Umsetzung

Die Lösung ist hier recht einfach: Seien Sie sich der Fristen bewusst und berücksichtigen Sie diese in der Projektplanung. Unterschätzen Sie die Dauer für eine saubere Implementierung eines ISMS nicht. Kommunizieren sie offen und ehrlich über Herausforderungen, um ein frühzeitiges Eingreifen zu ermöglichen.

©2024 – CISO Alliance e.V.

5. Ungenügende Unterstützung durch das Management

Warum ist das eine Stolperfalle?

Die Verantwortung für die TISAX-Umsetzung wird durch das Management zum CISO delegiert, eine weitere Einbindung des Managements erfolgt nicht.

Wer ist typischerweise betroffen?

Diese Herausforderung ist durch alle Branchen sichtbar. Insbesondere bei kleinen und mittleren Unternehmen mit begrenzten Ressourcen und Erfahrungen ist mit diesem Szenario zu rechnen.

Die Herausforderungen bei der TISAX-Umsetzung betreffen vor allem Zulieferer in der Automobilindustrie, insbesondere kleine und mittlere Unternehmen (KMUs). Die-se Unternehmen sind oft stark von Aufträgen der Automobilhersteller (OEMs) ab-hängig und sollen die Anforderungen erfüllen, um ihre Geschäftsbeziehungen aufrechtzuerhalten. Oftmals verfügen Sie nicht über ausreichend Ressourcen und Erfahrungen. Diese Konstellation führt zu unklaren Verantwortlichkeiten und fehlenden Auftragsklärungen.

Lösungsansätze

- Klären Sie das Management über die Bedeutung eines ISMS für das Unternehmen auf und verdeutlichen Sie die Rolle des Managements bei der Umsetzung und dem Betrieb des ISMS. Dokumentieren Sie die Anforderungen des Managements an das ISMS im Rahmen der Auftragsklärung.
- Erstellen Sie klare Rollen und Verantwortlichkeiten für die Umsetzungs- und Betriebsphase.
- Etablieren Sie einen regelmäßigen Austausch zwischen dem Management und den CISO, um Fortschritte zu besprechen, Herausforderungen zu identifizieren und Entscheidungen zu treffen.
- Notwendige Ressourcen (finanziell, personell) müssen dem CISO verfügbar gemacht werden.
- Arbeiten Sie als CISO (Fachpromotor) sehr eng mit den Führungskräften (Machtpromotor) zusammen. Binden Sie diese eng in das Umsetzungsprojekt ein.

Praxistipps für die Umsetzung

- Schaffen Sie ein Verständnis für den Soll Zustand.
- Ist die Motivation extrinsisch (Gesetz/Kunden Anforderung) oder intrinsisch (ich möchte mein Unternehmen schützen / Ich sehe meine Verantwortung für das allgemeine Wohl)
- Schaffen Sie für beide Seiten eine klare Auftragslage und zeigen Sie die Rolle des Managements deutlich auf.

©2024 – CISO Alliance e.V.

6. Überdokumentation

Warum ist das eine Stolperfalle?

Beim Aufbau oder der Anpassung eines ISMS nach TISAX ist es wichtig vorher zu prüfen, wo zwingend Dokumentation gefordert wird. Es muss nicht alles bis ins letzte Detail dokumentiert werden. Bei der ISO/IEC 27001, auf der TISAX grundsätzlich basiert, gibt es formal nur 5 Controls, zu denen ein schriftlicher Nachweis vorhanden sein muss. Für viele Dinge, insbesondere in kleineren Organisationen mit geringer Mitarbeiterfluktuation, ist es ausreichend, wenn das Wissen auf mindestens zwei bis drei Köpfe verteilt ist und alle Betroffenen genau wissen, was zu tun ist. In derartigen Situationen kann der Prüfer keine Neben- oder Hauptabweichung feststellen, sondern wird dann jeweils mindestens einen dieser Wissensträger befragen. Dies ist so-wohl für ein Assessment nach AL2 (Dokumentenprüfung/Plausibilitätskontrolle) als auch für die verschiedenen AL3-Assessments gültig.

