



knownow
TOOLS FOR BUSINESS SUCCESS

Dokumentierte Information TISAX

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Erläuterung zur Notwendigkeit von „dokumentierte Information“ zur Erfüllung der TISAX-Anforderungen, entsprechend dem VDA-ISA-Katalog

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Um einen gewissen Grad der Vergleichbarkeit zwischen TISAX und der ISO/IEC 27001:2022 sicherzustellen, differenzieren wir die dokumentierte Information auch für TISAX im Sinne der Norm:

1. Dokumentiere Information, die verfügbar sein muss.
Diese Vorgabedokumente sind aufrechtzuerhalten, d.h. sie müssen auf dem aktuellen Stand gehalten werden.
2. Dokumentiere Information, die aufbewahrt werden muss.
Diese Nachweisdokumente umfassen die sogenannten Aufzeichnungen, d.h. diese müssen vor Veränderungen geschützt werden.
Im Zusammenhang mit Aufzeichnungen, die zur Steuerung des Informationsmanagementsystems (ISMS) genutzt werden, wird ebenfalls die Anforderung aufgestellt, dass diese verfügbar sein müssen.

Sie möchten sich über dieses und weitere Tools

informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Ihr Vorteil, als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
1.1.1	Die Organisation benötigt mindestens eine Richtlinie für Informationssicherheit.	Zentrale Richtlinie für Informationssicherheit
1.2.2	Zusätzliche Richtlinien können je nach Größe und Aufbau der Organisation erforderlich sein. Verantwortlichkeiten für die Informationssicherheit in der Organisation sind definiert, strukturiert und zugewiesen.	(ggf. mit Verweis auf weitere Richtlinien) Alternativ in der zentralen Richtlinie
1.2.3	Durch eine geeignete Verankerung des Informations-Sicherheitsprozesses in den Projektmanagementverfahren der	Teil eines vorhandenen Projektmanagementverfahrens oder ggf.
	Organisation wird sichergestellt, dass keine Anforderungen übersehen werden.	Richtlinie Projektmanagement IT
1.2.4	Sollte: Bei IT-Diensten wurde die Konfiguration anhand der notwendigen Sicherheitsanforderungen konzipiert, umgesetzt und dokumentiert. Achtung: Bei „Zusatzanforderungen hoch“ müssen für Cloud-Dienste weitere Dokumente erzeugt werden.	Vertragliche Vereinbarungen mit IT-Dienstleistern. Ggf. Checkliste mit Sicherheitsanforderung an Cloud-Dienste.
1.3.2	Ein einheitliches Schema zur Klassifizierung von Informationswerten hinsichtlich des Schutzziele Vertraulichkeit ist verfügbar.	Richtlinie Informationsklassifizierung
1.4.1	Sollte: Es existiert eine Vorgehensweise, wie Informationssicherheitsrisiken innerhalb der Organisation identifiziert, beurteilt und bewertet werden.	Verfahren Risikomanagement IT
1.6.1	Es ist eine Definition für ein berichtspflichtiges Sicherheitsereignis, das eine berichtspflichtige sicherheitsrelevante Beobachtung vorhanden, die den Mitarbeitern und maßgeblichen Beteiligten bekannt ist.	Richtlinie Informationssicherheitsvorfälle IT (Meldeweg)

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Dokumentierte Information, die explizit verfügbar sein muss bzw. sollte

