MRIS for TISAX® 2027

Mythos-resistant information security — Analysis of the TISAX® questionnaire ISA 2027, module "Information Security"

Part I: Analysis and Gap Assessment. The Implementation Guide (Part II) is available as an independent follow-up publication.

Version 1.1 | July 2026

Creator: Richard Peddi

License and Notices

Independence Notice

TISAX® is a registered trademark of the ENX Association; The ENX Association administers TISAX® on behalf of the German Association of the Automotive Industry (VDA), which develops and publishes the underlying questionnaire (VDA ISA). This analysis is an independent, privately created work with no connection to the ENX Association or VDA. It is not part of the official TISAX® testing process, nor is it authorized, tested or confirmed by ENX, and does not replace a TISAX® maturity assessment by an accredited testing service provider.

Disclaimer

The classifications in this document are a professional assessment as of July 2026, not legal or certification advice. The application is carried out without guarantee and under your own responsibility.

Citation recommendation

Peddi, Richard (2026): MRIS for TISAX® 2027 — Part I: Analysis and Gap Assessment. v1.1

Change history

Version	Date	Description
1.0	June/July 2026	First published.
1.1	July 2026	Revision based on an externally commissioned audit report (July 2026, 9 findings F-01–F-09).

Version 1.1 in detail:

Finding	Topic	Implementation
F-01	Inconsistent counting arithmetic and chapter totals	Total number 324 → 330 corrected (chapter totals: 116/21/14/37/105/31/6; Methodology sharpened: only duplicate catalogues with the same word count as editorially removed); Control 1.6.3 reassessed on the basis of the primary source (ISA2027-EN.xlsx) (Table 15 → 19 rows, overall rating "5 out of 15" → "7 out of 19" Partially demoted); Control 5.2.8 "3 out of 14" → "3 out of 15"; Total number of individual findings 72 → 74 (cascade through management summary, cluster overview, priority table, pattern formation chapter and part II)
F-02	Characterization and citation accuracy	Quote for Control 5.2.5 corrected
F-03	Asymmetrical sources	re-researched four detailed claims (Cogent study, NIST AI Agent Standards Initiative, BSI C5:2026 OPS-25.01AC, Mythos benchmark figures); source apparatus supplemented by primary sources; unconfirmed BSI detailed values separated from the confirmed frame statement (footnote 2; analogous to Part II, MHC-09)
F-04	Editorial document control	introduced this change history; Dates unified to July 2026; Version note added (title page and citation recommendation); Orphaned reference "(Phase 5, see task list)" corrected
F-05	Lack of profitability analysis	concerns Part II (see there)
F-06	SME suitability of individual target values	concerns Part II (see there)
F-07	Lack of evidence mapping to the catalog	concerns Part II (see there)

Finding	Topic	Implementation
F-08	TISAX Label Expectation Management and Maturity Levels	no document defect (application note); No text change
F-09	Threat model dependency of reasoning	no document defect (application note); No text change

Foreword

With MRIS (Mythos-Resistant Information Security), I previously developed a methodology to specifically test existing ISMS rules for their resilience to AI-accelerated attackers — named after Claude Mythos, the AI model whose publication in April 2026 documented this threat shift for the first time concretely and publicly (see "On the name 'Mythos'"). MRIS-TISAX® 2027 transfers this test logic to the TISAX® questionnaire ISA 2027 — as an independent work, not as a derivation of an existing MRIS version: The threat basis is derived directly from primary sources (see methodology).

The claim of this document is deliberately limited: It evaluates the wording of 330 TISAX® requirements individually against a defined threat model and arranges the findings into recurring patterns. It's a diagnosis. The specific additional measures resulting from this are the subject of the separate follow-up publication (Implementation Guide, MHC). Feedback, objections and additions are expressly welcome — the CC-BY-NC license is also intended as an invitation to check, refute or further develop this analysis.

Richard Peddi
July 2026

Table of Contents

Management Summary

MRIS-TISAX® 2027 examines the 45 controls of the "Information Security" module in the TISAX® ISA 2027 questionnaire individually against a criteria grid derived from four documented threat shifts (attacker patience, time compression, capability decoupling, aggregation resistance). The wording of the requirements is evaluated, not the implementation at a specific organization. The catalogue contains 331 "+" marked requirements in the raw text (321 graded according to protection needs plus 10 for Simplified Group Assessments); 330 distinct requests are evaluated, since Control 1.6.3 contains a duplicate requirement in the source catalog (four other textually similar pairs of requests in Control 1.6.3 are editorial deviations in the source catalog itself, not true duplicates, and are counted as independent requirements; see Data Quality Note, Methodology). Prototype Protection and Data Protection are not part of this analysis.

At a glance

Key figure	Value
Rated Controls	45
Distinct requirements	330
Stable	4 Controls (9%)
Partially degraded	26 Controls (58 %)
Pure friction	1 Control (2%)*
Not affected	14 Controls (31%)
Recurring Pattern Categories (Phase 2)	8 clusters, 74 individual findings
Frame of Comparison (Phase 3)[2]	NIST CSF 2.0, BSI C5:2026, DORA, CRA, NIS2-RL/DVO, ISA/IEC 62443-2-1
Original Extension (Part II, beyond TISAX®)[3]	AI Agent/GenAI Security: MHC-13 (Enhanced) + MHC-16 Cover 8 of 10 OWASP ASI Threat Categories — TISAX® itself only regulates two requirements here (1.3.3, 1.3.4)

*Applies only to the pure password factor without a second factor (4.1.2, one of seven requirements). Classic MFA procedures (OTP/push) of the same control are partially degraded — weakened, but not ineffective; see Chapter 4.

[2] These six frameworks are the compliance/regulatory frameworks compared in Phase 3 against the TISAX® requirement wording. The OWASP Top 10 for Agentic Applications (next line) is not a framework of comparison in this sense, but a threat taxonomy against which only the original AI agent extension in Part II was tested — do not mix the two.

[3] Not derived from the TISAX® diagnosis, but the author's professional judgement on the basis of external threat research (primarily OWASP); marked as original throughout. See section "Original additions beyond TISAX®".

Key findings: The TISAX® requirements catalog does not collapse against a Gen AI-supported attacker, but degrades in the majority of controls: 58% lose some of their protective effect, mostly

because formulations such as "regularly" or "appropriate" do not prescribe an event-related or time-bound response mechanism. Only a single control (4.1.2, pure password authentication without a second factor) completely loses its core effect. The share of stationary work is low at 9% and is concentrated almost exclusively on chapter 5, where TISAX® requires concrete technical mechanisms instead of organizational processes.

The 74 individual requirements concerned form eight recurring patterns, led by periodic rather than event-related testing (19 findings over four chapters). The gap analysis against six external benchmarks shows that most of these patterns are already addressed elsewhere in the regulation — such as CVSS-bound patch deadlines in BSI C5:2026 or MFA or Continuous Authentication, which NIS2 Art. 21(2)(j) explicitly names as a suitable measure in the risk-based catalog of measures — and can be adopted accordingly for the planned curing controls synthesis. One exception: Capability decoupling by autonomously acting AI agents that independently integrate external services or software packages has not yet been regulated by any of the six comparison frameworks — even NIST only launched its own standardization initiative on this subject as recently as February 2026.

Part II responds to this with a deliberate, clearly marked exception to the otherwise TISAX-derived® methodology: An enhanced MHC-13 and a new MHC-16 address AI agent/GenAI security — agent identity, prompt injection, kill switch, multi-agent integrity — and cover 8 out of 10 threat categories defined there, tested against the OWASP Top 10 for Agentic Applications; TISAX® ISA 2027 itself touches this field only on two requirements (1.3.3, 1.3.4). The expansion is justified by the topicality of the threat: AI agents are already productive and vulnerable in today's operational environment, not just the subject of a future TISAX® release. See the section "Original Supplements Beyond TISAX®" for the complete identification of which parts are TISAX-derived® and which are original.

About the name "Mythos"

The name is not a free invention. Claude Mythos Preview is a real-world AI model published by Anthropic on April 7, 2026 — in Anthropic's own description (Frontier Red Team, lead author Nicholas Carlini) a "general-purpose language model that is strikingly capable at computer security tasks". Its existence became known back in March 2026 through an accidentally published blog post draft leak; Anthropic then confirmed to Fortune that the model represents a "step change in capabilities" with significant cybersecurity risk. Anthropic itself calls Mythos "in a different league" compared to its predecessor Opus 4.6: in a Firefox 147 exploit benchmark, Opus 4.6 managed two successful attempts in several hundred attempts, Mythos achieved 181 working exploits plus register control for 29 others; in an internal OSS fuzz benchmark, Opus 4.6 and Sonnet 4.6 achieved a Tier 3 crash at best, Mythos achieved 595 Tier 1/2 crashes and full control flow takeover (Tier 5) on 10 fully patched target systems — including a 27-year-old OpenBSD bug that has since been patched, a 16-year-old FFmpeg bug and an autonomous, human-assisted FreeBSD NFS remote code execution (CVE-2026-4747). The New York Times described the disclosure as "cybersecurity reckoning".

Anthropic explicitly did not publish the model publicly — "we do not plan to make Claude Mythos Preview generally available" — but granted access exclusively via "Project Glasswing" to selected industry partners and open source developers (including Microsoft, Apple, AWS, Cisco, Nvidia; over 40 companies) "to enable defenders to begin securing the most important systems before models with similar capabilities become broadly available". Their own risk assessment was blunt: "In the short term, this could be attackers, if frontier labs aren't careful about how they release these models." In the weeks that followed, independent findings confirmed the implications outside of the original Anthropic release: about two weeks after release, Mozilla reported 271 security vulnerabilities in Firefox found and fixed with Mythos, and on May 14, 2026, Calif.io employees reported a memory corruption exploit created with Mythos for the Apple M5.

Within days, disclosure and reported cases of unauthorized access triggered crisis responses around the world: the U.S. Treasury and Fed issued direct warnings to banks, central banks in Canada, the United Kingdom, India, Japan, and Australia convened emergency meetings, a U.S. congressional letter called for a revision of federal cybersecurity policy, and China was denied access. In June 2026, the situation escalated further: after a reported jailbreak that potentially turned Mythos 5 into an "unrestricted cyber tool," the U.S. Department of Commerce under Howard Lutnick ordered a worldwide blocking of access for all foreign nationals — an unprecedented intervention that was partially lifted at the end of June after negotiations with Anthropotic.

It is precisely this extent that justifies the choice of name: a single model revelation that simultaneously brought central banks, governments and a 40-member industry consortium to the scene within days, followed by a worldwide export control after a real jailbreak incident — this is the moment when the previously abstract risk of AI-accelerated attacks was concretely, publicly proven for the first time and occurred on a scale that no one had previously expected. "Mythos" thus does not stand for a metaphor, but for a dated, documented event.

