TISAX® Grundlagen

Anforderungen – VDA ISA

Zertifiziert nach AZAV
ZERT PUNKT
Trägerzulassung
Registriernummer: A-K-90402

Zertifiziert nach
ZERT PUNKT
DIN EN ISO 9001:2015

ipu fit for success
Lise-Meitner-Straße 1
85716 Unterschleißheim
www.ipu-fitforsuccess.de

Inhalte

Einführung: TISAX®

- TISAX® steht für „Trusted Information Security Assessment Exchange“
- Wie der Name schon verrät, ist eines der Ziele von TISAX®, der Austausch von Angaben bezüglich des Niveaus der Informationssicherheit der Beteiligten.
- Es ist ein von der Automobilindustrie definierter Standard für Informationssicherheit, welcher speziell für die Anforderungen der Branche angepasst wurde.
- Grundlage dieses Standards ist die ISO 27001, auf welche auch häufig verwiesen wird.
- Ebenso handelt es sich dabei um eine Plattform, mit deren Hilfe Unternehmen der Automobilindustrie das geforderte Niveau in der Informationssicherheit:
  - prüfen lassen,
  - dokumentieren und
  - nachweisen

  können.

Wozu dient der Standard?

- Schon früher hat jeder OEM Anforderungen an die Informationssicherheit seiner Lieferanten formuliert.
- Jedoch waren diese Auffassungen höchst unterschiedlich.
- Damit ging eine erhöhte Komplexität des Nachweisverfahrens einher, insbesondere dann, wenn ein Unternehmen Lieferant verschiedener OEM‘s war.
- TISAX® ermöglicht in der gesamten Automobilbranche eine einheitliche Auffassung von Informationssicherheit zu vertreten und effizient nachzuweisen.

Voraussetzungen und Abgrenzung

Voraussetzungen:

- Eine Zertifizierung nach 27001 (ISMS) oder 9001 (QMS) ist zwar keine zwingende Voraussetzung für TISAX®, stellt aber eine sehr gute Basis dafür dar
- Zum Verständnis: Die Abgrenzung von ISO 27001 und TISAX® sieht folgendermaßen aus:

Aspekte	ISO 27001	TISAX®
ISMS	- High Level Struktur - Grundlage der ISO 27001 Zertifizierung - Vollständiges Managementsystem - Formales Statement of Applicability (SoA)	- Ansatz für Informationssicherheit auf Basis ISO 27001 und VDA-ISA - Kein vollständiges Managementsystem - Ausgefülltes Self-Assessment = SoA
Zertifizierung	- Zertifizierung eines Informationssicherheitsmanagementsystems - Durchgeführt von einem Auditor - Veröffentlichung per Zertifikat	- Prüfung der Erfüllung der VDA-ISA Anforderungen - Durchgeführt von einem Prüfer - Veröffentlichung der Labels auf ENX Plattform
Gültigkeit	- 3 Jahre - Jährliche Überwachungsaudits	- 3 Jahre - Keine jährlichen Überwachungsaudits

TISAX® Prüfziele

Festlegung der TISAX® Prüfziele:

- Es sollte unbedingt darauf geachtet werden, dass vom Kunden ein konkretes Prüfziel vorgegeben wird
- Die konkrete Kundenvorgabe ist für den Prüfungsverlauf enorm wichtig und sollte entsprechend eingefordert werden
- Abhängig vom Schutzbedarf der jeweiligen Informationen wurden insgesamt 8 Prüfziele festgelegt
  - mindestens 1 Prüfziel muss ausgewählt werden
  - Auswahl von mehreren Prüfzielen ist möglich