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
1.6.3	Es ist eine geeignete Planung für die Reaktion auf und Erholung von Krisensituationen vorhanden. Verantwortlichkeiten und Befugnisse für das Krisenmanagement in der Organisation sind definiert, dokumentiert und zugewiesen.	Verfahren Notfallwiederherstellung (BCP = Business Continuity Plan)
2.1.1	Sensible Tätigkeitsbereiche und Stellen sind ermittelt. Die Anforderungen an Mitarbeiter bezüglich ihres Stellenprofils sind ermittelt und dokumentiert. Die Identität von potenziellen Mitarbeitern wird überprüft (z.B. Prüfung von Ausweisdokumenten).	Zuordnung im Organigramm, Checkliste Personal
2.1.2	Es besteht eine Verpflichtung zur Geheimhaltung. Es besteht eine Verpflichtung zur Einhaltung der Richtlinien zur Informationssicherheit.	Geheimhaltungsvereinbarung
2.1.3	Sollte: Ein Konzept zur Sensibilisierung und Schulung der Mitarbeiter ist erstellt.	Schulungs- und Sensibilisierungsprogramm
2.1.4	Die Anforderungen an mobiles Arbeiten sind ermittelt und erfüllt.	Richtlinie zum mobilen Arbeiten (Abgleich mit der Richtlinie Informationsklassifizierung)
3.1.1	Ein Sicherungszentrum ist einschließlich der zugehörigen Schutzmaßnahmen basierend auf den Anforderungen an den Umgang mit Informationswerten ist vorhanden.	Zutrittsrichtlinie ggf. kombiniert mit einer Clean-Desk-Richtlinie
3.1.3	Die Anforderungen an den Umgang mit Informationsträgern (Erstellung, Aufbewahrung, Reparatur, Verlust, Rückgabe, Entsorgung) sind ermittelt und erfüllt.	Richtlinie Umgang mit Informationsträgern (Entsorgungsrichtlinie)

Sie möchten sich über dieses und weitere Tools

informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Dokumentierte Information, die explizit verfügbar sein muss bzw. sollte

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
3.1.4	Die Anforderungen an mobile IT-Geräte und mobile Endgeräte sind ermittelt und erfüllt.	Typischerweise Gegenstand anderer Richtlinien/Verfahren: <ul style="list-style-type: none"> • Mobile Endgeräte • Kryptografie • Identifizierung • Schulung
4.1.2	Die Auswahl der Verfahren zur Benutzerauthentifizierung wurde auf Basis einer Risikoanalyse getroffen.	Verfahren zur Nutzer-authentifizierung
4.1.3	Der Zugang zu Informationen und IT-Systemen erfolgt über validierte Benutzerkonten, welche einer Person zugeordnet sind.	Richtlinie über die Bereitstellung von Benutzerzugängen zu IT-Systemen (Kennwortrichtlinie)
4.2.1	Die Anforderungen an das Management von Zugriffsrechten (Autorisierung) sind ermittelt und erfüllt.	Richtlinie Zugriffsmanagement
5.1.1	Sollte: Ein Nutzungskonzept für Kryptografie ist definiert und umgesetzt.	Verfahren Kryptografie
5.1.2	Richtlinien und Verfahren entsprechen den massgebenden Vorgaben zur Nutzung von Netzwerkdiensten sind definiert und umgesetzt.	Verknüpfung mit der Richtlinie Informationsklassifizierung
5.2.1	Ein formales Genehmigungsverfahren ist etabliert. Änderungen werden bezüglich möglicher Auswirkungen auf die Informationssicherheit verifiziert und bewertet.	Richtlinie Änderungsmanagement
6.1	Neu oder erweiterte Softwareentwicklung: Die Anforderungen an Entwicklungs- und Testumgebungen sind ermittelt und umgesetzt.	Entwicklungsrichtlinie

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Dokumentierte Information, die explizit verfügbar sein muss bzw. sollte

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
5.2.3	Anforderungen an den Schutz vor Schadsoftware sind ermittelt. Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt.	Richtlinie zum Schutz vor Schadsoftware
5.2.5	Ein angemessenes Patch-Management ist definiert und umgesetzt (z.B. Prüfung und Installation von Patches).	Richtlinie zum Patch-Management
5.2.7	Prozesse zur Verwaltung und Steuerung von Netzwerken sind ermittelt und erfüllt.	Netzwerkplan

5.2.8	Kritische IT-Dienste werden identifiziert, und die geschäftlichen Auswirkungen werden betrachtet. Anforderungen und Verantwortlichkeiten für die Kontinuität und Wiederherstellung dieser IT-Dienste sind den maßgeblichen Beteiligten bekannt und werden erfüllt.	Verknüpfung mit anderen Richtlinien: <ul style="list-style-type: none"> • Verfahren Risikomanagement IT • Verfahren Notfallbetriebsverfahren (Notfallplan) • Richtlinie Informationsklassifizierung
-------	--	--