Important for the methodology: The name anchors this analysis to a fixed historical point in time — it is not a confession that the four threat shifts (see methodology) depend on the capabilities of the Mythos model itself. The actual evidence base of the methodology is four independently documented incidents (Cogent CVE evaluation, GTG-1002 campaign, JadeBuffer ransomware — see methodology), not Mythos-specific benchmark results. In the rest of the document, "Mythos attacker" is a linguistic abbreviation for "attacker with the four proven, generation-independent abilities", not a reference to a specific product. Should Mythos become technically obsolete or withdrawn from the market in a few years, the methodology will remain valid as long as the underlying capabilities — automated exploit development, autonomous multi-stage attack execution, fragmented attack patterns, decoupled attacker capability — persist or evolve on any available system. The name is a historical marker for the state of knowledge July 2026, not a methodological dependency on a single provider or model.

Sources:

- Claude Mythos Preview — Anthropic (Primary Source)
- Frontier Red Team: Claude Mythos Preview — Anthropic (Primary Report with Benchmark Details on Exploit and Crash Numbers)
- The zero-days are numbered — The Mozilla Blog (primary source on the 271 vulnerabilities found and fixed in Firefox)
- First public kernel memory corruption exploit found by an AI agent — Calif.io (primary source for the 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

Methodology

What this analysis is — and what it is not

This analysis is an **efficacy add-on layer on top of the TISAX® maturity test, not a substitute for it.** A control can reach maturity level 3 ("Established", the TISAX® target value) in the audit and still be classified as "Partially demoted" in this analysis — the two are not mutually exclusive. Maturity measures whether a process is documented, introduced and lived. This analysis measures something else: whether the protection mechanism required by the requirement can still withstand a Gen AI-accelerated attacker. **Definition convention of this analysis:** "Stable" is deliberately linked here to the TISAX® target maturity level 3 — this is a methodological definition of MRIS-TISAX® 2027, not a statement of the TISAX® catalog itself. According to this convention, a requirement is considered "stable" if it bears maturity level 3 even under Mythos conditions without additional measures — not only "somehow still works".

The wording of the requirement **is evaluated**, not the actual implementation in a specific organization. "Stable" means: correctly implemented, withstands this requirement. Whether a particular organization has actually implemented it correctly can only be answered by an on-site audit — the regular TISAX® audit with maturity level and evidence (GWP) remains responsible for this.

Limit of this analysis: Requirements are assessed individually, not as an attack chain. A "stable" rating applies to the assessed mechanism in isolation, not to the overall system. Stable encryption (5.1.1) is of little use if the preceding access is via degraded authentication (4.1.2) — the combination of several controls along a realistic attack chain is not evaluated here. This is the task of the planned pattern formation (phase 2), which clusters individual findings along recurring attack patterns.

Proportions are a count, not a risk score. "3 out of 9 requirements affected" means: three out of nine text passages are weakened — not that the control is one-third risky. A single critical vulnerability (e.g., lack of phishing resistance in authentication) can outweigh five individual administrative findings in another control. A risk-weighted prioritization is not provided by this count, but by the later gap analysis (phase 2/3).

What this analysis does not (yet) provide: a prioritization of the findings according to urgency/effort, and an assignment to concrete types of evidence. This concrete level of improvement/completion — what has to be changed in a requirement in order for it to meet again — is deliberately not provided by this chapter, but by the later curing controls synthesis (phase 4) with subsequent linking back to chapters 1–7 (phase 5). The categories assigned here are the diagnosis; MHC synthesis is the prescription.

What this analysis does not assess (scope demarcation): MRIS-TISAX® 2027 is a requirement-level efficacy diagnosis. Explicitly out of scope:

- **Cost-effectiveness:** no cost-benefit analysis of individual hardening measures – the organisation decides whether a measure is financially viable.

- **Organization-specific risk:** no risk analysis for a specific organization (protection needs, asset criticality, probability of occurrence) — the organization's own ISMS risk management remains responsible for this.
- **Threat intelligence:** no assessment of specific attacker groups, campaigns, or target industries — the threat model below describes capabilities, not actors.
- **Probability of occurrence:** no statement about how likely a particular attack is to hit a particular organization.
- **Quantitative risk calculation:** no expected values, value-at-risk or comparable key figures. The categories assigned are ordinal (ranking), not metric, and the Threat Priority Score used in Part II is also a prioritization index, not a risk score (see Part II, section "Evaluation Logic").

These questions are answered by the organization's own risk analysis; MRIS provides the diagnosis at the requirement level as an input variable, not the finished result.

Controls vs. actual security: MRIS evaluates TISAX® requirements as text, not an organization's actual security posture. The "Steadfast" category means that the required mechanism will hold if implemented correctly — not that a particular organization is safe. Conversely, "partially degraded" does not mean that a specific incident is imminent, but that the assumption of protection anchored in the wording of the requirements should be sharpened. The categories are a prioritization tool for requirements improvements, not a security or maturity substitute for the organization as a whole.

Basis: four threat shifts and four evaluation criteria

MRIS-TISAX® 2027 is a standalone analysis. It has nothing formally in common with a possible MRIS elaboration for ISO 27002 except the goal of effectively and efficiently hardening an existing ISMS against Gen AI-supported threats. The threat model is therefore derived directly from publicly documented incidents and research reports 2025/2026, not from an overarching framework. Four shifts are thus documented:

1. **Patch gap window collapse**: A 2026 analysis of 69,159 CVE by Cogent Security shows that the average time from vulnerability disclosure to the first working exploit has decreased from 125.3 days (January 2025) to 0.5 days (April 2026); 62% of critical vulnerabilities with a known exploit already existed before the scanner detection signature.
2. **Reaction timeline compression:** Anthropic uncovered a state-driven campaign (GTG-1002) in September 2025 in which a hijacked AI agent system executed 80-90% of the attack steps against around 30 target organizations autonomously and at thousands of requests per second — a pace without a human-occupied counterpart.
3. **Fragmentation of the threat event:** The same campaign first performed an unobtrusive, low-and-slow reconnaissance within normal usage patterns, before moving on to the rest of the steps at machine speed — a pattern that does not coherently capture detection designed for human correlation of individual anomalies.
4. **Decoupling capability/actor:** In 2026, security vendor Sysdig documented the first ransomware campaign completely autonomously executed by an AI agent under the name "JadeBuffer". Via an unpatched vulnerability in the open-source platform Langflow (CVE-2025-3248, CVSS 9.8), the agent penetrated, moved laterally on its own, captured credentials from several AI and cloud providers, escalated privileges and encrypted 1,342 database/configuration elements via more

than 600 independently executed malware variants — a kill chain that has so far required a well-rehearsed, multi-member attacker team with specialized knowledge in initial access, lateral movement and ransomware operation. The outcome is significant: the agent forgot to secure the generated key and took a Bitcoin address from his own training data for the ransom demand — even victims willing to pay would not have received their data back. The real turning point lies precisely in this: despite this beginner's mistake, the complete technical attack chain succeeded up to comprehensive encryption. The capability, which previously required an experienced attacking team, is already decoupled from the actor today — incorrectly executed, but effective, not only in a future mature version.

Together, these four cases mark the turning point that makes hardening measures necessary in the first place: none of the four describes only a theoretical risk or a gradual exacerbation of existing threats. All four are already occurring, documented events in which an AI system has completed a task completely or largely without the human expertise, reaction time or conspicuousness previously required. A security concept that tacitly continues to rely on human limits on the part of the attacker thus evaluates a threat situation that no longer exists in this form. From these four shifts, four evaluation criteria are derived that are used to check each TISAX® requirement:

- **Attacker patience:** Is the protective effect based on the fact that an attack is too complex or cumbersome for the attacker?
- **Time compression:** Does the control require a human reaction time, even though the attacker now carries out the attack automatically and independently? **Differentiation:** The weakness is not "periodic" in itself, but **periodic without documented trigger logic and without risk-based event control.** A "periodic review" is only considered a time compression weakness if (1) the subject matter being checked is a technical-operational security element, the obsolescence of which opens up an exploitable window of time (e.g. software releases, access rights, backup concepts, log evaluation, supplier security status), AND (2) the wording of the requirements does not prescribe a supplementary reference to the occasion. If an organization supplements a periodic review with documented, risk-based triggers (e.g., immediate reassessment of a new critical vulnerability), this effectively closes the gap — but the wording of the requirements itself remains classified as demoted, as it does not require this trigger. Pure legal scans (which laws/contracts apply) are not counted as such, as legislation does not change at the pace of an automated attack.
- **Capability decoupling:** Is the assessment "hardly anyone can do that" based on an empirical value that no longer applies due to AI tools?
- **Aggregation resistance:** Does the control detect an attack even if it is broken down into many individual steps that seem harmless in themselves?

Why exactly four criteria: The four criteria are not an arbitrarily chosen grid width, but a direct translation of the four threat shifts documented above into testable questions — attacker patience translates the collapse of the patch gap window, time compression translates the compression of the reaction timeline, aggregation resistance translates the fragmentation of the threat event, capability decoupling translates the decoupling of capability and actor. Each criterion is examined independently of the other three; a requirement can degrade against several criteria at the same time (see e.g. 4.1.2, where both capability decoupling and time compression

apply — the justification column lists all applicable criteria in each case). The number four is thus a consequence of the threat model, not a pre-set number of categories.

Reproducibility: Each classification in the document follows the same chain: Requirements wording → comparison against the four threat shifts → examination of the four criteria → category (Stable/Partially Degraded/Pure Friction/Not Affected) → classification in one of the eight sample clusters (Phase 2) → MHC assignment (Phase 4, Part II). This chain is disclosed for each requirement in the justification column, not only in the result.

Timeliness and timeliness: MRIS-TISAX® 2027 reflects the state of knowledge as of July 2026 — both in the TISAX® requirement wording (ISA 2027) and in the underlying threat model (see above: Cogent CVE evaluation, GTG-1002, JadeBuffer, Mythos disclosure). Both sides can evolve: TISAX® regularly updates the ISA, and new AI capabilities can tighten or even mitigate existing classifications (for example, if phishing-resistant authentication becomes the industry standard and a requirement that is degraded today becomes de facto stable). Accordingly, this analysis should be read as a snapshot, not as a one-time final result — a reassessment makes sense as soon as either the TISAX® catalog or the proven attacker capability shifts significantly.

Classification of each requirement, gap analysis and implementation guide are developed independently for the TISAX® context.

