TISAX® Assessment Bericht

Erstprüfung

Optware GmbH

S4PW1Y

ATVXTM-1

10.08.2022

Version 1.0

Anfangsbemerkungen

Dieser Bericht und die zugrundeliegende Prüfung wurde von entsprechend qualifizierten Prüfern eines für den Trusted Information Security Assessment Exchange (TISAX) freigegebenen Prüfdienstleisters erstellt. Hierbei wird die Wirksamkeit der Steuerungsprozesse und deren derzeitige Umsetzung auf Basis der in den TISAX „Audit Criteria and Assessment Requirements“ (ACAR), wie zum Zeitpunkt der Berichtserstellung von ENX veröffentlicht, spezifizierten Vorgehensweise eingeschätzt.

TISAX wird von der ENX Association betrieben und verantwortet. TISAX dient allgemein anerkannten, von vertrauenswürdigen und im Wettbewerb stehenden Prüfdienstleistern auf Basis des ISA Prüfkataloges durchgeführten Prüfungen. Detaillierte Informationen zu TISAX finden sich auf http://www.enx.com/tisax/.

Dieser Assessment Report ist zur ausschließlichen Nutzung innerhalb von TISAX bestimmt. Eine Weiterleitung der TISAX Assessment Ergebnisse oder die Kommunikation ihrer Inhalte muss entsprechend den in den anwendbaren TISAX Vereinbarungen und Richtlinien für TISAX Teilnehmer bzw. TISAX Prüfdienstleister für eine Kommunikation entsprechender Inhalte festgelegten Vorgaben erfolgen.

Eine Kommunikation der TISAX Assessment Ergebnisse außerhalb der definierten TISAX Verfahren für einen Austausch entsprechender Informationen sowie jeglicher Austausch entsprechender Informationen mit Dritten außerhalb von TISAX ist nicht zulässig. Es wird darauf hingewiesen, dass bestimmte, sich aus dem anwendbaren TISAX Rechtsrahmen ergebende Rechte ggf. nicht bestehen, wenn die Kommunikation der TISAX Assessment Ergebnisse nicht entsprechend den TISAX Richtlinien erfolgt.

Auch wenn die diesem Bericht zugrundeliegende Prüfung mit aller gebotenen Sorgfalt durchgeführt wurde, handelt es sich lediglich um eine Momentaufnahme auf Basis einer stichprobenhaften Prüfung. Diese ist grundsätzlich nicht geeignet, alle Schwachstellen der geprüften Prozesse und Verfahren zu identifizieren.

Zudem geben TISAX Assessment Ergebnisse ausschließlich eine Aussage zum Zeitpunkt der Bewertung. Jegliche möglichen Änderungen nach dem Prüfungszeitraum wurden nicht bei der Bewertung berücksichtigt. Es wird ausdrücklich darauf hingewiesen, dass bei einer Projektion der Ergebnisse auf einen späteren Zeitpunkt inhärent die Gefahr besteht, dass die in diesem Bericht beschriebenen Ergebnisse durch geänderte Voraussetzungen oder über die Zeit nachlassende Umsetzung der Richtlinien, Prozesse und Verfahrensweisen an Aussagekraft verlieren können.

Struktur des Berichts

Dieser Bericht ist wie folgt aufgebaut:

A. Informationen zum Assessment (Assessment Related Information)
B. Gesamtübersicht Prüfergebnisse (Summarized Results)
C. Zusammenfassung der Ergebnisse des Assessments (Assessment Result Summary)
D. Reifegrade gem. ISA (Ergebnis-Tab des ISA) (Maturity Levels of ISA (Result Tab))
E. Detaillierte Ergebnisse zum Assessment (Detailed Assessment Results)

Die Struktur und die Überschriften entsprechen den möglichen Freigabestufen von Prüfergebnissen für andere TISAX Teilnehmer, die englischen Originalnamen werden aus Gründen der Transparenz in Klammern genannt.

Der Bericht beginnt mit allgemeinen Informationen über die Bewertung (A. Informationen zum Assessment). In den nächsten Abschnitten wird der Detailgrad von abstrakten Gesamtbewertungen (B. Gesamtübersicht Prüfergebnisse und C. Zusammenfassung der Ergebnisse des Assessments) bis hin zu den Einzelfeststellungen (D. Reifegrade gemäß ISA und E. Detaillierte Ergebnisse zum Assessment) kontinuierlich gesteigert.