Letztendlich führt eine „Überdokumentation“ eher zu Problemen, da ich diese nur mit erheblichem Aufwand aktuell halten kann. Wenn der Prüfer dann im Rahmen des Assessments feststellt, dass zwar alles bis ins letzte Detail dokumentiert ist, diese Dokumentation jedoch in Teilen obsolet oder falsch ist, dann fange ich mir Neben- oder gar Hauptabweichungen ein. Diese Abweichungen können darauf beruhen, dass die Dokumentation nicht aktuell gehalten ist, es widersprüchliche Regelungen gibt oder die Mitarbeiter auf Grund der Menge von Dokumentation diese gar nicht kennen und das ISMS damit unwirksam ist.

All dies hätte ich vermeiden können, indem ich wie vorher beschrieben eher weniger Dokumentation vorhalte, diese dafür aber aktuell halte und eine hohe Qualität erreiche.

Wer ist typischerweise betroffen?

Organisationen, die sich nicht gut auf die Einführung eines Managementsystems vorbereitet haben und sich ohne Hilfe in ein schwer beherrschbares Abenteuer stürzen. Ebenso Organisationen, die bereits Erfahrungen aus anderen, dokumentations-intensiveren Managementsystemen, wie z.B. dem BSI IT-Grundschutz oder der ISO 9001, haben.

Lösungsansätze

Wie so oft, ist weniger mehr. Stellen Sie im Zweifel jede Dokumentation, die Sie er-stellen wollen, erst einmal in Frage und versuchen das Minimum zu erreichen. So viel wie nötig, nicht so viel wie möglich. Lassen Sie sich von erfahrenen Beratern, mindestens für die Planungsphase, zur Einführung eines ISMS auf Basis von TISAX unterstützen.

Praxistipps für die Umsetzung

Erfahrene CISOs oder externe Berater können hier helfen, ein schlankes Managementsystem nach TISAX aufzubauen.

©2024 – CISO Alliance e.V.

7. Unzureichendes Risikomanagement

Warum ist das eine Stolperfalle?

Wenn Risikomanagement, und hier insbesondere Informationsrisikomanagement (IRM) nicht ernst genommen wird, steht das gesamte ISMS nach TISAX in Frage, da dann nicht die passenden Risikobehandlungsmaßnahmen umgesetzt werden und auch nicht bewusst Risiken akzeptiert werden können. Das ISMS ist ohne funktioierenden Risikomanagementprozess im Großen und Ganzen unwirksam. Dasselbe gilt, wenn das IRM nicht in das (hoffentlich vorhandene) Unternehmensrisikomanagement eingebettet wird und in beiden Risikomanagementsystemen nach unter-schiedlichen Maßstäben bewertet und gehandelt wird. IRM ist der Kernpunkt der meisten Standards zum Informationssicherheitsmanagement und eben auch bei TISAX. Was ebenfalls regelmäßig „übersehen“ wird ist die Anforderung, auch ein Chancenmanagement im Rahmen des Risikomanagements mit zu verankern. Risiken haben nicht nur negative Auswirkungen! Leider ist im deutschen Sprachraum aus den englischsprachigen Begriffen „Risk Management“ und „Threat Management“ nur der Begriff „Risikomanagement“ mit einer negativen Konnotation übriggeblieben. Korrekt wäre: Risikomanagement besteht aus Bedrohungsmanagement (negative Auswirkungen) und Chancenmanagement (positive Auswirkungen).

Wer ist typischerweise betroffen?

