MRIS for TISAX® 2027

Mythos-resistente Informationssicherheit — Analyse des TISAX®-Fragenkatalogs ISA 2027, Modul "Information Security"

Teil I: Analyse und Lückenbewertung. Der Implementation Guide (Teil II) liegt als eigenständige Folgepublikation vor.

Version 1.1 | Juli 2026

Ersteller: Richard Peddi

Lizenz und Hinweise

Unabhängigkeitshinweis

TISAX® ist eine eingetragene Marke der ENX Association; die ENX Association administriert TISAX® im Auftrag des Verbands der Automobilindustrie (VDA), der den zugrunde liegenden Fragenkatalog (VDA ISA) entwickelt und veröffentlicht. Diese Analyse ist eine unabhängige, privat erstellte Arbeit ohne Verbindung zu ENX Association oder VDA. Sie ist weder Bestandteil des offiziellen TISAX®-Prüfprozesses noch von ENX autorisiert, geprüft oder bestätigt, und ersetzt keine TISAX®-Reifegradbewertung durch einen akkreditierten Prüfdienstleister.

Haftungsausschluss

Die Einstufungen in diesem Dokument sind eine fachliche Einschätzung zum Stand Juli 2026, keine Rechts- oder Zertifizierungsauskunft. Die Anwendung erfolgt ohne Gewähr und in eigener Verantwortung.

Zitierempfehlung

Peddi, Richard (2026): MRIS for TISAX® 2027 — Teil I: Analyse und Lückenbewertung. v1.1

Änderungshistorie

Version	Datum	Beschreibung
1.0	Juni/Juli 2026	Erstveröffentlichung.
1.1	Juli 2026	Überarbeitung auf Basis eines extern beauftragten Prüfberichts (Juli 2026, 9 Feststellungen F-01–F-09).

Version 1.1 im Einzelnen:

Feststellung	Thema	Umsetzung
F-01	Inkonsistente Zählarithmetik und Kapitelsummen	Gesamtzahl 324 → 330 korrigiert (Kapitelsummen: 116/21/14/37/105/31/6; Methodik geschärft: nur wortgleiche Katalog-Duplikate zählen als redaktionell entfernt); Control 1.6.3 anhand der Primärquelle (ISA2027-EN.xlsx) neu bewertet (Tabelle 15 → 19 Zeilen, Gesamteinstufung "5 von 15" → "7 von 19" Teilweise degradiert); Control 5.2.8 "3 von 14" → "3 von 15"; Einzelbefund-Gesamtzahl 72 → 74 (Kaskade durch Management Summary, Cluster-Übersicht, Prioritäten-Tabelle, Musterbildungs-Kapitel sowie Teil II)
F-02	Charakterisierungs- und Zitiergenauigkeit	Zitat zu Control 5.2.5 korrigiert
F-03	Asymmetrische Quellenlage	vier Detailbehauptungen erneut recherchiert (Cogent-Studie, NIST AI Agent Standards Initiative, BSI C5:2026 OPS-25.01AC, Mythos-Benchmarkzahlen); Quellenapparat um Primärquellen ergänzt; unbestätigte BSI-Detailwerte von der bestätigten Rahmenaussage getrennt (Fußnote 2; analog in Teil II, MHC-09)
F-04	Editorische Dokumentensteuerung	diese Änderungshistorie eingeführt; Datumsangaben auf Juli 2026 vereinheitlicht; Versionsvermerk ergänzt (Titelblatt und Zitierempfehlung); verwaister Verweis "(Phase 5, siehe Aufgabenliste)" korrigiert
F-05	Fehlende Wirtschaftlichkeitsbetrachtung	betrifft Teil II (siehe dort)
F-06	KMU-Eignung einzelner Zielwerte	betrifft Teil II (siehe dort)
F-07	Fehlendes Evidence-Mapping zum Katalog	betrifft Teil II (siehe dort)
F-08	Erwartungsmanage	kein Dokumentmangel (Anwendungshinweis); keine

Feststellung	Thema	Umsetzung
	ment TISAX-Label und Reifegrade	Textänderung
F-09	Bedrohungsmodell -Abhängigkeit der Argumentation	kein Dokumentmangel (Anwendungshinweis); keine Textänderung

Vorwort

Mit MRIS (Mythos-resistente Informationssicherheit) habe ich zuvor eine Methodik entwickelt, um bestehende ISMS-Regelwerke gezielt auf ihre Widerstandsfähigkeit gegenüber KI-beschleunigten Angreifern zu prüfen — benannt nach Claude Mythos, dem KI-Modell, dessen Veröffentlichung im April 2026 diese Bedrohungsverschiebung erstmals konkret und öffentlich dokumentierte (siehe "Zum Namen 'Mythos'"). MRIS-TISAX® 2027 überträgt diese Prüflogik auf den TISAX®-Fragenkatalog ISA 2027 — als eigenständige Arbeit, nicht als Ableitung einer bestehenden MRIS-Fassung: Die Bedrohungsgrundlage wird direkt aus Primärquellen hergeleitet (siehe Methodik).

Der Anspruch dieses Dokuments ist bewusst begrenzt: Es bewertet den Wortlaut von 330 TISAX®-Anforderungen einzeln gegen ein definiertes Bedrohungsmodell und ordnet die Befunde zu wiederkehrenden Mustern. Es ist eine Diagnose. Welche konkreten Zusatzmaßnahmen daraus folgen, ist Gegenstand der separaten Folgepublikation (Implementation Guide, MHC). Rückmeldungen, Widerspruch und Ergänzungen sind ausdrücklich willkommen — die CC-BY-NC-Lizenz ist auch als Einladung gemeint, diese Analyse zu prüfen, zu widerlegen oder weiterzuentwickeln.

Richard Peddi
Juli 2026

Inhaltsverzeichnis

Management Summary

MRIS-TISAX® 2027 prüft die 45 Controls des Moduls "Information Security" im TISAX®-Fragenkatalog ISA 2027 einzeln gegen ein aus vier dokumentierten Bedrohungsverschiebungen abgeleitetes Kriterienraster (Angreifergeduld, Zeitkompression, Fähigkeitsentkopplung, Aggregationsresistenz). Bewertet wird der Anforderungswortlaut, nicht die Umsetzung bei einer konkreten Organisation. Der Katalog umfasst im Rohtext 331 "+"-markierte Anforderungen (321 nach Schutzbedarf gestaffelt plus 10 für Simplified Group Assessments); bewertet werden 330 distinkte Anforderungen, da Control 1.6.3 im Quellkatalog eine wortgleich doppelt vorkommende Anforderung enthält (vier weitere, textlich ähnliche Anforderungspaare in Control 1.6.3 sind redaktionelle Abweichungen im Quellkatalog selbst, keine echten Dubletten, und werden als eigenständige Anforderungen gezählt; siehe Datenqualitäts-Hinweis, Methodik). Prototype Protection und Data Protection sind nicht Teil dieser Analyse.

Auf einen Blick

Kennzahl	Wert
Bewertete Controls	45
Distinkte Anforderungen	330
Standfest	4 Controls (9 %)
Teilweise degradiert	26 Controls (58 %)
Reine Reibung	1 Control (2 %)*
Nicht betroffen	14 Controls (31 %)
Wiederkehrende Musterkategorien (Phase 2)	8 Cluster, 74 Einzelbefunde
Vergleichsrahmen (Phase 3)[2]	NIST CSF 2.0, BSI C5:2026, DORA, CRA, NIS2-RL/DVO, ISA/IEC 62443-2-1
Originäre Erweiterung (Teil II, jenseits TISAX®)[3]	KI-Agenten-/GenAI-Sicherheit: MHC-13 (erweitert) + MHC-16 decken 8 von 10 OWASP-ASI-Bedrohungskategorien ab — TISAX® selbst regelt hier nur zwei Anforderungen (1.3.3, 1.3.4)

*Betrifft ausschließlich den reinen Passwortfaktor ohne zweiten Faktor (4.1.2, eine von sieben Anforderungen). Klassische MFA-Verfahren (OTP/Push) desselben Controls sind Teilweise degradiert — geschwächt, aber nicht wirkungslos; siehe Kapitel 4.

[2] Diese sechs Rahmenwerke sind die in Phase 3 gegen den TISAX®-Anforderungswortlaut verglichenen Compliance-/Regulierungsrahmen. Die OWASP Top 10 for Agentic Applications (nächste Zeile) ist kein Vergleichsrahmen in diesem Sinn, sondern eine Bedrohungstaxonomie, gegen die ausschließlich die originäre KI-Agenten-Erweiterung in Teil II geprüft wurde — beides nicht vermischen.

[3] Nicht aus der TISAX®-Diagnose abgeleitet, sondern fachliches Urteil des Autors auf Basis externer Bedrohungsforschung (primär OWASP); durchgängig als originär gekennzeichnet. Siehe Abschnitt "Originäre Ergänzungen jenseits von TISAX®".

Kernbefunde: Der TISAX®-Anforderungskatalog kollabiert nicht gegen einen Gen-AI-gestützten Angreifer, degradiert aber in der Mehrheit der Controls: 58 % verlieren einen Teil ihrer Schutzwirkung, meist weil Formulierungen wie "regelmäßig" oder "angemessen" keinen anlassbezogenen oder zeitlich gebundenen Reaktionsmechanismus vorschreiben. Nur ein einziger Control (4.1.2, reine Passwort-Authentisierung ohne zweiten Faktor) verliert seine Kernwirkung vollständig. Der Standfest-Anteil ist mit 9 % gering und konzentriert sich fast ausschließlich auf Kapitel 5, wo TISAX® konkrete technische Mechanismen statt organisatorischer Prozesse verlangt.

Die 74 betroffenen Einzelanforderungen bilden acht wiederkehrende Muster, angeführt von periodischer statt anlassbezogener Prüfung (19 Funde über vier Kapitel). Die Lückenanalyse gegen sechs externe Vergleichsrahmen zeigt: die meisten dieser Muster sind bereits an anderer Stelle in der Regulierung adressiert — etwa CVSS-gebundene Patch-Fristen in BSI C5:2026 oder MFA bzw. Continuous Authentication, das NIS2 Art. 21(2)(j) ausdrücklich als geeignete Maßnahme im risikobasierten Maßnahmenkatalog benennt — und lassen sich für die geplante Härtungscontrols-Synthese entsprechend übernehmen. Eine Ausnahme: Fähigkeitsentkopplung durch autonom handelnde KI-Agenten, die eigenständig externe Dienste oder Softwarepakete einbinden, wird von keinem der sechs Vergleichsrahmen bislang geregelt — selbst NIST hat hierzu erst im Februar 2026 eine eigene Standardisierungsinitiative gestartet.

Teil II reagiert darauf mit einer bewussten, klar gekennzeichneten Ausnahme von der sonst durchgängig TISAX®-abgeleiteten Methodik: Ein erweitertes MHC-13 und ein neues MHC-16 adressieren KI-Agenten-/GenAI-Sicherheit — Agenten-Identität, Prompt Injection, Kill-Switch, Multi-Agent-Integrität — und decken, gegen die OWASP Top 10 for Agentic Applications geprüft, 8 von 10 dort definierten Bedrohungskategorien ab; TISAX® ISA 2027 selbst berührt dieses Feld nur an zwei Anforderungen (1.3.3, 1.3.4). Begründet ist die Erweiterung mit der Aktualität der Bedrohung: KI-Agenten sind im heutigen Einsatzumfeld bereits produktiv und angreifbar, nicht erst Gegenstand eines künftigen TISAX®-Release. Siehe Abschnitt "Originäre Ergänzungen jenseits von TISAX®" für die vollständige Kennzeichnung, welche Teile TISAX®-abgeleitet und welche originär sind.

Zum Namen "Mythos"

Der Name ist keine freie Erfindung. Claude Mythos Preview ist ein reales, am 7. April 2026 von Anthropic veröffentlichtes KI-Modell — in Anthropics eigener Beschreibung (Frontier Red Team, Lead-Autor Nicholas Carlini) ein "general-purpose language model that is strikingly capable at computer security tasks". Seine Existenz wurde bereits im März 2026 durch ein versehentlich veröffentlichtes Blogpost-Entwurfsleck bekannt; Anthropic bestätigte danach gegenüber Fortune, das Modell stelle einen "step change in capabilities" mit erheblichem Cybersicherheitsrisiko dar. Anthropic selbst nennt Mythos "in a different league" gegenüber dem Vorgängermodell Opus 4.6: in einem Firefox-147-Exploit-Benchmark gelangen Opus 4.6 zwei erfolgreiche Versuche in mehreren hundert Anläufen, Mythos erzielte 181 funktionierende Exploits plus Registerkontrolle bei 29 weiteren; in einem internen OSS-Fuzz-Benchmark erreichten Opus 4.6 und Sonnet 4.6 bestenfalls einen Tier-3-Crash, Mythos erzielte 595 Tier-1/2-Crashes und vollständige Kontrollfluss-Übernahme (Tier 5) bei 10 vollständig gepatchten Zielsystemen — darunter ein 27 Jahre alter, inzwischen gepatchter OpenBSD-Bug, ein 16 Jahre alter FFmpeg-Fehler und eine autonom, ohne menschliche Hilfe entwickelte FreeBSD-NFS-Remote-Code-Execution (CVE-2026-4747). Die New York Times bezeichnete die Offenlegung als "cybersecurity reckoning".

Anthropic veröffentlichte das Modell ausdrücklich nicht öffentlich — "we do not plan to make Claude Mythos Preview generally available" — sondern gewährte Zugriff ausschließlich über "Project Glasswing" an ausgewählte Industriepartner und Open-Source-Entwickler (u. a. Microsoft, Apple, AWS, Cisco, Nvidia; über 40 Unternehmen), "to enable defenders to begin securing the most important systems before models with similar capabilities become broadly available". Die eigene Risikoeinschätzung war unverblümt: "In the short term, this could be attackers, if frontier labs aren't careful about how they release these models." In den folgenden Wochen bestätigten unabhängige Funde die Tragweite außerhalb der ursprünglichen Anthropic-Veröffentlichung: rund zwei Wochen nach der Freigabe meldete Mozilla 271 mit Mythos gefundene und behobene Sicherheitslücken in Firefox, am 14. Mai 2026 meldeten Mitarbeitende von Calif.io einen mit Mythos erstellten Speicherkorruptions-Exploit für den Apple M5.

Innerhalb weniger Tage lösten Offenlegung und gemeldete Fälle unautorisierten Zugriffs weltweit Krisenreaktionen aus: US-Finanzministerium und Fed warnten Banken direkt, Zentralbanken in Kanada, Großbritannien, Indien, Japan und Australien beriefen Notfalltreffen ein, ein US-Kongressschreiben forderte eine Überarbeitung der föderalen Cybersicherheitspolitik, China wurde der Zugang verweigert. Im Juni 2026 eskalierte die Lage weiter: nach einem gemeldeten Jailbreak, der Mythos 5 potenziell in ein "unrestricted cyber tool" verwandelte, ordnete das US-Handelsministerium unter Howard Lutnick eine weltweite Sperrung des Zugangs für alle ausländischen Staatsangehörigen an — ein in dieser Form beispielloser Eingriff, der Ende Juni nach Verhandlungen mit Anthropic teilweise wieder aufgehoben wurde.

Genau dieses Ausmaß begründet die Namenswahl: eine einzelne Modell-Enthüllung, die binnen Tagen Zentralbanken, Regierungen und einen 40-köpfigen Industriekonsortium-Zugang

gleichzeitig auf den Plan rief, gefolgt von einer weltweiten Exportkontrolle nach einem realen Jailbreak-Vorfall — das ist der Moment, in dem das bis dahin abstrakte Risiko KI-beschleunigter Angriffe erstmals konkret, öffentlich belegt und in einem Ausmaß eintrat, das zuvor niemand erwartet hatte. "Mythos" steht damit nicht für eine Metapher, sondern für ein datiertes, dokumentiertes Ereignis.

Wichtig für die Methodik: Der Name verankert diese Analyse an einem festen historischen Zeitpunkt — er ist kein Bekenntnis, dass die vier Bedrohungsverschiebungen (siehe Methodik) von den Fähigkeiten des Mythos-Modells selbst abhängen. Die eigentliche Beweisgrundlage der Methodik sind vier unabhängig voneinander dokumentierte Vorfälle (Cogent-CVE-Auswertung, GTG-1002-Kampagne, JadePuffer-Ransomware — siehe Methodik), nicht Mythos-spezifische Benchmark-Ergebnisse. "Mythos-Angreifer" ist im weiteren Dokument eine sprachliche Abkürzung für "Angreifer mit den vier belegten, generationsunabhängigen Fähigkeiten", nicht ein Verweis auf ein bestimmtes Produkt. Sollte Mythos in einigen Jahren technisch überholt oder vom Markt genommen sein, bleibt die Methodik gültig, solange die zugrunde liegenden Fähigkeiten — automatisierte Exploit-Entwicklung, autonome mehrstufige Angriffsausführung, fragmentierte Angriffsmuster, entkoppelte Angreiferfähigkeit — bei irgendeinem verfügbaren System bestehen bleiben oder sich weiterentwickeln. Der Name ist ein historischer Marker für den Erkenntnisstand Juli 2026, keine methodische Abhängigkeit von einem einzelnen Anbieter oder Modell.

Quellen:

- Claude Mythos Preview — Anthropic (Primärquelle)
- Frontier Red Team: Claude Mythos Preview — Anthropic (Primärbericht mit Benchmark-Details zu Exploit- und Crash-Zahlen)
- The zero-days are numbered — The Mozilla Blog (Primärquelle zu den 271 in Firefox gefundenen und behobenen Schwachstellen)
- First public kernel memory corruption exploit found by an AI agent — Calif.io (Primärquelle zum Apple-M5-Exploit)
- Anthropic Claims Its New A.I. Model, Mythos, Is a Cybersecurity 'Reckoning' — The New York Times
- Anthropic Teams Up With Its Rivals to Keep AI From Hacking Everything — Wired
- Anthropic acknowledges testing new AI model representing 'step change' in capabilities — Fortune
- Anthropic Model Scare Sparks Urgent Bessent, Powell Warning to Bank CEOs — Bloomberg
- Anthropic Disabled Fable 5 And Mythos 5 After A U.S. Export-Control Order — Forbes
- White House drops export controls on Anthropic's Mythos and Fable AI models — The Washington Post

Methodik

Was diese Analyse ist — und was nicht

Diese Analyse ist eine **Wirksamkeits-Zusatzschicht über der TISAX®-Reifegradprüfung, kein Ersatz dafür.** Ein Control kann im Audit Reifegrad 3 ("Established", der TISAX®-Zielwert) erreichen und trotzdem in dieser Analyse als "Teilweise degradiert" eingestuft sein — beides schließt sich nicht aus. Reifegrad misst, ob ein Prozess dokumentiert, eingeführt und gelebt wird. Diese Analyse misst etwas anderes: ob der Schutzmechanismus, den die Anforderung verlangt, einem Gen-AI-beschleunigten Angreifer noch standhält. **Definitionskonvention dieser Analyse:** "Standfest" wird hier bewusst an den TISAX®-Zielreifegrad 3 gekoppelt — das ist eine methodische Festlegung von MRIS-TISAX® 2027, keine Aussage des TISAX®-Kataloges selbst. Nach dieser Konvention gilt eine Anforderung als "Standfest", wenn sie Reifegrad 3 auch unter Mythos-Bedingungen ohne Zusatzmaßnahme trägt — nicht nur "wirkt irgendwie noch".
Bewertet wird **der Wortlaut der Anforderung**, nicht die tatsächliche Umsetzung bei einer konkreten Organisation. "Standfest" heißt: korrekt umgesetzt, hält diese Anforderung stand. Ob eine bestimmte Organisation sie tatsächlich korrekt umgesetzt hat, beantwortet nur ein Audit vor Ort — dafür bleibt die reguläre TISAX®-Prüfung mit Reifegrad und Nachweisen (GWP) zuständig.
Grenze dieser Analyse: Anforderungen werden einzeln, nicht als Angriffskette bewertet. Eine "Standfest"-Einstufung gilt für den bewerteten Mechanismus isoliert, nicht für das Gesamtsystem. Eine standfeste Verschlüsselung (5.1.1) nützt wenig, wenn der davorliegende Zugriff über eine degradierte Authentisierung (4.1.2) erfolgt — die Kombination mehrerer Controls entlang einer realistischen Angriffskette wird hier nicht bewertet. Das ist Aufgabe der geplanten Musterbildung (Phase 2), die Einzelbefunde entlang wiederkehrender Angriffsmuster clustert.
Anteilsangaben sind eine Zählung, kein Risikoscore. "3 von 9 Anforderungen betroffen" heißt: drei von neun Textstellen sind geschwächt — nicht, dass der Control zu einem Drittel riskant ist. Eine einzelne kritische Lücke (z. B. fehlende Phishing-Resistenz bei der Authentisierung) kann schwerer wiegen als fünf administrative Einzelbefunde in einem anderen Control. Eine risikogewichtete Priorisierung liefert nicht diese Zählung, sondern die spätere Lückenanalyse (Phase 2/3).
Was diese Analyse (noch) nicht liefert: eine Priorisierung der Befunde nach Dringlichkeit/Aufwand, und eine Zuordnung zu konkreten Nachweistypen. Diese konkrete Verbesserungs-/Ergänzungsebene — was an einer Anforderung geändert werden muss, damit sie wieder standhält — liefert bewusst nicht dieses Kapitel, sondern die spätere Härtungscontrols-Synthese (Phase 4) mit anschließender Verknüpfung zurück in die Kapitel 1–7 (Phase 5). Die hier vergebenen Kategorien sind die Diagnose; die MHC-Synthese ist die Verschreibung.
Was diese Analyse nicht bewertet (Scope-Abgrenzung): MRIS-TISAX® 2027 ist eine Wirksamkeitsdiagnose auf Anforderungsebene. Ausdrücklich außerhalb des Scopes:

- **Wirtschaftlichkeit:** keine Kosten-Nutzen-Abwägung einzelner Härtungsmaßnahmen — ob sich eine Maßnahme finanziell rechnet, entscheidet die Organisation.
- **Organisationsspezifisches Risiko:** keine Risikoanalyse für eine konkrete Organisation (Schutzbedarf, Asset-Kritikalität, Eintrittswahrscheinlichkeit) — dafür bleibt das organisationseigene ISMS-Risikomanagement zuständig.
- **Threat Intelligence:** keine Bewertung konkreter Angreifergruppen, Kampagnen oder Zielbranchen — das Bedrohungsmodell unten beschreibt Fähigkeiten, nicht Akteure.
- **Eintrittswahrscheinlichkeit:** keine Aussage darüber, wie wahrscheinlich ein bestimmter Angriff eine bestimmte Organisation trifft.
- **Quantitative Risikoberechnung:** keine Erwartungswerte, Value-at-Risk oder vergleichbare Kennzahlen. Die vergebenen Kategorien sind ordinal (Rangfolge), nicht metrisch, und auch der in Teil II verwendete Threat Priority Score ist ein Priorisierungsindex, kein Risikoscore (siehe Teil II, Abschnitt "Bewertungslogik").

Diese Fragen beantwortet die organisationseigene Risikoanalyse; MRIS liefert dafür die Diagnose auf Anforderungsebene als Eingangsgröße, nicht das fertige Ergebnis.

Controls vs. tatsächliche Sicherheit: MRIS bewertet TISAX®-Anforderungen als Text, nicht die tatsächliche Sicherheitslage einer Organisation. Die Kategorie "Standfest" bedeutet, dass der geforderte Mechanismus bei korrekter Umsetzung hält — nicht, dass eine bestimmte Organisation sicher ist. Umgekehrt bedeutet "Teilweise degradiert" nicht, dass ein konkreter Vorfall bevorsteht, sondern dass die im Anforderungswortlaut verankerte Schutzannahme nachgeschärft werden sollte. Die Kategorien sind ein Priorisierungswerkzeug für Anforderungsverbesserungen, kein Sicherheits- oder Reifegrad-Ersatz für die Organisation als Ganzes.