TISAX® Prüfziele

Nr.	ISA-Kriterienkatalog	Schutzbedarf	TISAX-Prüfziel	Assessment-Level (AL)
1.	Informationssicherheit	Hoch	Informationen mit hohem Schutzbedarf Information with high protection needs	AL 2
2.	Informationssicherheit	Sehr hoch	Informationen mit sehr hohem Schutzbedarf Information with very high protection needs	AL 3
3.	Prototypenschutz	Hoch	Schutz von Prototypen-Bauteilen und -Komponenten Protection of prototype parts and components	AL 3
4.	Prototypenschutz	Hoch	Schutz von Prototypenfahrzeugen Protection of prototype vehicles	AL 3
5.	Prototypenschutz	Hoch	Umgang mit Erprobungsfahrzeugen Handling of test vehicles	AL 3
6.	Prototypenschutz	Hoch	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings Protection of prototypes during events and film or photo shootings	AL 3
7.	Datenschutz	Hoch	Datenschutz Gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz-Grundverordnung (DSGVO) Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	AL 2
8.	Datenschutz	Sehr hoch	Datenschutz bei besonderen Kategorien personenbezogener Daten Gemäß Artikel 28 („Auftragsverarbeiter“) mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben Data protection with special categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	AL 3

Tabelle 5. Zuordnung der ISA-Kriterienkataloge und Schutzbedarfe zu den TISAX-Prüfzielen

TISAX® Prüfziele

Nr.	TISAX-Prüfziel	Assessment-Level (AL)
1.	Informationen mit hohem Schutzbedarf Information with high protection needs	AL 2
2.	Informationen mit sehr hohem Schutzbedarf Information with very high protection needs	AL 3
3.	Schutz von Prototypen-Bauteilen und -Komponenten Protection of prototype parts and components	AL 3
4.	Schutz von Prototypenfahrzeugen Protection of prototype vehicles	AL 3
5.	Umgang mit Erprobungsfahrzeugen Handling of test vehicles	AL 3
6.	Schutz von Prototypen während Veranstaltungen und Film- und Fotoshootings Protection of prototypes during events and film or photo shootings	AL 3
7.	Datenschutz Gemäß Artikel 28 („Auftragsverarbeiter“) der Datenschutz-Grundverordnung (DSGVO) Data protection According to Article 28 (“Processor”) of the European General Data Protection Regulation (GDPR)	AL 2
8.	Datenschutz bei besonderen Kategorien personenbezogener Daten Gemäß Artikel 28 („Auftragsverarbeiter“) mit besonderen Kategorien personenbezogener Daten wie in Artikel 9 der Datenschutz-Grundverordnung (DSGVO) angegeben Data protection with special categories of personal data According to Article 28 (“Processor”) with special categories of personal data as specified in Article 9 of the European General Data Protection Regulation (GDPR)	AL 3

Tabelle 6. Zuordnung der TISAX-Prüfziele zu den Assessment-Leveln

Prüfmethode	Assessment-Level 1 (AL 1)	Assessment-Level 2 (AL 2)	Assessment-Level 3 (AL 3)
Selbsteinschätzung	Ja	Ja	Ja
Nachweise	Nein	Plausibilitätsprüfung	Eingehende Prüfung
Interviews	Nein	Als Telefonkonferenz[14]	Persönlich, vor Ort
Vor-Ort-Prüfung	Nein	Auf Ihren Wunsch	Ja

Tabelle 7. Applicability of assessment methods to different assessment levels

TISAX® Prüf Scope

Festlegung des TISAX® Prüf Scopes:

- Neben der Angabe der TISAX® Prüfziele, ist der Prüf Scope ein wichtiger Bestandteil der Registrierung als TISAX® Teilnehmer
- Der Prüf Scope beeinflusst ebenfalls zu einem großen Teil den Umfang der TISAX® Prüfung
- Als Basis für die Definition des Scopes dient der TISAX® Standard Scope

  ➔ Dieser wird von allen Kunden akzeptiert

- Der Standard Scope erfasst dabei alle Prozesse, Verfahren und beteiligte Ressourcen am jeweiligen Standort
- Abweichungen vom Standard Scope (=Einschränkungen oder Erweiterungen des Scopes) müssen zwingend mit dem Kunden abgestimmt werden