Organisationen, die bisher noch kein funktionierendes und formalisiertes Risikomanagement haben. Ebenso Unternehmen, die bereits BSI IT-Grundschutz eingeführt haben und nun ein TISAX-Label erlangen möchten, da der Ansatz zum Risikomanagement beim BSI IT-Grundschutz völlig anders ist. Im Gegensatz dazu verfolgt die ISO/IEC 27001 nahezu denselben Ansatz wie TISAX. Weiterhin sind Organisationen betroffen, die Risikomanagement wenig formalisiert haben oder eher exotische bzw. sehr spezielle Risikomanagement-Ansätze verwenden, wie z.B. die PESTEL-Analyse.

Lösungsansätze

Das IRM ist der Kernbereich des ISMS nach TISAX. Stecken Sie lieber etwas zu viel Aufwand zu Projektanfang in eine sinnvolle und passende Gestaltung eines Risiko-managements für Ihre Organisation. Diese Zeit ist nicht verloren, da bei Vernachlässigung des Themas Risikoanalyse zu einem späteren Zeitpunkt im Projekt im Zweifel alles noch einmal von vorne aufgerollt werden muss. Definieren Sie für Ihre Organisation passende Eintrittswahrscheinlichkeiten und Auswirkungen. Berücksichtigen Sie auch non-monetäres Auswirkungen wie Reputationsschäden. Kümmern Sie sich aktiv um das Chancenmanagement. Wenn Sie bereits ein gut funktionierendes und formalisiertes Unternehmens-Risikomanagement haben, bauen Sie Ihr IRM darauf auf.

Praxistipps für die Umsetzung

Nehmen Sie sich die Zeit, um ein passendes und effizientes IRM aufzubauen. Holen Sie sich am besten externe Hilfe von erfahrenen Beratern, wenn Sie noch kein etabliertes internes Unternehmensrisikomanagementsystem haben. Für die Liste der Bedrohungen eigenen sich die sogenannten „Elementargefährdungen“ des BSI IT-Grundschutz.

©2024 – CISO Alliance e.V.

8. Falsches Verständnis eines ISMS und der dazugehörigen Dokumente

Warum ist das eine Stolperfalle?

Unternehmen, welche noch keine Berührungspunkte mit Informationssicherheits-Managementsystemen (ISMS) hatten, stehen oft vor den Herausforderungen die Anforderungen zu erfassen. Dies kann zu verschiedenen Problemen führen.

Durch eine falsche Interpretation der Anforderung kann es schnell zu Problemen in Assessmentsituationen führen. Diese können dann zu deutlichen Mehraufwendungen, wie Zeit oder Kosten, führen.

Wer ist typischerweise betroffen?

Unternehmen, welche bisher keine Berührungspunkte mit den Anforderungen eines ISMS hatten und den Nutzen für das eigene Unternehmen noch nicht verinnerlicht haben. Sie laufen Gefahr, die Anforderungen fehlerhaft zu deuten.

Lösungsansätze

- Greifen Sie auf externe Berater bei der Implementierung Ihres ISMS zurück.
- Schulen Sie die verantwortlichen Bereiche über die allgemeinen Anforderungen und nutzen Sie dafür Beispiele.
- Nutzen Sie technologische Unterstützung, um wiederkehrende Aufgaben wie Audits, Dokumentenprüfungen und Wirksamkeitsprüfungen zu unterstützen.
- Agieren Sie als Partner und unterstützen Sie die Bereiche bei der Dokumentation.

Praxistipps für die Umsetzung

- Sehen Sie die Anforderungen als „Problem“ an, welches es zu lösen gilt. Erklären Sie das Problem und erfahren Sie in Interviews welche Lösungen es schon gibt. Fangen Sie klein an, um eine Überbelastung zu verhindern
- Nutzen Sie eine verständliche Sprache in Interview Situationen und bei der Dokumentation.
- Planen Sie bei der Etablierung einer Richtlinie oder einer Maßnahme ein, wie diese überwacht (Dokumentenprüfung, Wirksamkeitsprüfung) werden soll. Kalkulieren Sie den erwarteten Zeitaufwand dafür ein. Bei neuen Maßnahmen kann es hilfreich sein, diese zu Beginn häufiger zu prüfen. Dokumentieren Sie jede Überprüfung.
- Achten Sie darauf, dass die genutzte technologische Unterstützung in bestehende Unternehmensanwendungen integriert werden kann.