Sources:

- 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 (Primary Source)
- 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
- Jade buffer: The first AI ransomware attack doesn't just mess up the key — heise online
- JadeBuffer: 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 (Primary Source)
- NIST: Summary and Analysis of Responses to the Request for Information Regarding Security Considerations for AI Agents (Primary Source)
- BSI: Cloud Computing Compliance Criteria Catalogue C5:2026 (Primary document; PDF full text not technically extractable in the context of this search — see footnote 2, section "Gap analysis versus six comparison frames")

Categories and their practical significance

Category	Significance	What you do with it as a CISO
Stable	The security assumption of the requirement **does not collapse under the four evaluation criteria** — not synonymous with "an attack is impossible", but the	Citable as evidence in the Statement of Applicability equivalent (ISA catalogue maturity entry). No additional

Category	Significance	What you do with it as a CISO
	mechanism is based on a hard barrier (cryptography, physical separation, architecture) that also holds under Mythos conditions. Thus achieves TISAX® target maturity level 3 without any additional measures.	effort from the Mythos's point of view — continue auditing normally.
Partially degraded	**Reduced, not lacking effectiveness** compared to the original protection assumption: the mechanism continues to work, but is no longer sufficient to keep maturity level 3 effective against a Mythos attacker.	Candidate for the risk treatment plan. Needs a supplementary hardening measure (catalogue will follow in phase 4). **This requires additional budget and attention.**
Pure friction	Completely loses the core effect against a Mythos attacker — the protection assumption of the requirement no longer applies, regardless of the maturity level reached.	Needs to be replaced or fundamentally redesigned — a mere addition is not enough.
Not affected	**Affected by none of the four evaluation criteria** (attacker patience, time compression, capability decoupling, aggregation resistance) — no statement about whether the requirement is generally "secure", but that it remains unchanged against this specific threat shift (typically governance, law, contract, pure documentation).	Continue to test and implement in normal ISMS operation, but **deliberately do not prioritize** when allocating resources for the Mythos response. No need for compensation.

Ranking for mixed findings within a control: Pure friction > Partially degraded > Stable > Not affected. If a control contains both one friction and multiple degraded requirements, the overall rating is shown as "Pure Friction" — the weakest individual finding determines the overall picture, not the average.

Evaluation unit and structure per control

Each TISAX® control (e.g. 5.2.9) contains several individual requirements marked with "+", graded according to the protection requirement level: **must** and **should** always apply (normal protection requirement), **high** and **very high** are added with a correspondingly higher protection requirement of the affected asset — they do not replace must/should, but complement it. Each individual request is evaluated on its own, in the original English version of the source (citable, searchable).

Six controls in Chapter 1 (1.1.1, 1.2.1, 1.2.2, 1.5.1, 1.5.2, 1.6.2) contain additional **SGA requirements** ("Additional requirements for Simplified Group Assessments"): they apply regardless of the protection requirement, only if the organization uses the simplified TISAX® group assessment (several similar sites together). Marked as a separate level "SGA" in the tables and NOT included in must/should/high/very-high counts — the share specification per control shows SGA requirements separately.

At the end of each control there is an **overall classification**: for most controls, it is identical across all three protection requirement levels and is summarized as a sentence with a percentage indication ("3 out of 9 requirements affected"). For a few controls, the picture changes as the need for protection increases — there is a description of which additional requirement triggers the difference and what this means for you in practice.

Responsibility column: in the case of degraded/friction/stable requirements, the function typically responsible (IT operations, CISO function/ISMS, development/engineering, IAM team, purchasing/supplier management, human resources, facility/plant security) is also indicated. An organizational assignment, not a binding RACI — serves as the first classification of who typically processes the finding.

Data quality: Control 1.6.3, column "high", contains five strikingly similar pairs of requirements in the source catalog. Checked against the ISA 2027 original table, exactly one pair of them is word-for-word (counted once); the remaining four differ editorially (e.g. typos "outage of" vs. "outage oaf", wording "Methods" vs. "Instruments to monitor communication") and are considered to be distinct requirements (see Control 1.6.3 below). Control 3.1.2 does not contain its own requirements ("Superseded by 1.6.3, 5.2.8 and 5.2.9").

Chapter 1 — IS Policies and Organization (14 Controls, 116 distinct requirements incl. 10 SGA requirements)

1.1.1 — To what extent are information security policies available?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The requirements for information security have been determined, documented and adapted to the organization's goals."	Not affected	Governance basis of the policy, no reference to attack.	CISO Function
must	"A policy exists, and is approved by the organization's management."	Not affected	Act of approval, no defensive function.	CISO Function
must	"The policy includes objectives and the significance of information security within the organization."	Not affected	Minimum content requirement for the document itself.	CISO Function
must	"The policies are made available to employees in a suitable form (e.g., intranet)."	Not affected	Obligation to distribute, no reference to attack.	CISO Function
must	"Employees and external business partners are informed of any changes relevant to them."	Not affected	Duty to communicate, no reference to the attack.	CISO Function
should	"The information security requirements are based on the strategy of the organization. Legislation and contracts are considered in the policy."	Not affected	Content orientation of the directive, no technical protective effect.	CISO Function
should	"The policy indicates consequences in case of non-conformance."	Not affected	sanction clause, organizational.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
should	"Other relevant security policies are established."	Not affected	Completeness requirement for the guideline.	CISO Function
should	"Periodic review and, if required, revision of the policies are established."	**Partially degraded**	Time compression: "periodic" without a specific reason for testing. If new attack patterns emerge within a few weeks, but a fixed audit cycle runs annually, for example, the policy remains outdated in the meantime.	CISO Function
SGA	"Policies are published and implemented in the entire assessment scope."	Not affected	Reach requirement for group valuations (all locations in the scope), no defensive function.	CISO Function

Overall classification: Partially demoted (1 in 10 requirements affected), regardless of protection needs. In the case of Simplified Group Assessment, this also applies to all locations in the area of validity.
Curing reference: MHC-10 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The scope of the ISMS (the organization managed by the ISMS) is defined."	Not affected	Scope determination, governance.	CISO Function
must	"The organization's requirements for the ISMS are determined."	Not affected	Governance.	CISO Function
must	"The organizational management has	Not affected	Release act of the management.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
	commissioned and approved the ISMS."			
must	"The ISMS provides the organization's management with suitable monitoring and control means (e.g., management review)."	Not affected	Requires only the existence of a control instrument, no frequency specification — the frequency question follows separately.	CISO Function
must	"Applicable controls have been determined (e.g., ISO 27001 Statement of Applicability, or completed ISA catalogue)."	Not affected	Scoping governance.	CISO Function
must	"The effectiveness of the ISMS is regularly reviewed by the management."	**Partially degraded**	Time compression: an annual management review rhythm, as is common in practice, reacts structurally too slowly to a threat situation that changes within weeks.	CISO Function
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)."	Not affected	Release governance for the group-wide scope.	CISO Function

Overall classification: Partially demoted (1 out of 7 requirements affected), regardless of protection needs. In the case of Simplified Group Assessment, this also applies to all locations in the area of validity.

Curing reference: MHC-10 (see Part II)

1.2.2 — To what extent are information security responsibilities organized?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Responsibilities for information security within the organization are defined, documented, and assigned."	Not affected	Governance.	CISO Function
must	"The responsible employees are defined, qualified, and empowered for their task."	Not affected	Governance/Human Resources.	CISO Function
must	"The required resources are available."	Not affected	Resource commitment, no defensive function.	CISO Function
must	"The contact persons are known within the organization and to relevant business partners."	Not affected	Awareness of contact persons, organizational.	CISO Function
should	"There is a definition and documentation of an adequate information security structure within the organization."	Not affected	Governance.	CISO Function
should	"Security-relevant roles that are not part of the ISMS and are relevant for information security are considered."	Not affected	Scoping completeness; possible starting point for "shadow AI roles" in chapter 4/5, here is not yet a sufficiently concrete textual basis for a different classification.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
high	"An appropriate organizational separation of responsibilities should be established in order to avoid conflict of interests (segregation of duties). (C, I, A)"	**Partially degraded**	Skill decoupling: Separation of roles has so far provided protection because one person can hardly master two specialist roles at the same time. With AI support, a single person can convincingly complete the tasks of a second role if the separation is only enforced organizationally and not additionally through system rights.	IAM Team
SGA	"A named person with overall responsibility for the management system exists and is available."	Not affected	Governance/Accountability, Group-wide.	CISO Function

Overall classification: Inconspicuous with normal need for protection (Not affected, 0 of 7 incl. SGA) — no need for action. From a high need for protection, the obligation to separate duties is added, which shows a weakness without technical enforcement: Partially demoted (1 of 8 requirements affected). The SGA requirement also applies regardless of the need for protection and does not change this. Practical: only affects you if this control applies to high/very high rated values.

Reference to hardening: individual measure (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Projects are classified while taking into account the information security requirements."	Not affected	Governance/project management.	CISO Function
should	"The procedure and criteria for the classification of projects are documented."	Not affected	Documentation obligation.	CISO Function
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."	Not affected	Explicit double trigger ("early in the project AND repeated with changes") invalidates the time compression concern.	CISO Function
should	"For identified information security risks, measures are derived and considered in the project."	Not affected	Governance.	CISO Function
high	"The measures thus derived are reviewed regularly during the project and reassessed in case of changes to the assessment criteria. (C, I, A)"	Not affected	Also double triggers ("regularly AND with changes") available.	CISO Function

Overall classification: Not affected (0 out of 5 requirements affected), regardless of protection needs. Double triggers throughout — a good example of a formulation that structurally invalidates the time compression concern.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Information assets and other assets where security is relevant to the organization are identified and recorded."	Not affected	Inventory governance.	CISO Function
must	"The supporting assets processing the information assets are identified and recorded."	Not affected	Inventory governance.	CISO Function
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."	**Partially degraded**	Time compression: without a fixed reason for testing, the inventory remains incomplete between checks. Newly created, unrecorded systems (such as independently set up cloud or AI services) fall precisely into this time window — this is where automated attacks start first.	IT Operations

Overall classification: Partially demoted (1 out of 3 requirements affected), regardless of protection needs.
Curing reference: MHC-10 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available."	Not affected	Pure classification scheme; Effect only arises in downstream technical controls.	CISO Function
must	"Evaluation of the identified information assets is carried out according to the defined criteria, and assigned to the existing classification scheme."	Not affected	Application of the scheme, governance.	CISO Function
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."	Not affected	governance requirement; the technical effect lies in the referenced controls themselves.	CISO Function
should	"The protection goals of integrity and availability are taken into consideration."	Not affected	Completeness of the scheme.	CISO Function

Overall rating: Not affected (0 out of 4 requirements affected), regardless of protection needs.

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?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"External IT services are not used without explicit assessment and implementation of the information security	**Partially degraded**	Capability decoupling: the release obligation requires a person to consciously	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	requirements. The following aspects are considered: availability of a risk assessment of the external IT services, legal, regulatory, and contractual requirements."		select a specific external service and submit it for review. However, AI assistants with tool access can independently call external services as part of a task without anyone ever submitting this specific service for approval. No technical lock (e.g. network/access control) mentioned in the wording.	
must	"The external IT services have been harmonized with the protection need of the processed information assets."	Not affected	Checks whether the classification of the service fits the protection needs of the data — an assignment decision, not a defensive measure.	CISO Function
should	"Requirements regarding the procurement, commissioning and release associated with the use of external IT services are determined and fulfilled."	Not affected	procurement target.	Purchasing/Supplier Management
should	"A procedure for release in consideration of the protection need is established."	Not affected	Procedure for the release.	CISO Function
should	"External IT services and their approval are documented."	Not affected	Documentation obligation.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
should	"It is verified at regular intervals that only approved external IT services are used."	**Partially degraded**	Time compression: a fixed-spaced sampling check leaves a window of time open for an unreleased service to go undetected — greater than the response time of an automated attack without ongoing automated detection.	IT Operations

Overall classification: Partially demoted (2 out of 6 requirements affected), regardless of protection needs.
Curing reference: MHC-10, MHC-13 (see Part 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?