A. Informationen zum Assessment (Assessment Related Information)

A.1 Prüfscope

TISAX® Scope-ID	S4PW1Y
Scope-Typ	☒ Standard Scope 2.0 *Der TISAX Scope definiert den Umfang der Prüfung. Die Prüfung umfasst alle Prozesse, Verfahren und beteiligte Ressourcen, die unter der Verantwortung der zu prüfenden Organisation stehen und die für die Sicherheit der in den genannten Prüfzielen definierten Schutzobjekte und deren Schutzziele an den aufgeführten Standorten relevant sind.* *Die Bewertung wird mindestens im höchsten Assessment-Level durchgeführt, das in einem der aufgeführten Prüfungsziele gefordert ist. Alle in den aufgelisteten Prüfungszielen geforderten Kriterien sind Gegenstand der Beurteilung.* ☐ Erweiterter benutzerdefinierter Scope ☐ Vollständig benutzerdefinierter Scope
Prüfziele	☒ **Umgang mit Informationen von hohem Schutzbedarf** ☐ Umgang mit Informationen von sehr hohem Schutzbedarf ☐ Umgang mit schutzbedürftigen Prototypenkomponenten/-bauteilen ☐ Umgang mit schutzbedürftigen Prototypenfahrzeugen ☐ Nutzung von Erprobungsfahrzeugen ☐ Events und Bildaufnahmen mit schutzbedürftigen Objekten ☒ **Umgang mit personenbezogenen Daten gemäß Artikel 28 DSGVO (Auftragsverarbeiter)** ☐ Umgang mit besonderen Kategorien (Artikel 9 DSGVO) personenbezogener Daten gemäß Artikel 28 DSGVO (Auftragsverarbeiter)
Prüfanforderungen	ACAR – TISAX Specification of Assessment Version 2.1: Family-ID: ISA, Version 5.0

A.2 Geprüfte Standorte

Firmenname	Anschrift	Location-ID	Ansprechpartner
Optware GmbH	Prüfeninger Straße 20 93049 Regensburg Deutschland	LV4LTL	Martin Scherf martin.scherf@optware.de

Der Auditor bestätigt, dass alle oben genannten Informationen auf ihre Richtigkeit hin überprüft wurden.

A.3 Erstprüfung

TISAX® Assessment-ID	ATVXTM-1
Assessment Level	AL2
Prüfmethode	☒ Plausibilisierung der Selbstauskunft auf der Grundlage von bereitgestellten Dokumenten und anderen Nachweisen ☒ Detaillierte Überprüfung der Nachweise ☒ Interviews mit prozessbeteiligten Personen ☐ Vor-Ort-Prüfung ☐ Videobasierte Standortprüfung (Remote)
Datum Kick-Off Meeting	28.06.2022
Datum Opening Meeting	10.08.2022
Datum Closing Meeting (Stichtag Gültigkeit)	10.08.2022
Zustimmung des Geprüften	Der Geprüfte ☒ stimmt der sachlichen Korrektheit der Feststellungen zu. ☐ stimmt den Feststellungen mit Einschränkungen zu (Anmerkungen wurden in den Berichtstext aufgenommen und sind als solche gekennzeichnet).

Autoren

Auditor
Thomas Quietmeyer
Qualitätssicherung
Sandra Nowak

Köln, 17.08.2022

B. Gesamtübersicht Prüfergebnisse (Summarized Results)

B.1 Erstprüfung

AL2: Basierend auf der Erstprüfung ist die Gesamtbewertung des Scopes:

☒ **Konform**

☐ Nebenabweichend

☐ Hauptabweichend

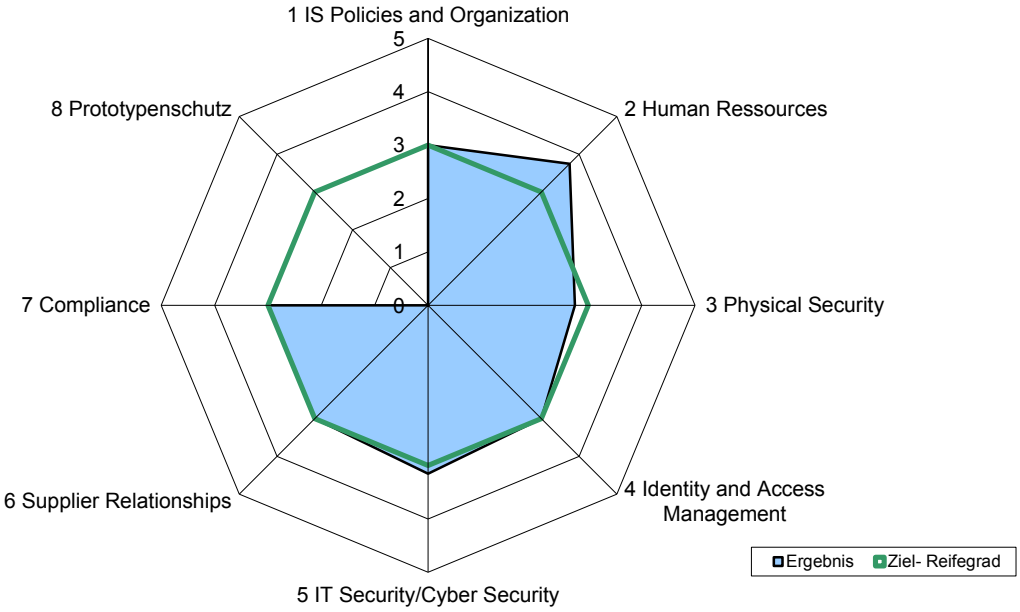
Es wurden keine Hauptabweichungen und keine Nebenabweichungen zu den geprüften Anforderungen identifiziert.

