



ISA 2027: Das Modul „Informationssicherheit“

Eine Betrachtung der Änderungen auf Control-Ebene

ISA 2027 bringt eine neue Versionsbezeichnung (Jahreszahl vs. Punkt-Version) sowie ein vereinfachtes Modul zum Prototypenschutz. Für Organisationen, die ihr Informationssicherheits-Management-System (ISMS) im Einklang mit TISAX® betreiben, sind jedoch die Änderungen innerhalb des Moduls **Informationssicherheit** von besonderer Bedeutung.

Nachfolgend werden die überarbeiteten Controls einzeln betrachtet. Der überwiegende Teil der insgesamt 43 Anpassungen dient der sprachlichen Präzisierung und besseren Verständlichkeit. Eine kleinere Anzahl beinhaltet jedoch inhaltliche Änderungen – darunter mehrere Anforderungen, die von einer Empfehlung („should“) zu einer verbindlichen Anforderung („must“) verschärft wurden. Diese Controls sollten im Hinblick auf das nächste TISAX® Assessment besonders sorgfältig bewertet werden.

Hinweis: Die nachfolgenden Informationen basieren auf den derzeit öffentlich verfügbaren Informationen zu ISA 2027. Die ACAR-Dokumente (Assessment Criteria and Audit Requirements), welche die Durchführung von TISAX® Assessments für Prüfdienstleister regeln, lagen zum Zeitpunkt der Veröffentlichung noch nicht vor.

Richtlinien, Rollen und Informationswerte

1.1.1 – Inwieweit sind Informationssicherheitsrichtlinien verfügbar?

Informationssicherheitsrichtlinien müssen künftig verfügbar sein und wirksam kommuniziert werden. Damit wird verdeutlicht, dass nicht allein die Existenz einer Richtlinie nachzuweisen ist, sondern auch deren Bekanntgabe an alle relevanten interessierten Parteien. Insbesondere Änderungen an Richtlinien müssen nachvollziehbar kommuniziert werden.

1.2.2 – Inwieweit sind Verantwortlichkeiten für die Informationssicherheit organisiert?

Verantwortlichkeiten müssen definiert, zugewiesen und mit den erforderlichen Befugnissen ausgestattet werden. Damit wird klargestellt, dass die bloße formale Benennung von Rollen nicht ausreicht. Rolleninhaber müssen über die notwendige Kompetenz und Entscheidungsbefugnis verfügen, um ihre Aufgaben wirksam wahrnehmen und durchsetzen zu können.

1.3.1 – Inwieweit werden Informationswerte identifiziert und erfasst?

Informationswerte müssen identifiziert, klassifiziert und einem Verantwortlichen (Asset Owner) zugeordnet werden. Gegenüber der bisherigen Version wird die Bedeutung einer nachvollziehbaren Klassifizierung sowie einer eindeutig geregelten Eigentümerschaft stärker hervorgehoben.

Behandlung von Sicherheitsvorfällen und Krisenmanagement

1.6.2 – Inwieweit werden gemeldete Sicherheitsereignisse behandelt?

Für Sicherheitsereignisse müssen Eskalationskriterien sowie verbindliche Reaktions- bzw. Eskalationsfristen festgelegt werden. Dadurch wird präzisiert, unter welchen Bedingungen eine Eskalation zu erfolgen hat und innerhalb welcher Zeit diese umzusetzen ist.

1.6.3 – Inwieweit ist die Organisation auf Krisensituationen vorbereitet?

Ein Krisenmanagementplan muss erstellt, umgesetzt und regelmäßig validiert bzw. getestet werden. Der Fokus liegt damit stärker auf der nachweisbaren Wirksamkeit des Krisenmanagements und nicht ausschließlich auf dessen Dokumentation.

Personal und Asset Management

2.1.4 – Inwieweit ist mobiles Arbeiten geregelt?

Der Begriff „Teleworking“ wurde durch „Mobile Work“ ersetzt. Diese Änderung dient ausschließlich der sprachlichen Modernisierung und hat keine inhaltlichen Auswirkungen auf die Anforderungen.

4.2.1 – Inwieweit werden Berechtigungen vergeben und verwaltet?