Level	Requirement (original wording)	Category	Justification	Responsible
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 requirements, software use rights and licensing, source/reputation of the software."	**Partially degraded**	Capability decoupling: an AI-supported programming assistant can independently reload software packages as part of a task without a human consciously submitting this specific package for approval.	Development/Engineering

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Software approval also applies to special purpose software such as maintenance tools."	**Partially degraded**	Same reasoning as above, here only scope clarification.	Development/Engineering
should	"The types of software such as firmware, operating systems, applications, libraries, device drivers to be managed are determined."	Not affected	Scoping governance.	IT Operations
should	"Repositories of managed software exist."	Not affected	Infrastructure existence.	IT Operations
should	"The software repositories are protected against unauthorized manipulation."	**Partially degraded**	The strength of the protection is open: a pure access list is unlikely to withstand a sufficiently capable automated attack, but a cryptographic signature check is — the wording is not fixed.	IT Operations
should	"Approval of software is regularly reviewed."	**Partially degraded**	Time compression: "regularly" without a specific reason for testing.	IT Operations
should	"Software versions and patch levels are known."	**Partially degraded**	Pure knowledge of the version and patch status says nothing about the reaction speed. When there are only hours between the vulnerability disclosure and a functioning attack,	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
			knowledge alone is not enough.	
very high	"Additional requirements for software use (e.g., need for control or monitoring of usage) are determined (if any) (C, I, A)"	Not affected	Too vaguely worded ("if applicable") for a concrete assessment.	IT Operations

Overall classification: Partially demoted (5 out of 8 requirements affected), regardless of protection needs.
Curing reference: MHC-10, MHC-09, MHC-13 (see Part II)

1.4.1 — To what extent are information security risks managed?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Risk assessments are carried out both at regular intervals and in response to events."	Not affected	Double trigger invalidates time compression concerns.	CISO Function
must	"Information security risks are appropriately assessed (e.g., for probability of occurrence and potential damage)."	**Partially degraded**	Capability decoupling: classic assessments of the probability of occurrence often assume that certain attacks are only accessible to a few highly specialized actors. This assumption no longer holds when AI tools make the same capability widely available. No updated valuation methodology required.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Information security risks are documented."	Not affected	Documentation obligation.	CISO Function
must	"A responsible person (risk owner) is assigned to each information security risk."	Not affected	Governance.	CISO Function
should	"A procedure is in place defining how to identify, assess and address security risks within the organization."	Not affected	Governance.	CISO Function
should	"Criteria for the assessment and handling of security risks exist."	**Partially degraded**	Same reasoning as above, here at the level of the evaluation criteria instead of the result.	CISO Function
should	"Measures for handling security risks and the persons responsible for these are specified and documented."	Not affected	Governance/Tracking.	CISO Function
should	"In case of changes to the environment (e.g., organizational structure, location, changes to regulations), reassessment is carried out in a timely manner."	Not affected	Occasion-related trigger available.	CISO Function

Overall classification: Partially demoted (2 out of 8 requirements affected), regardless of protection needs.
Reference to hardening: individual measure (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Observation of policies is verified throughout the organization."	Not affected	Existence of verification, governance.	CISO Function
must	"Information security policies and procedures are reviewed at regular intervals."	**Partially degraded**	Time compression: "regularly" without a specific reason for testing.	CISO Function
must	"Measures for correcting potential non-conformities (deviations) are initiated and pursued."	Not affected	Correction process, governance.	CISO Function
must	"Compliance with information security requirements (e.g., technical specifications) is verified at regular intervals."	**Partially degraded**	Same reasoning as above.	CISO Function
must	"The results of the conducted reviews are recorded and retained."	Not affected	Documentation obligation.	CISO Function
should	"A plan for content and framework conditions (time schedule, scope, controls) of the reviews to be conducted is provided."	Not affected	Planning artifact.	CISO Function
SGA	"Internal controls are implemented for all entities within the assessment scope."	Not affected	Reach requirement, governance.	CISO Function
SGA	"The implementation of all applicable security requirements and control objectives are included."	Not affected	Completeness requirement, governance.	CISO Function
SGA	"Suitably qualified and appropriate information security audit responsibilities and resources are defined."	Not affected	Resource/qualification governance.	CISO Function
SGA	"A detailed internal audit plan and schedule is defined and followed. [Entire assessment scope covered, Internal audits	**Partially degraded**	Time compression: the same "regularly without occasion reference" finding	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
	conducted regularly, Results tracked within ISMS structures]"		as for the must element above, here related to the group-wide audit plan — newly added sites without an occasion trigger are not necessarily included in the audit plan in a timely manner.	

Overall classification: Partially demoted (3 out of 10 requirements affected), regardless of protection needs.
Curing reference: MHC-10 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Information security reviews are carried out by an independent and competent body at regular intervals and after fundamental changes."	Not affected	Double trigger ("regularly AND after significant changes") — counterexample to 1.5.1, shows: the concrete formulation decides, not the topic itself.	CISO Function
must	"Measures for correcting potential deviations are initiated and pursued."	Not affected	Correction process.	CISO Function
should	"The results of conducted reviews are documented and reported to the management of the organization."	Not affected	Documentation/reporting.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
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))."	Not affected	Event-triggered ("in case of fundamental changes"), well formulated — same reasoning as for the must element above.	CISO Function
SGA	"Findings and implementation of corrective actions is tracked by the independent entity."	Not affected	Tracking process.	CISO Function

Overall classification: Not affected (0 out of 5 requirements affected), regardless of protection needs.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders."	Not affected	Definition governance.	CISO Function
must	"Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters."	**Partially degraded**	Aggregation resistance: a reporting system that depends on a person noticing something conspicuous does not recognize an attack that is deliberately broken down into many small steps that	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
			seem harmless in themselves — not a single step is noticeable.	
must	"Adequate channels for communication with event reporters exist."	Not affected	Infrastructure/Process.	CISO Function
should	"A common point of contact for event reporting exists."	Not affected	Organisationally.	CISO Function
should	"Different reporting channels according to perceived severity ... are available."	Not affected	Process/Infrastructure.	CISO Function
should	"Employees are obligated and trained to report relevant events."	Not affected	Compulsory training.	Human Resources
should	"Security event reports can also be submitted by external parties."	Not affected	Process/Channel.	CISO Function
should	"Mechanism to, and information how to, report incidents is accessible by all relevant reporters."	Not affected	Accessibility.	CISO Function
should	"A feedback procedure to reporters is established."	Not affected	process.	CISO Function
very high	"Tests and exercises of event and observation reporting are conducted regularly. (C, I, A)"	Not affected	Test activity — Consistently not treated like live detection (see 1.6.2).	CISO Function

Overall classification: Partially demoted (1 out of 9 requirements affected), regardless of protection needs.
Curing reference: MHC-05 (see Part II)

1.6.2 — To what extent are reported security events managed?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Reported events are processed without undue delay."	**Partially degraded**	Time compression: requires humans to complete the processing at the necessary pace. If an attacker carries out most of his or her procedure automatically and without human intervention, purely human-based processing cannot keep up structurally — automation is not required.	IT Operations
must	"An adequate reaction to reported security events is ensured."	**Partially degraded**	Same reasoning as above.	IT Operations
must	"Lessons learned are incorporated into continuous improvement."	Not affected	Improvement process.	CISO Function
should	"During processing, reported events are categorized, qualified, and prioritized."	Not affected	Process/Methodology.	IT Operations
should	"Responsibilities for handling events based on their category are defined and assigned."	Not affected	Governance.	CISO Function
should	"A strategy for reporting potentially criminal aspects of security incidents to relevant authorities when necessary or appropriate."	Not affected	Legal process.	Legal Department
high	"Maximum response times based on class,	**Partially degraded**	Defining a target does not mean that it can be met against an automated and	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	category and severity are defined."		fast-acting attacker — there is no automation obligation for this.	
high	"Events not processed appropriately according to their priority are escalated."	**Partially degraded**	Sensible safety net, but remains human-borne itself and does not resolve the time compression gap of the previous line.	IT Operations
high	"Lawful, regulatory, and contractual reporting obligations, and respective contact information are known."	Not affected	Legal knowledge.	Legal Department
high	"A communication strategy for security-related events exists."	Not affected	Communication planning.	CISO Function
high	"Procedures for response to supplier security incidents are established."	Not affected	Process, deepened in Chapter 6.	Purchasing/Supplier Management
very high	"Handling of events in different categories and priorities is regularly tested."	Not affected	Test activity.	CISO Function
SGA	"Standard mechanisms to report and track relevant security events are established."	Not affected	standardization requirement for group-wide consistency; the detection/response speed itself is already rated above.	CISO Function

Overall classification: Partially demoted (4 out of 13 requirements affected), regardless of protection needs.
Curing reference: MHC-11 (see Part II)

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

Data quality note: the column "high" contains five strikingly similar pairs of requirements in the source catalog. Only one pair is word-for-word (counted once, 19 instead of 20 raw lines); the remaining four differ editorially from each other (typos or different wording in the source catalog itself, including "outage of" vs. "outage oaf", "Methods" vs. "Instruments to monitor communication") and are listed below as separate lines.