Nach der Erstprüfung errechnet sich ein durchschnittlicher Gesamtreifegrad von **2,95**.

C. Zusammenfassung der Ergebnisse des Assessments (Assessment Result Summary)

C.1 Erstprüfung

Die einzelnen Bereiche des Reifegradniveaus werden wie folgt im Spinnennetzdiagramm dargestellt. Der ermittelte Reifegrad beträgt dabei **2,95** von 3.0.



Für die einzelnen Bereiche ergeben sich die folgenden Haupt- (HA)- und Nebenabweichungen (NA):

Lfd. Nr.	Bereich	Anzahl Controls mit Hauptabweichungen	Anzahl Controls mit Nebenabweichungen
1	IS Policies and Organization	0	0
2	Human Ressources	0	0
3	Physical Security and Business Continuity	0	0
4	Identity and Access Management	0	0
5	IT Security / Cyber Security	0	0
6	Supplier Relationships	0	0
7	Compliance	0	0

D. Reifegrade gem. ISA (Ergebnis-Tab des ISA) (Maturity Levels of ISA)

D.1 ISMS

Basierend auf dem aktuellen Stand der Umsetzung ergeben sich für die einzelnen Prüfpunkte aus dem Bereich ISMS die nachfolgenden Reifegrade:

Nr.	Thema	Ziel- Reifegrad	Ergebnis
1	***IS Policies and Organization***		
1.1	***Information Security Policies***		
1.1.1	Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?	3	**2**
1.2	***Organization of Information Security***		
1.2.1	Inwieweit wird in der Organisation Informationssicherheit gemanagt?	3	**3**
1.2.2	Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?	3	**3**
1.2.3	Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?	3	**3**
1.2.4	Inwieweit sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert?	3	**3**
1.3	***Asset Management***		
1.3.1	Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?	3	**3**
1.3.2	Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?	3	**3**
1.3.3	Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?	3	**3**
1.4	***IS Risk Management***		
1.4.1	Inwieweit werden Informationssicherheitsrisiken gemanagt?	3	**4**
1.5	***Assessments***		
1.5.1	Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?	3	**3**
1.5.2	Inwieweit wird das ISMS von einer unabhängigen Instanz überprüft?	3	**3**
1.6	***Incident Management***		

Nr.	Thema	Ziel- Reifegrad	Ergebnis
1.6.1	Inwieweit werden Informationssicherheitsereignisse verarbeitet?	3	**3**
2	***Human Ressources***		
2.1.1	Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?	3	**4**
2.1.2	Inwieweit werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet?	3	**4**
2.1.3	Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert?	3	**4**
2.1.4	Inwieweit ist mobiles Arbeiten geregelt?	3	**3**
3	***Physical Security and Business Continuity***		
3.1.1	Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?	3	**2**
3.1.2	Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt?	3	**2**
3.1.3	Inwieweit ist der Umgang mit Informationsträgern gemanagt?	3	**3**
3.1.4	Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?	3	**3**
4	***Identity and Access Management***		
4.1	***Identity Management***		
4.1.1	Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt?	3	**3**
4.1.2	Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?	3	**3**
4.1.3	Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?	3	**3**
4.2	***Access Management***		
4.2.1	Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?	3	**3**
5	***IT Security / Cyber Security***		
5.1	***Cryptography***		
5.1.1	Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?	3	**3**

Nr.	Thema	Ziel- Reifegrad	Ergebnis
5.1.2	Inwieweit werden Informationen während der Übertragung geschützt?	3	**3**
5.2	***Operations Security***		
5.2.1	Inwieweit werden Änderungen gesteuert?	3	**3**
5.2.2	Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?	3	**3**
5.2.3	Inwieweit werden IT-Systeme vor Schadsoftware geschützt?	3	**4**
5.2.4	Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?	3	**3**
5.2.5	Inwieweit werden Schwachstellen erkannt und behandelt?	3	**3**
5.2.6	Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)?	3	**3**
5.2.7	Inwieweit wird das Netzwerk der Organisation gemanagt?	3	**3**
5.3	***System acquisitions, requirement management and development***		
5.3.1	Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?	3	**3**
5.3.2	Inwieweit sind Anforderungen an Netzwerkdienste definiert?	3	**4**
5.3.3	Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus Organisationsfremden IT-Diensten geregelt?	3	**3**
5.3.4	Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?	3	**3**
6	***Supplier Relationships***		
6.1.1	Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?	3	**3**
6.1.2	Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?	3	**3**
7	***Compliance***		
7.1.1	Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?	3	**3**
7.1.2	Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?	3	**3**