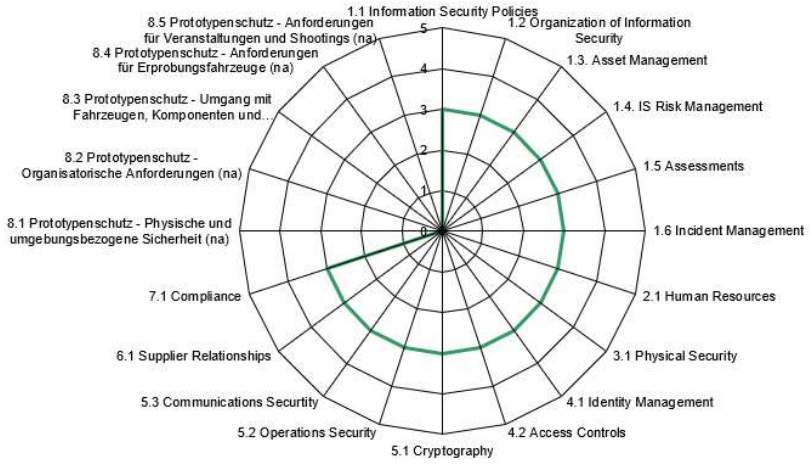
Ablauf eines TISAX®-Assessments

Definition des Scopes	Anforderung des Scopes und des Assessment-Levels durch den Kunden, z.B. mit oder ohne Prototypenschutz
Online-Registrierung als TISAX®-Teilnehmer	Online-Registrierung als TISAX®-Teilnehmer auf www.enx.com/TISAX®, danach erfolgt die Zuweisung der Scope ID durch ENX ➔ jährliche Servicegebühr
Durchführung des Assessments in zwei Schritten	Auswahl eines zugelassenen Prüfdienstleisters, danach Kick-Off, Dokumentenprüfung (Self-Assessment: nicht vor Ort) und anschließendes Assessment (Level 2: nicht vor Ort, Level 3: vor Ort)
Zwischenbericht und ggf. Maßnahmenfestlegung	Abschlussgespräch Erstprüfung, bei Abweichungen werden umzusetzende Maßnahmen vereinbart.
Schließung von Abweichungen	Bei Bedarf Maßnahmenumsetzung im vereinbarten Zeitraum. Nach Schließung der Abweichungen findet eine Wirksamkeitsprüfung mittels Nachprüfung statt.
Einstellen des Abschlussberichts	Der finale Abschlussbericht wird in der TISAX®-Online-Plattform eingestellt. Damit ist der Teilnehmer gelistet.

Selbsteinschätzung auf Basis des VDA ISA

- Damit die Prüfung nicht unnötig lang dauert oder sogar scheitert, können Sie Ihr Informationssicherheitsmanagementsystem, mit Hilfe der Selbsteinschätzung, auf Basis des VDA ISA Katalogs auf Herz und Nieren überprüfen.
- Damit sind Sie zu Beginn des eigentlichen Prüfungsprozesses in einer guten Ausgangssituation.
- Der Fragenkatalog des VDA ISA kann unter dem folgenden Link runtergeladen werden: https://www.vda.de/de/services/Publikationen/vda-isa-katalog-version-5.0.html
- **Der Fragenkatalog des VDA ISA besteht aus den drei Reitern:**

1. Informationssicherheit
2. Prototypenschutz (8)
3. Datenschutz (24)



Hauptbestandteile TISAX®-Prüfung

ISM-Leitlinien

Eine zusammenfassende Übersicht aller hinsichtlich der Informationssicherheit betreffenden Vorgaben und Verpflichtungen, welche innerhalb der Organisation festgelegt wurden, muss als bindende Vorgabe für alle Mitarbeiter erstellt und zur Verfügung gestellt werden.

Kennzahlen (KPI´s)

Zum Überwachen und Messen der Prozessergebnisse sowie der vorgegebenen Controls, werden von der TISAX® beispielhafte Key Performance Indicators vorgeschlagen, welche für ein zentrales Management der Informationssicherheit sehr hilfreich sind.

Dokumentation und Richtlinien

Mit Hilfe der Erstellung von bestimmten Richtlinien sowie einer strukturierten und gelenkten Dokumentation müssen die von der TISAX® geforderten Vorgaben durchgängig definiert, dokumentiert und für die Mitarbeiter zugänglich gemacht werden.

Prozesse und Vorgehensweisen

Die aus der TISAX® resultierenden Mindestanforderungen an die einzuführenden bzw. umzusetzenden Prozesse und Vorgehensweisen in einer Organisation können mit Hilfe von bestimmten Pflichtprozessen dargestellt und umgesetzt werden.