Level	Requirement (original wording)	Category	Justification	Responsible
must	"An appropriate plan to react to and recover from crisis situations exists and the required resources are available."	Not affected	Planning existence.	CISO Function
must	"Responsibilities and authority for crisis management within the organization are defined, documented, and assigned."	Not affected	Governance.	CISO Function
must	"The responsible employees are defined and qualified for their task."	Not affected	Governance/Human Resources.	CISO Function
should	"Methods to detect crisis situations are established. General indications for the existence or imminence of a crisis situation and specific predictable crisis are identified."	**Partially degraded**	Aggregation resistance and time compression: classic crisis detection is designed for gradually escalating situations. An IT incident that grows from many small, inconspicuous steps into a real crisis within hours is more likely to be detected too late.	IT Operations
should	"A procedure to invoke and/or escalate crisis management is in place."	Not affected	process.	CISO Function
should	"Strategic goals and their priority in crisis situations are defined and known to relevant personnel."	Not affected	Governance.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
should	"A crisis management team is defined and approved."	Not affected	Governance.	CISO Function
should	"Crisis policies and procedures are defined and approved."	Not affected	Governance.	CISO Function
should	"Crisis planning is reviewed and updated regularly."	**Partially degraded**	Time compression: "regularly" without a specific reason for testing.	CISO Function
high	"Relevant different potential crisis scenarios are identified."	**Partially degraded**	The example scenarios mentioned (personnel, resource, infrastructure failure) are classic failure scenarios; it does not explicitly provide for an AI-orchestrated, multi-pronged attack with rapid escalation.	CISO Function
high	"Relevant different potential crisis scenarios are identified." (second version of the catalogue, see data quality note)	**Partially degraded**	Identical requirement in terms of content, editorially listed twice in the source catalogue with different wording ("outage of" vs. "outage oaf") — same reason as the previous line.	CISO Function
high	"Necessary resources and information to handle crisis ... are identified."	Not affected	Resource planning.	CISO Function
high	"Necessary resources and information to handle crisis ... are identified." (second version of the catalogue, see data quality note)	Not affected	resource planning; editorial duplicate of the preceding line.	CISO Function
high	"A communication strategy for crisis situations exists."	**Partially degraded**	The same time compression concern as with crisis detection:	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
			no reference to a greatly shortened reaction window.	
high	"A communication strategy for crisis situations exists." (second version of the catalogue, see data quality note)	**Partially degraded**	Identical requirement in terms of content, editorially listed twice in the source catalog with different wording ("Methods" vs. "Instruments to monitor communication") — same reason as the previous line.	CISO Function
high	"The efficiency, feasibility, and appropriateness of the crisis planning is evaluated regularly."	**Partially degraded**	Time compression: "regularly" without a specific reason for testing.	CISO Function
high	"Spot based testing of crisis planning is conducted."	Not affected	Test activity.	CISO Function
high	"Spot based testing of crisis planning is conducted." (second version of the catalogue, see data quality note)	Not affected	Test activity; editorial duplicate of the preceding line.	CISO Function
very high	"Crisis exercises and simulations involving all relevant persons, including decision makers are conducted regularly."	Not affected	Test activity.	CISO Function

Overall classification: Partially demoted (7 out of 19 requirements affected), regardless of protection needs.
Hardening reference: MHC-10, MHC-05, individual measure (see Part II)

Summary Chapter 1

Control	Overall classification	Proportion affected
1.1.1	Partially degraded	1/10

Control	Overall classification	Proportion affected
1.2.1	Partially degraded	1/7
1.2.2	Not affected → from high: Partially degraded	0/7 → 1/8
1.2.3	Not affected	0/5
1.3.1	Partially degraded	1/3
1.3.2	Not affected	0/4
1.3.3	Partially degraded	2/6
1.3.4	Partially degraded	5/8
1.4.1	Partially degraded	2/8
1.5.1	Partially degraded	3/10
1.5.2	Not affected	0/5
1.6.1	Partially degraded	1/9
1.6.2	Partially degraded	4/13
1.6.3	Partially degraded	7/19

10 of 14 controls consistently demoted, 3 consistently unaffected, 1 depending on protection needs. No stability, no pure friction — to be expected, since Chapter 1 is a pure governance chapter with no cryptographic or architectural hard barriers. Two recurring patterns carry the high proportion of degraded: **(1)** "regular/periodic" without a specific reason for testing, **(2)** human-borne reporting/reaction speed towards an automated attacker. Responsible predominantly CISO function/ISMS processes — consistent with this being the governance chapter. SGA requirements (6 controls affected, 10 additional requirements, including 1 demoted) do not change the overall classification of any of the 14 controls — they expand the scope at the group level without introducing new weaknesses.

Chapter 2 — Human Resources (4 Controls, 21 Requirements)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Sensitive work fields and jobs are determined."	Not affected	Scoping governance.	Human Resources
must	"The requirements for employees with respect	Not affected	Governance.	Human Resources

Level	Requirement (original wording)	Category	Justification	Responsible
	to their job profiles are determined and fulfilled."			
must	"The identity of potential employees is verified (e.g., checking identity documents)."	**Partially degraded**	Capability decoupling: convincing fake identity documents and, in combination with video interviews, deepfake identities have so far been considered specialist knowledge. AI-generated document forgery and real-time video/audio deepfakes make deceptively real identity impersonation in the hiring process widely available today (well-known current pattern: fake remote employees).	Human Resources
should	"The personal suitability of potential employees is verified by means of simple methods (e.g., job interview)."	**Partially degraded**	Same reasoning: a live interview as a verification method is exactly the goal of real-time deepfake impersonation.	Human Resources
should	"An extended suitability verification depending on the respective work field and job is conducted (e.g., assessment centre, psychological analysis, checking of references,	**Partially degraded**	Capability decoupling: References, certificates, and diplomas can be forged more convincingly with AI tools than before;	Human Resources

Level	Requirement (original wording)	Category	Justification	Responsible
	certificates and diploma, checking of certificates of conduct, checking of professional and private background)."		even fictitious reference persons/companies are easier to portray.	

Overall classification: Partially demoted (3 out of 5 requirements affected), regardless of protection needs. Consistent theme: all three identity/suitability checks rely on human verification, which is based on "authenticity features" that are no longer reliable today.
Curing reference: MHC-15 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"A non-disclosure obligation is in effect."	Not affected	Contractually speaking, no reference to the challenge.	Legal Department
must	"An obligation to comply with the information security policies is in effect."	Not affected	Contract.	Legal Department
should	"A non-disclosure obligation beyond the employment contract is in effect."	Not affected	Contract.	Legal Department
should	"Information security aspects are considered in the employment contracts of the staff."	Not affected	Contract.	Legal Department
should	"A procedure for handling violations of said obligations is described."	Not affected	Process/Governance.	Human Resources

Overall classification: Not affected (0 out of 5 requirements affected), regardless of protection needs. Pure contract law without technical or behavioural protection — not affected by Mythos.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Employees are trained and made aware."	**Partially degraded**	Skill decoupling: classic awareness content trains the recognition of spelling mistakes, impersonal salutations and other "tells" of phishing/social engineering. AI-generated attacks are flawless, personalized, and linguistically unobtrusive — the trained identifiers no longer work reliably.	Human Resources
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]"	Not affected	Existence of a structured concept, governance.	CISO Function
should	"Target groups for training and awareness measures... are identified and considered in a training concept."	Not affected	Scoping governance.	CISO Function
should	"The concept has been approved by the responsible management."	Not affected	Release act.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
should	"Training and awareness measures are carried out both at regular intervals and in response to events."	Not affected	Double trigger invalidates the time compression concern.	Human Resources
should	"Participation in training and awareness measures is documented."	Not affected	Documentation obligation.	Human Resources
should	"Contact persons for information security are known to employees."	Not affected	Communication/Governance.	CISO Function

Overall classification: Partially demoted (1 out of 7 requirements affected), regardless of protection needs. The finding does not concern the existence or organization of training courses, but their *content*: Training concepts that do not explicitly convey that classic identifying features of deception attempts no longer apply leave the workforce with a false sense of security.
Curing reference: MHC-15 (see Part II)

2.1.4 — To what extent is mobile work regulated?

Level	Requirement (original wording)	Category	Justification	Responsible
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]"	Not affected	Physical-behavioral requirements; the technical access security is evaluated independently in 4.1.2/5.1.2, no double counting here.	IT Operations
should	"[Measures for travelling e.g., viewing by authorities,	Not affected	Travel/physical security, no specific Mythos reference.	CISO Function

Level	Requirement (original wording)	Category	Justification	Responsible
	Measures for travelling to security-critical countries]"			
should	"Employee awareness."	Not affected	In the context of this control, related to physical travel risks (over-the-shoulder looks, theft), not to the general phishing/social engineering training from 2.1.3.	Human Resources
high	"Protective measures against overhearing and viewing are implemented. (C)"	**Stable**	Physical/technical countermeasure (privacy screen, shielded rooms) — a hard barrier that acts regardless of the attacker's ability.	IT Operations

Overall classification: In case of normal need for protection Not affected (0 of 3 requirements affected) — no need for action. If there is a high need for protection, a physical stability requirement is added (privacy/eavesdropping protection); since there is no degraded requirement, the overall rating from high to **steady**. Practical: for mobile work scenarios with high/very high protection requirements, physical shielding is demonstrably effective and SoA-citable.

Summary Chapter 2

Control	Overall classification	Proportion affected
2.1.1	Partially degraded	3/5
2.1.2	Not affected	0/5
2.1.3	Partially degraded	1/7
2.1.4	Not affected → from high: Steadfast	0/3 → Stable

Chapter 2 shows a new pattern compared to Chapter 1: the degraded findings do not arise from vague test cycles, but from **human identity and aptitude verification** (recruitment process, awareness content), which is based on recognition features that are no longer reliable today — the same skill decoupling that is proven in the methodology in the JadeBuffer case can be seen

here at the level of identity verification instead of technical attack execution. First stationary example of the catalogue (physical privacy/eavesdropping protection).

Chapter 3 — Physical Security (4 controls, 14 requirements, including 1 control without its own requirements)

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

Level	Requirement (original wording)	Category	Justification	Responsible
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]"	Not affected	Concept Existence, Governance; the effectiveness of the measures themselves will be assessed in the following lines.	Facility/Plant Security
must	"The defined protective measures are implemented."	**Partially degraded**	The wording remains open as to WHICH measures will be implemented. Insofar as access control is based on human verification (reception, security service), it is vulnerable to AI-supported deception (fake IDs, convincing legends on the phone) — capability decoupling.	Facility/Plant Security
must	"The code of conduct for security zones is known to all persons involved."	Not affected	Communication of rules of conduct.	Facility/Plant Security

Level	Requirement (original wording)	Category	Justification	Responsible
should	"Procedures for allocation and revocation of access rights are established."	Not affected	Management process for physical access rights.	Facility/Plant Security
should	"Visitor management policies (including registration and escorting of visitors) are defined."	**Partially degraded**	Capability decoupling: Visitor registration/accompaniment is based on the verification of fake identity and appointments (fake supplier legitimation, fake appointment confirmation by phone/e-mail) — today it is easier to present.	Facility/Plant Security
should	"Policies for carrying along and using mobile IT devices and mobile data storage devices... are defined and implemented."	Not affected	Equipment Directive, technically deepened in 3.1.4.	IT Operations
should	"Network/infrastructure components (own or customer networks) are protected against unauthorized access."	**Stable**	Physical locking/enclosure of network components (server room, distribution cabinet) is a hard barrier regardless of attacker capability; the human access decision is already assessed in the preceding lines (no double counting).	Facility/Plant Security

Level	Requirement (original wording)	Category	Justification	Responsible
should	"External properties used for storing and processing information assets are considered in the security zone concept..."	Not affected	Scoping completeness.	Facility/Plant Security
high	"Protective measures against simple overhearing and viewing are implemented. (C)"	**Stable**	Physical-architectural measure, tough and independent of attackers.	Facility/Plant Security

Overall classification: Partially demoted (2 out of 9 requirements affected), regardless of protection needs. Two fixed elements (network component containment, privacy/eavesdropping protection from high) exist in parallel, but do not change the overall classification, as the human-mediated access/visitor check remains as a weak point.
Curing reference: MHC-15 (see Part II)

3.1.2 — Superseded by 1.6.3, 5.2.8 and 5.2.9

No own requirements — content fully covered in the mentioned controls. No classification required.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The requirements for the handling of supporting assets (e.g., transport, storage, repair, loss, return, disposal) are determined and fulfilled."	Not affected	Governance guidance for the lifecycle of physical assets; the technical disposal strength is evaluated separately below.	IT Operations
high	"Disposal of supporting assets is conducted in accordance with one of the relevant standards (e.g. ISO 21964, at least security level 4). (C)"	**Stable**	Physical destruction norm (e.g., defined shredder particle size) is a tough, verifiable process	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
			— an AI-powered attacker capability does not help reconstruct properly shredded disks.	