©2024 – CISO Alliance e.V.

9. Falsche Interpretation oder das Übersehen von Anforderungstexten

Warum ist das eine Stolperfalle?

In der Excel-Tabelle VDA-ISA gibt es neben der Spalte mit den „muss“-Anforderungen noch weitere Spalten mit „sollte“-Anforderungen sowie mit Zusatz-anforderungen für einen hohen bzw. sehr hohen Schutzbedarf. Viele Unternehmen berücksichtigten bei ihrer ersten TISAX-Implementierung nur die „muss“-Anforderungen. „Sollte“ bedeutet in diesem Fall jedoch praktisch auch „muss“. Wird diese Anforderung nicht umgesetzt, muss gut begründet werden, dass die Anforderung bewertet wurde und man zu der Einschätzung kam, dass die Umsetzung der Anforderung keinen Sinn macht.

Wer ist typischerweise betroffen?

Unternehmen, die sich das erste Mal auf ein TISAX-Assessment vorbereiten und auf keine TISAX-erfahrenen Berater oder Mitarbeiter zurückgreifen.

Lösungsansätze und Praxistipps für die Umsetzung

Betrachten Sie die „Sollte“-Anforderungen genauso wie eine „Muss“-Anforderung.

Die weiteren Spalten mit den Zusatzanforderungen für einen hohen bzw. einen sehr hohen Schutzbedarf kommen immer dann zum Tragen, wenn ein entsprechendes Label erreicht werden soll. Die Zusatzanforderungen sind auch dann umzusetzen, wenn es aktuell noch keine entsprechend klassifizierten Daten oder Projekte gibt. In diesem Fall ist alles so zu dokumentieren und vorzubereiten, dass die Anforderungen gleich umgesetzt werden können, wenn ein Projekt oder Daten mit der entsprechenden Klassifikation kommt.

©2024 – CISO Alliance e.V.

10. Handhabung von Projekten

Warum ist das eine Stolperfalle?

Es gibt im VDA-ISA die Anforderung, dass Informationssicherheitsaspekte bei Projekten berücksichtigt werden müssen. Viele Unternehmen denken bei Projekten nur an Kundenprojekte. Tatsächlich sind damit jedoch auch interne Projekte gemeint. Auch bei internen Projekten muss also sichergestellt werden, dass Informationssicherheitsaspekte berücksichtigt werden.

Wer ist typischerweise betroffen?

Unternehmen, die sich das erste Mal auf ein TISAX-Assessment vorbereiten und auf keine TISAX-erfahrenen Berater oder Mitarbeiter zurückgreifen.

Lösungsansätze

Berücksichtigen Sie, dass Informationssicherheitsaspekte auch bei internen Projekten eine Rolle spielen müssen.

Praxistipps für die Umsetzung

Überprüfen Sie Umsetzungsmöglichkeiten innerhalb Ihres Projektmanagements. Zum Beispiel eine Überprüfung, ob die im Rahmen des Projektes genutzten Systeme für das Sicherheitsniveau der verwendeten Informationen geeignet sind.

©2024 – CISO Alliance e.V.

Fazit

Ein TISAX-Label zu erlangen ist relativ einfach machbar, wenn Sie die 10 häufigsten Fehler vermeiden und spätestens mit Projektbeginn einen qualifizierten CISO benennen, der dauerhaft in Ihrer Organisation verankert bleibt. Dieser CISO kann bei größeren Organisationen intern sein, bei kleineren bietet sich ein externer CISO oder virtueller CISO an.