Berechtigungen müssen vergeben, regelmäßig überprüft und entzogen werden. Dadurch wird der vollständige Lebenszyklus des Berechtigungsmanagements ausdrücklich berücksichtigt und die kontinuierliche Überprüfung bestehender Berechtigungen stärker betont.

IT- und Cybersicherheit

5.2.4 – Inwieweit werden Ereignisprotokolle aufgezeichnet und ausgewertet?

Die Protokollierung muss künftig auch Remote-Sitzungen sowie Verstöße gegen Sicherheitsrichtlinien umfassen. Die Nachvollziehbarkeit administrativer Fernzugriffe wird dadurch verbessert. In der praktischen Umsetzung bleibt jedoch zu bewerten, welche Richtlinienverstöße technisch zuverlässig erkannt und protokolliert werden können.

5.2.6 – Inwieweit werden IT-Systeme und IT-Services technisch überprüft (System- und Service-Audit)?

Identifizierte Schwachstellen müssen innerhalb definierter Fristen behandelt bzw. behoben werden. Die reine Identifikation von Schwachstellen genügt künftig nicht mehr; vielmehr wird ein dokumentierter Schwachstellenmanagementprozess einschließlich verbindlicher Remediation-Zeiträume erwartet.

5.2.8 – Inwieweit besteht eine Kontinuitätsplanung für IT-Services?

Die Kontinuitätsplanung muss künftig konkrete Bedrohungsszenarien, beispielsweise Ransomware-, DDoS- oder vergleichbare Cyberangriffe, explizit berücksichtigen. Dadurch sollen Wiederanlauf- und Wiederherstellungsmaßnahmen an den jeweiligen Szenarien ausgerichtet werden, anstatt ausschließlich generische Notfallkonzepte vorzuhalten.

5.2.9 – Inwieweit sind Datensicherung und Wiederherstellung von Daten und IT-Services sichergestellt?

Für Backup- und Recovery-Prozesse müssen Sicherungsverfahren, Wiederherstellungsprozesse, Wiederherstellungsreihenfolge sowie die Isolation von Sicherungen definiert werden. Der Schwerpunkt liegt verstärkt auf der tatsächlichen Wiederherstellbarkeit, der Berücksichtigung von Abhängigkeiten zwischen Systemen sowie auf dem Schutz der Datensicherungen selbst, beispielsweise vor Manipulation oder Verschlüsselung.

Lieferantenbeziehungen

6.1.1 – Inwieweit wird Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?

Anforderungen an die Informationssicherheit müssen festgelegt, überwacht und regelmäßig überprüft (auditiert) werden. Da sich das Risikoprofil eines Lieferanten im Zeitverlauf verändern kann, gewinnen wiederkehrende Bewertungen und Audits zunehmend an Bedeutung, um die Einhaltung der Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit dauerhaft nachzuweisen.

Im Rahmen unserer Quality Reviews beobachten wir regelmäßig, dass Organisationen die Anforderungen von TISAX® nicht konsequent auf ihre Lieferkette übertragen. Kritische Lieferanten, deren Leistungen für die Verfügbarkeit eigener Produkte oder Dienstleistungen wesentlich sind, sollten ein entsprechendes Sicherheitsniveau nachweisen. Gleiches gilt für Lieferanten, denen vertrauliche Informationen bereitgestellt werden.

6.1.3 (vormals 1.2.4) – Inwieweit sind die Verantwortlichkeiten zwischen externen IT-Service-Providern und der Organisation geregelt?

Dieses Control wurde in das Kapitel Supplier Relationships verschoben. Gleichzeitig wurde der Begriff „IT Suppliers“ durch „IT Service Providers“ ersetzt und damit der Geltungsbereich präzisiert. Er umfasst nun ausdrücklich sämtliche extern bereitgestellten IT- und OT-Services, einschließlich Cloud-Services, SaaS-Angeboten sowie webbasierter Dienste.