Grundlage: vier Bedrohungsverschiebungen und vier Bewertungskriterien

MRIS-TISAX® 2027 ist eine eigenständige Analyse. Sie hat mit einer etwaigen MRIS-Ausarbeitung für ISO 27002 formal nichts gemeinsam außer dem Ziel, ein bestehendes ISMS wirksam und effizient gegen Gen-AI-gestützte Bedrohungen zu härten. Das Bedrohungsmodell wird deshalb direkt aus öffentlich dokumentierten Vorfällen und Forschungsberichten 2025/2026 abgeleitet, nicht aus einem übergeordneten Rahmenwerk übernommen. Vier Verschiebungen sind so belegt:

1. **Kollaps des Patch-Gap-Fensters:** Eine 2026 veröffentlichte Auswertung von 69'159 CVE durch Cogent Security zeigt, dass sich die durchschnittliche Zeit von Schwachstellen-Veröffentlichung bis zum ersten funktionierenden Exploit von 125,3 Tagen (Januar 2025) auf 0,5 Tage (April 2026) verkürzt hat; bei 62 % der kritischen Schwachstellen mit bekanntem Exploit existierte dieser bereits vor der Scanner-Erkennungssignatur.
2. **Kompression der Reaktions-Zeitachse:** Anthropic deckte im September 2025 eine staatlich gesteuerte Kampagne (GTG-1002) auf, bei der ein gekapertes KI-Agentensystem 80–90 % der Angriffsschritte gegen rund 30 Zielorganisationen autonom und mit tausenden Anfragen pro Sekunde ausführte — ein Tempo ohne menschlich besetztes Gegenstück.
3. **Fragmentierung des Bedrohungsereignisses:** Dieselbe Kampagne führte zunächst eine unauffällige, "low-and-slow" angelegte Aufklärung innerhalb normaler Nutzungsmuster durch,

bevor die restlichen Schritte im Maschinentempo folgten — ein Muster, das eine auf menschliche Korrelation einzelner Auffälligkeiten ausgelegte Erkennung nicht zusammenhängend erfasst.

4. **Entkopplung Fähigkeit/Akteur:** Der Sicherheitsanbieter Sysdig dokumentierte 2026 unter dem Namen "JadePuffer" die erste vollständig durch einen KI-Agenten autonom ausgeführte Ransomware-Kampagne. Über eine ungepatchte Schwachstelle in der Open-Source-Plattform Langflow (CVE-2025-3248, CVSS 9.8) drang der Agent ein, bewegte sich eigenständig lateral, erbeutete Zugangsdaten mehrerer KI- und Cloud-Anbieter, eskalierte Rechte und verschlüsselte 1'342 Datenbank-/Konfigurationselemente über mehr als 600 selbstständig ausgeführte Schadprogramm-Varianten — eine Kill-Chain, die bislang ein eingespieltes, mehrköpfiges Angreiferteam mit Spezialwissen in Erstzugriff, lateraler Bewegung und Ransomware-Betrieb voraussetzte. Bezeichnend ist der Ausgang: der Agent vergaß, den erzeugten Schlüssel zu sichern, und übernahm für die Lösegeldforderung eine Bitcoin-Adresse aus seinen eigenen Trainingsdaten — selbst zahlungswillige Opfer hätten ihre Daten nicht zurückerhalten. Der eigentliche Wendepunkt liegt genau darin: trotz dieses Anfängerfehlers gelang die komplette technische Angriffskette bis zur flächendeckenden Verschlüsselung. Die Fähigkeit, die bislang ein erfahrenes Angreiferteam voraussetzte, ist vom Akteur bereits heute entkoppelt — fehlerhaft ausgeführt, aber wirksam, nicht erst in einer zukünftigen ausgereiften Version.

Diese vier Fälle markieren zusammen den Wendepunkt, der Härtungsmaßnahmen erst notwendig macht: keiner der vier beschreibt mehr nur ein theoretisches Risiko oder eine graduelle Verschärfung bestehender Bedrohungen. Alle vier sind bereits eingetretene, dokumentierte Ereignisse, in denen ein KI-System eine Aufgabe vollständig oder größtenteils ohne die bislang dafür nötige menschliche Fachkompetenz, Reaktionszeit oder Auffälligkeit erledigt hat. Ein Sicherheitskonzept, das stillschweigend weiter auf menschliche Grenzen beim Angreifer setzt, bewertet damit eine Bedrohungslage, die es in dieser Form nicht mehr gibt.
Aus diesen vier Verschiebungen leiten sich vier Bewertungskriterien ab, mit denen jede TISAX®-Anforderung geprüft wird:

- **Angreifergeduld:** Beruht die Schutzwirkung darauf, dass ein Angriff für den Angreifer zu aufwändig oder mühsam ist?
- **Zeitkompression:** Setzt das Control eine menschliche Reaktionszeit voraus, obwohl der Angreifer die Attacke inzwischen automatisiert und selbstständig durchführt? **Abgrenzung:** Nicht "periodisch" an sich ist die Schwäche, sondern **periodisch ohne dokumentierte Triggerlogik und ohne risikobasierte Ereignissteuerung.** Eine "periodische Überprüfung" gilt nur dann als Zeitkompressions-Schwäche, wenn (1) der überprüfte Gegenstand ein technisch-operatives Sicherheitselement ist, dessen Veralten ein ausnutzbares Zeitfenster öffnet (z. B. Software-Freigaben, Zugriffsrechte, Backup-Konzepte, Log-Auswertung, Lieferanten-Sicherheitsstatus), UND (2) der Anforderungswortlaut keinen ergänzenden Anlassbezug vorschreibt. Ergänzt eine Organisation eine periodische Prüfung um dokumentierte, risikobasierte Auslöser (z. B. sofortige Neubewertung bei neuer kritischer Schwachstelle), schließt das die Lücke faktisch — der Anforderungswortlaut selbst bleibt aber degradiert eingestuft, da er diesen Auslöser nicht verlangt. Reine Rechtslage-Scans (welche Gesetze/Verträge gelten) werden nicht so gewertet, da sich Gesetzgebung nicht im Tempo eines automatisierten Angriffs ändert.
- **Fähigkeitsentkopplung:** Beruht die Einschätzung "das kann kaum jemand" auf einem Erfahrungswert, der durch KI-Werkzeuge nicht mehr gilt?
- **Aggregationsresistenz:** Erkennt das Control einen Angriff auch dann, wenn er in viele einzelne, für sich harmlos wirkende Schritte zerlegt wird?

Warum genau vier Kriterien: Die vier Kriterien sind keine willkürlich gewählte Rasterbreite, sondern eine direkte Übersetzung der vier oben belegten Bedrohungsverschiebungen in prüfbare Fragen — Angreifergeduld übersetzt den Kollaps des Patch-Gap-Fensters, Zeitkompression übersetzt die Kompression der Reaktions-Zeitachse, Aggregationsresistenz übersetzt die Fragmentierung des Bedrohungsereignisses, Fähigkeitsentkopplung übersetzt die Entkopplung von Fähigkeit und Akteur. Jedes Kriterium wird unabhängig von den übrigen dreien geprüft; eine Anforderung kann gleichzeitig gegen mehrere Kriterien degradieren (siehe z. B. 4.1.2, wo sowohl Fähigkeitsentkopplung als auch Zeitkompression greifen — die Begründungsspalte nennt jeweils alle zutreffenden Kriterien). Die Vierzahl ist damit eine Konsequenz des Bedrohungsmodells, keine vorab gesetzte Kategorienzahl.
Reproduzierbarkeit: Jede Einstufung im Dokument folgt derselben Kette: Anforderungswortlaut → Abgleich gegen die vier Bedrohungsverschiebungen → Prüfung der vier Kriterien → Kategorie (Standfest/Teilweise degradiert/Reine Reibung/Nicht betroffen) → Einordnung in eines der acht Muster-Cluster (Phase 2) → MHC-Zuordnung (Phase 4, Teil II). Diese Kette ist je Anforderung in der Begründungsspalte offengelegt, nicht nur im Ergebnis.
Zeitbezug und Aktualität: MRIS-TISAX® 2027 bildet den Erkenntnisstand Juli 2026 ab — sowohl beim TISAX®-Anforderungswortlaut (ISA 2027) als auch beim zugrunde liegenden Bedrohungsmodell (siehe oben: Cogent-CVE-Auswertung, GTG-1002, JadePuffer, Mythos-Offenlegung). Beide Seiten können sich weiterentwickeln: TISAX® aktualisiert die ISA regelmäßig, und neue KI-Fähigkeiten können bestehende Einstufungen verschärfen oder auch entschärfen (etwa wenn phishing-resistente Authentisierung branchenweit zum Standard wird und eine heute degradierte Anforderung dadurch faktisch standfest wird). Diese Analyse ist entsprechend als Momentaufnahme zu lesen, nicht als einmalig gültiges Endergebnis — eine Neubewertung ist sinnvoll, sobald sich entweder der TISAX®-Katalog oder die belegte Angreiferfähigkeit wesentlich verschiebt.
Klassifikation jeder Anforderung, Lückenanalyse und Implementation Guide werden eigenständig für den TISAX®-Kontext erarbeitet.
Quellen:

- Cogent Research: Exploits Outpace Scanner Detection for 62% of Critical Vulnerabilities as AI Compresses Time-to-Exploit to Under 12 Hours
- Cogent Security: 2026 Q2 Detection Gap Report — Key Findings (Primärquelle)
- AI Shrinks Cyberattack Exploit Time From Years to Days — GovInfoSecurity
- Mapping AI-enabled cyber threats — Anthropic
- AI Agents Drive First Large-Scale Autonomous Cyberattack — Cybersecurity Magazine
- The agentic shift: how autonomous AI is reshaping the global threat landscape — Control Risks
- Jadepuffer: Die erste KI-Ransomware-Attacke verbaselt nicht nur den Schlüssel — heise online
- JadePuffer: The First Successful LLM-Driven Ransomware Attack — Dark Reading
- JadePuffer ransomware used AI agent to automate entire attack — BleepingComputer
- NIST: Announcing the AI Agent Standards Initiative for Interoperable and Secure AI Agents (Primärquelle)
- NIST: Summary and Analysis of Responses to the Request for Information Regarding Security Considerations for AI Agents (Primärquelle)

- BSI: Cloud Computing Compliance Criteria Catalogue C5:2026 (Primärdokument; PDF-Volltext im Rahmen dieser Recherche technisch nicht extrahierbar — siehe Fußnote 2, Abschnitt "Lückenanalyse gegenüber sechs Vergleichsrahmen")

Kategorien und ihre Praxisbedeutung

Kategorie	Bedeutung	Was Sie als CISO damit tun
Standfest	Die Sicherheitsannahme der Anforderung **kollabiert unter den vier Bewertungskriterien nicht** — nicht gleichbedeutend mit "ein Angriff ist unmöglich", sondern der Mechanismus beruht auf einer harten Barriere (Kryptografie, physische Trennung, Architektur), die auch unter Mythos-Bedingungen trägt. Erreicht damit den TISAX®-Zielreifegrad 3 ohne Zusatzmaßnahme.	Als Nachweis im Statement-of-Applicability-Äquivalent (ISA-Katalog-Reifegrad-Eintrag) zitierbar. Kein Zusatzaufwand aus Mythos-Sicht — normal weiter auditieren.
Teilweise degradiert	**Reduzierte, nicht fehlende Wirksamkeit** gegenüber der ursprünglichen Schutzannahme: der Mechanismus wirkt weiterhin, reicht aber nicht mehr aus, um Reifegrad 3 gegen einen Mythos-Angreifer wirksam zu halten.	Kandidat für den Risikobehandlungsplan. Braucht eine ergänzende Härtungsmaßnahme (Katalog folgt in Phase 4). **Hierhin gehört zusätzliches Budget und Aufmerksamkeit.**
Reine Reibung	Verliert die Kernwirkung gegenüber einem Mythos-Angreifer vollständig — die Schutzannahme der Anforderung trifft nicht mehr zu, unabhängig vom erreichten Reifegrad.	Muss ersetzt oder grundlegend umgestaltet werden — eine bloße Ergänzung genügt nicht.
Nicht betroffen	**Durch keines der vier Bewertungskriterien** (Angreifergeduld, Zeitkompression, Fähigkeitsentkopplung, Aggregationsresistenz) **beeinflusst** — keine Aussage darüber, ob die Anforderung allgemein "sicher" ist, sondern dass sie gegenüber dieser spezifischen Bedrohungsverschiebung unverändert bleibt (typischerweise Governance, Recht, Vertrag, reine Dokumentation).	Weiter im normalen ISMS-Betrieb prüfen und umsetzen, aber **bewusst nicht priorisieren**, wenn Sie Ressourcen für die Mythos-Reaktion verteilen. Kein Kompensationsbedarf.

Rangfolge bei gemischten Befunden innerhalb eines Controls: Reine Reibung > Teilweise degradiert > Standfest > Nicht betroffen. Enthält ein Control sowohl eine Reibungs- als auch mehrere Degradiert-Anforderungen, wird die Gesamteinstufung als "Reine Reibung" ausgewiesen — der schwächste Einzelbefund bestimmt das Gesamtbild, nicht der Durchschnitt.

Bewertungseinheit und Aufbau je Control

Jedes TISAX®-Control (z. B. 5.2.9) enthält mehrere mit "+" markierte **Einzelanforderungen**, gestaffelt nach Schutzbedarfsstufe: **must** und **should** gelten immer (normaler Schutzbedarf), **hoch** und **sehr hoch** kommen bei entsprechend höherem Schutzbedarf des betroffenen Assets zusätzlich hinzu — sie ersetzen must/should nicht, sondern ergänzen sie. Bewertet wird jede Einzelanforderung für sich, im englischen Originalwortlaut der Quelle (zitierfähig, durchsuchbar).

Sechs Controls in Kapitel 1 (1.1.1, 1.2.1, 1.2.2, 1.5.1, 1.5.2, 1.6.2) enthalten zusätzlich **SGA-Anforderungen** ("Additional requirements for Simplified Group Assessments"): sie gelten unabhängig vom Schutzbedarf, ausschließlich wenn die Organisation die vereinfachte TISAX®-Konzernbewertung (mehrere gleichartige Standorte gemeinsam) nutzt. In den Tabellen als eigene Ebene "SGA" gekennzeichnet und in must/should/hoch/sehr-hoch-Zählungen NICHT enthalten — die Anteilsangabe je Control weist SGA-Anforderungen separat aus.

Am Ende jedes Controls steht eine **Gesamteinstufung**: bei den meisten Controls ist sie über alle drei Schutzbedarfsstufen identisch und wird als ein Satz mit Anteilsangabe ("3 von 9 Anforderungen betroffen") zusammengefasst. Bei einigen wenigen Controls ändert sich das Bild mit steigendem Schutzbedarf — dort wird ausgeschrieben, welche zusätzliche Anforderung den Unterschied auslöst und was das für Sie praktisch bedeutet.

Verantwortlich-Spalte: bei degradierten/Reibungs-/standfesten Anforderungen zusätzlich angegeben, welche Funktion typischerweise zuständig ist (IT-Betrieb, CISO-Funktion/ISMS, Entwicklung/Engineering, IAM-Team, Einkauf/Lieferantenmanagement, Personalabteilung, Facility/Werkschutz). Eine Organisationszuordnung, kein verbindliches RACI — dient der ersten Einordnung, wer das Finding typischerweise bearbeitet.

Datenqualität: Control 1.6.3, Spalte "hoch", enthält im Quellkatalog fünf auffällig ähnliche Anforderungspaare. Gegen die ISA-2027-Originaltabelle geprüft ist davon genau ein Paar wortgleich (wird einmal gezählt); die übrigen vier weichen redaktionell voneinander ab (u. a. Tippfehler "outage of" vs. "outage oaf", Wortwahl "Methods" vs. "Instruments to monitor communication") und werden als eigenständige, distinkte Anforderungen gewertet (siehe Control 1.6.3 unten). Control 3.1.2 enthält keine eigenen Anforderungen ("Superseded by 1.6.3, 5.2.8 and 5.2.9").

Kapitel 1 — IS Policies and Organization (14 Controls, 116 distinkte Anforderungen inkl. 10 SGA-Anforderungen)

1.1.1 — To what extent are information security policies available?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The requirements for information security have been determined, documented and adapted to the organization's goals."	Nicht betroffen	Governance-Grundlage der Richtlinie, kein Angriffsbezug.	CISO-Funktion
must	"A policy exists, and is approved by the organization's management."	Nicht betroffen	Genehmigungsakt, keine Abwehrfunktion.	CISO-Funktion
must	"The policy includes objectives and the significance of information security within the organization."	Nicht betroffen	Inhaltliche Mindestanforderung an das Dokument selbst.	CISO-Funktion
must	"The policies are made available to employees in a suitable form (e.g., intranet)."	Nicht betroffen	Verteilungspflicht, kein Angriffsbezug.	CISO-Funktion
must	"Employees and external business partners are informed of any changes relevant to them."	Nicht betroffen	Kommunikationspflicht, kein Angriffsbezug.	CISO-Funktion
should	"The information security requirements are based on the strategy of the organization. Legislation and contracts are considered in the policy."	Nicht betroffen	Inhaltliche Ausrichtung der Richtlinie, keine technische Schutzwirkung.	CISO-Funktion
should	"The policy indicates consequences in case of non-conformance."	Nicht betroffen	Sanktionsklausel, organisatorisch.	CISO-Funktion
should	"Other relevant security	Nicht	Vollständigkeits-	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	policies are established."	betroffen	Anforderung an das Richtlinienwerk.	
should	"Periodic review and, if required, revision of the policies are established."	**Teilweise degradiert**	Zeitkompression: "periodisch" ohne konkreten Prüfanlass. Wenn neue Angriffsmuster sich innerhalb weniger Wochen zeigen, ein fester Prüfzyklus aber z. B. jährlich läuft, bleibt die Richtlinie zwischenzeitlich veraltet.	CISO-Funktion
SGA	"Policies are published and implemented in the entire assessment scope."	Nicht betroffen	Reichweiten-Anforderung für Konzernbewertungen (alle Standorte im Geltungsbereich), keine Abwehrfunktion.	CISO-Funktion

Gesamteinstufung: Teilweise degradiert (1 von 10 Anforderungen betroffen), unabhängig vom Schutzbedarf. Gilt bei Simplified Group Assessment zusätzlich für alle Standorte im Geltungsbereich.
Härtungsverweis: MHC-10 (siehe Teil II)

1.2.1 — To what extent is information security managed within the organization?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The scope of the ISMS (the organization managed by the ISMS) is defined."	Nicht betroffen	Geltungsbereichs-Festlegung, Governance.	CISO-Funktion
must	"The organization's requirements for the ISMS are determined."	Nicht betroffen	Governance.	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The organizational management has commissioned and approved the ISMS."	Nicht betroffen	Freigabeakt der Leitung.	CISO-Funktion
must	"The ISMS provides the organization's management with suitable monitoring and control means (e.g., management review)."	Nicht betroffen	Verlangt nur die Existenz eines Steuerungsinstruments, keine Frequenzangabe — die Frequenzfrage folgt separat.	CISO-Funktion
must	"Applicable controls have been determined (e.g., ISO 27001 Statement of Applicability, or completed ISA catalogue)."	Nicht betroffen	Scoping-Governance.	CISO-Funktion
must	"The effectiveness of the ISMS is regularly reviewed by the management."	**Teilweise degradiert**	Zeitkompression: ein jährlicher Management-Review-Rhythmus, wie in der Praxis üblich, reagiert strukturell zu langsam auf eine Bedrohungslage, die sich innerhalb von Wochen verändert.	CISO-Funktion
SGA	"The management system is approved by an entity that has the necessary authority for the entire assessment scope (i.e., all locations within the scope)."	Nicht betroffen	Freigabe-Governance für den konzernweiten Geltungsbereich.	CISO-Funktion

Gesamteinstufung: Teilweise degradiert (1 von 7 Anforderungen betroffen), unabhängig vom Schutzbedarf. Gilt bei Simplified Group Assessment zusätzlich für alle Standorte im Geltungsbereich.
Härtungsverweis: MHC-10 (siehe Teil II)

1.2.2 — To what extent are information security responsibilities organized?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Responsibilities for information security within the organization are defined, documented, and assigned."	Nicht betroffen	Governance.	CISO-Funktion
must	"The responsible employees are defined, qualified, and empowered for their task."	Nicht betroffen	Governance/Personal.	CISO-Funktion
must	"The required resources are available."	Nicht betroffen	Ressourcenzusage, keine Abwehrfunktion.	CISO-Funktion
must	"The contact persons are known within the organization and to relevant business partners."	Nicht betroffen	Bekanntheit von Ansprechpartnern, organisatorisch.	CISO-Funktion
should	"There is a definition and documentation of an adequate information security structure within the organization."	Nicht betroffen	Governance.	CISO-Funktion
should	"Security-relevant roles that are not part of the ISMS and are relevant for information security are considered."	Nicht betroffen	Scoping-Vollständigkeit; möglicher Anknüpfungspunkt für "Schatten-KI-Rollen" in Kapitel 4/5, hier noch keine hinreichend konkrete Textgrundlage für	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			eine andere Einstufung.	
hoch	"An appropriate organizational separation of responsibilities should be established in order to avoid conflict of interests (segregation of duties). (C, I, A)"	**Teilweise degradiert**	Fähigkeitsentkopplung: Rollentrennung schützt bislang, weil eine Person kaum zwei Fachrollen gleichzeitig beherrscht. Mit KI-Unterstützung kann eine einzelne Person die Aufgaben einer zweiten Rolle überzeugend mit erledigen, wenn die Trennung nur organisatorisch und nicht zusätzlich durch Systemrechte durchgesetzt wird.	IAM-Team
SGA	"A named person with overall responsibility for the management system exists and is available."	Nicht betroffen	Governance/Accountability, konzernweit.	CISO-Funktion

Gesamteinstufung: Bei normalem Schutzbedarf unauffällig (Nicht betroffen, 0 von 7 inkl. SGA) — kein Handlungsbedarf. Ab hohem Schutzbedarf kommt die Pflicht zur Aufgabentrennung hinzu, die ohne technische Durchsetzung eine Schwäche zeigt: Teilweise degradiert (1 von 8 Anforderungen betroffen). Die SGA-Anforderung gilt unabhängig vom Schutzbedarf zusätzlich und ändert daran nichts. Praktisch: betrifft Sie nur, wenn dieses Control für hoch/sehr hoch eingestufte Werte gilt.

Härtungsverweis: Einzelmaßnahme (siehe Teil II)

1.2.3 — To what extent are information security requirements considered in projects?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Projects are classified while taking into account the information security requirements."	Nicht betroffen	Governance/Projektsteuerung.	CISO-Funktion
should	"The procedure and criteria for the classification of projects are documented."	Nicht betroffen	Dokumentationspflicht.	CISO-Funktion
should	"During an early stage of the project, risk assessment is conducted based on the defined procedure and repeated in case of changes to the project."	Nicht betroffen	Expliziter Doppel-Auslöser ("früh im Projekt UND bei Änderungen wiederholt") entkräftet die Zeitkompressions-Sorge.	CISO-Funktion
should	"For identified information security risks, measures are derived and considered in the project."	Nicht betroffen	Governance.	CISO-Funktion
hoch	"The measures thus derived are reviewed regularly during the project and reassessed in case of changes to the assessment criteria. (C, I, A)"	Nicht betroffen	Ebenfalls Doppel-Auslöser ("regelmäßig UND bei Änderungen") vorhanden.	CISO-Funktion

Gesamteinstufung: Nicht betroffen (0 von 5 Anforderungen betroffen), unabhängig vom Schutzbedarf. Durchgängig doppelte Auslöser — gutes Beispiel für eine Formulierung, die die Zeitkompressions-Sorge strukturell entkräftet.

