mabs4.0 Deutschland GmbH

modelling advanced business security

TISAX®

Gegenüberstellung VDA-ISA Version 4.1.1 und Version 5.0
Welche Anforderungen haben sich geändert?

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

modelling advanced business security

Vorwort

Liebe Interessenten,

herzlichen Dank für Ihr Interesse an unserem Portfolio.

Die **mabs4.0 Deutschland GmbH** aus Düsseldorf ist eine Managementberatung 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

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 Mitarbeitenden

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.

4 Vorwort

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.

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 Schutzbedarfs wird der Prüf-Scope definiert, von diesem das Assessment-Level abgeleitet wird.

Seit Oktober 2020 gilt der VDA-ISA Katalog in der Version 5.0. Somit müssen Unternehmen die derzeit ein TISAX®-Label auf der Version 4.x.x haben, ihr Informationssicherheitsmanagementsystem auf die neuen Anforderungen anpassen, um ein erneutes TISAX®-Label zu erhalten.

Welche TISAX®-Anforderungen sich durch die neue Version 5.0 geändert haben, erfahren Sie in diesem Whitepaper.

Wir weisen darauf hin, dass das Whitepaper nicht durch den VDA überprüft wurde und es sich somit um keine durch den VDA freigegebene Gegenüberstellung handelt.

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 Zusammenfassung

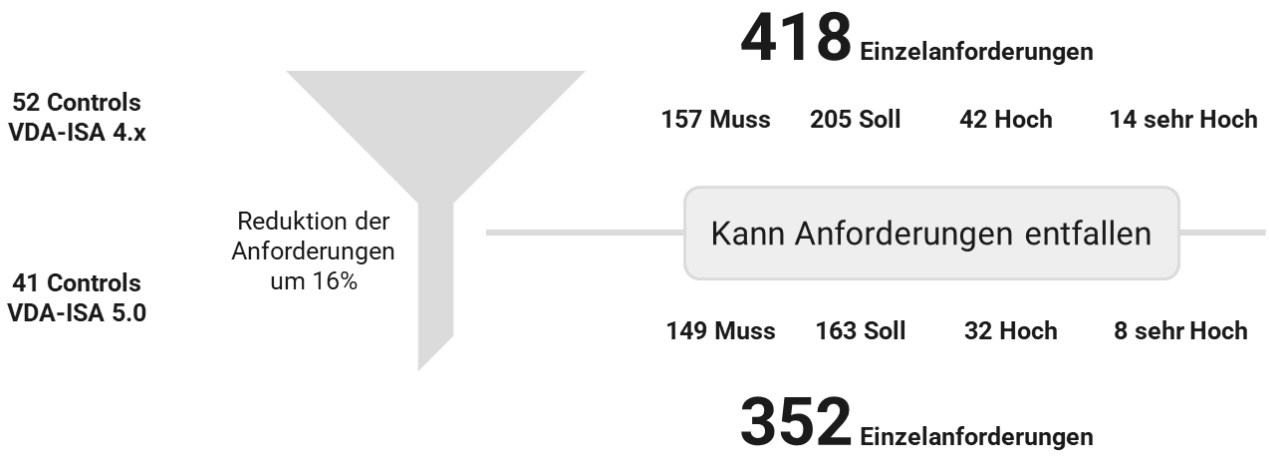
Was sofort auffällt ist die neue Darstellung der Anforderungen im Tabellenformat, welches a) eine bessere Übersicht liefert und b) eine vereinfachte Exportfunktion zulässt, sofern sich der Anwender eigene Arbeitsunterlagen zur Umsetzung kreieren möchte. Auch sind nun die Hinweise und Erläuterungen direkt im Modul Informationssicherheit zu finden. Des Weiteren wurden die Fragestellungen und die Zielsetzungen sowie die Anforderungen umformuliert, bzw. konkretisiert. Der zu erreichende Zielreifegrad hat nun einheitlich den Zielwert von 3. Darüber hinaus ist das Modul „Anbindung Dritter“ entfallen.

Teilweise sind die Anforderungen die in Version 4.x unter „sollte“ waren, nun in Version 5.0 eine „muss“-Anforderung oder eine Zusatzanforderung bei hohem Schutzbedarf. An manchen Stellen sind „muss“-Anforderungen nun eine Zusatzanforderung bei hohem Schutzbedarf. Das „kann“ Kriterium ist entweder weggefallen oder in eine „sollte“-Anforderung aufgenommen worden.