Die überarbeitete Formulierung verdeutlicht außerdem, dass externe IT-Service-Provider vertraglich – beispielsweise über Service Level Agreements (SLAs) oder eine Supplier Statement of Applicability (SoA) – zur Einhaltung definierter Informationssicherheitsanforderungen verpflichtet werden können. Die Verantwortung für interne Regelungen zum sicheren Umgang mit Informationen verbleibt jedoch bei der Organisation.

Compliance

7.1.2 – Inwieweit wird der Schutz personenbezogener Daten bei der Umsetzung der Informationssicherheit berücksichtigt?

Neben dem in den ISO-Normen etablierten Begriff „Personally Identifiable Information (PII)“ verwendet ISA 2027 nun auch den allgemein verständlicheren Begriff „personenbezogene Daten“. Damit erfolgt eine sprachliche Harmonisierung mit rechtlichen Regelwerken wie der Datenschutz-Grundverordnung (DSGVO), ohne den fachlichen Bezug zu den etablierten ISO-Normen aufzugeben.

Weiterhin bestehendes Verbesserungspotenzial: Berücksichtigung von OT

Aus Sicht der DQS besteht weiterhin Optimierungspotenzial hinsichtlich der Berücksichtigung von Operational Technology (OT). Nach den Definitionen des ISA-Katalogs umfasst der Begriff IT-System sämtliche Systeme zur elektronischen Informationsverarbeitung und schließt damit ausdrücklich auch OT-Komponenten wie Switches, Kameras, Sensoren oder industrielle Steuerungssysteme ein. In der Praxis wird dieser Geltungsbereich häufig zu eng interpretiert. Controls mit Bezug auf IT-Systeme – insbesondere solche, die sich an IEC 62443-2-1 orientieren – gelten grundsätzlich sowohl für klassische IT- als auch für OT-Umgebungen.

Bereits mit dem ISA Katalog 6.0 war dies fachlich zutreffend. Aus unserer Sicht hätte ISA 2027 diesen Aspekt jedoch deutlicher hervorheben können. Sofern IT- und OT-Umgebungen organisatorisch getrennt betrieben oder unterschiedlich abgesichert werden, empfiehlt es sich, diese auch in der Selbstbewertung getrennt zu beschreiben.

Auswirkungen auf die Praxis

Die Änderungen erfordern grundsätzlich keine grundlegende Neuausrichtung des Informationssicherheits-Managementsystems (ISMS). Vor dem nächsten TISAX® Assessment sollte jedoch insbesondere geprüft werden, ob...

- ✓ Informationssicherheitsrichtlinien nachweislich kommuniziert werden,
- ✓ Rollen und Verantwortlichkeiten mit angemessenen Befugnissen ausgestattet sind,
- ✓ Informationswerte vollständig klassifiziert und Verantwortlichen zugeordnet wurden,
- ✓ Eskalationskriterien und Reaktionszeiten für Sicherheitsvorfälle definiert sind,
- ✓ Krisenmanagementpläne regelmäßig getestet werden,
- ✓ Berechtigungen regelmäßig rezertifiziert und zeitnah entzogen werden,
- ✓ verbindliche Fristen für die Behandlung von Schwachstellen festgelegt wurden,
- ✓ Kontinuitäts- und Wiederherstellungsplanungen konkrete Cyberangriffsszenarien berücksichtigen,
- ✓ Lieferanten regelmäßig hinsichtlich der Informationssicherheitsanforderungen überwacht und auditiert werden,
- ✓ OT-Systeme im Scope des ISMS und der TISAX®-Selbstbewertung angemessen berücksichtigt werden.

Wer einen Gesamtüberblick über sämtliche Änderungen des ISA Katalogs 2027 – einschließlich der Vereinfachung des Prototypenschutzes und des neuen jährlichen Veröffentlichungszyklus – erhalten möchte, findet weitere Informationen in unserem Fachbeitrag „**ISA 2027: Was sich im neuen TISAX®-Katalog ändert**“.



Diese Information basiert auf den zum Zeitpunkt der Veröffentlichung öffentlich verfügbaren Informationen zu ISA 2027. ENX und VDA können im Zuge der Veröffentlichung der finalen Dokumente weitere Klarstellungen zum Übergangsprozess oder zu einzelnen Anforderungen vornehmen.