1.3.1 — To what extent are information assets identified and recorded?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Information assets and other assets where security is relevant to the organization are identified and recorded."	Nicht betroffen	Inventar-Governance.	CISO-Funktion
must	"The supporting assets processing the information assets are identified and recorded."	Nicht betroffen	Inventar-Governance.	CISO-Funktion
should	"A catalogue of the relevant information assets exists. The following aspects are considered: the corresponding supporting assets are assigned to each relevant information asset, a person responsible for these information assets is assigned, the catalogue is subject to regular review."	**Teilweise degradiert**	Zeitkompression: ohne festen Prüfanlass bleibt das Inventar zwischen den Überprüfungen unvollständig. Neu entstandene, nicht erfasste Systeme (etwa selbstständig eingerichtete Cloud- oder KI-Dienste) fallen genau in dieses Zeitfenster — dort setzen automatisierte Angriffe zuerst an.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (1 von 3 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-10 (siehe Teil II)

1.3.2 — To what extent are information assets classified and managed in terms of their protection needs?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available."	Nicht betroffen	Reines Klassifikationsschema; Wirkung entsteht erst in nachgelagerten technischen Controls.	CISO-Funktion
must	"Evaluation of the identified information assets is carried out according to the defined criteria, and assigned to the existing classification scheme."	Nicht betroffen	Anwendung des Schemas, Governance.	CISO-Funktion
must	"Specifications for the handling of supporting assets (e.g., identification, usage, transport, storage, return, deletion/disposal) depending on the classification of information assets are in place and implemented."	Nicht betroffen	Governance-Vorgabe; die technische Wirkung liegt in den referenzierten Controls selbst.	CISO-Funktion
should	"The protection goals of integrity and availability are taken into consideration."	Nicht betroffen	Vollständigkeit des Schemas.	CISO-Funktion

Gesamteinstufung: Nicht betroffen (0 von 4 Anforderungen betroffen), unabhängig vom Schutzbedarf.

1.3.3 — To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"External IT services are not used without explicit	**Teilweise degradiert**	Fähigkeitsentkopplung: die	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	assessment and implementation of the information security requirements. The following aspects are considered: availability of a risk assessment of the external IT services, legal, regulatory, and contractual requirements."		Freigabepflicht setzt voraus, dass ein Mensch bewusst einen bestimmten externen Dienst auswählt und zur Prüfung einreicht. KI-Assistenten mit Werkzeug-Zugriff können externe Dienste jedoch selbstständig im Rahmen einer Aufgabe aufrufen, ohne dass jemand diesen konkreten Dienst je zur Freigabe vorgelegt hat. Keine technische Sperre (z. B. Netzwerk-/Zugangskontrolle) im Wortlaut genannt.	
must	"The external IT services have been harmonized with the protection need of the processed information assets."	Nicht betroffen	Prüft, ob die Einstufung des Dienstes zum Schutzbedarf der Daten passt — eine Zuordnungsentscheidung, keine Abwehrmaßnahme.	CISO-Funktion
should	"Requirements regarding the procurement, commissioning and release associated with the use of external IT services are determined and fulfilled."	Nicht betroffen	Beschaffungsvorgabe.	Einkauf/Lieferantenmanagement
should	"A procedure for release in	Nicht	Verfahrensvorgabe	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	consideration of the protection need is established."	betroffen	für die Freigabe.	
should	"External IT services and their approval are documented."	Nicht betroffen	Dokumentationspflicht.	CISO-Funktion
should	"It is verified at regular intervals that only approved external IT services are used."	**Teilweise degradiert**	Zeitkompression: eine Stichprobenprüfung in festen Abständen lässt ein Zeitfenster offen, in dem ein nicht freigegebener Dienst unentdeckt bleibt — ohne laufende automatisierte Erkennung größer als die Reaktionszeit eines automatisierten Angriffs.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (2 von 6 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-10, MHC-13 (siehe Teil II)

1.3.4 — To what extent is it ensured that only evaluated and approved software is used for processing the organization's information assets?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Software is approved before installation or use. The following aspects are considered: limited approval for specific use-cases or roles, conformance to the information security	**Teilweise degradiert**	Fähigkeitsentkopplung: ein KI-gestützter Programmier-Assistent kann im Rahmen einer Aufgabe	Entwicklung/Engineering

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	requirements, software use rights and licensing, source/reputation of the software."		eigenständig Softwarepakete nachladen, ohne dass ein Mensch dieses konkrete Paket bewusst zur Freigabe vorlegt.	
must	"Software approval also applies to special purpose software such as maintenance tools."	**Teilweise degradiert**	Gleiche Begründung wie oben, hier nur Geltungsbereichs-Klarstellung.	Entwicklung/Engineering
should	"The types of software such as firmware, operating systems, applications, libraries, device drivers to be managed are determined."	Nicht betroffen	Scoping-Governance.	IT-Betrieb
should	"Repositories of managed software exist."	Nicht betroffen	Infrastruktur-Existenz.	IT-Betrieb
should	"The software repositories are protected against unauthorized manipulation."	**Teilweise degradiert**	Die Stärke des Schutzes ist offen: eine reine Zugriffsliste hält einem hinreichend befähigten automatisierten Angriff eher nicht stand, eine kryptografische Signaturprüfung schon — der Wortlaut legt sich nicht fest.	IT-Betrieb
should	"Approval of software is regularly reviewed."	**Teilweise degradiert**	Zeitkompression: "regelmäßig" ohne konkreten Prüfanlass.	IT-Betrieb
should	"Software versions and patch	**Teilweise**	Reine Kenntnis von	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	levels are known."	**degradiert**	Version und Patch-Stand sagt nichts über die Reaktionsgeschwindigkeit aus. Wenn zwischen Schwachstellen-Veröffentlichung und funktionierendem Angriff nur noch Stunden liegen, genügt Wissen allein nicht.	
sehr hoch	"Additional requirements for software use (e.g., need for control or monitoring of usage) are determined (if any) (C, I, A)"	Nicht betroffen	Zu unbestimmt formuliert ("falls zutreffend") für eine konkrete Bewertung.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (5 von 8 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-10, MHC-09, MHC-13 (siehe Teil II)

1.4.1 — To what extent are information security risks managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Risk assessments are carried out both at regular intervals and in response to events."	Nicht betroffen	Doppel-Auslöser entkräftet Zeitkompressions-Sorge.	CISO-Funktion
must	"Information security risks are appropriately assessed (e.g., for probability of occurrence and potential damage)."	**Teilweise degradiert**	Fähigkeitsentkopplung: klassische Einschätzungen der Eintrittswahrscheinlichkeit gehen oft davon aus, dass bestimmte Angriffe	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			nur wenigen hochspezialisierten Akteuren zugänglich sind. Diese Annahme trägt nicht mehr, wenn KI-Werkzeuge dieselbe Fähigkeit breit zugänglich machen. Keine aktualisierte Bewertungsmethodik vorgeschrieben.	
must	"Information security risks are documented."	Nicht betroffen	Dokumentationspflicht.	CISO-Funktion
must	"A responsible person (risk owner) is assigned to each information security risk."	Nicht betroffen	Governance.	CISO-Funktion
should	"A procedure is in place defining how to identify, assess and address security risks within the organization."	Nicht betroffen	Governance.	CISO-Funktion
should	"Criteria for the assessment and handling of security risks exist."	**Teilweise degradiert**	Gleiche Begründung wie oben, hier auf Ebene der Bewertungskriterien statt des Ergebnisses.	CISO-Funktion
should	"Measures for handling security risks and the persons responsible for these are specified and documented."	Nicht betroffen	Governance/Nachverfolgung.	CISO-Funktion
should	"In case of changes to the environment (e.g., organizational structure, location, changes to regulations), reassessment is	Nicht betroffen	Anlassbezogener Auslöser vorhanden.	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	carried out in a timely manner."			

Gesamteinstufung: Teilweise degradiert (2 von 8 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: Einzelmaßnahme (siehe Teil II)

1.5.1 — To what extent is compliance with information security ensured in procedures and processes?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Observation of policies is verified throughout the organization."	Nicht betroffen	Existenz der Verifikation, Governance.	CISO-Funktion
must	"Information security policies and procedures are reviewed at regular intervals."	**Teilweise degradiert**	Zeitkompression: "regelmäßig" ohne konkreten Prüfanlass.	CISO-Funktion
must	"Measures for correcting potential non-conformities (deviations) are initiated and pursued."	Nicht betroffen	Korrekturprozess, Governance.	CISO-Funktion
must	"Compliance with information security requirements (e.g., technical specifications) is verified at regular intervals."	**Teilweise degradiert**	Gleiche Begründung wie oben.	CISO-Funktion
must	"The results of the conducted reviews are recorded and retained."	Nicht betroffen	Dokumentationspflicht.	CISO-Funktion
should	"A plan for content and framework conditions (time schedule, scope, controls) of the reviews to be conducted is provided."	Nicht betroffen	Planungsartefakt.	CISO-Funktion
SGA	"Internal controls are implemented for all entities within the assessment scope."	Nicht betroffen	Reichweiten-Anforderung, Governance.	CISO-Funktion
SGA	"The implementation of all	Nicht	Vollständigkeits-	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	applicable security requirements and control objectives are included."	betroffen	Anforderung, Governance.	
SGA	"Suitably qualified and appropriate information security audit responsibilities and resources are defined."	Nicht betroffen	Ressourcen-/Qualifikations-Governance.	CISO-Funktion
SGA	"A detailed internal audit plan and schedule is defined and followed. [Entire assessment scope covered, Internal audits conducted regularly, Results tracked within ISMS structures]"	**Teilweise degradiert**	Zeitkompression: derselbe "regelmäßig ohne Anlassbezug"-Befund wie beim must-Element oben, hier auf den konzernweiten Auditplan bezogen — neu hinzugekommene Standorte werden ohne Anlass-Trigger nicht zwingend zeitnah in den Prüfplan aufgenommen.	CISO-Funktion

Gesamteinstufung: Teilweise degradiert (3 von 10 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-10 (siehe Teil II)

1.5.2 — To what extent is the ISMS reviewed by an independent authority?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Information security reviews are carried out by an independent and competent body at regular intervals and after fundamental changes."	Nicht betroffen	Doppel-Auslöser ("regelmäßig UND nach wesentlichen Änderungen") — Gegenbeispiel zu	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			1.5.1, zeigt: die konkrete Formulierung entscheidet, nicht das Thema an sich.	
must	"Measures for correcting potential deviations are initiated and pursued."	Nicht betroffen	Korrekturprozess.	CISO-Funktion
should	"The results of conducted reviews are documented and reported to the management of the organization."	Nicht betroffen	Dokumentation/Reporting.	CISO-Funktion
SGA	"In case of fundamental changes, audits are conducted by an independent and appropriately qualified entity (i.e., external entities or special internal departments which are objective, competent and free from undue influence (independent))."	Nicht betroffen	Ereignisgetriggert ("in case of fundamental changes"), gut formuliert — gleiche Begründung wie beim must-Element oben.	CISO-Funktion
SGA	"Findings and implementation of corrective actions is tracked by the independent entity."	Nicht betroffen	Nachverfolgungsprozess.	CISO-Funktion

Gesamteinstufung: Nicht betroffen (0 von 5 Anforderungen betroffen), unabhängig vom Schutzbedarf.

1.6.1 — To what extent are information security relevant events or observations reported?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders."	Nicht betroffen	Definitions-Governance.	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters."	**Teilweise degradiert**	Aggregationsresistenz: ein Meldewesen, das davon abhängt, dass ein Mensch etwas Auffälliges bemerkt, erkennt keinen Angriff, der bewusst in viele kleine, für sich harmlos wirkende Schritte zerlegt ist — kein einzelner Schritt fällt dabei auf.	IT-Betrieb
must	"Adequate channels for communication with event reporters exist."	Nicht betroffen	Infrastruktur/Prozess.	CISO-Funktion
should	"A common point of contact for event reporting exists."	Nicht betroffen	Organisatorisch.	CISO-Funktion
should	"Different reporting channels according to perceived severity ... are available."	Nicht betroffen	Prozess/Infrastruktur.	CISO-Funktion
should	"Employees are obligated and trained to report relevant events."	Nicht betroffen	Schulungspflicht.	Personalabteilung
should	"Security event reports can also be submitted by external parties."	Nicht betroffen	Prozess/Kanal.	CISO-Funktion
should	"Mechanism to, and information how to, report incidents is accessible by all relevant reporters."	Nicht betroffen	Zugänglichkeit.	CISO-Funktion
should	"A feedback procedure to reporters is established."	Nicht betroffen	Prozess.	CISO-Funktion
sehr hoch	"Tests and exercises of event and observation reporting are conducted regularly. (C, I, A)"	Nicht betroffen	Testaktivität — wird konsistent nicht wie Live-Erkennung	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			behandelt (siehe 1.6.2).	

Gesamteinstufung: Teilweise degradiert (1 von 9 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-05 (siehe Teil II)

1.6.2 — To what extent are reported security events managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Reported events are processed without undue delay."	**Teilweise degradiert**	Zeitkompression: setzt voraus, dass Menschen die Bearbeitung im nötigen Tempo schaffen. Wenn ein Angreifer den größten Teil seines Vorgehens automatisiert und ohne menschliches Zutun durchführt, kann eine rein menschlich getragene Bearbeitung strukturell nicht mithalten — Automatisierung wird nicht verlangt.	IT-Betrieb
must	"An adequate reaction to reported security events is ensured."	**Teilweise degradiert**	Gleiche Begründung wie oben.	IT-Betrieb
must	"Lessons learned are incorporated into continuous improvement."	Nicht betroffen	Verbesserungsprozess.	CISO-Funktion
should	"During processing, reported events are categorized, qualified, and prioritized."	Nicht betroffen	Prozess/Methodik.	IT-Betrieb
should	"Responsibilities for handling of events based on their category are defined	Nicht betroffen	Governance.	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	and assigned."			
should	"A strategy for reporting potentially criminal aspects of security incidents to relevant authorities when necessary or appropriate."	Nicht betroffen	Rechtlicher Prozess.	Rechtsabteilung
hoch	"Maximum response times based on class, category and severity are defined."	**Teilweise degradiert**	Eine Zielvorgabe zu definieren heißt nicht, dass sie gegen einen automatisiert und schnell agierenden Angreifer auch eingehalten werden kann — dafür fehlt eine Automatisierungspflicht.	IT-Betrieb
hoch	"Events not processed appropriately according to their priority are escalated."	**Teilweise degradiert**	Sinnvolles Sicherheitsnetz, bleibt aber selbst menschlich getragen und löst die Zeitkompressions-Lücke der vorherigen Zeile nicht auf.	IT-Betrieb
hoch	"Lawful, regulatory, and contractual reporting obligations, and respective contact information are known."	Nicht betroffen	Rechtliches Wissen.	Rechtsabteilung
hoch	"A communication strategy for security related events exists."	Nicht betroffen	Kommunikationsplanung.	CISO-Funktion
hoch	"Procedures for response to supplier security incidents are established."	Nicht betroffen	Prozess, vertieft in Kapitel 6.	Einkauf/Lieferantenmanagement
sehr hoch	"Handling of events in different categories and priorities is regularly tested."	Nicht betroffen	Testaktivität.	CISO-Funktion
SGA	"Standard	Nicht	Standardisierungs-	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	mechanisms to report and track relevant security events are established."	betroffen	Anforderung für konzernweite Konsistenz; die Erkennungs-/Reaktionsgeschwindigkeit selbst ist bereits oben bewertet.	

Gesamteinstufung: Teilweise degradiert (4 von 13 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-11 (siehe Teil II)

1.6.3 — To what extent is the organization prepared to handle crisis situations?

Datenqualitäts-Hinweis: die Spalte "hoch" enthält im Quellkatalog fünf auffällig ähnliche Anforderungspaare. Nur ein Paar ist wortgleich (wird einmal gezählt, 19 statt 20 Rohzeilen); die übrigen vier weichen redaktionell voneinander ab (Tippfehler bzw. abweichende Wortwahl im Quellkatalog selbst, u. a. "outage of" vs. "outage oaf", "Methods" vs. "Instruments to monitor communication") und werden unten als eigenständige Zeilen geführt.

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"An appropriate plan to react to and recover from crisis situations exists and the required resources are available."	Nicht betroffen	Planungsexistenz.	CISO-Funktion
must	"Responsibilities and authority for crisis management within the organization are defined, documented, and assigned."	Nicht betroffen	Governance.	CISO-Funktion
must	"The responsible employees are defined and qualified for their task."	Nicht betroffen	Governance/Personal.	CISO-Funktion
should	"Methods to detect crisis situations are established. General indications for the existence or imminence of a crisis situation and specific	**Teilweise degradiert**	Aggregationsresistenz und Zeitkompression: klassische Krisenerkennung ist auf allmählich eskalierende	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	predictable crisis are identified."		Lagen ausgelegt. Ein IT-Vorfall, der aus vielen kleinen, unauffälligen Schritten binnen Stunden zu einer echten Krise anwächst, wird eher zu spät erkannt.	
should	"A procedure to invoke and/or escalate crisis management is in place."	Nicht betroffen	Prozess.	CISO-Funktion
should	"Strategic goals and their priority in crisis situations are defined and known to relevant personnel."	Nicht betroffen	Governance.	CISO-Funktion
should	"A crisis management team is defined and approved."	Nicht betroffen	Governance.	CISO-Funktion
should	"Crisis policies and procedures are defined and approved."	Nicht betroffen	Governance.	CISO-Funktion
should	"Crisis planning is reviewed and updated regularly."	**Teilweise degradiert**	Zeitkompression: "regelmäßig" ohne konkreten Prüfanlass.	CISO-Funktion
hoch	"Relevant different potential crisis scenarios are identified."	**Teilweise degradiert**	Die genannten Beispielszenarien (Personal-, Ressourcen-, Infrastrukturausfall) sind klassische Ausfallszenarien; ein KI-orchestrierter, mehrgleisiger Angriff mit rascher Eskalation ist darin nicht ausdrücklich vorgesehen.	CISO-Funktion
hoch	"Relevant different potential crisis scenarios are	**Teilweise degradiert**	Inhaltlich identische Anforderung, im	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	identified." (zweite Katalogfassung, siehe Datenqualitäts-Hinweis)		Quellkatalog redaktionell doppelt mit abweichendem Wortlaut ("outage of" vs. "outage oaf") geführt — gleiche Begründung wie vorstehende Zeile.	
hoch	"Necessary resources and information to handle crisis ... are identified."	Nicht betroffen	Ressourcenplanung.	CISO-Funktion
hoch	"Necessary resources and information to handle crisis ... are identified." (zweite Katalogfassung, siehe Datenqualitäts-Hinweis)	Nicht betroffen	Ressourcenplanung; redaktionelle Dublette der vorstehenden Zeile.	CISO-Funktion
hoch	"A communication strategy for crisis situations exists."	**Teilweise degradiert**	Gleiche Zeitkompressions-Sorge wie bei der Krisenerkennung: kein Bezug zu einem stark verkürzten Reaktionsfenster.	CISO-Funktion
hoch	"A communication strategy for crisis situations exists." (zweite Katalogfassung, siehe Datenqualitäts-Hinweis)	**Teilweise degradiert**	Inhaltlich identische Anforderung, im Quellkatalog redaktionell doppelt mit abweichendem Wortlaut ("Methods" vs. "Instruments to monitor communication") geführt — gleiche Begründung wie vorstehende Zeile.	CISO-Funktion
hoch	"The efficiency, feasibility, and appropriateness of the crisis planning is evaluated regularly."	**Teilweise degradiert**	Zeitkompression: "regelmäßig" ohne konkreten Prüfanlass.	CISO-Funktion
hoch	"Spot based testing of crisis	Nicht	Testaktivität.	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	planning is conducted."	betroffen		
hoch	"Spot based testing of crisis planning is conducted." (zweite Katalogfassung, siehe Datenqualitäts-Hinweis)	Nicht betroffen	Testaktivität; redaktionelle Dublette der vorstehenden Zeile.	CISO-Funktion
sehr hoch	"Crisis exercises and simulations involving all relevant persons, including decision makers are conducted regularly."	Nicht betroffen	Testaktivität.	CISO-Funktion

Gesamteinstufung: Teilweise degradiert (7 von 19 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: MHC-10, MHC-05, Einzelmaßnahme (siehe Teil II)

Zusammenfassung Kapitel 1

Control	Gesamteinstufung	Anteil betroffen
1.1.1	Teilweise degradiert	1/10
1.2.1	Teilweise degradiert	1/7
1.2.2	Nicht betroffen → ab hoch: Teilweise degradiert	0/7 → 1/8
1.2.3	Nicht betroffen	0/5
1.3.1	Teilweise degradiert	1/3
1.3.2	Nicht betroffen	0/4
1.3.3	Teilweise degradiert	2/6
1.3.4	Teilweise degradiert	5/8
1.4.1	Teilweise degradiert	2/8
1.5.1	Teilweise degradiert	3/10
1.5.2	Nicht betroffen	0/5
1.6.1	Teilweise degradiert	1/9
1.6.2	Teilweise degradiert	4/13
1.6.3	Teilweise degradiert	7/19

10 von 14 Controls durchgängig degradiert, 3 durchgängig nicht betroffen, 1 schutzbedarfsabhängig. Kein Standfest, keine Reine Reibung — erwartbar, da Kapitel 1 ein

reines Governance-Kapitel ohne kryptografische oder architektonische Hartbarrieren ist. Zwei wiederkehrende Muster tragen den hohen Degradiert-Anteil: **(1)** "regelmäßig/periodisch" ohne konkreten Prüfanlass, **(2)** menschlich getragene Melde-/Reaktionsgeschwindigkeit gegenüber einem automatisiert operierenden Angreifer. Verantwortlich überwiegend CISO-Funktion/ISMS-Prozesse — konsistent damit, dass dies das Governance-Kapitel ist. SGA-Anforderungen (6 Controls betroffen, 10 zusätzliche Anforderungen, davon 1 degradiert) ändern an keinem der 14 Controls die Gesamteinstufung — sie erweitern den Geltungsbereich auf Konzernebene, ohne neue Schwächen einzuführen.

Kapitel 2 — Human Resources (4 Controls, 21 Anforderungen)

2.1.1 — To what extent is the qualification of employees for sensitive work fields ensured?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Sensitive work fields and jobs are determined."	Nicht betroffen	Scoping-Governance.	Personalabteilung
must	"The requirements for employees with respect to their job profiles are determined and fulfilled."	Nicht betroffen	Governance.	Personalabteilung
must	"The identity of potential employees is verified (e.g., checking identity documents)."	**Teilweise degradiert**	Fähigkeitsentkopplung: überzeugende gefälschte Ausweisdokumente und -in Kombination mit Video-Interviews- Deepfake-Identitäten galten bislang als Spezialistenwissen. KI-generierte Dokumentenfälschung und Echtzeit-Video-/Audio-Deepfakes machen täuschend echte Identitätsvortäuschung im Einstellungsprozess	Personalabteilung

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			heute breit zugänglich (bekanntes aktuelles Muster: fingierte Remote-Mitarbeitende).	
should	"The personal suitability of potential employees is verified by means of simple methods (e.g., job interview)."	**Teilweise degradiert**	Gleiche Begründung: ein Live-Interview als Verifikationsmethode ist genau das Ziel von Echtzeit-Deepfake-Impersonation.	Personalabteilung
should	"An extended suitability verification depending on the respective work field and job is conducted (e.g., assessment centre, psychological analysis, checking of references, certificates and diploma, checking of certificates of conduct, checking of professional and private background)."	**Teilweise degradiert**	Fähigkeitsentkopplung: Referenzen, Zeugnisse und Diplome lassen sich mit KI-Werkzeugen überzeugender fälschen als zuvor; auch fingierte Referenzpersonen/-firmen sind leichter darstellbar.	Personalabteilung

Gesamteinstufung: Teilweise degradiert (3 von 5 Anforderungen betroffen), unabhängig vom Schutzbedarf. Durchgehendes Thema: alle drei Identitäts-/Eignungsprüfungen setzen auf menschliche Verifikation, die auf heute nicht mehr zuverlässigen "Echtheitsmerkmalen" beruht.
Härtungsverweis: MHC-15 (siehe Teil II)

2.1.2 — To what extent is all staff contractually bound to comply with information security policies?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"A non-disclosure obligation is in effect."	Nicht betroffen	Vertragsrechtlich, kein Angriffsbezug.	Rechtsabteilung
must	"An obligation to comply with the information	Nicht betroffen	Vertragsrechtlich.	Rechtsabteilung

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	security policies is in effect."			
should	"A non-disclosure obligation beyond the employment contract is in effect."	Nicht betroffen	Vertragsrechtlich.	Rechtsabteilung
should	"Information security aspects are considered in the employment contracts of the staff."	Nicht betroffen	Vertragsrechtlich.	Rechtsabteilung
should	"A procedure for handling violations of said obligations is described."	Nicht betroffen	Prozess/Governance.	Personalabteilung

Gesamteinstufung: Nicht betroffen (0 von 5 Anforderungen betroffen), unabhängig vom Schutzbedarf. Reines Vertragsrecht ohne technische oder verhaltensbasierte Schutzwirkung — durch Mythos nicht berührt.