ISM-Leitlinie

- Die Erstellung der ISM-Leitlinien bildet die grundlegende Basis für die TISAX®-Implementierung und deckt bereits einen Großteil aller zu erfüllenden Anforderungen ab
- Die ISM-Leitlinie gilt für alle Mitarbeiter, Angestellten und Auftragnehmer einer Organisation, einschließlich Zeitarbeitskräfte und Auftragnehmer mit Zugang zu Informationen und Datenverarbeitungssystemen
- Mit Hilfe der ISM-Leitlinie wird sichergestellt, dass **JEDER** Mitarbeiter:
  - weiß, dass ein ISM-System in der Organisation implementiert ist
  - sich mit dem ISM-System vertraut machen kann
  - die Informationssicherheitsdokumentation, welche für jeden Bereich und jedes Verfahren gilt, anwendet
  - sich strikt an alle Vorschriften und Anforderungen der Informationssicherheit hält
- Jedes Hauptkapitel der ISM-Leitlinien enthält zusätzliche Informationen zu:
  - den Zielen einer Sicherheitsmaßnahme und was mit dieser erreicht werden soll
  - einer oder mehreren Sicherheitsmaßnahmen, um das angewandte Ziel zu erreichen

Geforderte KPI‘s

- Zur Überwachung fordert die TISAX® explizit eine durchgängige Erhebung, Messung und Dokumentation von festgelegten Kennzahlen.
- Alle von der TISAX® mindestens geforderten KPI‘s werden in der VDA ISA (=Excel-Datei) im Tabellenreiter „Beispiele KPI“ aufgelistet und explizit beschrieben.
- Der Inhalt des Tabellenblattes dient zwar als reine Hilfestellung zur Identifizierung eigener, passender KPI‘s, wird jedoch in den meisten Fällen einfach übernommen.

Control VDA ISA 5.0	2.1.3 Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert?		4.1.3 Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?			5.2.1 Inwieweit v
Control VDA ISA 4.1	7.2 Sensibilisierung und Schulung der Mitarbeiter		9.2 Benutzerregistrierung			12.1 Än (Cha
Bereich	ABDECKUNG	EFFEKTIVITÄT	ABDECKUNG	ABDECKUNG	EFFEKTIVITÄT	ABDECKUNG
ID	Abdeckungsgrad Awareness Maßnahmen	Effektivität von Awareness-Maßnahmen	Abdeckungsgrad Review "Benutzer-Accounts" (Benutzerkonten)	Abdeckungsgrad Review "Berechtigungen"	"Sammelaccounts" (Sammel-Konten)	Abdeckungsgrad Char Management
Beschreibung	Sensibilisierte Mitarbeiter stellen eine wichtige Säule für die Informationssicherheit im Unternehmen dar. Awareness Maßnahmen sollten möglichst alle Mitarbeiter erreichen. Der KPI misst den Abdeckungsgrad von Schulungen, wie z. B. E-Learnings, Präsenz-Trainings.	Die Inhalte von Awareness Maßnahmen sollten Erkenntnisse aus Informationssicherheits-vorfällen berücksichtigen. Der KPI misst die Effektivität von Awareness-Maßnahmen durch eine Erfassung (Anzahl- oder Kosten-bezogen) der Sicherheitsvorfälle mit menschlichen Fehlhandlungen als Ursache.	Regelmäßige Überprüfungen der IT-Systeme auf nicht notwendige Accounts sind die Voraussetzung für eine konsistente und aktuelle Benutzerbasis nach dem Need-to-know Prinzip. Der KPI misst den Abdeckungsgrad der Maßnahme "regelmäßiger Benutzer-Review".	Regelmäßige Überprüfungen der Benutzer Accounts auf nicht notwendige Berechtigungen sind die Voraussetzung für eine konsistente und aktuelle Berechtigungsbasis nach dem Need-to-know Prinzip. Der KPI misst den Abdeckungsgrad der Maßnahme "regelmäßiger Berechtigungs-Review".	Sammelaccounts sollten grundsätzlich nicht bzw. nur in Ausnahmefällen genutzt werden, da eine eindeutige Zuordnung von Benutzeraktivitäten erschwert wird. Der KPI misst die Anzahl von genutzten Sammelaccounts unter Berücksichtigung von genehmigten Ausnahmen.	Ein flächendeckend und durchgängig eingehaltene Change-Management Pro ist die Grundlage für eine sicheren Betrieb. Der KPI den Abdeckungsgrad von Vorgaben-konformen Cha

... | Reifegrade | Definitionen | Informationssicherheit | Prototypenschutz | Datenschutz | Ergebnisse (ISA5) | Ergebnisse (ISA4) | Beispiele KPI | Lizenz | ...