Overall Rating: For normal protection needs Not affected (0 out of 1) — only a general process requirement. If there is a high need for protection, a physical destruction standard is added, and the overall classification becomes **stable**. Practically: a positive example — TISAX® explicitly requires a resilient, Mythos-resistant disposal method for higher protection requirements.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The requirements for mobile IT devices and mobile data storage devices are determined and fulfilled. [Encryption, Access protection e.g. PIN/password, Marking]"	**Partially degraded**	"Encryption" is only one of several equally mentioned aspects, not mandatory and comprehensively prescribed (this only happens at high). Where encryption is absent or only partially present, PIN/password protection remains the effective barrier — vulnerable to automated/AI-assisted guessing	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
			or social engineering.	
should	"Registration of the IT devices."	Not affected	Inventory.	IT Operations
high	"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)"	**Stable**	Committed to *general* (comprehensive) encryption — a hard cryptographic barrier that specifically closes the gap open at the must level.	IT Operations

Overall classification: With normal protection requirements Partially demoted (1 out of 2) because there is only an incomplete encryption requirement. If there is a high need for protection, the obligation for general encryption closes precisely this gap — overall classification becomes **stable**. Practical: Devices with normal protection requirements remain structurally less protected than those with high/very high protection requirements; check whether "normal" devices in your inventory are in fact still fully encrypted.
Reference to hardening: individual measure (see Part II)

Summary Chapter 3

Control	Overall classification	Proportion affected
3.1.1	Partially degraded	2/9
3.1.2	(no requirements)	–
3.1.3	Not affected → from high: Steadfast	0/1 → Stable
3.1.4	Partially demoted → from high: Stable	1/2 → Stable

Physical security provides the densest concentration of stability to date: physical destruction, general encryption, privacy/eavesdropping protection, and enclosure of network technology are all hard, attacker-independent barriers. The remaining degraded findings consistently arise at the same point: the human-mediated access/visitor check.

Chapter 4 — Identity and Access Management (4 Controls, 37 Requirements)

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

Level	Requirement (original wording)	Category	Justification	Responsible
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]"	Not affected	Lifecycle governance for IDs/tokens; the actual counterfeit protection is the subject of other controls (cryptography: 5.1.1).	IAM Team
should	"Identification means can be produced under controlled conditions only."	Not affected	Controls the legitimate issuance channel (only authorized entities produce badges) — a governance control over the manufacturing process, not a statement about third-party	IAM Team

Level	Requirement (original wording)	Category	Justification	Responsible
			counterfeit detection.	
high	"A strategy of blocking or invalidation of identification means in case of loss is prepared and implemented as far as possible. (C, I, A)"	**Partially degraded**	Time compression: "as far as possible" without mandatory immediate/automated blocking leaves a time window open in which a lost or copied means of identification remains valid — an automated attacker exploits exactly this window faster than a manual blocking can take effect.	IAM Team

Overall classification: In case of normal protection needs Not affected (0 of 2 requirements affected). If there is a high need for protection, the blocking/invalidity strategy is added, whose non-binding wording ("as far as possible") opens up a time compression gap — overall classification is **partially downgraded** (1 out of 3). Practical: check whether your blocking processes for lost IDs/tokens actually take effect automatically/immediately instead of relying on the optional wording.
Curing reference: MHC-03 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
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)."	Not affected	selection methodology; the strength of the selected method is evaluated independently in the following line.	IAM Team
must	"State of the art procedures for user authentication are applied."	**Partially degraded**	Capability decoupling/time compression: "State of the art" does not explicitly oblige phishing-resistant methods (e.g. FIDO2/WebAuthn). Automated real-time phishing relays (adversary-in-the-middle) undermine OTP/push-based practices, which are still considered "state of the art" in many organizations. Target state: a mandatory use of phishing-resistant procedures would raise this requirement to a stable level, as the assumption of protection would then be structural and not just gradual.	IAM Team
should	"The user authentication procedures are defined and	Not affected	Process of deriving requirements.	IAM Team

Level	Requirement (original wording)	Category	Justification	Responsible
	implemented based on the business-related and security-relevant requirements"			
should	"Users are authenticated at least by means of strong passwords according to proven and widely accepted practices."	**Pure friction**	The protective assumption of this requirement — only the authorized person knows the password — no longer applies to automated, AI-scaled phishing, regardless of the password strength: the attacker receives the correct password directly from the user, not by guessing. Unlike the line below (privileged accounts, where PAM offers at least session monitoring as partial protection), there is no second factor and no compensation mechanism in the wording — the requirement loses its core effect completely, not just partially.	IAM Team
should	"Superior procedures are used for the authentication of privileged user accounts (e.g., privileged access management, two-factor authentication)."	**Partially degraded**	The "e.g." formulation allows simple two-factor authentication without phishing resistance to suffice — the same AITM relay vulnerability as above, here related to privileged accounts.	IAM Team

Level	Requirement (original wording)	Category	Justification	Responsible
			Remains "only" degraded instead of friction, because PAM as a mentioned alternative can offer additional session monitoring/time limit, which partially absorbs a compromised factor.	
high	"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)"	**Partially degraded**	The options list allows fulfillment via weaker measures (automatic logout, brute force protection) that do not address the AITM/phishing relay vulnerability; only the option "continuous access monitoring" would actually help, but is not mandatory.	IAM Team
very high	"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)"	**Partially degraded**	Same gap as above: the example mentions classic two-factor authentication instead of explicitly phishing-resistant methods.	IAM Team

Overall classification: Pure friction (1 out of 7 requirements completely loses the core effect; a total of 5 out of 7 affected, 4 of which remain effective but weakened), regardless of the need for protection. According to the hierarchy convention (Pure Friction > Partially Demoted > Stable > Not Affected), the pure password factor determines the overall classification, even if the other four detections of this control are only weakened, not ineffective. The first pure friction finding of the entire catalog — the consistent pattern in control remains the lack of a phishing-resistant (FIDO2/WebAuthn-like) authentication obligation. Target state: with a mandatory phishing-resistant procedure (FIDO2/WebAuthn/Passkey) for all seven requirements, the control would be

stable throughout, not just the pure password factor solved — this target state is the subject of MHC-03 (see Part II).
Curing reference: MHC-03 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The creating, changing, and deleting of user accounts is conducted."	Not affected	Basic process.	IAM Team
must	"Unique and personalized user accounts are used."	Not affected	Traceability principle, structural.	IAM Team
must	"The use of \"shared accounts\" is regulated (e.g., restricted to cases where traceability of actions is dispensable)."	Not affected	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)."	Not affected	"immediately" is a clear instant trigger without a time compression gap in the wording.	IAM Team
must	"User accounts are regularly reviewed."	**Partially degraded**	Time compression: periodic check without reference to the occasion leaves orphaned/superfluous accounts undetected between cycles.	IAM Team
must	"The login information is provided to the user in a secure manner."	Not affected	Submission process.	IAM Team

Level	Requirement (original wording)	Category	Justification	Responsible
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]"	Not affected	Hygiene/Conduct Policy; the mechanism strength of authentication itself is assessed independently in 4.1.2 (no double counting).	IAM Team
should	"A basic user account with minimum access rights and functionalities is existent and used."	Not affected	Least privilege baseline, structural.	IAM Team
should	"Default accounts and passwords pre-configured by manufacturers are disabled (e.g., by blocking or changing of password)."	Not affected	One-time curing step; closed as soon as implemented, regardless of attacker ability.	IT Operations
should	"User accounts are created or authorized by the responsible body."	Not affected	Governance.	IAM Team
should	"Creating user accounts is subject to an approval process (four-eyes principle)."	Not affected	Four-eyes principle, organizationally robust.	IAM Team
should	"User accounts of service providers are disabled upon completion of their task."	Not affected	Clearly event-triggered.	IAM Team
should	"Deadlines for disabling and deleting user accounts are defined."	Not affected	Governance/Deadline Setting.	IAM Team

Level	Requirement (original wording)	Category	Justification	Responsible
should	"The use of default passwords is technically prevented."	Not affected	Technical enforcement, binary, uniquely effective.	IT Operations
should	"Where strong authentication is applied, the use of the medium (e.g., ownership factor) is secure."	**Partially degraded**	Capability decoupling: the possession factor (e.g., phone number for SMS OTP) is vulnerable through SIM swapping; convincing pretending to telco support employees has become easier with AI support.	IAM Team
should	"User accounts are reviewed at regular intervals. This also includes user accounts in customers' IT systems."	**Partially degraded**	Same time compression justification as for the must element above, here additionally related to customer systems.	IAM Team
should	"Interactive login for service accounts (technical accounts) is technically prevented."	Not affected	Technical, structural enforcement.	IT Operations

Overall rating: Partially demoted (3 out of 17 requirements affected), regardless of protection needs (Control has no high/very-high requirements).
Curing reference: MHC-10, MHC-03 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
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]"	Not affected	Event-triggered withdrawal logic ("when no longer needed") instead of vague periodicism — well formulated.	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."	**Partially degraded**	Time compression: classic periodic review pattern without occasion reference.	IAM Team
should	"Strategies for authorizing access to information are prepared."	Not affected	Governance.	IAM Team
should	"Authorization roles are used."	Not affected	RBAC design, structural.	IAM Team
should	"Rights are allocated on a need-to-use basis and according to the role and/or area of responsibility."	Not affected	Design principle.	IAM Team
should	"Normal user accounts are not granted privileged access rights."	Not affected	Structural separation.	IAM Team
should	"The user's access rights are updated after the user's responsibilities have changed (e.g., to another field of responsibility)."	Not affected	Event-triggered, well formulated.	IAM Team
high	"The access rights are approved by the responsible internal	Not affected	Additional release governance.	IAM Team

Level	Requirement (original wording)	Category	Justification	Responsible
	Information Officer. (C, I, A)"			
very high	"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)"	**Stable**	File-level content encryption is a hard cryptographic barrier that works even against privileged insiders or bypassed access controls.	IT Operations
very high	"Existing access rights are regularly reviewed at shorter intervals (e.g., quarterly). (C)"	**Partially degraded**	Shortens the test interval, but remains periodically without reference to the occasion — the structural time compression gap remains, only the time window becomes smaller.	IAM Team

Overall classification: Partially degraded (1 out of 7 requirements affected by normal protection needs; 2 out of 10 incl. high/very high), regardless of protection needs. Remarkably, if there is a very high need for protection, file level encryption adds a real stable element, but it does not overturn the overall classification, since the periodic access check remains as an independent weakness.
Curing reference: MHC-10 (see Part II)

Summary Chapter 4

Control	Overall classification	Proportion affected
4.1.1	Not affected → from high: Partially degraded	0/2 → 1/3
4.1.2	Pure friction	1/7 (friction) + 4/7 (degraded)
4.1.3	Partially degraded	3/17
4.2.1	Partially degraded	1/7 → 2/10

Identity and Access Management provides the first and so far only pure friction finding of the entire catalog: the pure password factor in 4.1.2 loses its core effect against automated phishing completely, not only partially. Control also remains the most affected overall (5 out of 7 requirements) — a consistent pattern is the lack of an explicit obligation for phishing-resistant authentication. In addition, the well-known periodic review pattern is repeated (4.1.1, 4.1.3, 4.2.1). A steady ray of hope for very high protection requirements: content-based encryption (4.2.1).