2.1.3 — To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Employees are trained and made aware."	**Teilweise degradiert**	Fähigkeitsentkopplung: klassische Awareness-Inhalte trainieren das Erkennen von Rechtschreibfehlern, unpersönlicher Anrede und anderen "Tells" von Phishing/Social Engineering. KI-generierte Angriffe sind fehlerfrei, personalisiert und sprachlich unauffällig — die trainierten Erkennungsmerkmale funktionieren nicht	Personalabteilung

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			mehr zuverlässig.	
should	"A concept for awareness and training of employees is prepared. [Policy, Event reporting, Malware reaction, Password policy, Compliance, NDA use, External IT services use]"	Nicht betroffen	Existenz eines strukturierten Konzepts, Governance.	CISO-Funktion
should	"Target groups for training and awareness measures... are identified and considered in a training concept."	Nicht betroffen	Scoping-Governance.	CISO-Funktion
should	"The concept has been approved by the responsible management."	Nicht betroffen	Freigabeakt.	CISO-Funktion
should	"Training and awareness measures are carried out both at regular intervals and in response to events."	Nicht betroffen	Doppel-Auslöser entkräftet die Zeitkompressions-Sorge.	Personalabteilung
should	"Participation in training and awareness measures is documented."	Nicht betroffen	Dokumentationspflicht.	Personalabteilung
should	"Contact persons for information security are known to employees."	Nicht betroffen	Kommunikation/Governance.	CISO-Funktion

Gesamteinstufung: Teilweise degradiert (1 von 7 Anforderungen betroffen), unabhängig vom Schutzbedarf. Der Befund betrifft nicht die Existenz oder Organisation von Schulungen, sondern deren *Inhalt*: Schulungskonzepte, die nicht explizit vermitteln, dass klassische Erkennungsmerkmale von Täuschungsversuchen nicht mehr greifen, lassen die Belegschaft mit einer falschen Sicherheit zurück.
Härtungsverweis: MHC-15 (siehe Teil II)

2.1.4 — To what extent is mobile work regulated?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The requirements for mobile work are determined and fulfilled. [Behavior in private surroundings, Behavior in public surroundings, Secure handling of and access to information, Protection from theft, Measures to ensure a secure access to organization's IT-services]"	Nicht betroffen	Physisch-verhaltensbezogene Vorgaben; die technische Zugriffssicherung wird in 4.1.2/5.1.2 eigenständig bewertet, hier keine Doppelzählung.	IT-Betrieb
should	"[Measures for travelling e.g., viewing by authorities, Measures for travelling to security-critical countries]"	Nicht betroffen	Reise-/physische Sicherheit, kein spezifischer Mythos-Bezug.	CISO-Funktion
should	"Employee awareness."	Nicht betroffen	Im Kontext dieses Controls auf physische Reiserisiken bezogen (Überschulterblicke, Diebstahl), nicht auf die allgemeine Phishing-/Social-Engineering-Schulung aus 2.1.3.	Personalabteilung
hoch	"Protective measures against overhearing and viewing are implemented. (C)"	**Standfest**	Physische/technische Gegenmaßnahme (Sichtschutz, abgeschirmte Räume) — eine harte Barriere,	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			die unabhängig von der Angreiferfähigkeit wirkt.	

Gesamteinstufung: Bei normalem Schutzbedarf Nicht betroffen (0 von 3 Anforderungen betroffen) — kein Handlungsbedarf. Ab hohem Schutzbedarf kommt eine physische Standfest-Anforderung hinzu (Sicht-/Abhörschutz); da keine Degradiert-Anforderung existiert, wird die Gesamteinstufung ab hoch zu **Standfest**. Praktisch: für Mobile-Work-Szenarien mit hohem/sehr hohem Schutzbedarf ist die physische Abschirmung nachweisbar wirksam und SoA-zitierfähig.

Zusammenfassung Kapitel 2

Control	Gesamteinstufung	Anteil betroffen
2.1.1	Teilweise degradiert	3/5
2.1.2	Nicht betroffen	0/5
2.1.3	Teilweise degradiert	1/7
2.1.4	Nicht betroffen → ab hoch: Standfest	0/3 → Standfest

Kapitel 2 zeigt ein neues Muster gegenüber Kapitel 1: die Degradiert-Befunde entstehen nicht aus vagen Prüfzyklen, sondern aus **menschlicher Identitäts- und Eignungsverifikation** (Einstellungsprozess, Awareness-Inhalte), die auf heute nicht mehr verlässlichen Erkennungsmerkmalen beruht — dieselbe Fähigkeitsentkopplung, die in der Methodik am JadePuffer-Fall belegt wird, zeigt sich hier auf der Ebene der Identitätsprüfung statt der technischen Angriffsausführung. Erstes Standfest-Beispiel des Katalogs (physischer Sicht-/Abhörschutz).

Kapitel 3 — Physical Security (4 Controls, 14 Anforderungen, davon 1 Control ohne eigene Anforderungen)

3.1.1 — To what extent are security zones managed to protect information assets?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"A security zone concept including the associated protective measures based on the requirements for the handling of information assets is in place. [Physical conditions in the definition of security zones, Delivery and shipping areas]"	Nicht betroffen	Konzept-Existenz, Governance; die Wirksamkeit der Maßnahmen selbst wird in den folgenden Zeilen bewertet.	Facility/Werkschutz
must	"The defined protective measures are implemented."	**Teilweise degradiert**	Der Wortlaut bleibt offen, WELCHE Maßnahmen implementiert werden. Soweit die Zutrittskontrolle auf menschlicher Prüfung beruht (Empfang, Sicherheitsdienst), ist sie durch KI-gestützte Vortäuschung (gefälschte Ausweise, überzeugende Legenden am Telefon) angreifbar — Fähigkeitsentkopplung.	Facility/Werkschutz
must	"The code of conduct for	Nicht	Kommunikation	Facility/Werkschutz

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	security zones is known to all persons involved."	betroffen	von Verhaltensregeln.	
should	"Procedures for allocation and revocation of access rights are established."	Nicht betroffen	Verwaltungsprozess für physische Zutrittsrechte.	Facility/Werkschutz
should	"Visitor management policies (including registration and escorting of visitors) are defined."	**Teilweise degradiert**	Fähigkeitsentkopplung: Besucherregistrierung/-begleitung beruht auf der Prüfung vorgetäuschter Identität und Termine (gefälschte Lieferanten-Legitimation, gefälschte Terminbestätigung per Anruf/E-Mail) — heute einfacher darstellbar.	Facility/Werkschutz
should	"Policies for carrying along and using mobile IT devices and mobile data storage devices... are defined and implemented."	Nicht betroffen	Geräte-Richtlinie, technisch vertieft in 3.1.4.	IT-Betrieb
should	"Network/infrastructure components (own or customer networks) are protected against unauthorized access."	**Standfest**	Physische Verriegelung/Einhausung von Netzwerkkomponenten (Serverraum, Verteilerschrank) ist eine harte Barriere unabhängig von Angreiferfähigkeit; die menschliche Zutrittsentscheidu	Facility/Werkschutz

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			ng ist bereits in den vorstehenden Zeilen bewertet (keine Doppelzählung).	
should	"External properties used for storing and processing information assets are considered in the security zone concept..."	Nicht betroffen	Scoping-Vollständigkeit.	Facility/Werkschutz
hoch	"Protective measures against simple overhearing and viewing are implemented. (C)"	**Standfest**	Physisch-architektonische Maßnahme, hart und angreiferunabhängig.	Facility/Werkschutz

Gesamteinstufung: Teilweise degradiert (2 von 9 Anforderungen betroffen), unabhängig vom Schutzbedarf. Zwei Standfest-Elemente (Netzwerkkomponenten-Einhausung, Sicht-/Abhörschutz ab hoch) bestehen parallel, ändern aber die Gesamteinstufung nicht, da die menschlich vermittelte Zutritts-/Besucherprüfung als Schwachstelle bestehen bleibt.
Härtungsverweis: MHC-15 (siehe Teil II)

3.1.2 — Superseded by 1.6.3, 5.2.8 and 5.2.9

Keine eigenen Anforderungen — Inhalt vollständig in den genannten Controls abgedeckt. Keine Klassifikation erforderlich.

3.1.3 — To what extent is the handling of supporting assets managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The requirements for the handling of supporting assets (e.g., transport, storage, repair, loss, return, disposal) are determined and fulfilled."	Nicht betroffen	Governance-Vorgabe für den Lebenszyklus physischer Assets; die technische Entsorgungsstärke wird unten	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			separat bewertet.	
hoch	"Disposal of supporting assets is conducted in accordance with one of the relevant standards (e.g. ISO 21964, at least security level 4). (C)"	**Standfest**	Physische Vernichtungsnorm (z. B. definierte Schredder-Partikelgrösse) ist ein harter, verifizierbarer Prozess — eine KI-gestützte Angreiferfähigkeit hilft nicht bei der Rekonstruktion ordnungsgemäss vernichteter Datenträger.	IT-Betrieb

Gesamteinstufung: Bei normalem Schutzbedarf Nicht betroffen (0 von 1) — nur eine allgemeine Prozessanforderung. Ab hohem Schutzbedarf kommt eine physische Vernichtungsnorm hinzu, die Gesamteinstufung wird **Standfest**. Praktisch: ein positives Beispiel — TISAX® verlangt bei höherem Schutzbedarf explizit eine belastbare, Mythos-resistente Entsorgungsmethode.

3.1.4 — To what extent is the handling of mobile IT devices and mobile data storage devices managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The requirements for mobile IT devices and mobile data storage devices are determined and fulfilled. [Encryption, Access protection e.g. PIN/password, Marking]"	**Teilweise degradiert**	"Encryption" ist nur einer von mehreren gleichrangig genannten Aspekten, nicht verpflichtend und umfassend vorgeschrieben (das geschieht erst bei hoch). Wo	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			Verschlüsselung fehlt oder nur teilweise vorliegt, bleibt PIN/Passwortschutz die wirksame Barriere — anfällig für automatisiertes/KI-gestütztes Erraten oder Social Engineering.	
should	"Registration of the IT devices."	Nicht betroffen	Inventarisierung.	IT-Betrieb
hoch	"General encryption of mobile data storage devices or the information assets stored thereon. Where this is technically not feasible, information is protected by similarly effective measures. (C, I)"	**Standfest**	Verpflichtet zu *genereller* (umfassender) Verschlüsselung — eine harte kryptografische Barriere, die die am must-Niveau offene Lücke gezielt schließt.	IT-Betrieb

Gesamteinstufung: Bei normalem Schutzbedarf Teilweise degradiert (1 von 2), da nur eine unvollständige Verschlüsselungspflicht besteht. Ab hohem Schutzbedarf schließt die Pflicht zur generellen Verschlüsselung genau diese Lücke — Gesamteinstufung wird **Standfest**. Praktisch: Geräte mit normalem Schutzbedarf bleiben strukturell schwächer geschützt als solche mit hohem/sehr hohem Schutzbedarf; prüfen Sie, ob "normale" Geräte in Ihrem Bestand faktisch trotzdem vollverschlüsselt sind.
Härtungsverweis: Einzelmaßnahme (siehe Teil II)

Zusammenfassung Kapitel 3

Control	Gesamteinstufung	Anteil betroffen
3.1.1	Teilweise degradiert	2/9
3.1.2	(keine Anforderungen)	–
3.1.3	Nicht betroffen → ab hoch: Standfest	0/1 → Standfest
3.1.4	Teilweise degradiert → ab hoch: Standfest	1/2 → Standfest

Physical Security liefert die bislang dichteste Standfest-Konzentration: physische Vernichtung, generelle Verschlüsselung, Sicht-/Abhörschutz und Einhausung von Netzwerktechnik sind sämtlich harte, angreiferunabhängige Barrieren. Die verbleibenden Degradiert-Befunde entstehen konsistent an derselben Stelle: der menschlich vermittelten Zutritts-/Besucherprüfung.

Kapitel 4 — Identity and Access Management (4 Controls, 37 Anforderungen)

4.1.1 — To what extent is the use of identification means managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The requirements for the handling of identification means over the entire lifecycle are determined and fulfilled. [Creation/handover/return/destruction, Validity periods, Traceability, Handling of loss]"	Nicht betroffen	Lebenszyklus-Governance für Ausweise/Token; die tatsächliche Fälschungssicherheit ist Gegenstand anderer Controls (Kryptografie: 5.1.1).	IAM-Team
should	"Identification means can be produced under controlled conditions only."	Nicht betroffen	Kontrolliert den legitimen Ausstellungskanal (nur autorisierte Stellen produzieren Ausweise) — ein Governance-Control über den Herstellungsprozess, keine	IAM-Team

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			Aussage über die Fälschungserkennung durch Dritte.	
hoch	"A strategy of blocking or invalidation of identification means in case of loss is prepared and implemented as far as possible. (C, I, A)"	**Teilweise degradiert**	Zeitkompression: "as far as possible" ohne verpflichtende sofortige/automatisierte Sperrung lässt ein Zeitfenster offen, in dem ein verlorenes oder kopiertes Ausweismittel weiter gültig bleibt — ein automatisiert agierender Angreifer nutzt genau dieses Fenster schneller aus, als eine manuelle Sperrung greifen kann.	IAM-Team

Gesamteinstufung: Bei normalem Schutzbedarf Nicht betroffen (0 von 2 Anforderungen betroffen). Ab hohem Schutzbedarf kommt die Sperr-/Ungültigkeitsstrategie hinzu, deren unverbindliche Formulierung ("as far as possible") eine Zeitkompressions-Lücke öffnet — Gesamteinstufung wird **Teilweise degradiert** (1 von 3). Praktisch: prüfen Sie, ob Ihre Sperrprozesse für verlorene Ausweise/Token tatsächlich automatisiert/sofort greifen, statt sich auf die Kann-Formulierung zu verlassen.
Härtungsverweis: MHC-03 (siehe Teil II)

4.1.2 — To what extent is the user access to IT services and IT systems secured?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been considered (e.g., direct accessibility via the internet)."	Nicht betroffen	Auswahlmethodik; die Stärke des gewählten Verfahrens wird in der folgenden Zeile eigenständig bewertet.	IAM-Team
must	"State of the art procedures for user authentication are applied."	**Teilweise degradiert**	Fähigkeitsentkopplung/ Zeitkompression: "Stand der Technik" verpflichtet nicht ausdrücklich zu phishing-resistenten Verfahren (z. B. FIDO2/WebAuthn). Automatisierte Echtzeit-Phishing-Relays (Adversary-in-the-Middle) hebeln OTP-/Push-basierte Verfahren aus, die in vielen Organisationen weiterhin als "Stand der Technik" gelten. Zielzustand: ein verpflichtender Einsatz phishing-resistenter Verfahren würde diese Anforderung auf Standfest-Niveau heben, da die Schutzannahme dann strukturell und nicht nur graduell hält.	IAM-Team
should	"The user authentication	Nicht	Prozess der	IAM-Team

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	procedures are defined and implemented based on the business-related and security-relevant requirements"	betroffen	Anforderungsableitung.	
should	"Users are authenticated at least by means of strong passwords according to proven and widely accepted practices."	**Reine Reibung**	Die Schutzannahme dieser Anforderung — nur die berechtigte Person kennt das Passwort — trifft gegen automatisiertes, KI-skaliertes Phishing nicht mehr zu, unabhängig von der Passwortstärke: der Angreifer erhält das korrekte Passwort direkt von der Nutzerin/dem Nutzer, nicht durch Erraten. Anders als bei der Zeile darunter (privilegierte Konten, wo PAM zumindest Session-Überwachung als Teilschutz bietet) existiert hier kein zweiter Faktor und kein Kompensationsmechanismus im Wortlaut — die Anforderung verliert ihre Kernwirkung vollständig, nicht nur teilweise.	IAM-Team
should	"Superior procedures are used for the authentication of privileged user accounts (e.g., privileged access management, two-factor	**Teilweise degradiert**	Die "e.g."-Formulierung lässt einfache Zwei-Faktor-Authentisierung ohne Phishing-Resistenz genügen —	IAM-Team

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	authentication)."		dieselbe AITM-Relay-Lücke wie oben, hier auf privilegierte Konten bezogen. Bleibt "nur" degradiert statt Reibung, weil PAM als genannte Alternative zusätzliche Session-Überwachung/Zeitbegrenzung bieten kann, die einen kompromittierten Faktor teilweise auffängt.	
hoch	"Depending on the risk assessment, authentication procedure and access control have been enhanced by supplementary measures (e.g., continuous access monitoring with respect to irregularities or use of strong authentication, automatic logout, disabling in case of inactivity, or brute force prevention). (C, I, A)"	**Teilweise degradiert**	Die Optionsliste erlaubt Erfüllung über schwächere Maßnahmen (automatischer Logout, Brute-Force-Schutz), die die AITM-/Phishing-Relay-Lücke nicht adressieren; nur die Option "kontinuierliches Zugriffsmonitoring" würde tatsächlich helfen, ist aber nicht verpflichtend.	IAM-Team
sehr hoch	"Before gaining access to data of very high protection needs, users are authenticated by means of strong authentication (e.g., two-factor authentication) according to the state of the art. (C, I)"	**Teilweise degradiert**	Gleiche Lücke wie oben: das Beispiel nennt klassische Zwei-Faktor-Authentisierung statt ausdrücklich phishing-resistenter Verfahren.	IAM-Team

Gesamteinstufung: Reine Reibung (1 von 7 Anforderungen verliert die Kernwirkung vollständig; insgesamt 5 von 7 betroffen, davon 4 weiterhin wirksam, aber geschwächt), unabhängig vom

Schutzbedarf. Nach der Rangfolge-Konvention (Reine Reibung > Teilweise degradiert > Standfest > Nicht betroffen) bestimmt der reine Passwortfaktor die Gesamteinstufung, auch wenn die übrigen vier Funde dieses Controls nur geschwächt, nicht wirkungslos sind. Erster Reine-Reibung-Fund des gesamten Katalogs — durchgängiges Muster im Control bleibt die fehlende Pflicht zu phishing-resistenter (FIDO2/WebAuthn-artiger) Authentisierung. Zielzustand: mit verpflichtendem phishing-resistentem Verfahren (FIDO2/WebAuthn/Passkey) für alle sieben Anforderungen wäre der Control durchgängig Standfest, nicht nur der reine Passwortfaktor gelöst — dieser Zielzustand ist Gegenstand von MHC-03 (siehe Teil II).
Härtungsverweis: MHC-03 (siehe Teil II)

4.1.3 — To what extent are user accounts and login information securely managed and applied?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The creating, changing, and deleting of user accounts is conducted."	Nicht betroffen	Basisprozess.	IAM-Team
must	"Unique and personalized user accounts are used."	Nicht betroffen	Nachvollziehbarkeits-Prinzip, strukturell.	IAM-Team
must	"The use of \"shared accounts\" is regulated (e.g., restricted to cases where traceability of actions is dispensable)."	Nicht betroffen	Governance.	IAM-Team
must	"User accounts are disabled immediately after the user has resigned from or left the organization (e.g., upon termination of the employment contract)."	Nicht betroffen	"immediately" ist ein klarer Sofort-Auslöser ohne Zeitkompressions-Lücke im Wortlaut.	IAM-Team
must	"User accounts are regularly reviewed."	**Teilweise degradiert**	Zeitkompression: periodische Prüfung ohne Anlassbezug lässt verwaiste/überflüssige Konten zwischen den Zyklen	IAM-Team

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			unentdeckt.	
must	"The login information is provided to the user in a secure manner."	Nicht betroffen	Übermittlungsprozess.	IAM-Team
must	"A policy for the handling of login information is defined and implemented. [No disclosure, No writing down/unencrypted storage, Immediate change on suspected compromise, No reuse, Change of temporary credentials after first login, Quality requirements]"	Nicht betroffen	Hygiene-/Verhaltensrichtlinie; die Mechanismus-Stärke der Authentisierung selbst wird eigenständig in 4.1.2 bewertet (keine Doppelzählung).	IAM-Team
should	"A basic user account with minimum access rights and functionalities is existent and used."	Nicht betroffen	Least-Privilege-Baseline, strukturell.	IAM-Team
should	"Default accounts and passwords pre-configured by manufacturers are disabled (e.g., by blocking or changing of password)."	Nicht betroffen	Einmaliger Härtungsschritt; sobald umgesetzt, unabhängig von Angreiferfähigkeit geschlossen.	IT-Betrieb
should	"User accounts are created or authorized by the responsible body."	Nicht betroffen	Governance.	IAM-Team
should	"Creating user accounts is subject to an approval process (four-eyes principle)."	Nicht betroffen	Vier-Augen-Prinzip, organisatorisch robust.	IAM-Team
should	"User accounts of service providers are disabled upon completion of their task."	Nicht betroffen	Klar ereignisgetriggert.	IAM-Team
should	"Deadlines for disabling	Nicht betroffen	Governance/Frist	IAM-Team

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	and deleting user accounts are defined."		setzung.	
should	"The use of default passwords is technically prevented."	Nicht betroffen	Technische Durchsetzung, binär, einmalig wirksam.	IT-Betrieb
should	"Where strong authentication is applied, the use of the medium (e.g., ownership factor) is secure."	**Teilweise degradiert**	Fähigkeitsentkopplung: der Besitzfaktor (z. B. Telefonnummer für SMS-OTP) ist durch SIM-Swapping angreifbar; überzeugendes Vortäuschen gegenüber Telko-Support-Mitarbeitenden ist mit KI-Unterstützung leichter geworden.	IAM-Team
should	"User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems."	**Teilweise degradiert**	Gleiche Zeitkompressions-Begründung wie beim must-Element oben, hier zusätzlich auf Kundensysteme bezogen.	IAM-Team
should	"Interactive login for service accounts (technical accounts) is technically prevented."	Nicht betroffen	Technische, strukturelle Durchsetzung.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (3 von 17 Anforderungen betroffen), unabhängig vom Schutzbedarf (Control hat keine hoch-/sehr-hoch-Anforderungen).
Härtungsverweis: MHC-10, MHC-03 (siehe Teil II)

4.2.1 — To what extent are access rights assigned and managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The requirements for the management of access rights (authorization) are determined and fulfilled. [Procedure for application/verification/approval, Need-to-know/least-privilege, Access rights revoked when no longer needed]"	Nicht betroffen	Ereignisgetriggerte Entzugslogik ("when no longer needed") statt vager Periodik — gut formuliert.	IAM-Team
must	"The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers."	**Teilweise degradiert**	Zeitkompression: klassisches periodisches-Review-Muster ohne Anlassbezug.	IAM-Team
should	"Strategies for authorizing access to information are prepared."	Nicht betroffen	Governance.	IAM-Team
should	"Authorization roles are used."	Nicht betroffen	RBAC-Design, strukturell.	IAM-Team
should	"Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility."	Nicht betroffen	Design-Prinzip.	IAM-Team
should	"Normal user accounts are not granted privileged access rights."	Nicht betroffen	Strukturelle Trennung.	IAM-Team
should	"The user's access rights are updated after the user's responsibilities have changed (e.g., to another field of responsibility)."	Nicht betroffen	Ereignisgetriggert, gut formuliert.	IAM-Team
hoch	"The access rights are approved by the responsible internal Information Officer."	Nicht betroffen	Zusätzliche Freigabe-Governance.	IAM-Team

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	(C, I, A)"			
sehr hoch	"Information is stored in encrypted form at content level (e.g., file level) to prevent unauthorized persons from gaining access and information (privileged users). Where encryption is not feasible, information shall be protected by similarly effective measures. (C)"	**Standfest**	Inhaltsverschlüsselung auf Dateiebene ist eine harte kryptografische Barriere, die selbst gegen privilegierte Insider oder umgangene Zugriffskontrollen wirkt.	IT-Betrieb
sehr hoch	"Existing access rights are regularly reviewed at shorter intervals (e.g., quarterly). (C)"	**Teilweise degradiert**	Verkürzt das Prüfintervall, bleibt aber periodisch ohne Anlassbezug — die strukturelle Zeitkompressions-Lücke bleibt bestehen, nur das Zeitfenster wird kleiner.	IAM-Team

Gesamteinstufung: Teilweise degradiert (1 von 7 Anforderungen betroffen bei normalem Schutzbedarf; 2 von 10 inkl. hoch/sehr hoch), unabhängig vom Schutzbedarf. Bemerkenswert: bei sehr hohem Schutzbedarf kommt mit der Dateiebenen-Verschlüsselung ein echtes Standfest-Element hinzu, das die Gesamteinstufung jedoch nicht kippt, da die periodische Zugriffsprüfung als eigenständige Schwäche bestehen bleibt.
Härtungsverweis: MHC-10 (siehe Teil II)

Zusammenfassung Kapitel 4

Control	Gesamteinstufung	Anteil betroffen
4.1.1	Nicht betroffen → ab hoch: Teilweise degradiert	0/2 → 1/3
4.1.2	Reine Reibung	1/7 (Reibung) + 4/7 (degradiert)
4.1.3	Teilweise degradiert	3/17
4.2.1	Teilweise degradiert	1/7 → 2/10

Identity and Access Management liefert den ersten und bislang einzigen Reine-Reibung-Fund des gesamten Katalogs: der reine Passwortfaktor in 4.1.2 verliert seine Kernwirkung gegen automatisiertes Phishing vollständig, nicht nur teilweise. Der Control bleibt insgesamt auch der

am stärksten betroffene (5 von 7 Anforderungen) — durchgängiges Muster ist das Fehlen einer expliziten Pflicht zu phishing-resistenter Authentisierung. Daneben wiederholt sich das bekannte periodische-Review-Muster (4.1.1, 4.1.3, 4.2.1). Ein Standfest-Lichtblick bei sehr hohem Schutzbedarf: inhaltsbasierte Verschlüsselung (4.2.1).