- Für Controls, bei denen ein Zielreifegrad Level 4 definiert wurde als auch für weitere Controls, bei denen eine Messung sinnvoll erscheint, müssen konkrete KPI‘s definiert und durchgängig erhoben, dokumentiert und bewertet werden.

Geforderte „Prozesse“

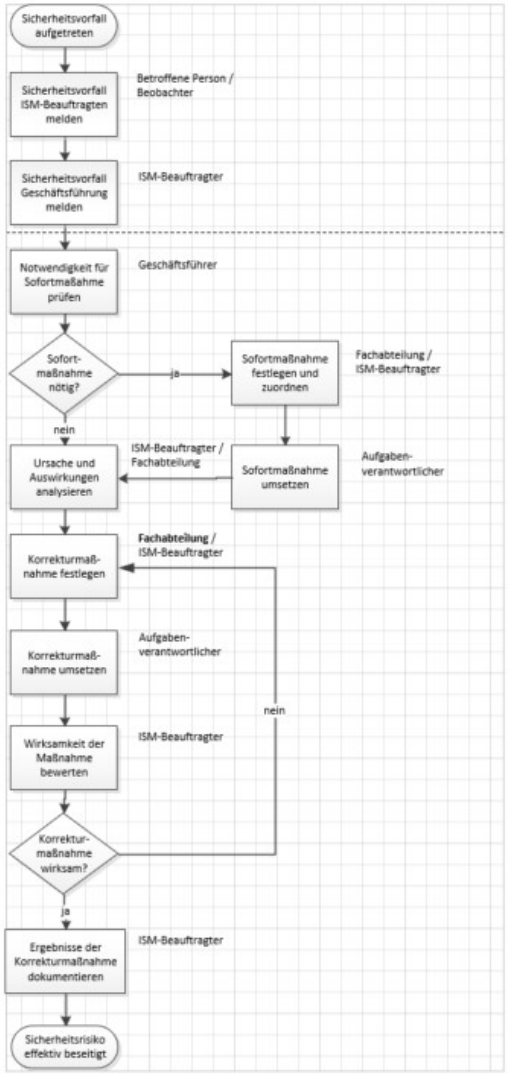
Geforderte TISAX® „Prozesse“:

- Prozesse zur Identifikation, Bewertung und Behandlung von Informationssicherheits-Risiken
- Prozess zur regelmäßigen Prüfung und Überarbeitung der ISM-Leitlinie
- Prozess zum Umgang mit Informationssicherheitsvorfällen
- Prozess zur Asset-Verwaltung (Terminierungsprozess)
- Prozess zur Benutzerverwaltung (Vergabe, Änderung, Löschung von Benutzerkennungen)
- Prozess zur Verwaltung von Zutritts- sowie Zugriffsrechten
- Prozess für das Änderungsmanagement
- Genehmigungsprozess für die Verwendung von externen Diensten (z.B. Instant Messaging, Web-Meeting, Web-Mail)
- Prozess zur Überwachung der Gültigkeit von befristeten Vereinbarungen (z.B. Geheimhaltungsvereinbarungen)
- Entwicklungsprozess für Software und IT-Systeme
- Prozess zum Managen von Testdaten (Genehmigungsprozess)
- Beschaffungsprozess zur Evaluierung und Freigabe von externen IT-Diensten (z.B. Cloud-Dienste)
- Prozess zur Überwachung und Überprüfung von Dienstleistern (Lieferantenmanagement)
- Disaster Recovery Prozess zur Weiterführung eines ISMS in Krisensituationen
- Prozess und Verfahren zum Schutz personenbezogener Informationen (Datenschutz)

Umsetzungsbeispiele: Prozesse I

Beispielprozess:

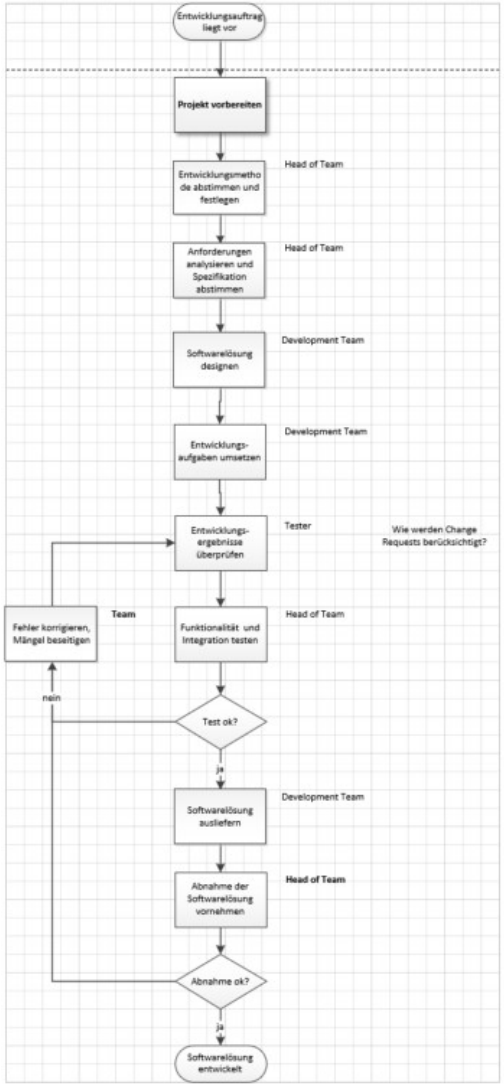
Sicherheitsvorfälle managen



Umsetzungsbeispiele: Prozesse II

Beispielprozess:

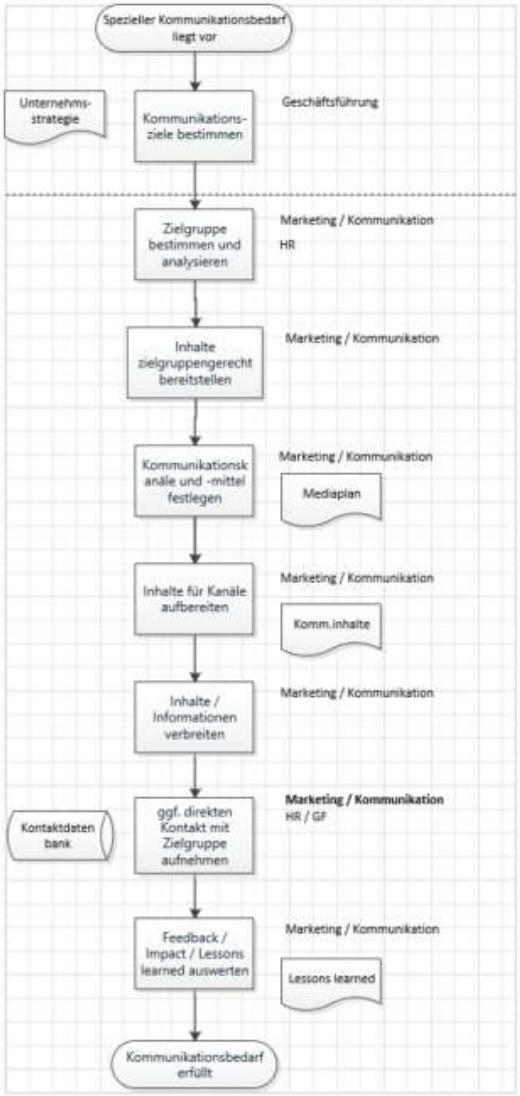
Softwarelösung entwickeln



Umsetzungsbeispiele: Prozesse III

Beispielprozess:

Kommunikationsbedarf erfüllen



So finden Sie uns….

Firmensitz

ipu fit for success
Lise-Meitner-Straße 1
85716 Unterschleißheim

Tel.: 089 / 319 017 580
Fax: 089 / 319 017 588

info@ipu-fitforsuccess.de
www.ipu-fitforsuccess.de