Sie möchten sich über dieses und weitere Tools

informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

5.2.9	Für jeden maßgeblichen IT-Dienst ist ein Sicherungs- und Wiederherstellungs-Konzept vorhanden.	Richtlinie zur Datensicherung
5.3.1	Die Anforderungen an die Informationssicherheit bei der Planung und Entwicklung von IT-Systemen sind ermittelt und werden berücksichtigt.	IT-Beschaffungsrichtlinie. Verknüpfung mit der Richtlinie Änderungsmanagement
5.3.2	Anforderungen an die Informationssicherheit von Netzwerkdiensten sind ermittelt und erfüllt.	Netzwerksicherheitsrichtlinie

Dokumentierte Information, die explizit verfügbar sein muss bzw. sollte

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
5.3.3, 5.3.4	Ein Verfahren zur Rückgabe und sicheren Entfernung von Informationswerten aus jedem organisationsfremden IT-Dienst ist definiert und umgesetzt. Eine wirksame Trennung (z. B. physische, logische oder virtuelle) muss unbefugten Nutzern anderer Organisationen auf die eigenen Informationen zugegriffen wird.	IT-Cloud-Anbietergespräch mit Regelungen zur Rückgabe und Löschung von Daten
6.1.1	Mit Auftragnehmern und Lieferanten, wenn ein Vertrag durch vertragliche Vereinbarungen ein angemessenes Informationssicherheitsniveau sichergestellt.	Vertrag mit Regelungen zur Vergabe von Unteraufträgen durch den IT-Dienstleister
7.1.1	Gesetzliche, regulatorische und vertragliche Bestimmungen mit Relevanz für die Informationssicherheit (siehe Beispiele) werden in regelmäßigen Abständen ermittelt.	Verfahren zur Erfassung von Anforderungen (Rechtskataster, Anforderungen interessierter Parteien)
7.1.2	Gesetzliche und vertragliche Anforderungen an die Informationssicherheit bezüglich der Verfahren und der Prozesse bei der Verarbeitung von personenbezogenen Daten sind ermittelt.	Verfahren zur Verarbeitung personenbezogener Daten

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:
Registrieren und downloaden!

Dokumentierte Information, die explizit aufbewahrt werden müssen

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
1.2.1	Festlegung des Scopes des ISMS • Assets und Daten • Prüfziele • Standards • Externe Prozesse (IT-Dienstleister) • Enabler (Werkzeuge)	Geltungsbereich
1.2.1	Das ISMS stellt der Organisationsleitung geeignete Kontroll- und Steuerungen unter zur Verfügung (z.B. Management-Review).	Entscheidungsprotokolle (Managementbewertung)
	Informationen und andere Assets, deren Sicherheit für die Organisation relevant ist,	Asset-Inventar
	sind identifiziert und erfasst.	
1.3.3	Es werden keine organisationsfremden IT-Dienste ohne explizite Bewertung und Umsetzung von Sicherheitsanforderungen eingesetzt.	Liste (Bewertung) der freigegebenen IT-Dienste (Bezug zur zentralen Richtlinie)
1.4.1	Informationssicherheitsrisiken sind dokumentiert.	Siehe Verfahren Risikomanagement IT
1.5.1	Die Einhaltung von Anforderungen der Informationssicherheit (z.B. technische Vorgaben) werden in regelmäßigen Abständen überprüft.	Auditprogramm, System- bzw. Dienstaudit, Lieferantenaudits, Auditberichte
5.2.6	Die Ergebnisse der durchgeführten Überprüfung werden in geeigneter Weise dokumentiert und aufbewahrt.	
1.5.2	Überprüfungen der Informationssicherheit werden von einer unabhängigen und sachkundigen Stelle in regelmäßigen Abständen und bei wesentlichen Änderungen durchgeführt.	Externe Audits durch einen Prüfdienstleister
1.6.2	Sobald Sicherheitsereignisse gemeldet werden, ist es erforderlich, ihr Umgang mit den Ereignissen zu verwalten.	Gemeldete Ereignisse und deren Bearbeitung