Kapitel 5 — IT Security/Cyber Security (15 Controls, 105 Anforderungen, größtes Kapitel)

5.1.1 — To what extent is the use of cryptographic procedures managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"All cryptographic procedures used (e.g., encryption, signature, and hash algorithms, protocols) provide the security required by the respective application field according to the recognized industry standard to the extent legally feasible."	**Standfest**	Verpflichtet zu Industriestandard-Kryptografie. Korrekt implementierte moderne Kryptografie (AES-256, aktuelles TLS etc.) ist gegen einen Gen-AI-gestützten Angreifer mathematisch hart — KI verkürzt weder Faktorisierung noch Brute-Force gegen moderne Schlüssellängen. (Post-Quantum-Risiko ist ein eigenständiges, hier bewusst nicht behandeltes Bedrohungsfeld — kein Mythos-/Gen-AI-Bezug.)	CISO-Funktion
should	"A concept for the application of cryptography is defined and implemented. [Methods, Key strengths, Full lifecycle: generation/storage/archiving/retrieval/distribution/deactivation/renewal/deletion]"	Nicht betroffen	Schlüsselverwaltungs-Prozess, Governance; die kryptografische Stärke selbst ist bereits oben bewertet.	IT-Betrieb
hoch	"Key sovereignty	Nicht	Rechtlich-vertragliche	CISO-Funktion

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	requirements (particularly in case of external processing) are determined and fulfilled. (C, I)"	betroffen	Souveränitätsfrage (Jurisdiktion bei Cloud-Verarbeitung), kein Mythos-Bezug.	

Gesamteinstufung: Standfest (kein Degradiert-/Reibungs-Element vorhanden), unabhängig vom Schutzbedarf. Ordnungsgemäss implementierte Kryptografie ist eines der klarsten Beispiele einer echten Hartbarriere im gesamten Katalog — direkt als SoA-Nachweis zitierfähig.

5.1.2 — To what extent is information protected during transfer?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The network services used to transfer information are identified and documented."	Nicht betroffen	Inventar/Governance.	IT-Betrieb
must	"Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented."	Nicht betroffen	Governance.	IT-Betrieb
must	"Measures for the protection of transferred contents against unauthorized access are implemented."	**Teilweise degradiert**	Unspezifische "Maßnahmen" ohne verpflichtenden Mindeststandard (z. B. Verschlüsselung) lassen Raum für schwächeren Schutz, den ein netzwerktechnisch positionierter, KI-gestützter Angreifer aushebeln kann. Erst hoch/sehr hoch schließen die Lücke explizit (siehe unten).	IT-Betrieb
should	"Measures for ensuring correct addressing and	Nicht betroffen	Übertragungskorrektheit, keine	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	correct transfer of information are implemented."		Angreiferbarriere im engeren Sinn.	
should	"Electronic data exchange is conducted using content or transport encryption according to the respective classification."	**Standfest**	Verpflichtet explizit zu Inhalts- oder Transportverschlüsselung — schließt die must-Lücke für Organisationen, die dieses Should-Element umsetzen.	IT-Betrieb
should	"Remote access connections to the organization's network possess adequate security features. [Encryption, Authentication strength, Granting/termination of access, Secured connection e.g. VPN]"	**Teilweise degradiert**	Fernzugriff ist das bevorzugte Ziel von Echtzeit-Phishing-Relay-Angriffen (siehe 4.1.2) — VPN-Verschlüsselung schützt den Transportweg, löst aber nicht die Authentisierungs-Schwäche, falls diese konventionell (Passwort/OTP) bleibt.	IT-Betrieb
hoch	"Information is transported or transferred in encrypted form (at least transport-encryption) or protected by similarly effective measures. (C)"	**Standfest**	Explizite Verschlüsselungspflicht für hohen Schutzbedarf.	IT-Betrieb
sehr hoch	"Information is transported or transferred in content-encrypted form. (C)"	**Standfest**	Inhaltsverschlüsselung, die stärkste Form — Ende-zu-Ende-artige Absicherung.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (2 von 6 Anforderungen betroffen), unabhängig vom Schutzbedarf. Zwei getrennte Schwachstellen: die vage must-Formulierung wird durch das Should-Element zur Verschlüsselung weitgehend geschlossen; die Fernzugriffs-

Authentisierungslücke (identisch mit dem Befund in 4.1.2) bleibt jedoch unabhängig davon über alle Stufen bestehen.
Härtungsverweis: MHC-03, Einzelmaßnahme (siehe Teil II)

5.2.1 — To what extent are changes managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Information security requirements for changes to the organization, business processes, IT systems are determined and fulfilled."	Nicht betroffen	Governance.	IT-Betrieb
should	"A formal approval procedure is established."	Nicht betroffen	Governance.	IT-Betrieb
should	"The potential impact on the information security of changes is assessed."	Nicht betroffen	Prozessbewertung.	IT-Betrieb
should	"Changes affecting the information security are subjected to planning and testing."	Nicht betroffen	Prozess.	IT-Betrieb
should	"Procedures for fallback in fault cases are considered."	Nicht betroffen	Resilienz-Governance.	IT-Betrieb
hoch	"Compliance with the information security requirements is verified during and after the changes are applied. (C, I, A)"	Nicht betroffen	Doppelter, klar definierter Prüfzeitpunkt ("während und danach") — gut formuliert, kein Zeitkompressions-Bezug.	IT-Betrieb

Gesamteinstufung: Nicht betroffen (0 von 6 Anforderungen betroffen), unabhängig vom Schutzbedarf. Sauber spezifizierte Prozesskontrolle ohne Mythos-relevante Lücke — gutes Beispiel für ein durchweg unauffälliges Governance-Control.

5.2.2 — To what extent are development and testing environments separated from operational environments?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The IT systems have been subjected to risk assessment in order to determine the necessity of their separation into development, testing and operational systems."	Nicht betroffen	Bewertungsprozess.	Entwicklung/Engineering
must	"A segmentation is implemented based on the results of risk analysis."	**Standfest**	Architektonische Trennung ist eine strukturelle Barriere: einmal korrekt umgesetzt, wirkt sie unabhängig davon, wie ein Angreifer seinen initialen Zugriffsversuch automatisiert.	IT-Betrieb
should	"The requirements for development and testing environments are determined and fulfilled. [Separation of dev/test/prod, No dev tools on operational systems, Different user profiles]"	**Standfest**	Vertieft dieselbe strukturelle Trennung (getrennte Profile, keine Entwicklungswerkzeuge in Produktion) — schließt laterale Bewegung und Werkzeug-Missbrauch in der Produktivumgebung architektonisch aus.	IT-Betrieb

Gesamteinstufung: Standfest (kein Degradiert-/Reibungs-Element), unabhängig vom Schutzbedarf. Hinweis: die Wirksamkeit gilt für korrekt umgesetzte Segmentierung; eine unvollständige/fehlerhafte Umsetzung ist eine Implementierungsfrage, keine wortlautbedingte Schwäche.

5.2.3 — To what extent are IT systems protected against malware?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Requirements for protection against malware are determined."	Nicht betroffen	Governance.	IT-Betrieb
must	"Technical and organizational measures for protection against malware are defined and implemented."	**Teilweise degradiert**	Fähigkeitsentkopplung: klassischer, signaturbasierter Malwareschutz ist gegen KI-generierte/polymorphe Schadsoftware strukturell schwächer, da Signaturen erst nach Bekanntwerden einer Variante greifen.	IT-Betrieb
should	"Unnecessary network services are disabled."	Nicht betroffen	Angriffsflächenreduktion, strukturell/binär.	IT-Betrieb
should	"Access to network services is restricted to necessary access through suitable protective measures (see examples)."	Nicht betroffen	Zugriffskontrolle, strukturell.	IT-Betrieb
should	"Malware protection software is installed and updated automatically at regular intervals (e.g., virus scanner)."	**Teilweise degradiert**	Das genannte Beispiel "Virenscanner" signalisiert signaturbasierte Erkennung; automatische, aber periodische Updates hinken KI-generierten Varianten strukturell hinterher.	IT-Betrieb
should	"Received files and software are automatically inspected for malware prior to their execution (on-access scan)."	**Teilweise degradiert**	Gleiche Signatur-Erkennungsgrenze.	IT-Betrieb
should	"The entire data contents of	**Teilweise**	Doppelte Schwäche:	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	all systems is regularly inspected for malware."	**degradiert**	periodische Prüfung (Zeitkompression) und Signaturerkennung (Fähigkeitsentkopplung).	
should	"Data transferred by central gateways (e.g., e-mail, internet, third-party networks) is automatically inspected by means of protection software. [Encrypted connections, Encrypted content]"	**Teilweise degradiert**	Verschlüsselter Inhalt umgeht die Gateway-Inspektion strukturell — ein bekannter, durch KI-gestützte Angreifer gezielt genutzter Umgehungsweg.	IT-Betrieb
should	"Measures to prevent protection software from being deactivated or altered by users are defined and implemented."	Nicht betroffen	Manipulationsschutz für den Schutzagenten selbst, strukturell/binär.	IT-Betrieb
should	"For IT systems operated without the use of malware protection software, alternative measures... are implemented."	Nicht betroffen	Kompensationskontrolle, generisch.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (5 von 10 Anforderungen betroffen), unabhängig vom Schutzbedarf. Einer der am stärksten degradierten Controls des Katalogs — signaturbasierte Malware-Erkennung ist ein klassisches Beispiel für Fähigkeitsentkopplung: KI-generierte, polymorphe Schadsoftware unterläuft Signaturabgleich systematisch.
Härtungsverweis: MHC-05 (siehe Teil II)

5.2.4 — To what extent are event logs recorded and analysed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Information security requirements regarding the handling of event logs are determined and fulfilled."	Nicht betroffen	Governance.	IT-Betrieb
must	"Security-relevant	Nicht	Scoping.	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	requirements regarding the logging of activities of system administrators and users are determined and fulfilled."	betroffen		
must	"The IT systems used are assessed regarding the necessity of logging."	Nicht betroffen	Bewertungsprozess.	IT-Betrieb
must	"When using external IT services, information on the monitoring options is obtained and considered in the assessment."	Nicht betroffen	Lieferanten-/Governance-Aspekt.	IT-Betrieb
must	"Event logs are checked regularly for policy violations and noticeable problems in compliance with the permissible legal and organizational provisions."	**Teilweise degradiert**	Aggregationsresistenz und Zeitkompression: periodische, auf "auffällige" Ereignisse ausgerichtete manuelle Prüfung erkennt einen bewusst in viele unauffällige Einzelschritte fragmentierten Angriff strukturell nicht.	IT-Betrieb
should	"A procedure for the escalation of relevant events to the responsible body... is defined and established."	Nicht betroffen	Nachgelagerter Eskalationsprozess.	IT-Betrieb
should	"Event logs (contents and meta data) are protected against alteration. (e.g., by a dedicated environment)."	**Standfest**	Manipulationsschutz für Logdaten (z. B. WORM-Speicher, getrenntes Log-System) ist eine strukturelle Barriere, unabhängig von Angreiferfähigkeit.	IT-Betrieb
should	"Adequate monitoring and recording of any actions on	Nicht betroffen	Existenz der Aufzeichnung; die	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	the network that are relevant to information security are established."		Auswertungsqualität ist bereits oben bewertet.	
hoch	"Information security requirements relevant to the security during the handling of event logs, e.g., contractual requirements, are determined and implemented. (C, I, A)"	Nicht betroffen	Vertraglich/governance -bezogen.	IT-Betrieb
hoch	"Events related to establishing and terminating remote access sessions (e.g., for remote maintenance). (C, I, A)"	Nicht betroffen	Scoping (was geloggt wird), keine Auswertungsaussage.	IT-Betrieb
sehr hoch	"Logging of any access to data of very high protection needs as far as technically feasible and as permissible according to legal and organizational provisions. (C, I)"	Nicht betroffen	Scoping.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (1 von 8 Anforderungen betroffen), unabhängig vom Schutzbedarf. Die Schwäche liegt gezielt in der *Auswertung* ("regelmäßig geprüft"), nicht in der Protokollierung selbst — die Log-Integrität ist mit einem eigenen Standfest-Element sogar gut abgesichert.
Härtungsverweis: MHC-05 (siehe Teil II)

5.2.5 — To what extent are vulnerabilities identified and addressed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Information on technical vulnerabilities for the IT systems in use is gathered (e.g., information from the manufacturer, system audits, CVS database) and	Nicht betroffen	Informationsbeschaffung; die zeitkritische Bewertung erfolgt in der nächsten Zeile.	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	evaluated (e.g., Common Vulnerability Scoring System CVSS)."			
must	"Potentially affected IT systems and software are identified and the risk caused by the vulnerability is assessed."	**Teilweise degradiert**	Kollaps des Patch-Gap-Fensters (siehe Methodik, Cogent-Security-Auswertung 2026): klassische Risikobewertungen kalkulieren üblicherweise mit Wochen bis zu einem funktionierenden Exploit. Belegt verkürzt sich dieses Fenster durch KI-gestützte Exploit-Entwicklung auf teils unter einen Tag — eine Bewertungsmethodik ohne diese Berücksichtigung unterschätzt systematisch die Dringlichkeit.	IT-Betrieb
must	"Risks arising from vulnerabilities are treated."	Nicht betroffen	Behandlungsprozess, nachgelagert.	IT-Betrieb
should	"An adequate patch management is defined and implemented (e.g., patch testing and installation)."	**Teilweise degradiert**	Gleiche Patch-Gap-Begründung: "adequate" ohne verpflichtende Geschwindigkeits-SLA garantiert kein Tempo, das mit KI-beschleunigter Exploit-Verfügbarkeit mithält.	IT-Betrieb
should	"Risk minimizing measures are implemented, as	Nicht betroffen	Generische Kompensationsmaßnah	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	necessary."		me.	
should	"Successful installation of patches is verified in an appropriate manner."	Nicht betroffen	Qualitätssicherung, nachgelagert.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (3 von 6 Anforderungen betroffen), unabhängig vom Schutzbedarf. Zentraler Befund des gesamten Katalogs: dieser Control bildet direkt die in der Methodik belegte Verschiebung "Kollaps des Patch-Gap-Fensters" ab — Priorität für die spätere Härtungscontrols-Synthese.
Härtungsverweis: MHC-09 (siehe Teil II)

5.2.6 — To what extent are IT systems and services technically checked (system and service audit)?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Requirements for auditing IT systems or services are determined."	Nicht betroffen	Governance.	IT-Betrieb
must	"The scope of the system audit is specified in a timely manner."	Nicht betroffen	Planung.	IT-Betrieb
must	"System or service audits are coordinated with the operator and users of the IT systems or services."	Nicht betroffen	Koordination.	IT-Betrieb
must	"The results of system or service audits are stored in a traceable manner and reported to the relevant management."	Nicht betroffen	Dokumentation/Reporting.	IT-Betrieb
must	"Measures are derived from the results and are implemented in an appropriate timeframe."	**Teilweise degradiert**	Zeitkompression: "appropriate timeframe" ist unbestimmt und ohne verbindliche Obergrenze relativ zu einem beschleunigten	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			Bedrohungstempo.	
should	"System and service audits are planned taking into account any security risks they might cause (e.g., disturbances)."	Nicht betroffen	Planungssicherheit.	IT-Betrieb
should	"Regular system or service audits are performed. [Qualified personnel, Suitable tools e.g. vulnerability scanners, From internet and internal network]"	**Teilweise degradiert**	Periodische statt kontinuierliche Prüfung lässt zwischen den Audit-Zyklen dieselbe Patch-Gap-Lücke wie in 5.2.5 offen.	IT-Betrieb
should	"Within a reasonable period following completion of the audit, a report is prepared."	Nicht betroffen	Dokumentationstempo, nachgelagert.	IT-Betrieb
hoch	"For critical IT systems or services, additional system or service audit requirements have been identified and are fulfilled (e.g., service specific tests and tools and/or human penetration tests, risk-based time intervals). (A)"	Nicht betroffen	"Risk-based time intervals" ist eine adaptive, gut formulierte Anforderung ohne starre Periodizität.	IT-Betrieb
sehr hoch	"IT systems and services are regularly scanned for vulnerabilities. Suitable protective measures must be implemented for systems and services that may not be scanned. (C, I, A)"	**Teilweise degradiert**	Auch auf der höchsten Schutzbedarfsstufe nur "regelmäßig" statt kontinuierlich gescannt — die Chance auf eine verpflichtende Nahezu-Echtzeit-Prüfung bei sehr hohem Schutzbedarf bleibt ungenutzt.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (2 von 8 Anforderungen betroffen bei normalem Schutzbedarf; 3 von 10 inkl. sehr hoch), unabhängig vom Schutzbedarf. Durchgängiges Thema: periodische statt kontinuierliche Prüfung, konsistent mit dem Patch-Gap-Befund aus 5.2.5.
Härtungsverweis: MHC-09 (siehe Teil II)

5.2.7 — To what extent is the network of the organization managed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Requirements for the management and control of networks are determined and fulfilled."	Nicht betroffen	Governance.	IT-Betrieb
must	"Requirements regarding network segmentation are determined and fulfilled."	**Standfest**	Segmentierungspflicht — konsistent mit der architektonischen Standfest-Bewertung in 5.2.2.	IT-Betrieb
should	"Procedures for the management and control of networks are defined."	Nicht betroffen	Governance.	IT-Betrieb
should	"For a risk-based network segmentation. [Limitations for connecting IT systems, Security technologies, Performance/trust/availability/security/safety, Limitation of impact if compromised, Detection of potential attacks and lateral movement, Separation of networks with different purpose, Internet-exposure risk, Technology-specific separation for external IT services, Separation from customer networks, Detection/prevention of data loss]"	**Teilweise degradiert**	Die Detektions-Teilaspekte (laterale Bewegung, Datenabfluss) sind der schwächere Bestandteil: generische "Erkennung" ohne Vorgabe verhaltensbasierter/anomaliebasierter Methoden ist eher auf offensichtliche als auf fragmentierte, langsam ablaufende Angriffsmuster ausgelegt.	IT-Betrieb
hoch	"Extended requirements for the management and	**Teilweise degradier**	Der Verweis auf Fernzugriffsrisiken	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	control of networks are determined and implemented. [Authentication of IT systems on the network, Restricted access to management interfaces, Specific risks e.g. wireless and remote access] (C, I, A)"	**t**	importiert dieselbe Authentisierungslücke wie in 4.1.2/5.1.2; die übrigen Teilaspekte (Geräteauthentisierung, Management-Interface-Schutz) sind für sich strukturell solide.	

Gesamteinstufung: Teilweise degradiert (1 von 4 Anforderungen betroffen bei normalem Schutzbedarf; 2 von 5 inkl. hoch), unabhängig vom Schutzbedarf. Die Segmentierungspflicht selbst ist Standfest; die Schwäche liegt in der Erkennungs- und Fernzugriffs-Dimension.
Härtungsverweis: MHC-03, MHC-05 (siehe Teil II)

5.2.8 — To what extent is continuity planning for IT services in place?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Critical IT services are identified, and business impact is considered."	Nicht betroffen	Business-Impact-Analyse, Governance.	IT-Betrieb
must	"Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled."	Nicht betroffen	Governance.	IT-Betrieb
should	"Critical IT systems are identified. [Classification for appropriate protection need, Implementation of adequate security measures]"	Nicht betroffen	Governance/Klassifikation.	IT-Betrieb
should	"Continuity planning exists and is regularly reviewed and updated. [Alternative communication, Alternative storage, Alternative	**Teilweise degradiert**	Zeitkompression: periodische Aktualisierung ohne Anlassbezug für Szenarien, die heute	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	power/network]"		schneller eskalieren (z. B. Ransomware-Ausbreitungsgeschwindigkeit).	
should	"Continuity planning includes at least (Distributed) Denial of Service attacks, successful ransomware attacks and other sabotage activities, system failure scenarios, and natural disaster scenarios affecting critical IT systems."	Nicht betroffen	Explizit moderne Angriffsszenarien (DDoS, Ransomware, Sabotage) benannt — eine gut abgesicherte Formulierung unabhängig davon, wie ein Angriff im Detail orchestriert wird.	IT-Betrieb
hoch	"Continuity planning includes predefined time frames (Recovery Time Objective) for resumption of operation in line with requirements. (A)"	Nicht betroffen	Definierter RTO-Parameter.	IT-Betrieb
hoch	"Appropriate SLAs with external service providers according to continuity planning are in place. (A)"	Nicht betroffen	Vertraglich.	Einkauf/Lieferantenmanagement
hoch	"Continuity plans include coordination of contractually agreed communication with business partners. (A)"	Nicht betroffen	Vertraglich/Prozess.	CISO-Funktion
hoch	"Continuity planning is regularly tested including a full recovery and reconstitution of the system to a known state and compliance with defined target times. (A)"	Nicht betroffen	Testaktivität.	IT-Betrieb
hoch	"A backup and recovery strategy for critical IT	Nicht betroffen	Existenz der Strategie; die konkrete Backup-	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	services and information is defined and implemented. (C, I, A)"		Mechanik wird eigenständig in 5.2.9 bewertet (keine Doppelzählung).	
hoch	"Backups of critical IT services and information are sufficiently protected against unauthorized modification or deletion by malicious software, (I, A)"	**Teilweise degradiert**	"Sufficiently protected" ohne Unveränderlichkeits-Vorgabe lässt zu, dass Ransomware mit kompromittierten Backup-Admin-Rechten Sicherungen dennoch löschen/verschlüsseln kann. Erst 5.2.9 (sehr hoch) schließt diese Lücke explizit über unveränderliche/Offline-Backups.	IT-Betrieb
hoch	"Backups of critical IT services and information are sufficiently protected against unauthorized access by malicious software or operators. (C, I)"	**Teilweise degradiert**	Gleiche Begründung, hier die Vertraulichkeitsseite.	IT-Betrieb
sehr hoch	"Continuity planning is coordinated with the continuity plans of relevant external service providers. (A)"	Nicht betroffen	Koordination/vertraglich.	Einkauf/Lieferantenmanagement
sehr hoch	"Continuance of essential mission and business functions with minimal or no loss of operational continuity is possible. [Alternate operation strategies/separated standby systems, Alternate/backup storage	**Standfest**	Räumlich getrennte Standby-Systeme/Standorte mit gleichwertigen Kontrollen sind eine architektonische Redundanz — wirkt unabhängig von	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	sites with equivalent controls]"		Angreiferfähigkeit.	
sehr hoch	"Continuity planning is tested regularly. Test scenarios, results, and lessons learned are recorded. (I, A)"	Nicht betroffen	Testaktivität.	IT-Betrieb