Chapter 5 — IT Security/Cyber Security (15 Controls, 105 Requirements, Largest Chapter)

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

Level	Requirement (original wording)	Category	Justification	Responsible
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."	**Stable**	Committed to industry-standard cryptography. Correctly implemented modern cryptography (AES-256, up-to-date TLS, etc.) is mathematically hard against a Gen AI-powered attacker — AI does not shorten factorization or brute force against modern key lengths. (Post-quantum risk is a separate threat field that is deliberately not covered here — not a Mythos/gene AI reference.)	CISO Function
should	"A concept for the application of cryptography is defined and implemented. [Methods, Key strengths, Full lifecycle: generation/storage/archivin	Not affected	Key Management Process, Governance; the cryptographic strength itself is already assessed above.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	g/retrieval/distribution/deactivation/renewal/deletion]"			
high	"Key sovereignty requirements (particularly in case of external processing) are determined and fulfilled. (C, I)"	Not affected	Legal-contractual sovereignty question (jurisdiction in cloud processing), no Mythos reference.	CISO Function

Overall classification: Stable (no degraded/friction element present), regardless of the need for protection. Properly implemented cryptography is one of the clearest examples of a true hard barrier in the entire catalog — directly citable as SoA evidence.

5.1.2 — To what extent is information protected during transfer?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The network services used to transfer information are identified and documented."	Not affected	Inventory/Governance.	IT Operations
must	"Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented."	Not affected	Governance.	IT Operations
must	"Measures for the protection of transferred contents against unauthorized access are implemented."	**Partially degraded**	Non-specific "measures" without a mandatory minimum standard (e.g. encryption) leave room for weaker protection, which can be undermined by an AI-supported attacker positioned in network technology. Only high/very high explicitly	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
			close the gap (see below).	
should	"Measures for ensuring correct addressing and correct transfer of information are implemented."	Not affected	Transmission correctness, not an attacker barrier in the narrower sense.	IT Operations
should	"Electronic data exchange is conducted using content or transport encryption according to the respective classification."	**Stable**	Explicitly commits to content or transport encryption — closes the must gap for organizations that implement this should element.	IT Operations
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]"	**Partially degraded**	Remote access is the preferred target of real-time phishing relay attacks (see 4.1.2) — VPN encryption protects the transport path, but does not solve the authentication weakness if it remains conventional (password/OTP).	IT Operations
high	"Information is transported or transferred in encrypted form (at least transport-encryption) or protected by similarly effective measures. (C)"	**Stable**	Explicit encryption obligation for high protection requirements.	IT Operations
very high	"Information is transported or transferred in content-encrypted form. (C)"	**Stable**	Content encryption, the strongest form — end-to-end security.	IT Operations

Overall classification: Partially demoted (2 out of 6 requirements affected), regardless of protection needs. Two separate vulnerabilities: the vague must formulation is largely closed by

the should element for encryption; however, the remote access authentication vulnerability (identical to the finding in 4.1.2) remains independent of all levels.
Curing reference: MHC-03, individual measure (see Part II)

5.2.1 — To what extent are changes managed?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Information security requirements for changes to the organization, business processes, IT systems are determined and fulfilled."	Not affected	Governance.	IT Operations
should	"A formal approval procedure is established."	Not affected	Governance.	IT Operations
should	"The potential impact on the information security of changes is assessed."	Not affected	Process evaluation.	IT Operations
should	"Changes affecting the information security are subjected to planning and testing."	Not affected	process.	IT Operations
should	"Procedures for fallback in fault cases are considered."	Not affected	Resilience governance.	IT Operations
high	"Compliance with the information security requirements is verified during and after the changes are applied. (C, I, A)"	Not affected	Double, clearly defined test time ("during and after") — well formulated, no time compression reference.	IT Operations

Overall classification: Not affected (0 of 6 requirements affected), regardless of protection needs. Clearly specified process control without a Mythos-relevant gap — a good example of consistently inconspicuous governance control.

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

Level	Requirement (original wording)	Category	Justification	Responsible
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."	Not affected	Evaluation process.	Development/Engineering
must	"A segmentation is implemented based on the results of risk analysis."	**Stable**	Architectural separation is a structural barrier: once implemented correctly, it works regardless of how an attacker automates his initial access attempt.	IT Operations
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]"	**Stable**	Deepens the same structural separation (separate profiles, no development tools in production) — architecturally excludes lateral movement and tool misuse in the production environment.	IT Operations

Overall classification: Stable (no degraded/friction element), regardless of the need for protection. Note: effectiveness applies to correctly implemented segmentation; an incomplete/incorrect implementation is an implementation question, not a weakness due to wording.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Requirements for protection against malware are determined."	Not affected	Governance.	IT Operations
must	"Technical and organizational measures for protection against malware are defined and implemented."	**Partially degraded**	Capability decoupling: Classic, signature-based malware protection is structurally weaker against AI-generated/polymorphic malware, as signatures only take effect after a variant becomes known.	IT Operations
should	"Unnecessary network services are disabled."	Not affected	Attack surface reduction, structural/binary.	IT Operations
should	"Access to network services is restricted to necessary access through suitable protective measures (see examples)."	Not affected	Access control, structural.	IT Operations
should	"Malware protection software is installed and updated automatically at regular intervals (e.g., virus scanner)."	**Partially degraded**	The example "virus scanner" signals signature-based detection; automatic but periodic updates are structurally lagging behind AI-generated variants.	IT Operations
should	"Received files and software are automatically inspected for malware prior to their execution (on-access scan)."	**Partially degraded**	Same signature recognition limit.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
should	"The entire data contents of all systems is regularly inspected for malware."	**Partially degraded**	Double weakness: periodic testing (time compression) and signature recognition (capability decoupling).	IT Operations
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]"	**Partially degraded**	Encrypted content structurally bypasses the gateway inspection — a well-known evasion route targeted by AI-powered attackers.	IT Operations
should	"Measures to prevent protection software from being deactivated or altered by users are defined and implemented."	Not affected	Tamper protection for the protection agent itself, structural/binary.	IT Operations
should	"For IT systems operated without the use of malware protection software, alternative measures... are implemented."	Not affected	Compensation control, generic.	IT Operations

Overall classification: Partially demoted (5 out of 10 requirements affected), regardless of protection needs. One of the most degraded controls in the catalog — signature-based malware detection — is a classic example of capability decoupling: AI-generated, polymorphic malware systematically undermines signature matching.
Curing reference: MHC-05 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Information security requirements regarding the handling of event logs are determined and fulfilled."	Not affected	Governance.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled."	Not affected	Scoping.	IT Operations
must	"The IT systems used are assessed regarding the necessity of logging."	Not affected	Evaluation process.	IT Operations
must	"When using external IT services, information on the monitoring options is obtained and considered in the assessment."	Not affected	Supplier/governance aspect.	IT Operations
must	"Event logs are checked regularly for policy violations and noticeable problems in compliance with the permissible legal and organizational provisions."	**Partially degraded**	Aggregation resistance and time compression: Periodic manual checks aimed at "conspicuous" events do not structurally detect an attack that is deliberately fragmented into many inconspicuous individual steps.	IT Operations
should	"A procedure for the escalation of relevant events to the responsible body... is defined and established."	Not affected	Downstream escalation process.	IT Operations
should	"Event logs (contents and meta data) are protected against alteration. (e.g., by a dedicated environment)."	**Stable**	Tamper protection for log data (e.g. WORM memory, separate log system) is a structural barrier, regardless of attacker capability.	IT Operations
should	"Adequate monitoring and recording of any actions on	Not affected	existence of the record; the evaluation quality	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	the network that are relevant to information security are established."		has already been assessed above.	
high	"Information security requirements relevant to the security during the handling of event logs, e.g., contractual requirements, are determined and implemented. (C, I, A)"	Not affected	Contractual/governance-related.	IT Operations
high	"Events related to establishing and terminating remote access sessions (e.g., for remote maintenance). (C, I, A)"	Not affected	Scoping (what is logged), not an evaluation statement.	IT Operations
very high	"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)"	Not affected	Scoping.	IT Operations

Overall classification: Partially demoted (1 of 8 requirements affected), regardless of protection needs. The weakness lies specifically in the *evaluation* ("regularly checked"), not in the logging itself — the log integrity is even well secured with its own stability element.
Curing reference: MHC-05 (see Part II)

5.2.5 — To what extent are vulnerabilities identified and addressed?