Sie möchten sich über dieses und weitere Tools informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Dokumentierte Information, die explizit aufbewahrt werden müssen

Ihr Vorteil als Know-NOW User:

- Freie Nutzung kostenloser Tools und Experten-Links
- Einrichtung und Nutzung eines Prepay-Kontos
- Einsparungen durch attraktive Bonusprogramme

Kostenlos und unverbindlich registrieren unter

www.know-now.de/join

Abschnitt	Umfang bzw. Inhalte	Hinweis
2.1.1	Nachweise zur Identität von potenziellen Mitarbeitern (z.B. Prüfungszeugnisse, von Ausweisdokumenten).	Zuordnung im Organigramm, Checkliste Personal
2.1.2	Bereits bei der Erstellung von Mitarbeitermustern muss sichergestellt werden, dass sich Mitarbeiter zur Einhaltung der Richtlinien verpflichten und ihnen die Folgen eines Fehlverhaltens bewusst sind.	Geheimhaltung vereinbarung
2.1.3	Nachweise, dass die Beschäftigten geschult und sensibilisiert sind.	Teilnahmebescheinigungen, Screenshot, ...
4.1.1	Nachweise beim Umgang mit Identifikationsmitteln: <ul style="list-style-type: none"> • Erstellung, Übergabe, Rückgabe und Vernichtung • Gültigkeitszeiträume • Rückverfolgbarkeit • Umgang mit Verlust. 	Ggf. Bestandteil der zentralen Richtlinie bzw. der Zutrittsrichtlinie
4.1.2	Dauerhafte Zugriffsüberwachung hinsichtlich Unregelmäßigkeiten. Hinweis: Datenschutz beachten.	Monitoring (Log-Files)
5.2.4	Sicherheitsrelevante Anforderungen an die Protokollierung der Aktivitäten von Systemadministratoren und Nutzern sind ermittelt und erfüllt. Hinweis: Datenschutz beachten.	Ereignisprotokolle (Log-Files)
6.1.1	Auftragnehmer und Kooperationspartner werden einer (Risiko-)Bewertung bezüglich der Informationsrelevanz unterzogen. Serviceberichte und Dokumente von Auftragnehmern und Kooperationspartnern werden übergeben.	Lieferantenbewertung, Lieferantenselbstauskunft (Zertifikate ISO 27001) Verknüpfung mit 1.3.3).
6.1.2	Vor der Weitergabe von sensiblen Informationen an Dienstleister sind gültige Geheimhaltungsvereinbarungen abgeschlossen.	Geheimhaltungsvereinbarung

Sie möchten sich über dieses und weitere Tools

informieren?

... nutzen Sie unseren Tool-Online-Shop:

Registrieren und downloaden!

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

- (1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
- (2) Für Garantien haftet der Lizenzgeber unbeschränkt.
- (3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
- (4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
- (5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
- (6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
- (7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
- (8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.

Hinweis auf geschützte Abschnitte bei Nutzung als Formular:

Das Dokument ist abschnittsbezogen als Formular geschützt, sodass Sie z.B. die Kontrollkästen oder Dropdown-Felder (im Sinne eines Formulars) am PC direkt anwählen und ausfüllen können. Es ist kein Kennwort festgelegt.

Schutz entfernen in MS Office 2003:

Symbolleiste „Formular“ aktivieren und auf das „Schloss-Symbol“ klicken.

Schutz entfernen in MS Office 2010:

In der Symbolleiste „Überprüfen“ das Symbol „Bearbeitung einschränken“ aktivieren. Daraufhin öffnet sich das Fenster „Formatierung und Bearbeitung“. In diesem Fenster rechts unten auf die Schaltfläche „Schutz aufheben“ klicken.

Wollen Sie die integrierte Funktionalität nicht nutzen, können Sie die Felder aus der Tabelle einfach entfernen.