Gesamteinstufung: Teilweise degradiert (1 von 5 Anforderungen betroffen bei normalem Schutzbedarf; 3 von 15 inkl. hoch/sehr hoch), unabhängig vom Schutzbedarf. **Querverweis:** die Backup-Unveränderlichkeitslücke bei hoch wird durch Control 5.2.9 (sehr hoch) explizit geschlossen — siehe dort für die vollständige Einordnung.
Härtungsverweis: MHC-08 (siehe Teil II)

5.2.9 — To what extent is the backup and recovery of data and IT services ensured?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Backup concepts exist for relevant IT systems. Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups are considered."	Nicht betroffen	Konzept-Existenz; die konkrete Mechanik wird bei hoch/sehr hoch spezifisch bewertet.	IT-Betrieb
must	"Recovery concepts exist for relevant IT services."	Nicht betroffen	Konzept-Existenz.	IT-Betrieb
should	"A backup and recovery concept exists for each relevant IT service. Dependencies between IT services and the sequence for recovery are considered."	Nicht betroffen	Planung/Sequenzierung.	IT-Betrieb
hoch	"Backup and recovery concepts are methodically reviewed at regular intervals. (A)"	**Teilweise degradiert**	Zeitkompression: periodische Überprüfung des Konzepts ohne	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			Anlassbezug — ein Konzept kann veralten, auch wenn das zugrunde liegende Speichermedium (siehe sehr hoch) unveränderlich ist.	
hoch	"General restore capability is considered and tested (e.g., sample testing, test systems). (I, A)"	Nicht betroffen	Stichprobenartige Testaktivität.	IT-Betrieb
hoch	"Backup and recovery concepts exist. [RPO, RTO, Required resources for recovery, Avoidance of overload scenarios, Appropriate spatial redundancy e.g. separate room/fire section/data center/site] (A)"	**Standfest**	Räumliche Redundanz (getrennter Serverraum/Brandabschnitt/Standort) ist eine architektonische Barriere, die unabhängig von Angreiferfähigkeit wirkt.	IT-Betrieb
sehr hoch	"(Additional) Backups are performed via offline procedures, immutable backups or by using an isolated IAM solution. (I, A)"	**Standfest**	Offline-/unveränderliche Backups oder isolierte IAM-Lösung sind eine harte architektonische Barriere gegen Ransomware und credential-basierte Angriffe — eines der stärksten Standfest-Beispiele des gesamten Katalogs.	IT-Betrieb
sehr hoch	"Restore procedures are technically tested in a methodical way at regular intervals. (I, A)"	Nicht betroffen	Testaktivität.	IT-Betrieb
sehr hoch	"Geographical redundancy is considered in data	**Standfest**	Geografische Redundanz, strukturell.	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	backup and recovery concepts. (A)"			

Gesamteinstufung: Bei normalem Schutzbedarf Nicht betroffen (0 von 3 Anforderungen betroffen) — nur Konzept-Existenz gefordert. Ab hohem Schutzbedarf kommt die periodische Konzept-Überprüfung ohne Anlassbezug hinzu — Gesamteinstufung wird **Teilweise degradiert** (1 von 6), gleichzeitig aber auch räumliche Redundanz als Standfest-Element. Bei sehr hohem Schutzbedarf verstärkt sich die Standfest-Seite deutlich (unveränderliche/Offline-Backups, geografische Redundanz) — **die Gesamteinstufung bleibt dennoch Teilweise degradiert** (1 von 9), weil die periodische-Überprüfung-Lücke aus der hoch-Stufe unverändert fortbesteht. Praktisch: selbst eine Organisation mit vorbildlichen unveränderlichen Backups gilt hier als "Teilweise degradiert", weil sich die beiden Anforderungen auf unterschiedliche Aspekte beziehen — Backup-*Medium* (unveränderlich, stark) versus Backup-*Konzept*-Prüfzyklus (periodisch, schwach). **Querverweis:** ergänzt die Backup-Unveränderlichkeitslücke aus Control 5.2.8 (hoch).
Härtungsverweis: MHC-10 (siehe Teil II)

Zusammenfassung (Kapitel 5, Teil 1: 5.1.1–5.2.9)

Control	Gesamteinstufung	Anteil betroffen
5.1.1	Standfest	0/3
5.1.2	Teilweise degradiert	2/6
5.2.1	Nicht betroffen	0/6
5.2.2	Standfest	0/3
5.2.3	Teilweise degradiert	5/10
5.2.4	Teilweise degradiert	1/8
5.2.5	Teilweise degradiert	3/6
5.2.6	Teilweise degradiert	2/8 → 3/10
5.2.7	Teilweise degradiert	1/4 → 2/5
5.2.8	Teilweise degradiert	1/5 → 3/15
5.2.9	Nicht betroffen → ab hoch: Teilweise degradiert	0/3 → 1/6 → 1/9

5.3.1 — To what extent is information security considered in new or further developed IT service?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The information security requirements associated with the design and development of IT service are determined and considered."	Nicht betroffen	Governance.	Entwicklung/Engineering
must	"The information security requirements associated with the acquisition or extension of IT service and IT components are determined and considered."	Nicht betroffen	Governance.	Einkauf/Lieferantenmanagement
must	"Information security requirements associated with changes to developed IT services are considered."	Nicht betroffen	Governance, thematisch verwandt mit 5.2.1.	Entwicklung/Engineering
must	"System approval tests are carried out under consideration of the information security requirements."	Nicht betroffen	Freigabe-Gate, Existenzebene.	Entwicklung/Engineering
should	"Requirement specifications are prepared. [IS requirements, Vendor recommendations/best practices, Best practices/security guidelines, Fail safe design]"	Nicht betroffen	Dokumentation/Design-Input.	Entwicklung/Engineering
should	"Requirement specifications are reviewed against the information security requirements."	Nicht betroffen	Review-Governance.	Entwicklung/Engineering
should	"The IT service is reviewed for compliance with specifications prior to	Nicht betroffen	Freigabe-Gate.	Entwicklung/Engineering

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	productive use."			
should	"The use of production data for testing purposes is avoided as far as possible (if applicable, anonymization or pseudonymization). [Lifecycle requirements for test data, Case-related generation specs]"	**Teilweise degradiert**	Fähigkeitsentkopplung: die Re-Identifizierung pseudonymisierter/anonymisierter Daten durch Korrelation mit Zusatzinformationen erforderte bislang statistisches Spezialwissen. KI-gestützte Korrelationsverfahren machen dies breiter zugänglich, ohne dass die Anforderung eine Re-Identifizierungs-resistente Methodik vorschreibt.	Entwicklung/Engineering
should	"Test-systems are provided with protective measures comparable to those in the operational environment where productive data are used for testing purposes."	Nicht betroffen	Kompensationskontrolle, strukturell vergleichbar.	Entwicklung/Engineering
sehr hoch	"The security of purpose built software or significantly customized software is tested (e.g., penetration testing) during commissioning, in case of significant changes, or at regular intervals. (C, I, A)"	Nicht betroffen	Dreifach-Auslöser (Inbetriebnahme, wesentliche Änderungen, Regelintervall) — gut abgesicherte Formulierung ohne isolierte Zeitkompressions-Lücke.	Entwicklung/Engineering

Gesamteinstufung: Teilweise degradiert (1 von 10 Anforderungen betroffen), unabhängig vom Schutzbedarf.
Härtungsverweis: Einzelmaßnahme (siehe Teil II)

5.3.2 — To what extent are requirements for network services defined?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Requirements regarding the information security of network services are determined and fulfilled."	Nicht betroffen	Governance.	IT-Betrieb
should	"A procedure for securing and using network services is defined and implemented."	Nicht betroffen	Governance/Prozess.	IT-Betrieb
should	"The requirements are agreed in the form of SLAs."	Nicht betroffen	Vertraglich.	Einkauf/Lieferantenmanagement
should	"Adequate redundancy solutions are implemented."	**Standfest**	Redundanz ist eine strukturelle Verfügbarkeits-Maßnahme, konsistent mit anderen Redundanz-Bewertungen im Katalog.	IT-Betrieb
hoch	"Procedures for monitoring the quality of network traffic (e.g., traffic flow analyses, availability measurements) are defined and carried out. (A)"	Nicht betroffen	Qualitäts-/Verfügbarkeitsmonitoring, kein Sicherheitsdetektions-Bezug (davon getrennt in 5.2.7 bewertet).	IT-Betrieb

Gesamteinstufung: Standfest (kein Degradiert-/Reibungs-Element), unabhängig vom Schutzbedarf.

5.3.3 — To what extent is the return and secure removal of information assets from external IT services regulated?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"A procedure for the return and secure removal of information assets from each external IT service is defined and implemented."	Nicht betroffen	Governance/Vertragsprozess.	Einkauf/Lieferantenmanagement
should	"A description of the	Nicht	Vertraglich.	Einkauf/Lieferant

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	termination process is given, adapted to any changes, and contractually regulated."	betroffen		enmanagement

Gesamteinstufung: Nicht betroffen (0 von 2 Anforderungen betroffen), unabhängig vom Schutzbedarf.

5.3.4 — To what extent is information protected in shared external IT services?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Effective segregation (e.g., segregation of customers) prevents access to own information by unauthorized users of other organizations."	**Standfest**	Mandantentrennung ist bei korrekter Umsetzung (kryptografische Isolation, strikte Zugriffskontrollen) eine strukturelle Barriere — konsistent mit der Segmentierungs-Bewertung in 5.2.2/5.2.7.	IT-Betrieb
should	"The provider's segregation concept is documented and adapted to any changes. [Separation of data/functions/software/OS /storage/network, Risk assessment for shared environment]"	Nicht betroffen	Dokumentation des Konzepts; die Mechanismus-Stärke ist bereits oben bewertet.	Einkauf/Lieferant enmanagement

Gesamteinstufung: Standfest (kein Degradiert-/Reibungs-Element), unabhängig vom Schutzbedarf.

Zusammenfassung Kapitel 5 (gesamt, 15 Controls)

Control	Gesamteinstufung	Anteil betroffen
5.1.1	Standfest	0/3
5.1.2	Teilweise degradiert	2/6
5.2.1	Nicht betroffen	0/6
5.2.2	Standfest	0/3
5.2.3	Teilweise degradiert	5/10
5.2.4	Teilweise degradiert	1/8
5.2.5	Teilweise degradiert	3/6
5.2.6	Teilweise degradiert	2/8 → 3/10
5.2.7	Teilweise degradiert	1/4 → 2/5
5.2.8	Teilweise degradiert	1/5 → 3/15
5.2.9	Nicht betroffen → ab hoch: Teilweise degradiert	0/3 → 1/6 → 1/9
5.3.1	Teilweise degradiert	1/10
5.3.2	Standfest	0/5
5.3.3	Nicht betroffen	0/2
5.3.4	Standfest	0/2

Kapitel 5 ist das technisch dichteste Kapitel und zeigt die größte Bandbreite: 4 durchgehend Standfest (Kryptografie, Dev/Test/Prod-Trennung, Netzwerk-Redundanz, Mandantentrennung — sämtlich architektonische/kryptografische Hartbarrieren), 9 Teilweise degradiert, 2 Nicht betroffen, 1 schutzbedarfsabhängig (5.2.9, mit der ausführlich begründeten Ausnahme, dass die sehr starke Standfest-Ergänzung bei sehr hohem Schutzbedarf die Degradiert-Gesamteinstufung nicht kippt). Zwei marktreife Mythos-Kernbefunde dieses Kapitels: der Kollaps des Patch-Gap-Fensters (5.2.5, 5.2.6) und die durchgängig fehlende Pflicht zu phishing-resistenter Authentisierung (5.1.2, 5.2.7, deckungsgleich mit 4.1.2).

Kapitel 6 — Supplier Relationships (3 Controls, 31 Anforderungen)

6.1.1 — To what extent is information security ensured among contractors and cooperation partners?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Contractors and partners are subjected to a security risk assessment."	Nicht betroffen	Governance/Prozess.	Einkauf/Lieferantenmanagement
must	"An appropriate level of information security is ensured by contractual agreements with contractors and partners."	Nicht betroffen	Vertraglich.	Einkauf/Lieferantenmanagement
must	"Where applicable, contractual agreements with clients and customers are passed on to contractors and partners."	Nicht betroffen	Vertraglich, Durchreichung.	Einkauf/Lieferantenmanagement
should	"Contractors and partners are contractually obligated to pass on any requirements regarding an appropriate level of information security to their subcontractors."	Nicht betroffen	Vertragliche Kaskadierung.	Einkauf/Lieferantenmanagement
should	"Service reports and documents by contractors and partners are reviewed."	**Teilweise degradiert**	Fähigkeitsentkopplung: die Prüfung basiert auf vom Lieferanten vorgelegten Dokumenten. KI-Werkzeuge machen überzeugend gefälschte oder beschönigte Berichte/Nachweise leichter erstellbar, ohne dass eine unabhängige Gegenprüfung verlangt	Einkauf/Lieferantenmanagement

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			wird.	
hoch	"Evidence is provided that the information security level of the supplier is adequate for the protection needs of the information (e.g., checked questionnaire/self-assessment, attestation, certificate, supplier audit). (C, I, A)"	**Teilweise degradiert**	Die Beispielliste lässt reine Selbstauskunft/Attestierung genügen — dieselbe Dokumenten-Fälschungslücke wie oben, hier auf formale Nachweise bezogen. Erst sehr hoch schließt dies über die Pflicht zum Drittaudit (siehe unten).	Einkauf/Lieferantenmanagement
hoch	"The supplier's level of compliance with the required evidence is documented, regularly and in case of changes... reviewed and monitored. (C, I, A)"	**Teilweise degradiert**	Die Prüf-Frequenz ist mit Doppel-Auslöser gut formuliert; das zugrunde liegende Nachweis-Echtheitsproblem bleibt jedoch unabhängig davon bestehen.	Einkauf/Lieferantenmanagement
hoch	"The supplier's compliance with contractual agreements is checked, documented, regularly and in case of changes... reviewed and monitored. (C, I, A)"	**Teilweise degradiert**	Gleiche Begründung.	Einkauf/Lieferantenmanagement
sehr hoch	"The adequate level of information security should be demonstrated by a third party audit (an adequate TISAX® label or equivalent) or an adequate supplier audit covering agreed and applicable customer requirements. If an audit was not conducted, a risk-	**Standfest**	Verpflichtet zu unabhängigem Drittaudit (TISAX®-Label o. ä.) statt Selbstauskunft — ein Vor-Ort-Audit mit Interviews und Stichprobenprüfung ist ungleich schwerer im großen Stil zu fälschen	Einkauf/Lieferantenmanagement

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	based decision must be made by the organization's management to continue doing business with the supplier. A record of this decision exists. (C, I, A)"		als ein eingereichtes Dokument. Schließt die bei hoch benannte Lücke gezielt.	
sehr hoch	"Contractual obligations with customers regarding transparency of supply chain risks are fulfilled. (C, I, A)"	Nicht betroffen	Vertraglich.	Einkauf/Lieferantenmanagement

Gesamteinstufung: Teilweise degradiert (1 von 5 Anforderungen betroffen bei normalem Schutzbedarf; 4 von 8 ab hoch; 4 von 10 inkl. sehr hoch), unabhängig vom Schutzbedarf. Bei sehr hohem Schutzbedarf wird die Selbstauskunfts-Schwäche durch die Drittaudit-Pflicht (TISAX®-Label) explizit und wirksam geschlossen — die Gesamteinstufung bleibt dennoch "Teilweise degradiert", weil die beiden Monitoring-Anforderungen bei hoch unabhängig von der Nachweisart nur "regelmäßig" geprüft werden müssen. Praktisch: fordern Sie bei kritischen Lieferanten aktiv ein TISAX®-Label oder gleichwertiges Drittaudit ein, statt sich auf Selbstauskünfte zu verlassen — dies ist der wirksamste Einzelhebel in diesem Control.
Härtungsverweis: MHC-14 (siehe Teil II)

6.1.2 — To what extent is non-disclosure regarding the exchange of information contractually agreed?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The non-disclosure requirements are determined and fulfilled."	Nicht betroffen	Rechtlich.	Rechtsabteilung
must	"Requirements and procedures for applying non-disclosure agreements are known to all persons passing on information in need of protection."	Nicht betroffen	Kommunikation/Awareness.	Rechtsabteilung
must	"Valid non-disclosure agreements are concluded prior to forwarding sensitive	Nicht betroffen	Rechtliches Gate.	Rechtsabteilung

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	information."			
must	"The requirements and procedures for the use of non-disclosure agreements and the handling of information requiring protection are reviewed at regular intervals."	**Teilweise degradiert**	Zeitkompression: umfasst ausdrücklich auch die *operativen* Verfahren zum Umgang mit schutzbedürftigen Informationen (nicht nur den Vertragstext) — eine veraltete Handhabungsanleitung ohne Anlassbezug ist ein technisch-operatives, nicht rein rechtliches Risiko.	Rechtsabteilung
should	"Non-disclosure agreement templates are available and checked for legal applicability."	Nicht betroffen	Rechtlich.	Rechtsabteilung
should	"Non-disclosure agreements include the persons/organizations involved, the type of information covered by the agreement, the subject of the agreement, the validity period of the agreement and the responsibilities of the obliged party."	Nicht betroffen	Rechtlicher Mindestinhalt.	Rechtsabteilung
should	"Non-disclosure agreements include provisions for the handling of sensitive information beyond the contractual relationship."	Nicht betroffen	Rechtlich.	Rechtsabteilung
should	"Options of demonstrating compliance with specifications (e.g., review by an independent third-	Nicht betroffen	Vertraglicher Mechanismus.	Rechtsabteilung

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	party or audit rights) are defined."			
should	"A process for monitoring the validity period of temporary non-disclosure agreements and initiating their extension in due time is defined and implemented."	Nicht betroffen	"In due time" bezieht sich auf ein bekanntes Ablaufdatum — ein kalendergetriebener, kein vager periodischer Auslöser.	Rechtsabteilung

Gesamteinstufung: Teilweise degradiert (1 von 9 Anforderungen betroffen), unabhängig vom Schutzbedarf. Einziger Befund in einem sonst rein rechtlich geprägten Control — betrifft gezielt die operative Handhabungsanleitung, nicht den Vertragstext selbst.
Härtungsverweis: MHC-10 (siehe Teil II)

6.1.3 — To what extent are the responsibilities between external IT service providers and the own organization defined?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"The IT services concerned are identified."	Nicht betroffen	Scoping.	Einkauf/Lieferantenmanagement
must	"The security requirements relevant to the IT service are determined."	Nicht betroffen	Governance.	Einkauf/Lieferantenmanagement
must	"The organization responsible for implementing the requirement is defined and aware of its responsibility."	Nicht betroffen	Governance/Accountability.	Einkauf/Lieferantenmanagement
must	"Mechanisms for shared responsibilities are specified and implemented."	Nicht betroffen	Governance.	Einkauf/Lieferantenmanagement
must	"The responsible organization fulfils its respective responsibilities."	Nicht betroffen	Erfüllungsebene, kein spezifischer Mechanismus zur Bewertung genannt.	Einkauf/Lieferantenmanagement
should	"In case of IT services,	Nicht	Dokumentation.	IT-Betrieb

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	configuration has been conceptualized, implemented, and documented based on the necessary security requirements."	betroffen		
should	"The responsible staff is adequately trained."	Nicht betroffen	Schulung zu Verantwortlichkeiten, thematisch getrennt von der Phishing-Awareness aus 2.1.3.	Personalabteilung
hoch	"A list exists indicating the IT services concerned and the respective responsible IT service providers. (C, I, A)"	Nicht betroffen	Inventar.	Einkauf/Lieferantenmanagement
hoch	"The applicability of the ISA controls has been evaluated and documented. (C, I, A)"	Nicht betroffen	Governance/Scoping (die TISAX®-Anwendbarkeitsprüfung selbst).	CISO-Funktion
hoch	"The service configuration is included in the regular security assessments. (C, I, A)"	**Teilweise degradiert**	Zeitkompression: periodische statt kontinuierliche Einbindung in Sicherheitsbewertungen lässt Konfigurationsabweichungen bei extern betriebenen Diensten zwischen den Zyklen unentdeckt — konsistent mit dem Audit-Zyklus-Befund aus 5.2.6.	Einkauf/Lieferantenmanagement
hoch	"Proof is provided that the IT service providers fulfil their responsibility. (C, I, A)"	**Teilweise degradiert**	Fähigkeitsentkopplung: unspezifizierter "Nachweis" ohne Vorgabe unabhängiger Verifikation importiert	Einkauf/Lieferantenmanagement

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
			dieselbe Dokumenten-Echtheitslücke wie in 6.1.1.	
hoch	"Integration into local protective measures (such as secure authentication mechanisms) is established and documented. (C, I, A)"	**Teilweise degradiert**	Verweist auf "sichere Authentisierungsmechanismen" ohne explizite Phishing-Resistenz-Pflicht — importiert dieselbe Lücke wie 4.1.2.	IAM-Team

Gesamteinstufung: Bei normalem Schutzbedarf Nicht betroffen (0 von 7 Anforderungen betroffen). Ab hohem Schutzbedarf kommen drei zusätzliche Anforderungen hinzu (regelmäßige Einbindung in Sicherheitsbewertungen, unabhängig verifizierbarer Verantwortungs-Nachweis, sichere Authentisierungs-Integration) — Gesamteinstufung wird **Teilweise degradiert** (3 von 12). Praktisch: betrifft nur Dienstleister-Beziehungen für Werte mit hohem/sehr hohem Schutzbedarf; bei normalem Schutzbedarf besteht kein Mythos-spezifischer Zusatzbedarf.
Härtungsverweis: MHC-10, MHC-03, MHC-14 (siehe Teil II)

Zusammenfassung Kapitel 6

Control	Gesamteinstufung	Anteil betroffen
6.1.1	Teilweise degradiert	1/5 → 4/10
6.1.2	Teilweise degradiert	1/9
6.1.3	Nicht betroffen → ab hoch: Teilweise degradiert	0/7 → 3/12

Durchgängiges Kapitelmuster: Lieferantensicherheit stützt sich stark auf eingereichte Dokumente/Selbstauskünfte, deren Fälschungssicherheit durch KI-Werkzeuge sinkt. TISAX® schließt dies bei sehr hohem Schutzbedarf (6.1.1) explizit über die Pflicht zum unabhängigen Drittaudit — der wirksamste Einzelhebel im ganzen Kapitel.

Kapitel 7 — Compliance (2 Controls, 6 Anforderungen)

7.1.1 — To what extent is compliance with regulatory and contractual provisions ensured?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Legal, regulatory, and contractual provisions of relevance to information security (see examples) are determined at regular intervals."	Nicht betroffen	Reiner Rechtslage-Scan: Gesetzgebung ändert sich nicht im Tempo eines automatisierten Angriffs — die periodische Betrachtung ist hier sachgerecht, nicht Zeitkompressions-relevant.	Rechtsabteilung
must	"Policies regarding compliance with the provisions are defined, implemented, and communicated to the responsible persons."	Nicht betroffen	Governance/Kommunikation.	Rechtsabteilung
should	"The integrity of records in accordance with legal, regulatory, and contractual provisions and business requirements is considered."	Nicht betroffen	Governance-Ebene (Berücksichtigung), kein konkreter technischer Mechanismus benannt.	Rechtsabteilung

Gesamteinstufung: Nicht betroffen (0 von 3 Anforderungen betroffen), unabhängig vom Schutzbedarf.

7.1.2 — To what extent is the protection of personal data considered when implementing information security?

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
must	"Legal and contractual information security	Nicht betroffen	Rechtlich.	Rechtsabteilung

Ebene	Anforderung (Originalwortlaut)	Kategorie	Begründung	Verantwortlich
	requirements regarding the procedures and processes in the processing of personal data are determined."			
must	"Regulations regarding the compliance with legal and contractual requirements for the protection of personal data are defined and known to the involved persons."	Nicht betroffen	Rechtlich/Kommunikation.	Rechtsabteilung
must	"Processes and procedures for the protection of personally identifiable information are considered in the information security management system."	Nicht betroffen	Governance-Verknüpfung ISMS/Datenschutz.	Rechtsabteilung/ CISO-Funktion

Gesamteinstufung: Nicht betroffen (0 von 3 Anforderungen betroffen), unabhängig vom Schutzbedarf.