Diese Änderungen haben eine große Auswirkung auf die Umsetzung der Anforderungen, der damit verbundenen Prozesse und letztendlich auf das TISAX®-Assessment.

Hinweis: „sollte“-Anforderungen können so gut wie nicht ausgeschlossen werden und es empfiehlt sich daher diese genau wie „muss“-Anforderung bei der Umsetzung zu behandeln.

6 Überblick der Verschiebung der Anforderungen



Die Reduktion der Anforderungen ist trügerisch, da teilweise Anforderungen aus dem VDA-ISA Katalog 4.1 zusammengefasst wurden. Durch den Wegfall der Kann Anforderungen sind „Muss“- und „Soll“-Anforderungen wesentlich enger in der Auslegung gefasst, bzw. erhöhen die Komplexität des Controls.

Hierdurch erhöht sich die Abweichungsgefahr während des Assessments.

7 Tabellarische Übersicht der Anpassungen

Diese Tabelle dient dazu, einen allgemeinen Überblick über die neue Struktur des VDA ISA Katalog Version 5.0 zu geben, bzw. ein Anforderungs-Mapping zwischen dem alten und neuen VDA-ISA Katalog herzustellen.

Wir haben für Sie die adressierten Themenblöcke farblich (abwechselnd grün und gelb) gruppiert und die jeweiligen Anforderungen sofern notwendig zusammengeführt, da sich auch die Nummerierung der Anforderungen geändert haben.

Änderungen im Anforderungskatalog erkennen Sie einfach durch das „x“. Alle signifikanten Änderungen zwischen der Version 4.x und 5.0 haben wir zusätzlich rot gekennzeichnet.

Mapping VDA ISA 5.0 zu VDA ISA 4.x							
VDA ISA 5.0		Muss	Sollte	hoher	sehr hoher	**VDA ISA 4.x**	
1.1.1	Informationssicherheitsrichtlinie	x	x			05.1	Informationssicherheitsrichtlinie
1.2.1	Freigabe eines Informationssicherheits-managementsystems (ISMS)	x	x			01.1	Freigabe eines Informationssicherheits-managementsystems (ISMS)
						01.3	Wirksamkeit des ISMS
1.2.2	Zuweisung der Verantwortung für Informationssicherheit	x	x	x		06.1	Zuweisung der Verantwortung für Informationssicherheit
1.2.3	Informationssicherheit in Projekten	x	x	x		06.2	Informationssicherheit in Projekten
1.2.4	Rollen und Verantwortlichkeiten bei externen IT-Diensteanbietern	x	x	x		06.4	Rollen und Verantwortlichkeiten bei externen IT-Diensteanbietern
1.3.1	Inventarverzeichnis	x	x			08.1	Inventarverzeichnis
1.3.2	Klassifizierung von Informationen	x	x			08.2	Klassifizierung von Informationen
1.3.3	Freigabe von externen IT-Diensten	x	x			14.4	Freigabe von externen IT-Diensten
1.4.1	IS-Risikomanagement	x	x			01.2	IS-Risikomanagement
1.5.1	Wirksamkeitsprüfung	x	x			18.4	Wirksamkeitsprüfung
1.5.2	Prüfung des ISMS durch unabhängige Instanzen	x	x			18.3	Prüfung des ISMS durch unabhängige Instanzen
1.6.1	Berichtswesen für Vorfälle in der Informationssicherheit (Incident Management)	x	x	x		16.1	Berichtswesen für Vorfälle in der Informationssicherheit (Incident Management)
						16.2	Bearbeitung von Informationssicherheitsvorfällen
2.1.1	Eignung von Mitarbeiter der Mitarbeiter	x	x			07.1.a (neu)	Eignung von Mitarbeiter der Mitarbeiter
2.1.2	Vertragliche Verpflichtung zur Informationssicherheit der Mitarbeiter	x	x			07.1	Vertragliche Verpflichtung zur Informationssicherheit der Mitarbeiter
2.1.3	Sensibilisierung und Schulung der Mitarbeiter	x	x			07.2	Sensibilisierung und Schulung der Mitarbeiter
2.1.4	Mobiles Arbeiten	x	x	x		06.3.a (neu)	Mobiles Arbeiten

