

## Checkliste zur TISAX® Umsetzung

### basierend auf VDA-ISA Information Security Assessment

Bitte füllen Sie den nachfolgenden Fragebogen aus - auf Basis Ihrer Antworten werden wir uns in einem persönlichen Gespräch detailliert mit Ihnen austauschen und ein für Ihr Unternehmen passendes Angebot erstellen.

|     | <b>Erforderliche Pflichtdokumente</b>   | <b>Abschnitte gemäß VDA-ISA</b> | <b>Vorhanden?</b> | <b>Wenn „ja“ – Ablageort<br/>Wenn „nein“ – warum nicht?</b> |
|-----|---|---------------------------------|-------------------|---|
| 1.  | Ist der <b>Anwendungsbereich des ISMS</b> definiert und dokumentiert?   | 1.1                             |                   |   |
| 2.  | Ist die <b>Leitlinie zur Informationssicherheit</b> abgestimmt und dokumentiert?  | 1.1                             |                   |   |
| 3.  | Sind die <b>Informationssicherheitsziele</b> festgelegt und dokumentiert?   | 1.1                             |                   |   |
| 4.  | Ist die <b>Risikobewertungs- und Risikobehandlungsmethodik</b> definiert?   | 1.2                             |                   |   |
| 5.  | Ist ein <b>Risikobehandlungsplan</b> formuliert und dokumentiert? Sind die <b>Ergebnisse der Risikobehandlung</b> dokumentiert?         | 1.2                             |                   |   |
| 6.  | Ist ein <b>Risikobewertungsbericht</b> vorhanden?   | 1.2                             |                   |   |
| 7.  | Wurden die <b>Überwachungs- und Messergebnisse</b> ausgewertet?   | 1.3                             |                   |   |
| 8.  | Sind die <b>Ergebnisse aus Managementbewertungen</b> vorhanden?   | 1.3                             |                   |   |
| 9.  | Sind die <b>Sicherheits-Rollen und Verantwortlichkeiten</b> definiert?  | 6.1                             |                   |   |
| 10. | Ist eine <b>Selbsteinschätzung</b> gemäß VDA-ISA vorhanden?   | 6.1.3 d)                        |                   |   |
| 11. | Sind die <b>Aufzeichnungen über Schulungen, Fähigkeiten, Erfahrung und Qualifikationen</b> der Mitarbeiter vorhanden?                   | 7.2                             |                   |   |
| 12. | Ist ein <b>Verzeichnis der Informationen</b> vorhanden?   | 8.1                             |                   |   |
| 13. | Sind Regeln zum <b>Umgang mit Informationen</b> definiert?  | 8.1                             |                   |   |
| 14. | Ist eine <b>Richtlinie für die Zugriffskontrolle</b> dokumentiert und kommuniziert?   | 9.1                             |                   |   |
| 15. | Sind <b>Richtlinien für einen sicheren IT-Betrieb</b> (Change Management, Backup, Schutz vor Schadsoftware, Patchmanagement) vorhanden? | 12.1, 12.3, 12.4, 12.7          |                   |   |
| 16. | Ist eine <b>Richtlinie für die Verwendung von kryptographischen Algorithmen</b> vorhanden?  | 10.1                            |                   |   |
| 17. | Werden <b>Logdateien</b> erstellt, aufbewahrt und regelmäßig ausgewertet?   | 12.5, 12.6                      |                   |   |

|     | <b>Erforderliche Pflichtdokumente</b>   | <b>Abschnitte gemäß VDA-ISA</b> | <b>Vorhanden?</b> | <b>Wenn „ja“ – Ablageort<br/>Wenn „nein“ – warum nicht?</b> |
|-----|---|---------------------------------|-------------------|---|
| 18. | Sind Anforderungen zur Einhaltung der <b>Vertraulichkeit und Geheimhaltung mit Kunden und Lieferanten</b> vereinbart? | 13.5                            |                   |   |
| 19. | Sind <b>Prinzipien zum sicheren Betrieb der IT-Systeme</b> festgelegt?  | 14.2                            |                   |   |
| 20. | Gibt es eine Richtlinie für <b>Lieferantenbeziehungen</b> und wurde diese kommuniziert, implementiert und überwacht?  | 15.1, 15.2                      |                   |   |
| 21. | Ist ein Verfahren zum <b>Umgang mit Sicherheitsvorfällen</b> definiert, implementiert und kommuniziert?               | 16.1                            |                   |   |
| 22. | Ist die <b>Informationssicherheit</b> ein wesentlicher Bestandteil des Business Continuity Management?                | 17.1                            |                   |   |
| 23. | Sind alle <b>gesetzlichen, behördlichen und vertraglichen Anforderungen erfasst</b> und erfüllt? (inkl. Datenschutz)  | 18.1                            |                   |   |
| 24. | Sind die sieben verpflichtenden <b>Key Performance Indikatoren (KPIs)</b> definiert?                                  | KPI                             |                   |   |

*TISAX® ist eine eingetragene Marke der ENX Association*

Anmerkung: Die OPTIMAbit GmbH bietet nur Informationen zur Umsetzung des VDA Information Security Assessment und ist kein Zertifizierer gemäß TISAX®.

Haben Sie noch Fragen? - Wir helfen Ihnen gerne weiter und freuen uns gemeinsam mit Ihnen auf die Umsetzung!

*Ihr OPTIMAbit-Expertenteam*