Zusammenfassung Kapitel 7

Control	Gesamteinstufung	Anteil betroffen
7.1.1	Nicht betroffen	0/3
7.1.2	Nicht betroffen	0/3

Kapitel 7 ist vollständig Nicht betroffen — sauberes Beispiel für originär rechtlich/regulatorisch geprägte Controls außerhalb des Mythos-Wirkbereichs.

Phase 1 abgeschlossen: Gesamtübersicht aller 7 Kapitel

Verteilung je Kapitel (Gesamteinstufung dominant, normaler Schutzbedarf)

Kapitel	Controls	Standfest	Teilweise degradiert	Reine Reibung	Nicht betroffen
1. IS Policies and Organization	14	0	10	0	4 (davon 1 wird ab hoch Degradiert)
2. Human Resources	4	0	2	0	2 (davon 1 wird ab hoch Standfest)
3. Physical Security	3 (+1 ohne Anforderungen)	0	2	0	1 (wird ab hoch Standfest; zusätzlich wird 1 der 2 Degradiert-Controls [3.1.4] ab hoch ebenfalls Standfest, siehe dort)
4. Identity and Access Management	4	0	2	1	1 (wird ab hoch Degradiert)
5. IT Security/Cyber Security	15	4	8	0	3 (davon 1 wird ab hoch Degradiert)
6. Supplier Relationships	3	0	2	0	1 (wird ab hoch Degradiert)
7. Compliance	2	0	0	0	2
Summe (45 Controls)	**45**	**4 (9 %)**	**26 (58 %)**	**1 (2 %)**	**14 (31 %)**

Einordnung der Verteilung

TISAX® enthält einen einzigen Reine-Reibung-Fall (4.1.2, Passwort-only-Authentisierung ohne zweiten Faktor) — praktisch alle übrigen auch stark betroffenen Controls verlieren ihre Kernwirkung nicht vollständig, sie degradieren auf "Teilweise degradiert". Der Standfest-Anteil ist mit 9 % vergleichsweise gering — das Modul "Information Security" ist überwiegend prozess-/organisationslastig formuliert (viele Governance-Anforderungen ohne konkreten technischen Mechanismus). Der Standfest-Anteil konzentriert sich fast vollständig auf Kapitel 5 (Kryptografie, Segmentierung, Mandantentrennung, Redundanz) — dort, wo TISAX® explizit technische/architektonische Anforderungen stellt.

Wiederkehrende Musterkategorien (Vorschau auf Phase 2)

Über alle Kapitel hinweg lassen sich die 26 Teilweise-degradiert- und der eine Reine-Reibung-Befund vier bis fünf wiederkehrenden Ursachen zuordnen, die in Phase 2 zu Clustern verdichtet werden:

1. **Periodische statt anlassbezogene Prüfung** (Zeitkompression) — betrifft Policy-Reviews, Software-Freigaben, Zugriffsrechte-Reviews, Log-Auswertung, Schwachstellen-/Patch-Management, System-/Service-Audits, Backup-Konzept-Überprüfung, Lieferanten-Monitoring. Der mit Abstand häufigste Einzelbefund.
2. **Kollaps des Patch-Gap-Fensters** — Risikobewertung und Patch-Geschwindigkeit ohne Berücksichtigung KI-beschleunigter Exploit-Entwicklung (5.2.5, 5.2.6).
3. **Fehlende Pflicht zu phishing-resistenter Authentisierung** — durchgängig in Authentisierungs- und Fernzugriffs-Controls (4.1.2 — hier als Reine Reibung beim reinen Passwortfaktor, sonst als Teilweise degradiert —, 5.1.2, 5.2.7, 6.1.3).
4. **Dokumenten-/Nachweisfälschung durch KI** (Fähigkeitsentkopplung) — Einstellungsverfahren (2.1.1), Lieferantennachweise (6.1.1, 6.1.3), Compliance-Dokumentation.
5. **Signaturbasierte Erkennung** (Fähigkeitsentkopplung) — Malware-Schutz (5.2.3).

Diese fünf Cluster decken die häufigsten, aber nicht alle betroffenen Anforderungen ab.

Musterbildung und Lückenanalyse (Phase 2 und 3)

Analyseeinheit: Die Kapitel-Zusammenfassungen zählen 26 Controls mit Gesamteinstufung "Teilweise degradiert" und 1 Control mit "Reine Reibung" (27 von 45) — diese Zahl bezieht sich auf die Gesamteinstufung je Control bei *normalem* Schutzbedarf und bildet mehrere gleichzeitig vorliegende Befund-Ursachen pro Control nicht ab (z. B. 4.1.2: sowohl fehlende Phishing-Resistenz als auch reine Zeitkompression, je nach Schutzbedarfsstufe). 4 weitere Controls (1.2.2, 4.1.1, 5.2.9, 6.1.3) sind bei normalem Schutzbedarf unauffällig, degradieren aber bei hoch/sehr hoch und tauchen in der 27er-Zahl entsprechend nicht auf, obwohl sie einzelne betroffene Anforderungen enthalten. Die Musterbildung arbeitet daher auf Ebene der **74 einzelnen betroffenen Anforderungen** (73 Teilweise degradiert + 1 Reine Reibung) über **31 distinkte Controls**, nach demselben Extraktionsverfahren aus dem Dokumenttext geparst wie die Prioritäten-Tabelle im Anhang. Dieser Wert wurde bei der Überarbeitung von ursprünglich 71 auf 72 und mit Version 1.1 auf 74 korrigiert: Der frühere Kompakter-Index hatte bei Control 1.4.1 eine der beiden betroffenen Anforderungen (should-Ebene, Bewertungskriterien) nicht erfasst, obwohl Kapitel 1 selbst diese bereits korrekt als Teilweise degradiert auswies; mit Version 1.1 kommen zwei weitere Einzelbefunde aus Control 1.6.3 hinzu, die aus der primärquellenbasierten Neubewertung der dortigen redaktionellen Katalog-Duplikate resultieren (siehe Methodik, Datenqualitäts-Hinweis).

Methodisches Vorgehen: Die acht Cluster wurden induktiv aus den 74 Einzelbefunden gebildet, nicht aus einem vorab festgelegten Kategorienraster abgeleitet. Jeder Einzelbefund wurde zunächst anhand seiner Begründung aus Kapitel 1–7 einzeln betrachtet; erst wiederkehrende Ursachenmuster (z. B. "periodisch statt anlassbezogen") wurden anschließend zu einem benannten Cluster zusammengefasst. Die Clusterzahl acht ist damit ein empirisches Ergebnis dieser konkreten Analyse, keine methodische Vorgabe — ein anderer TISAX®-Modul oder ein anderer Anforderungskatalog könnte zu einer anderen Clusterzahl führen.

Cluster-Übersicht

Cluster	Funde	Controls	Kapitel	Dominantes Kriterium
1. Periodische statt anlassbezogene Prüfung	19	12 (1.1.1, 1.2.1, 1.3.1, 1.3.3, 1.3.4, 1.5.1, 1.6.3, 4.1.3, 4.2.1, 5.2.9, 6.1.2, 6.1.3)	1, 4, 5, 6	Zeitkompression
2. Kollaps des Patch-Gap-Fensters / Ransomware-Resilienz	9	4 (1.3.4, 5.2.5, 5.2.6, 5.2.8)	1, 5	Zeitkompression
3. Fehlende phishing-resistente	10	6 (4.1.1, 4.1.2, 4.1.3, 5.1.2, 5.2.7, 6.1.3)	4, 5, 6	Fähigkeitsentkopplung /

Cluster	Funde	Controls	Kapitel	Dominantes Kriterium
Authentisierung				Zeitkompression
4. KI-gestützte Identitäts- und Dokumentenfälschung	11	5 (2.1.1, 2.1.3, 3.1.1, 6.1.1, 6.1.3)	2, 3, 6	Fähigkeitsentkopplung
5. Signaturbasierte Erkennung vs. KI-Schadsoftware	5	1 (5.2.3)	5	Fähigkeitsentkopplung
6. Aggregationsresistenz	4	4 (1.6.1, 1.6.3, 5.2.4, 5.2.7)	1, 5	Aggregationsresistenz
7. Autonome KI-Agenten unterlaufen Freigabeprozesse	4	2 (1.3.3, 1.3.4)	1	Fähigkeitsentkopplung
8. Fehlende Automatisierungspflicht in der Reaktion	4	1 (1.6.2)	1	Zeitkompression
Einzelbefunde (kein wiederkehrendes Muster)	8	6 (1.2.2, 1.4.1, 1.6.3, 3.1.4, 5.1.2, 5.3.1)	1, 3, 5	—

Summe: 74. Cluster 1 (Periodische Prüfung) ist mit weitem Abstand der größte und deckt vier von sieben Kapiteln ab — die Zeitkompressions-Lücke ist kein Einzelphänomen einzelner Fachbereiche, sondern ein strukturelles Muster über CISO-Funktion, IT-Betrieb, IAM und Einkauf hinweg.

Lückenanalyse gegenüber sechs Vergleichsrahmen

Methodik: Für jeden Cluster wird geprüft, ob NIST CSF 2.0, BSI C5:2026, DORA, CRA, NIS2-Richtlinie/DVO und ISA/IEC 62443-2-1:2024 dieselbe strukturelle Lücke bereits schließen. Das ist ein Vergleich auf Ebene der regulatorischen/normativen Grundhaltung (Reifegrad der Best Practice), keine Aussage darüber, ob ein Unternehmen diesen sechs Rahmenwerken formal unterliegt — DORA adressiert Finanzunternehmen und ihre kritischen IKT-Dienstleister, CRA adressiert Hersteller von Produkten mit digitalen Elementen, NIS2 wesentliche/wichtige Einrichtungen bestimmter Sektoren. Die Einordnung basiert auf einer Web-Recherche vom Juli 2026 zu den öffentlich verfügbaren Texten und Sekundärquellen; sie ersetzt keine klauselgenaue Zertifizierungsprüfung.
Legende: ✓ = adressiert die Lücke explizit und mit verbindlicher Frist/Methode · **~** = mildert die Lücke, schließt sie aber nicht vollständig · ✗ = teilt dieselbe strukturelle Lücke · **n/a** = außerhalb des sachlichen Geltungsbereichs des Rahmenwerks

Cluster	NIST CSF 2.0	BSI C5:2026	DORA	CRA	NIS2-RL/DVO	ISA/IEC 62443-2-1:2024
1. Periodische Prüfung	~	~	✓ (Meldewesen)	n/a	~	~
2. Patch-Gap/Ransomware	~	~[2]	~	✓ (Offenlegung)	~	~
3. Phishing-resistente Auth	~	n/a[1]	~	n/a	~	~
4. Dokumentenfälschung	✗	n/a[1]	✓ (Lieferanten)	n/a	~	n/a[1]
5. Signaturbasierte Erkennung	~[1]	n/a[1]	n/a[1]	n/a	n/a[1]	~[1]
6. Aggregationsresistenz	~	n/a[1]	n/a[1]	n/a	n/a[1]	~
7. Autonome KI-Agenten	✗	✗	✗	✗	✗	✗
8. Automatisierungspflicht Reaktion	~	~	✓ (faktisch)	~ (faktisch)	~	~

[1] Für diese Zellen konnte in der Recherche keine hinreichend konkrete, zitierfähige Einzelvorgabe verifiziert werden; Einstufung ist vorsichtig/tendenziell, nicht klauselscharf.

[2] Gilt nur für die Schwachstellen-Fristen-Hälfte des Clusters: C5:2026 OPS-25.01AC verlangt einen definierten, überwachten, CVSS-gebundenen Fristenrahmen für die Behebung von Schwachstellen, verbindlich ab Prüfzeiträumen ab 1. Juni 2027 — diese strukturelle Anforderung ist über mehrere Sekundärquellen bestätigt. Die konkreten CVSS-gestaffelten Beispiel-Fristwerte im Kriterienkatalog selbst konnten dagegen nicht direkt am BSI-Primärdokument verifiziert werden (der PDF-Volltext war technisch nicht extrahierbar); eine geprüfte Sekundärquelle nennt hierzu abweichende Werte. Sie werden deshalb hier bewusst nicht beziffert. Die Ransomware-/Backup-Unveränderlichkeits-Hälfte (Control 5.2.8) bleibt auch unter dieser vorsichtigeren Einordnung offen: Die Kriterien OPS-06 bis OPS-09 verlangen Verschlüsselung, RTO/RPO-Ausrichtung, Monitoring und regelmäßige Restore-Tests, aber an

keiner Stelle Unveränderlichkeit/WORM — der Begriff "immutable" kommt im gesamten Kriterienkatalog nur im Kontext von Container-Images vor (OPS-26), nicht bei Backups.

Die wichtigsten Einzelbefunde:

Cluster 2 (Patch-Gap/Ransomware) ist beim Schwachstellen-Fristen-Aspekt der am klarsten geschlossene Fall, bei der Backup-Unveränderlichkeit dagegen nicht: BSI C5:2026 (verbindlich ab Prüfzeiträumen ab 1. Juni 2027) verlangt in Kriterium OPS-25.01AC einen definierten und überwachten, CVSS-gebundenen Fristenrahmen für die Behebung von Schwachstellen (siehe Fußnote 2 zur Quellenlage der genauen Fristwerte). Das ist exakt die Präzisierung, die den vagen TISAX®-Formulierungen fehlt — "adequate patch management" ohne Geschwindigkeits-SLA (5.2.5, should) und "appropriate timeframe" (5.2.6, must) —, und bestätigt unabhängig, dass der hier diagnostizierte Patch-Gap-Kollaps kein Sonderfall dieser Analyse ist, sondern von einer deutschen Aufsichtsbehörde bereits 2026 als Regulierungslücke behandelt wurde. Für die Backup-Unveränderlichkeit gilt das nicht: Die C5:2026-Kriterien OPS-06 bis OPS-09 (Data Backup and Recovery) verlangen Verschlüsselung, RTO/RPO-Ausrichtung, Monitoring und mindestens jährliche, bei Verschärfung tägliche Restore-Tests — der Begriff "immutable" taucht im gesamten Kriterienkatalog nur im Kontext von Container-Images auf (OPS-26), nicht bei Backups. Die in Control 5.2.8 diagnostizierte Lücke bleibt insofern auch gegenüber C5:2026 offen. Der CRA verpflichtet Hersteller zusätzlich zu einer 24-Stunden-Meldung aktiv ausgenutzter Schwachstellen an ENISA, mit Folgebericht nach 72 Stunden und Abschlussbericht 14 Tage nach Verfügbarkeit einer Abhilfemaßnahme — bindend ab 11. September 2026. Das betrifft die Offenlegungspflicht für das eigene Produkt, nicht das interne Patch-Management der IT-Umgebung, ist aber ein Präzedenzfall für taktgebundene statt vage formulierte Fristen.

Cluster 3 (Phishing-Resistenz) zeigt eine feinere Nuance: NIS2 Art. 21(2)(j) verlangt als erstes EU-Recht überhaupt namentlich Multi-Faktor- oder kontinuierliche Authentisierung — schließt also die "gar kein zweiter Faktor"-Lücke. Die AITM-Relay-Lücke (Echtzeit-Phishing hebelt OTP/Push aus) bleibt jedoch bestehen, weil weder NIS2 noch die übrigen fünf Rahmenwerke im Kerntext ausdrücklich phishing-resistente Verfahren (FIDO2/WebAuthn) vorschreiben. Diese Präzisierung existiert bislang nur in sekundären technischen Leitfäden (z. B. NIST SP 800-63B, AAL3) — TISAX® ISA 2027 teilt diese Lücke also mit der Mehrheit der Vergleichsrahmen, nicht nur mit sich selbst.

Cluster 4 (Dokumentenfälschung) zeigt eine belastbare Rangfolge unter den Vergleichsrahmen selbst: DORA Art. 30(3) — sektorspezifischer Referenzrahmen für Finanzunternehmen und ihre kritischen IKT-Dienstleister, siehe Methodik oben — verlangt ein uneingeschränktes Prüf- und Zugangsrecht und stellt ausdrücklich klar, dass vorgelegte Zertifizierungen die eigene Prüfung "unterstützen, aber nicht ersetzen". NIS2 Art. 21(2)(d)/(3) i. V. m. NIS2-DVO Nr. 5.1.4 verlangt ebenfalls eine dokumentierte Lieferantenbewertung mit vertraglich verankerten Prüfrechten bzw. Zugang zu Prüfberichten — mit Verhältnismässigkeits-Spielraum ("wo angemessen") statt DORAs uneingeschränktem Anspruch, jedoch ohne dass Standardzertifikate (ISO 27001, SOC 2 Type II, TISAX®-Assessment, CSA STAR) diese Prüfrechte ausdrücklich ersetzen dürften. TISAX® ISA 2027 bleibt mit reiner Selbstauskunft/Attestierung die schwächste der drei Vorgaben. Für

den Personalprozess (2.1.1: Deepfake-Identität im Bewerbungsverfahren) findet sich in keinem der sechs Rahmenwerke eine Entsprechung — dieser Teil des Clusters bleibt vollständig TISAX®-originär.

Cluster 7 (Autonome KI-Agenten) ist der einzige Cluster, bei dem alle sechs Vergleichsrahmen dieselbe Lücke wie TISAX® ISA 2027 teilen — und das ist selbst durch aktuelle Recherche belegt, nicht nur angenommen: Weder NIST AI RMF noch ISO/IEC 42001 noch der EU AI Act enthalten bislang eine Referenz auf "Agent"/"agentisch"/autonome KI-Systeme. NIST hat dies selbst erkannt und im Februar 2026 die "AI Agent Standards Initiative" gestartet (937 eingegangene Stellungnahmen auf ein Request for Information); ein "AI Agent Interoperability Profile" ist frühestens für Q4 2026 angekündigt — nach dem Stand dieser Analyse also noch nicht verfügbar. Der hier diagnostizierte Befund (1.3.3, 1.3.4: KI-Assistenten rufen externe Dienste/Pakete eigenständig auf, ohne dass ein Mensch das konkrete Werkzeug je zur Freigabe vorgelegt hat) ist damit keine TISAX®-Eigenheit, sondern eine Lücke an der Front der Regulierung insgesamt. Ein zweiter, engerer NIST-Ansatz befindet sich ebenfalls noch im Entwurfsstadium: Das NIST Cyber AI Profile (NIST IR 8596) veröffentlichte im Dezember 2025 einen ersten Entwurf mit Kommentierungsfrist bis Ende Januar 2026; der Bearbeitungsstand ist laut der NIST-eigenen Projektseite zum Zeitpunkt dieser Analyse "Reviewing Comments" — ein finaler Text liegt nicht vor, und ein von Sekundärquellen behaupteter ausdrücklicher Agentenbezug ließ sich nicht gegen den NIST-Primärtext verifizieren (siehe Teil II, MHC-13, Abschnitt 2). Der MHC-Katalog in Teil II geht an dieser Stelle bewusst über die reine TISAX®-Diagnose hinaus (siehe Abschnitt "Originäre Ergänzungen jenseits von TISAX®" unten).

Cluster 5 (Signaturbasierte Erkennung) und Cluster 6 (Aggregationsresistenz) liessen sich nicht mit vergleichbarer Präzision verifizieren: Die Recherche fand keine hinreichend konkrete, zitierfähige Einzelvorgabe zu verhaltensbasierter/KI-gestützter Malware-Erkennung oder zur expliziten Pflicht, bewusst fragmentierte Angriffsketten zu erkennen, in einem der sechs Rahmenwerke. ISA/IEC 62443-2-1:2024 erwähnt in Sekundärquellen "behavioral analytics" und "continuous monitoring for anomaly detection" als Erweiterung gegenüber der Vorversion, ohne dass sich daraus eine scharfe, zitierfähige Pflicht ableiten ließ. Diese beiden Cluster werden daher vorsichtiger eingestuft (~ statt ✓) als die übrigen.

Einzelbefunde außerhalb der Cluster

8 Anforderungen über 6 Controls ließen sich keinem wiederkehrenden Muster zuordnen: 1.2.2 (Rollentrennung durch KI-Doppelrolle unterlaufen), 1.4.1 (veraltete Eintrittswahrscheinlichkeits-Annahmen in der Risikomethodik — sowohl auf Ebene der Bewertung selbst als auch der zugrunde liegenden Bewertungskriterien, 2 Anforderungen), 1.6.3 hoch (KI-orchestrierte Szenarien in der Krisenplanung nicht vorgesehen, inklusive der redaktionell doppelt geführten zweiten Katalogfassung, 2 Anforderungen), 3.1.4 (PIN/Passwort als Rückfalloption bei fehlender Verschlüsselungspflicht), 5.1.2 must (unspezifische Maßnahmen für Fernzugriff ohne Mindeststandard), 5.3.1 (Re-Identifizierung pseudonymisierter Daten durch KI-gestützte Korrelation). Für Einzelbefunde ohne wiederkehrendes Muster ist eine Sechs-Rahmen-Lückenanalyse nicht aussagekräftig; sie bleiben mit ihrer vollständigen Begründung in Kapitel 1–

7 verankert und fließen als eigenständige Einzelmaßnahmen direkt in den MHC-Katalog (Phase 4) ein.

Einordnung für Phase 4

Cluster	Einordnung	Empfehlung für MHC
1. Periodische Prüfung	Industrieweit teilweise adressiert	An CSF-Kontinuierlichkeitsprinzip (DE.CM) und NIS2-Sprache ("weg von periodischen Momentaufnahmen") anlehnen, aber TISAX®-spezifisch zu einem einzigen anlassbezogenen Grundprinzip verdichten — 12 betroffene Controls brauchen keine 12 verschiedenen Formulierungen
2. Patch-Gap/Ransomware	Patch-Fristen industrieweit gelöst, Backup-Unveränderlichkeit weiterhin offen	Bei Patch-Fristen eng an BSI-C5:2026-Prinzip anlehnen (definierter, CVSS-gebundener Fristenrahmen statt "adequate"/"appropriate"); Backup-Unveränderlichkeit erfordert trotz C5:2026-Prüfung eine eigenständige MHC-Vorgabe
3. Phishing-resistente Auth	Industrieweit teilweise adressiert	NIS2 benennt MFA/Continuous Authentication bereits namentlich als geeignete Maßnahme; die Phishing-Resistenz-Präzisierung (FIDO2/WebAuthn) muss der MHC selbst liefern, kein Rahmenwerk schreibt sie bereits verbindlich vor
4. Dokumentenfälschung (Lieferanten)	Industrieweit teilweise adressiert	DORA-Prinzip (sektorspezifisch: Finanzsektor) "Zertifikat ersetzt nicht eigene Prüfung" übernehmbar
4. Dokumentenfälschung (Personal und Zutritt, inkl. 3.1.1)	TISAX®-originär	Kein Vergleichsrahmen einschlägig — eigenständige MHC-Entwicklung nötig (Deepfake-Verifikation im Einstellungs- und Zutrittsprozess)
5. Signaturbasierte Erkennung	Überwiegend originär	Ansatzpunkt bei IEC-62443-2-1-Verhaltensanalytik, im Kern aber eigenständige MHC-Formulierung
6. Aggregationsresistenz	Überwiegend originär	Kein Rahmenwerk mit scharfer Vorgabe gefunden — eigenständige MHC-Entwicklung
7. Autonome KI-Agenten	Universell ungelöst	Größte Chance für einen genuin vorlaufenden MHC-Beitrag — selbst NIST ist hier erst am Anfang (Ergebnis frühestens Q4 2026)
8. Automatisierungspflicht	Industrieweit	DORA-Prinzip (sektorspezifisch: Finanzsektor)

Cluster	Einordnung	Empfehlung für MHC
Reaktion	faktisch adressiert	übernehmbar: harte Frist statt weiche Pflicht erzwingt Automatisierung faktisch, ohne sie wörtlich zu verlangen

Cluster 8 und die Patch-Fristen-Hälfte von Cluster 2 sind die "leichtesten" Fälle für Phase 4 — die Lösung existiert bereits außerhalb von TISAX® und muss nur übernommen werden; die Backup-Unveränderlichkeits-Hälfte von Cluster 2 erfordert dagegen trotz Prüfung eine eigenständige Formulierung. Cluster 7 ist der wertvollste Einzelbefund dieser Analyse: eine Lücke, die derzeit kein einschlägiges Rahmenwerk schließt, wodurch ein MHC-Beitrag hier tatsächlich neuen Boden beschreibt statt bereits vorhandene Praxis nur zu spiegeln.