Mapping VDA ISA 5.0 zu VDA ISA 4.x							
VDA ISA 5.0		Muss	Sollte	hoher	sehr hoher	VDA ISA 4.x	
3.1.1	Sicherheitszonen	x	x	x		11.1	Sicherheitszonen
						11.3	Schutzmaßnahmen im Anlieferungs- und Versandbereich
3.1.2	Aspekte der Informationssicherheit für das Business Continuity Management (BCM)	x	x			11.2	Schutz vor äußeren Einflüssen und externen Bedrohungen
						12.4	Informationssicherung (Backup)
						17.1	Aspekte der Informationssicherheit für das Business Continuity Management (BCM)
3.1.3	Verwendung von Betriebsmitteln	x		x	x	11.4	Verwendung von Betriebsmitteln
3.1.4	Mobile Endgeräte	x	x	x		06.3	Mobile Endgeräte
						08.3	Speicherung von Informationen auf mobilen Datenträgern
						12.4	Informationssicherung (Backup)
4.1.1	Umgang mit Identifikationsmitteln	x	x	x		09.2.a (neu)	Umgang mit Identifikationsmitteln
4.1.2	Zugang zu Netzwerken und Netzwerkdiensten	x	x	x	x	09.1	Zugang zu Netzwerken und Netzwerkdiensten
4.1.3	Benutzerregistrierung	x	x			09.2	Benutzerregistrierung
						09.4	Vertraulichkeit von Authentifizierungsinformationen
4.2.1	Zugriff auf Informationen und Applikationen	x	x	x	x	09.3	Privilegierte Benutzerkonten
						09.5	Zugriff auf Informationen und Applikationen
5.1.1	Verschlüsselung	x	x	x		10.1	Verschlüsselung
5.1.2	Elektronischer Austausch von Informationen	x	x	x	x	13.4	Elektronischer Austausch von Informationen
5.2.1	Änderungsmanagement (Change Management)	x	x	x		12.1	Änderungsmanagement (Change Management)
5.2.2	Trennung der Entwicklungs-, Test- und Produktivumgebung	x	x			12.2	Trennung der Entwicklungs-, Test- und Produktivumgebung
5.2.3	Schutz vor Schadsoftware	x	x			12.3	Schutz vor Schadsoftware

Mapping VDA ISA 5.0 zu VDA ISA 4.x							
VDA ISA 5.0		Muss	Sollte	hoher	sehr hoher	VDA ISA 4.x	
5.2.4	Event-Logging	x	x	x	x	12.5	Event-Logging
						12.6	Protokollierung Administrationstätigkeiten
5.2.5	Verfolgung von Schwachstellen (Patch Management)	x	x			12.7	Verfolgung von Schwachstellen (Patch Management)
5.2.6	Überprüfung von Informationssystemen	x	x			12.8	Überprüfung von Informationssystemen
5.2.7	Verwaltung der Netzwerke	x	x	x		13.1	Verwaltung der Netzwerke
						13.3	Trennung von Netzwerken (Netzwerk-Segmentierung)
5.3.1	Anforderungen an die Beschaffung von Informationssystemen	x	x			14.1	Anforderungen an die Beschaffung von Informationssystemen
						14.2	Sicherheit im Software-Entwicklungsprozess
						14.3	Management von Testdaten
5.3.2	Sicherheitsanforderungen an Netzwerke/-dienste	x	x	x		13.2	Sicherheitsanforderungen an Netzwerke/-dienste
5.3.3	Entfernen von extern gespeicherten Information-Assets	x	x			08.4	Entfernen von extern gespeicherten Information-Assets
5.3.4	Trennung von Informationen in gemeinsam genutzten Umgebungen	x	x			09.6	Trennung von Informationen in gemeinsam genutzten Umgebungen
6.1.1	Risikomanagement bei der Zusammenarbeit mit Lieferanten	x	x	x		15.1	Risikomanagement bei der Zusammenarbeit mit Lieferanten
						15.2	Überprüfung der von Lieferanten erbrachten Leistungen
6.1.2	Geheimhaltungsvereinbarungen beim Informationsaustausch mit Dritten	x	x			13.5	Geheimhaltungsvereinbarungen beim Informationsaustausch mit Dritten
7.1.1	Gesetzliche und vertragliche Bestimmungen	x	x			18.1	Gesetzliche und vertragliche Bestimmungen
7.1.2	Vertraulichkeit und Schutz von personenbezogenen Daten	x				18.2	Vertraulichkeit und Schutz von personenbezogenen Daten
Anforderung nicht mehr relevant						12.9	Berücksichtigung kritischer administrativer Funktionen von Cloud-Diensten

Hinweis: Die Tabelle erhebt weder einen Anspruch auf Vollständigkeit und Korrektheit.