Über die CISO Alliance e.V. und den Arbeitskreis TISAX

Die CISO Alliance versteht sich in erster Linie als Interessenvertretung der Experten und Führungskräfte mit CISO-nahen Berufsfunktionen. Im Mittelpunkt steht deshalb eine vielfältige fachliche Unterstützung der persönlichen Mitglieder sowie der Austausch untereinander. Wir freuen uns über weitere engagierte Mitglieder. Wir sind unter https://www.ciso-alliance.de erreichbar.

Im Arbeitskreis TISAX der CISO Alliance tauschen wir uns über unsere Herausforderungen und Erfahrungen mit TISAX aus. Der Arbeitskreis TISAX steht allen Mitgliedern des CISO Alliance e.V. offen. Sie können die Leitung des Arbeitskreises unter folgender E-Mailadresse erreichen:
leiter.ak-tisax@ciso-alliance.de

Links

1) https://enx.com
2) https://www.vda.de/de/themen/digitalisierung/daten/informationssicherheit
3) https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html
4) https://www.enx.com/handbook/tisax-teilnehmerhandbuch.html#ID3532

©2024 – CISO Alliance e.V.

Version:	*1.0*
Datum:	*21.10.2024*
Nächste Überprüfung:	*Spätestens 10/2026*
Klassifizierung:	***ÖFFENTLICH***
Status:	*in Arbeit / vorgelegt **/ freigegeben***
Autor(en):	*Thomas FAUSER*, Thorsten BERTRAM, Robert HELLWIG, unter Mitwirkung von Sascha HASSELBACH (zertifizierter TISAX®-Prüfer)*
Dokumentenverantwortung:	**Leiter Arbeitskreis „TISAX“*
Ablage:	*SharePoint CISO Alliance, AK TISAX Veröffentlichung: Webseite CISO Alliance e.V.*
Verteiler:	
Alle	alle Mitglieder

Dokumentenhistorie

Version	Datum	Autor	Bemerkung
1.0	21.10.2024	Thomas FAUSER et al.	Erste zur Veröffentlichung freigegebene Fassung

Definitionen, Abkürzungen, Verweise

Begriff	Definition
AK	Arbeitskreis
ALx	Assessment Level x (x=1, 2, 3)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISO	Chief Information Security Officer
DSB	Datenschutzbeauftragter
ENX	European (Automotive) Network Exchange
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO/IEC	International Organization of Standardization/International Electro-technical Commission
IT	Informationstechnologie
IT-SiBe	IT-Sicherheitsbeauftragter
PESTEL	Political, Economic, Sociocultural, Technological, Environmental, Legal
TISAX®	Trusted Information Security Assessment Exchange
VDA-ISA	Verband der Automobilindustrie - Information Security Assessment

©2024 – CISO Alliance e.V.

Abstimmungstabelle

Empfänger	Organisation	RACI	Bemerkung
Vorstand	CISO Alliance e.V.	A	
Arbeitskreis	CISO Alliance e.V.	R	
Mitglieder	CISO Alliance e.V.	C/I	
Alle	Externe	I	Nach offizieller Freigabe

RACI Legende: **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed

Tabelle 1: RACI Abstimmungstabelle[1]

Verbundene Dokumente

Stammpfad:

Dokumentenname	Ablageort

[1] **Responsible** - verantwortlich (**Durchführungsverantwortung**), zuständig für die eigentliche Durchführung. Die Person, die die Initiative für die Durchführung (durch Andere) gibt oder die die Aktivität selbst durchführt.
Accountable - rechenschaftspflichtig (**Kostenverantwortung**), verantwortlich im Sinne von „genehmigen“, „billigen“ oder „unterschreiben“. Die Person, die im rechtlichen oder kaufmännischen Sinne die Verantwortung trägt.
Consulted - konsultiert (**Fachverantwortung**). Eine Person, deren Rat eingeholt wird. Wird auch als Verantwortung aus fachlicher Sicht interpretiert.
Informed - zu informieren (Informationsrecht)

©2024 – CISO Alliance e.V.