Originäre Ergänzungen jenseits von TISAX®

Der MHC-Katalog in Teil II ist mit einer Ausnahme durchgängig aus einem konkreten TISAX®-Anforderungsbefund dieses Dokuments abgeleitet (siehe Methodik, "Was diese Analyse ist — und was nicht"). Bei einem Thema wird diese Grenze bewusst und ausdrücklich überschritten: der Absicherung von KI-Agenten.

Anlass: Cluster 7 zeigt, dass TISAX® ISA 2027 KI-Agenten nur an zwei Stellen berührt (1.3.3, 1.3.4 — nicht geprüfte Werkzeug-/Diensteinbindung) und dass diese Lücke von keinem der sechs Vergleichsrahmen aus Phase 3 geschlossen wird. Ein Abgleich mit der OWASP Top 10 for Agentic Applications (ASI01–ASI10, Stand Juni 2026) — einer eigens für KI-Agenten entwickelten, community-basierten Bedrohungstaxonomie — zeigt, dass der ursprünglich aus Cluster 7 abgeleitete MHC-13 nur eine dieser zehn Bedrohungskategorien vollständig und zwei weitere teilweise abdeckte. Sieben Kategorien blieben unadressiert — nicht weil sie für Unternehmen irrelevant wären, sondern weil TISAX® ISA 2027 sie an keiner Stelle konkret genug anspricht, um daraus einen eigenständigen Befund abzuleiten.

Vorgehen: Teil II erweitert MHC-13 um vier zusätzliche Mindeststandards — (a) Agenten-Identität/NHI-Governance, (b) Grundhärtung gegen Prompt Injection, (c) Kill-Switch, (d) kontinuierliche Neubewertung freigegebener Komponenten — und ergänzt ein neues, eigenständiges MHC-16 (Multi-Agent-Integrität) für Bedrohungen, die eine Architektur mit mehreren kommunizierenden Agenten voraussetzen. Damit deckt der Katalog acht der zehn OWASP-ASI-Kategorien ab (ASI01, ASI02, ASI03, ASI04, ASI05 über MHC-13; ASI06, ASI07, ASI08 über MHC-16). Zwei Kategorien bleiben auch nach dieser Erweiterung unadressiert: ASI09 (Human-Agent Trust Exploitation) und ASI10 (Rogue Agents) — das wird hier bewusst offen benannt, statt stillschweigend als gelöst zu behandeln.

Warum diese Kennzeichnung wichtig ist: Der methodische Wert von MRIS liegt darin, dass jede Einstufung auf einen konkreten, zitierfähigen TISAX®-Anforderungstext zurückgeführt werden kann (siehe Methodik, "Reproduzierbarkeit"). Die hier beschriebenen Ergänzungen erfüllen dieses Kriterium nicht — sie sind fachliches Urteil des Autors auf Basis externer Bedrohungsforschung (primär OWASP), keine aus einem TISAX®-Anforderungstext destillierte Diagnose. Diese Sektion sowie MHC-13 und MHC-16 (jeweils Abschnitt 9) in Teil II kennzeichnen

deshalb durchgängig, welcher Teil TISAX®-abgeleitet und welcher originär ist, damit beide Kategorien nicht vermischt werden. Die "74 Einzelbefunde über 31 Controls" der Kernanalyse (siehe Management Summary) bleiben von dieser Erweiterung unberührt.

Regulatorischer Ausblick: Das NIST Cyber AI Profile (NIST IR 8596) befindet sich zum Zeitpunkt dieser Analyse noch im Entwurfsstadium (Status "Reviewing Comments", siehe Cluster 7 oben) und war zu keinem Zeitpunkt zitierfähig genug, um daraus eine TISAX®-vergleichbare Anforderung abzuleiten. Sollte NIST IR 8596 oder ein künftiges TISAX®-ISA-Release Agenten-Sicherheit ausdrücklich adressieren, wären die hier originär ergänzten Inhalte zu überprüfen und gegebenenfalls in eine TISAX®-abgeleitete Klassifikation zu überführen.

Anhang: Prioritäten-Tabelle und Standard-Querverweise

Dieser Anhang enthält zwei ergänzende Übersichten zu Kapitel 1–7: eine Prioritäten-Tabelle aller Einzelbefunde mit Handlungsbedarf samt MHC-Verweis für die Umsetzung, sowie die Zuordnung jedes Controls zu ISO 27001/27017, ISA/IEC 62443-2-1 und NIST CSF 2.0 als Vorarbeit für die Lückenanalyse in Phase 2 und 3.

SGA-Nachtrag: 10 der 330 ausgewiesenen Anforderungen (Ebene "SGA") wurden nachträglich ergänzt und waren nicht Teil der ursprünglichen 320-Anforderungen-Zählung von Phase 1 — betroffen: 1.1.1, 1.2.1, 1.2.2, 1.5.1 (4), 1.5.2 (2), 1.6.2. Sie gelten unabhängig vom Schutzbedarf, ausschließlich bei Simplified Group Assessment.

Standard-Querverweise je Control

Control	Referenz zu anderen Standards (ISO 27001/27017, ISA/IEC 62443-2-1, NIST CSF 2.0)
1.1.1	ISO 27001:2022: A.5.1 ; ISA/IEC 62443-2-1: 6.2.1 ; NIST CSF 2.0: GV.PO-1, GV.PO-2
1.2.1	ISO 27001:2022: 4, 9.3 ; NIST CSF 2.0: GV.OC-01, GV.OC-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.RM-01, ID.IM-01, ID.IM-03, ID.IM-04
1.2.2	ISO 27001:2022: A.5.2, A.5.3 ; ISA/IEC 62443-2-1: 6.2.3, 6.2.5 ; NIST CSF 2.0: GV.RR-02, GV.RR-03
1.2.3	ISO 27001:2022: A.5.8 ; NIST CSF 2.0: GV.OC-04
1.3.1	ISO27001:2022: A.5.9 ; ISA/IEC 62443-2-1: 7.2.1 ; NIST CSF 2.0: ID.AM-01, ID.AM-07
1.3.2	ISO 27001:2022: A.5.10, A.5.12, A.5.13, A.8.10 ; ISA/IEC 62443-2-1: 10.2.1, 10.2.2, 13.3.4 ; NIST CSF 2.0: ID.AM-05, GV.OC-02, PR.PS-03, PR.DS-01, PR.DS-02, PR.DS-10
1.3.3	ISO 27001:2022: A.5.23 ISO 27017: 14.1.1 ; NIST CSF 2.0: ID.RA-10, ID.AM-02, ID.AM-04, GV.SC-07, GV.SC-09, GV.SC-10, PR.PS-02, PR.PS-05
1.3.4	ISO 27001:2022: A.5.19 ; ISA/IEC 62443-2-1: 9.4.x ; NIST CSF 2.0: ID.AM-02
1.4.1	ISO 27001:2022: 6.1, 6.2, 8.2, 8.3 ; ISA/IEC 62443-2-1: 6.3.1 ; NIST CSF 2.0: GV.RM-

Control	Referenz zu anderen Standards (ISO 27001/27017, ISA/IEC 62443-2-1, NIST CSF 2.0)
	01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-06, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06
1.5.1	ISO 27001:2022: 9.2 ISO 27001:2022: A.5.36 ; ISA/IEC 62443-2-1: 6.3.4 ; NIST CSF 2.0: ID.RA-07, ID.IM-01
1.5.2	ISO 27001:2022: A.5.35 ; ISA/IEC 62443-2-1: 6.3.4
1.6.1	ISO 27001:2022: A.5.24, A.6.8 ; ISA/IEC 62443-2-1: 6.2.6, 12.2.1, 12.2.2, 12.2.3 ; NIST CSF 2.0: GV.RM-05, DE.CM-06
1.6.2	ISO 27001:2022: A.5.24-27 ; ISA/IEC 62443-2-1: 12.2.7, 12.2.8 ; NIST CSF 2.0: RS.MA-02, RS.MA-03, RS.MA-04, GV.SC-08, ID.IM-02, ID.IM-04, RS.MA-01, RS.MA-05, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02, RC.RP-01, RC.RP-02, RC.RP-04, RC.RP-05, RC.RP-06, RC.CO-03, RC.CO-04
1.6.3	ISO 27001:2022: A.5.29 ; ISA/IEC 62443-2-1: 13.2.1
2.1.1	ISO 27001:2022: A.6.1 ; ISA/IEC 62443-2-1: 6.2.2 ; NIST CSF 2.0: GV.RR-04 PR.AT-02
2.1.2	ISO 27001:2022: A.6.2, A.6.5
2.1.3	ISO 27002: A.7.2.1, A.7.2.2 ; ISA/IEC 62443-2-1: 6.2.4 ; NIST CSF 2.0: PR.AT-01, PR.AT-02, GV.RR-01, GV.RR-02, GV.OC-02, GV.RR-04
2.1.4	ISO 27001:2022: A.6.7, A.8.1 ; ISA/IEC 62443-2-1: 8.4.2
3.1.1	ISO 27001:2022: A.7.1 - A.7.6 ; ISA/IEC 62443-2-1: 6.4.1 ; NIST CSF 2.0: GV.OC-04, PR.AA-06, DE.CM-02, DE.CM-03
3.1.2	—
3.1.3	ISO 27001:2022: A.5.10, A.5.11 ; ISA/IEC 62443-2-1: 9.2.2
3.1.4	ISO 27001:2022: A.6.7, A.7.10, A.8.1 ; ISA/IEC 62443-2-1: 9.2.2
4.1.1	ISO 27001:2022: A.5.18 ; NIST CSF 2.0: PR.AA-01
4.1.2	ISO 27001:2022: A.5.15, A.8.5 ; NIST CSF 2.0: PR.AA-02, PR.AA-03
4.1.3	ISO 27001:2022: A.5.16, A.5.17, A.5.18, A.8.9 ; NIST CSF 2.0: PR.AA-04
4.2.1	ISO 27001:2022 A.5.18 ; ISA/IEC 62443-2-1: 11.2.4, 11.3.1, 11.3.4 ; NIST CSF 2.0: PR.AA-05
5.1.1	ISO 27001:2022: A.8.24 ; ISA/IEC 62443-2-1: 10.2.8
5.1.2	ISO 27001:2022: A.5.14 ; NIST CSF 2.0: PR.DS-02, PR.IR-01
5.2.1	ISO 27001:2022: A.8.32 ; ISA/IEC 62443-2-1: 7.2.4 ; NIST CSF 2.0: PR.PS-01, PR.PS-04
5.2.2	ISO 27001:2022: A.8.31 ; ISA/IEC 62443-2-1: 6.3.3
5.2.3	ISO 27001:2022: A.8.1 ; ISA/IEC 62443-2-1: 9.2.1, 9.3.1, 9.3.2, 9.3.3
5.2.4	ISO 27001:2022: A.5.17, A.8.15 ; ISA/IEC 62443-2-1: 10.2.5, 12.2.4, 12.2.5 ; NIST CSF 2.0: PR.PS-04, DE.AE-02, DE.AE-03, DE.AE-04, DE-AE-08, DE.CM-01, DE.CM-09, DE.AE-06

Control	Referenz zu anderen Standards (ISO 27001/27017, ISA/IEC 62443-2-1, NIST CSF 2.0)
5.2.5	ISO 27001:2022: A.8.8, A.8.19 ; ISA/IEC 62443-2-1: 9.4.2, 12.2.9 ; NIST CSF 2.0: ID.RA-01, ID.RA-08
5.2.6	ISO 27001:2022: A.5.36, A.8.34, A.8.8 ; ISA/IEC 62443-2-1: 6.3.2 ; NIST CSF 2.0: ID.IM-02, DE.CM-09, IR.RA-09
5.2.7	ISO 27001:2022: A.8.20, A.8.22 ; ISA/IEC 62443-2-1: 6.3.2, 8.2.1, 8.2.2, 8.2.6, 8.2.8 ; NIST CSF 2.0: ID.AM-03, PR.IR-01, PR.IR-03
5.2.8	ISO 27001:2022: A.5.30 ; ISA/IEC 62443-2-1: 13.2.1 ; NIST CSF 2.0: PR.IR-02
5.2.9	ISO 27001:2022: A.8.13 ; ISA/IEC 62443-2-1: 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5 ; NIST CSF 2.0: PR.DS-11, RC.RP-03
5.3.1	ISO 27001:2022: A.5.8, A.8.25 ; NIST CSF 2.0: PR.PS-01, PR.PS-06
5.3.2	ISO 27001:2022: A.8.21 ; NIST CSF 2.0: PR.IR-04
5.3.3	ISO 27001:2022: A.5.23 ; ISO 27017: CLD.8.1.5 ISA/IEC 62443-2-1: 10.2.6 NIST CSF 2.0: ID.AM-08, GV.RR-04, PR.PS-03
5.3.4	ISO 27017: CLD.9.5.1, CLD.9.5.2 ; NIST CSF 2.0: DE.CM-06, PR.IR-01, GV.SC-07
6.1.1	ISO 27001:2022: A.5.19 - A.5.22 ; NIST CSF 2.0: GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06
6.1.2	ISO 27001:2022: A.5.14, A.6.6
6.1.3	ISO 27001:2022: A.5.23 ISO 27001:2022: A.8.9 ; ISO 27017: CLD.6.3.1 ; ISA/IEC 62443-2-1: 6.2.3 ; NIST CSF 2.0: GV.OC-05, GV.SC-01, GV.SC-02
7.1.1	ISO 27001:2022: A.5.31, A.5.32, A.5.33 ; NIST CSF 2.0: GV.SC-02, GV.OC-03
7.1.2	ISO 27001:2022: A.5.34

Prioritäten-Tabelle: Einzelbefunde mit Handlungsbedarf

Diese Tabelle ersetzt den früheren "Kompakter Index je Anforderung". Statt aller 330 bewerteten Anforderungen zeigt sie nur die 74 Einzelbefunde mit Handlungsbedarf (Kategorie Teilweise degradiert oder Reine Reibung), je mit Kurzbezeichnung und direktem Verweis auf den zuständigen MHC-Eintrag in Teil II. Unauffällige Anforderungen (Nicht betroffen, Standfest) sind hier nicht aufgeführt; sie stehen mit vollem Wortlaut und Begründung in Kapitel 1–7.

Control	Kurzbezeichnung	Kategorie	Härtungsverweis
1. IS Policies and Organization			
1.1.1	Richtlinien-Review ohne Anlassbezug ("periodisch")	Teilweise degradiert	MHC-10
1.2.1	ISMS-Wirksamkeitsprüfung ohne Anlassbezug	Teilweise degradiert	MHC-10

Control	Kurzbezeichnung	Kategorie	Härtungsverweis
1.2.2	Rollentrennung nur organisatorisch, nicht technisch durchgesetzt	Teilweise degradiert	Einzelmaßnahme
1.3.1	Asset-Inventar-Pflege ohne Anlassbezug	Teilweise degradiert	MHC-10
1.3.3	KI-Agent kann externe Dienste ohne Freigabe aufrufen	Teilweise degradiert	MHC-13
1.3.3	Freigabe-Stichprobenprüfung ohne laufende Erkennung	Teilweise degradiert	MHC-10
1.3.4	KI-Coding-Assistent lädt Softwarepakete ohne Freigabe nach	Teilweise degradiert	MHC-13
1.3.4	Gleiche Lücke bei Spezialsoftware (Wartungswerkzeuge)	Teilweise degradiert	MHC-13
1.3.4	Repository-Schutz: Signaturprüfung nicht verpflichtend	Teilweise degradiert	MHC-13
1.3.4	Software-Freigabeprüfung ohne Anlassbezug	Teilweise degradiert	MHC-10
1.3.4	Patch-Stand bekannt, aber keine Reaktionsgeschwindigkeit gefordert	Teilweise degradiert	MHC-09
1.4.1	Risikobewertung unterstellt weiterhin enge Angreiferkreise	Teilweise degradiert	Einzelmaßnahme
1.4.1	Gleiche Lücke auf Ebene der Bewertungskriterien	Teilweise degradiert	Einzelmaßnahme
1.5.1	Richtlinien-Compliance-Prüfung ohne Anlassbezug	Teilweise degradiert	MHC-10
1.5.1	Anforderungs-Compliance-Prüfung ohne Anlassbezug	Teilweise degradiert	MHC-10
1.5.1	Konzernweiter Auditplan ohne Anlass-Trigger für neue Standorte	Teilweise degradiert	MHC-10
1.6.1	Meldewesen erkennt fragmentierte Angriffsschritte nicht	Teilweise degradiert	MHC-05
1.6.2	Vorfallbearbeitung rein menschlich, keine Automatisierungspflicht	Teilweise degradiert	MHC-11
1.6.2	Gleiche Lücke bei der Reaktion auf Meldungen	Teilweise degradiert	MHC-11
1.6.2	Reaktionszeit-Ziele ohne Automatisierungspflicht zur Einhaltung	Teilweise degradiert	MHC-11
1.6.2	Eskalationsmechanismus bleibt selbst menschlich getragen	Teilweise degradiert	MHC-11

Control	Kurzbezeichnung	Kategorie	Härtungsverweis
1.6.3	Krisenerkennung auf allmähliche, nicht schnelle Eskalation ausgelegt	Teilweise degradiert	MHC-05
1.6.3	Krisenplan-Aktualisierung ohne Anlassbezug	Teilweise degradiert	MHC-10
1.6.3	Krisenszenarien ohne KI-orchestrierten Mehrfachangriff	Teilweise degradiert	Einzelmaßnahme
1.6.3	Krisenszenarien ohne KI-orchestrierten Mehrfachangriff (redaktionelle Katalogdublette, siehe Datenqualitäts-Hinweis)	Teilweise degradiert	Einzelmaßnahme
1.6.3	Kommunikationsstrategie ohne verkürztes Reaktionsfenster	Teilweise degradiert	MHC-05
1.6.3	Kommunikationsstrategie ohne verkürztes Reaktionsfenster (redaktionelle Katalogdublette, siehe Datenqualitäts-Hinweis)	Teilweise degradiert	MHC-05
1.6.3	Krisenplan-Bewertung ohne Anlassbezug	Teilweise degradiert	MHC-10
2. Human Resources			
2.1.1	Identitätsprüfung anfällig für Deepfake-Bewerberidentität	Teilweise degradiert	MHC-15
2.1.1	Live-Interview anfällig für Echtzeit-Deepfake	Teilweise degradiert	MHC-15
2.1.1	Referenzen/Zeugnisse leichter fälschbar	Teilweise degradiert	MHC-15
2.1.3	Awareness-Training auf veraltete Phishing-Erkennungsmerkmale ausgelegt	Teilweise degradiert	MHC-15
3. Physical Security			
3.1.1	Zutrittskontrolle anfällig für KI-gestützte Vortäuschung	Teilweise degradiert	MHC-15
3.1.1	Besucherregistrierung anfällig für gefälschte Legitimation	Teilweise degradiert	MHC-15
3.1.4	Verschlüsselung mobiler Geräte nicht verpflichtend vorgeschrieben	Teilweise degradiert	Einzelmaßnahme
4. Identity and			

Control	Kurzbezeichnung	Kategorie	Härtungsverweis
Access Management			
4.1.1	Sperrung verlorener Ausweismittel nicht sofort/automatisiert	Teilweise degradiert	MHC-03
4.1.2	"Stand der Technik" erzwingt keine Phishing-Resistenz	Teilweise degradiert	MHC-03
4.1.2	Passwortstärke wirkungslos gegen Echtzeit-Phishing	Reine Reibung	MHC-03
4.1.2	Privilegierte Konten: einfache 2FA ohne Phishing-Resistenz genügt	Teilweise degradiert	MHC-03
4.1.2	Optionsliste erlaubt Erfüllung ohne Phishing-Resistenz	Teilweise degradiert	MHC-03
4.1.2	Zwei-Faktor-Beispiel ohne Phishing-Resistenz-Pflicht	Teilweise degradiert	MHC-03
4.1.3	Konten-Review ohne Anlassbezug	Teilweise degradiert	MHC-10
4.1.3	Besitzfaktor (SMS-OTP) anfällig für SIM-Swapping	Teilweise degradiert	MHC-03
4.1.3	Konten-Review in Kundensystemen ohne Anlassbezug	Teilweise degradiert	MHC-10
4.2.1	Zugriffsrechte-Review ohne Anlassbezug	Teilweise degradiert	MHC-10
4.2.1	Kürzeres Prüfintervall bleibt periodisch ohne Anlassbezug	Teilweise degradiert	MHC-10
5. IT Security/Cyber Security			
5.1.2	Transportschutz ohne verpflichtenden Verschlüsselungs-Mindeststandard	Teilweise degradiert	Einzelmaßnahme
5.1.2	Fernzugriff: VPN schützt Transportweg, nicht Authentisierung	Teilweise degradiert	MHC-03
5.2.3	Signaturbasierter Malwareschutz gegen KI-Varianten schwach	Teilweise degradiert	MHC-05
5.2.3	Virenscanner-Beispiel signalisiert Signaturerkennung	Teilweise degradiert	MHC-05
5.2.3	Gleiche Signaturerkennungsgrenze bei Dateiprüfung	Teilweise degradiert	MHC-05
5.2.3	Vollprüfung periodisch und	Teilweise	MHC-05

Control	Kurzbezeichnung	Kategorie	Härtungsverweis
	signaturbasiert — doppelte Schwäche	degradiert	
5.2.3	Verschlüsselter Inhalt umgeht Gateway-Inspektion	Teilweise degradiert	MHC-05
5.2.4	Log-Prüfung erkennt fragmentierte Angriffsmuster nicht	Teilweise degradiert	MHC-05
5.2.5	Schwachstellenbewertung unterschätzt verkürztes Exploit-Fenster	Teilweise degradiert	MHC-09
5.2.5	Patch-Management ohne verpflichtende Geschwindigkeits-SLA	Teilweise degradiert	MHC-09
5.2.6	Behebungsfrist ("appropriate timeframe") unbestimmt	Teilweise degradiert	MHC-09
5.2.6	Audit-Zyklus lässt Patch-Gap zwischen Prüfungen offen	Teilweise degradiert	MHC-09
5.2.6	Scan-Frequenz auch bei sehr hoch nur periodisch	Teilweise degradiert	MHC-09
5.2.7	Erkennung lateraler Bewegung ohne Verhaltensbasierung	Teilweise degradiert	MHC-05
5.2.7	Fernzugriffsrisiko importiert Authentisierungslücke aus 4.1.2	Teilweise degradiert	MHC-03
5.2.8	Notfallplan-Aktualisierung ohne Anlassbezug	Teilweise degradiert	MHC-08
5.2.8	Backup-Schutz ohne Unveränderlichkeits-Vorgabe (Integrität)	Teilweise degradiert	MHC-08
5.2.8	Gleiche Lücke, Vertraulichkeitsseite	Teilweise degradiert	MHC-08
5.2.9	Backup-Konzept-Überprüfung ohne Anlassbezug	Teilweise degradiert	MHC-10
5.3.1	Testdaten: keine re-identifizierungsresistente Anonymisierung gefordert	Teilweise degradiert	Einzelmaßnahme
6. Supplier Relationships			
6.1.1	Lieferantenberichte ohne unabhängige Gegenprüfung	Teilweise degradiert	MHC-14
6.1.1	Selbstauskunft/Attestierung als Nachweis ausreichend	Teilweise degradiert	MHC-14
6.1.1	Prüf-Frequenz gut, Nachweis-Echtheitsproblem bleibt	Teilweise degradiert	MHC-14

Control	Kurzbezeichnung	Kategorie	Härtungsverweis
6.1.1	Gleiche Nachweis-Echtheitslücke bei Vertragsprüfung	Teilweise degradiert	MHC-14
6.1.2	NDA-Handhabungsverfahren ohne Anlassbezug	Teilweise degradiert	MHC-10
6.1.3	Dienstleister-Konfiguration periodisch statt kontinuierlich geprüft	Teilweise degradiert	MHC-10
6.1.3	Unspezifizierter Nachweis ohne unabhängige Verifikation	Teilweise degradiert	MHC-14
6.1.3	Authentisierungsmechanismen ohne Phishing-Resistenz-Pflicht	Teilweise degradiert	MHC-03