8 Übersicht der benötigten Risikobewertungen gemäß VDA-ISA Katalog 5.0

Informationssicherheit basiert immer auf einem etablierten Riskmanagement. Der VDA-ISA 5.0 fordert daher teilweise eine Entscheidungsgrundlage auf durchgeführten Risikobewertungen. Diese Risikobewertungen sind nachweislich zu erbringen.

Hierbei gibt es keine Vorgaben wie die Risikobewertungen durchzuführen sind.

Control	Kontrollfrage	Anforderungen (muss)	Anforderungen (sollte)	Zusatzanforderungen bei hohem Schutzbedarf	Zusatzanforderungen bei sehr hohem Schutzbedarf
1.2.3	**Inwieweit werden Informationssicherheitsan-forderungen in Projekten berücksichtigt?**		in einer frühen Phase des Projektes wird eine Risikobewertung auf Basis der definierten Vorgehensweise durchgeführt und bei Änderungen des Projektes wiederholt.		
1.3.3	**Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?**	Eine Risikobewertung der organisations-fremden IT-Dienste liegt vor			
3.1.1	**Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?**			Nachweise zur angemessenen Umsetzung müssen über eine entsprechende Risikobeurteilung mit Berücksichtigung der eingeschätzten Widerstandsklasse erbracht werden - Orientierung für die Risikobeurteilung: Umsetzung der Anforderung ohne Mindestwiderstandszeit	Einsehbarkeit: Sicherheitsmaßnahmen gemäß Risikobewertung für den Standort bzw. für die IT-Systeme sind etabliert (z. B. permanenter Sichtschutz/Geräuschdämpfung). Widerstandswerte: Falls keine Einfriedung vorhanden ist, dann Ausführung Fenster und Türen in der Gebäudeaußenhaut in RC2 oder vergleichbar nach Risikoeinschätzung
4.1.2	**Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?**	Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikobewertung getroffen. Mögliche Angriffsszenarien wurden berücksichtigt (z. B. direkte Zugriffsmöglichkeit aus dem Internet).			
5.2.2	**Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?**	Eine Risikobewertung der IT-Systeme wurde durchgeführt, um zu ermitteln, inwiefern eine Trennung der IT-Systeme in Entwicklungs- und Produktivsysteme notwendig ist.			
5.3.4	**Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?**		Risikobewertung für den Betrieb von Fremdsoftware innerhalb der geteilten Umgebung.		
6.1.1	**Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?**	Auftragnehmer und Kooperationspartner werden einer Risikobewertung bzgl. der Informationssicherheit unterzogen.			

9 Fazit

Der neue VDA-ISA Katalog richtet sich an die Verantwortlichkeiten in der Organisation und ist somit kein alleiniges Thema der IT-Abteilung. Darüber hinaus richten sich die Anforderungen nicht nur an Informationswerte der eigentlichen Wertschöpfungskette, sondern ganzheitlich an die Organisation und jedem Mitarbeitenden.

Die scheinbare Reduktion der Anforderungen lässt auf den ersten Blick vermuten, dass die Anforderungen gesenkt wurden, dies ist jedoch nicht der Fall. Durch den Wegfall der „Kann"- Anforderungen sind „Muss"- und „Soll"- Anforderungen wesentlich enger in der Auslegung gefasst, bzw. erhöhen die Komplexität des Controls.

Auch wenn der Reifegrad nun einen einheitlichen Zielwert von 3 hat, so bedeutet dieses im Umkehrschluss, dass die Selbstauskunft wesentlich detaillierter ausgefüllt werden muss.

10 Nützliche Links

https://mabs40.de.com/
https://mabs40.de.com/download/
https://portal.enx.com/de-de/
https://portal.enx.com/de-de/TISAX/downloads/

11 Zusätzliche Informationen

11.1 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.

11.2 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 Mitarbeitenden zur „Human Firwall“ und minimieren Sie Ihre Risiken durch ein durchgängiges Rahmenwerk mit entsprechender Prozesssicherheit.
Durch entsprechende Unterweisungen werden Ihre Mitarbeitenden 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.