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Information on technical vulnerabilities for the IT systems in use is gathered (e.g., information from the manufacturer, system audits, CVS database) and evaluated (e.g., Common	Not affected	Information gathering; the time-critical evaluation is done in the next line.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	Vulnerability Scoring System CVSS)."			
must	"Potentially affected IT systems and software are identified and the risk caused by the vulnerability is assessed."	**Partially degraded**	Collapse of the patch gap window (see Methodology, Cogent Security Evaluation 2026): classic risk assessments usually calculate with weeks until a working exploit. If proven by AI-supported exploit development, this window is shortened to less than a day in some cases — an evaluation methodology without this consideration systematically underestimates the urgency.	IT Operations
must	"Risks arising from vulnerabilities are treated."	Not affected	treatment process, downstream.	IT Operations
should	"An adequate patch management is defined and implemented (e.g., patch testing and installation)."	**Partially degraded**	Same patch gap reasoning: "adequate" without a mandatory speed SLA does not guarantee a pace that can keep up with AI-accelerated exploit availability.	IT Operations
should	"Risk minimizing measures are implemented, as necessary."	Not affected	Generic compensation measure.	IT Operations
should	"Successful installation of patches is verified in an appropriate manner."	Not affected	Quality assurance, downstream.	IT Operations

Overall classification: Partially demoted (3 out of 6 requirements affected), regardless of protection needs. The central finding of the entire catalog: this control directly depicts the shift "collapse of the patch gap window" documented in the methodology — priority for the later curing controls synthesis.
Curing reference: MHC-09 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Requirements for auditing IT systems or services are determined."	Not affected	Governance.	IT Operations
must	"The scope of the system audit is specified in a timely manner."	Not affected	Planning.	IT Operations
must	"System or service audits are coordinated with the operator and users of the IT systems or services."	Not affected	Coordination.	IT Operations
must	"The results of system or service audits are stored in a traceable manner and reported to the relevant management."	Not affected	Documentation/reporting.	IT Operations
must	"Measures are derived from the results and are implemented in an appropriate timeframe."	**Partially degraded**	Time compression: "appropriate timeframe" is indefinite and without a binding upper limit relative to an accelerated threat pace.	IT Operations
should	"System and service audits are planned taking into account any security risks they might cause (e.g., disturbances)."	Not affected	Planning security.	IT Operations
should	"Regular system or service audits are performed. [Qualified personnel,	**Partially degraded**	Periodic instead of continuous testing leaves the same patch	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	Suitable tools e.g. vulnerability scanners, From internet and internal network]"		gap open between audit cycles as in 5.2.5.	
should	"Within a reasonable period following completion of the audit, a report is prepared."	Not affected	Documentation pace, downstream.	IT Operations
high	"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)"	Not affected	"Risk-based time intervals" is an adaptive, well-formulated requirement without rigid periodicity.	IT Operations
very high	"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)"	**Partially degraded**	Even at the highest level of protection needs, scanned only "regularly" instead of continuously — the opportunity for a mandatory near-real-time check in the case of very high protection needs remains unused.	IT Operations

Overall classification: Partially demoted (2 out of 8 requirements affected by normal protection needs; 3 out of 10 incl. very high), regardless of protection needs. Consistent theme: periodic instead of continuous testing, consistent with the patch gap finding from 5.2.5.
Curing reference: MHC-09 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Requirements for the management and control of	Not affected	Governance.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	networks are determined and fulfilled."			
must	"Requirements regarding network segmentation are determined and fulfilled."	**Stable**	Segmentation obligation — consistent with the architectural stability assessment in 5.2.2.	IT Operations
should	"Procedures for the management and control of networks are defined."	Not affected	Governance.	IT Operations
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]"	**Partially degraded**	The detection sub-aspects (lateral movement, data outflow) are the weaker component: generic "detection" without specification of behavior-based/anomaly-based methods is designed for obvious rather than fragmented, slow-moving attack patterns.	IT Operations
high	"Extended requirements for the management and control of networks are determined and implemented. [Authentication of IT systems on the network, Restricted access to management interfaces, Specific risks e.g. wireless	**Partially degraded**	The reference to remote access risks imports the same authentication vulnerability as in 4.1.2/5.1.2; the other sub-aspects (device authentication, management interface protection) are structurally sound in their own right.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	and remote access] (C, I, A)"			

Overall classification: Partially demoted (1 out of 4 requirements affected by normal protection needs; 2 out of 5 incl. high), regardless of protection needs. The segmentation obligation itself is stable; the weakness lies in the detection and remote access dimension.
Curing reference: MHC-03, MHC-05 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Critical IT services are identified, and business impact is considered."	Not affected	Business Impact Analysis, Governance.	IT Operations
must	"Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled."	Not affected	Governance.	IT Operations
should	"Critical IT systems are identified. [Classification for appropriate protection need, Implementation of adequate security measures]"	Not affected	Governance/Classification.	IT Operations
should	"Continuity planning exists and is regularly reviewed and updated. [Alternative communication, Alternative storage, Alternative power/network]"	**Partially degraded**	Time compression: Periodic update without reference to the occasion for scenarios that escalate faster today (e.g., ransomware spread velocity).	IT Operations
should	"Continuity planning includes at least (Distributed) Denial of Service attacks, successful	Not affected	Explicitly named modern attack scenarios (DDoS, ransomware,	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	ransomware attacks and other sabotage activities, system failure scenarios, and natural disaster scenarios affecting critical IT systems."		sabotage) — a well-secured formulation regardless of how an attack is orchestrated in detail.	
high	"Continuity planning includes predefined time frames (Recovery Time Objective) for resumption of operation in line with requirements. (A)"	Not affected	Defined RTO parameter.	IT Operations
high	"Appropriate SLAs with external service providers according to continuity planning are in place. (A)"	Not affected	Contractually.	Purchasing/Supplier Management
high	"Continuity plans include coordination of contractually agreed communication with business partners. (A)"	Not affected	Contractual/Process.	CISO Function
high	"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)"	Not affected	Test activity.	IT Operations
high	"A backup and recovery strategy for critical IT services and information is defined and implemented. (C, I, A)"	Not affected	existence of the strategy; the specific backup mechanic is evaluated independently in 5.2.9 (no double counting).	IT Operations
high	"Backups of critical IT services and information are sufficiently protected against unauthorized	**Partially degraded**	"Sufficiently protected" with no immutability requirement allows ransomware with	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	modification or deletion by malicious software, (I, A)"		compromised backup admin privileges to still delete/encrypt backups. Only 5.2.9 (very high) explicitly closes this gap via immutable/offline backups.	
high	"Backups of critical IT services and information are sufficiently protected against unauthorized access by malicious software or operators. (C, I)"	**Partially degraded**	Same reasoning, here is the confidentiality page.	IT Operations
very high	"Continuity planning is coordinated with the continuity plans of relevant external service providers. (A)"	Not affected	Coordination/contract.	Purchasing/Supplier Management
very high	"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 sites with equivalent controls]"	**Stable**	Spatially separated standby systems/locations with equivalent controls are an architectural redundancy — acts independently of attacker capability.	IT Operations
very high	"Continuity planning is tested regularly. Test scenarios, results, and lessons learned are recorded. (I, A)"	Not affected	Test activity.	IT Operations

Overall classification: Partially degraded (1 out of 5 requirements affected by normal protection needs; 3 out of 15 incl. high/very high), regardless of protection needs. **Cross-reference:** the

backup immutability gap at high is explicitly closed by Control 5.2.9 (very high) — see there for the complete classification.

Curing reference: MHC-08 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Backup concepts exist for relevant IT systems. Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups are considered."	Not affected	concept existence; the concrete mechanics are specifically rated at high/very high.	IT Operations
must	"Recovery concepts exist for relevant IT services."	Not affected	Concept existence.	IT Operations
should	"A backup and recovery concept exists for each relevant IT service. Dependencies between IT services and the sequence for recovery are considered."	Not affected	Planning/sequencing.	IT Operations
high	"Backup and recovery concepts are methodically reviewed at regular intervals. (A)"	**Partially degraded**	Time compression: periodic review of the concept without reference to the occasion — a concept can become obsolete even if the underlying storage medium (see very high) is immutable.	IT Operations
high	"General restore capability is considered and tested (e.g., sample testing, test systems). (I, A)"	Not affected	Random testing activity.	IT Operations
high	"Backup and recovery concepts exist. [RPO, RTO,	**Stable**	Spatial redundancy (separate server	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	Required resources for recovery, Avoidance of overload scenarios, Appropriate spatial redundancy e.g. separate room/fire section/data center/site] (A)"		room/fire compartment/location) is an architectural barrier that acts independently of attacker capability.	
very high	"(Additional) Backups are performed via offline procedures, immutable backups or by using an isolated IAM solution. (I, A)"	**Stable**	Offline/immutable backups or isolated IAM solution are a hard architectural barrier against ransomware and credential-based attacks — one of the strongest Standfest examples in the entire catalog.	IT Operations
very high	"Restore procedures are technically tested in a methodical way at regular intervals. (I, A)"	Not affected	Test activity.	IT Operations
very high	"Geographical redundancy is considered in data backup and recovery concepts. (A)"	**Stable**	Geographical redundancy, structural.	IT Operations

Overall classification: For normal protection needs Not affected (0 of 3 requirements affected) — only concept existence required. From a high need for protection, the periodic concept review without reference to the occasion is added — overall classification is **partially downgraded** (1 out of 6), but at the same time spatial redundancy is also used as a stable element. If the need for protection is very high, the Stationary side is significantly strengthened (immutable/offline backups, geographical redundancy) — **the overall rating still remains partially demoted** (1 out of 9) because the periodic review gap from the high level remains unchanged. Practically, even an organization with exemplary immutable backups is considered "partially degraded" here because the two requirements refer to different aspects — backup *medium* (immutable, strong) versus backup *concept* test cycle (periodic, weak). **Cross-reference:** Fixes the backup immutability vulnerability from Control 5.2.8 (high).
Curing reference: MHC-10 (see Part II)

Summary (Chapter 5, Part 1: 5.1.1–5.2.9)

Control	Overall classification	Proportion affected
5.1.1	Stable	0/3
5.1.2	Partially degraded	2/6
5.2.1	Not affected	0/6
5.2.2	Stable	0/3
5.2.3	Partially degraded	5/10
5.2.4	Partially degraded	1/8
5.2.5	Partially degraded	3/6
5.2.6	Partially degraded	2/8 → 3/10
5.2.7	Partially degraded	1/4 → 2/5
5.2.8	Partially degraded	1/5 → 3/15
5.2.9	Not affected → from high: Partially degraded	0/3 → 1/6 → 1/9

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The information security requirements associated with the design and development of IT service are determined and considered."	Not affected	Governance.	Development/Engineering
must	"The information security requirements associated with the acquisition or extension of IT service and IT components are determined and considered."	Not affected	Governance.	Purchasing/Supplier Management
must	"Information security requirements associated with changes to developed IT services are considered."	Not affected	Governance, thematically related to 5.2.1.	Development/Engineering
must	"System approval tests are carried out under consideration of the information security requirements."	Not affected	Release-gate, plane of existence.	Development/Engineering
should	"Requirement specifications are prepared. [IS requirements, Vendor recommendations/best practices, Best practices/security guidelines, Fail safe design]"	Not affected	Documentation/design input.	Development/Engineering
should	"Requirement specifications are reviewed against the information security requirements."	Not affected	Review governance.	Development/Engineering

Level	Requirement (original wording)	Category	Justification	Responsible
should	"The IT service is reviewed for compliance with specifications prior to productive use."	Not affected	Release gate.	Development/Engineering
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]"	**Partially degraded**	Capability decoupling: the re-identification of pseudonymised/anonymised data by correlation with additional information has so far required specialist statistical knowledge. AI-powered correlation methods make this more widely accessible without the requirement prescribing a re-identification-resistant methodology.	Development/Engineering
should	"Test-systems are provided with protective measures comparable to those in the operational environment where productive data are used for testing purposes."	Not affected	Compensation control, structurally comparable.	Development/Engineering
very high	"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)"	Not affected	Triple actuators (commissioning, significant changes, control interval) — well-secured formulation without isolated time compression gap.	Development/Engineering

Overall classification: Partially demoted (1 in 10 requirements affected), regardless of protection needs.
Reference to hardening: individual measure (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Requirements regarding the information security of network services are determined and fulfilled."	Not affected	Governance.	IT Operations
should	"A procedure for securing and using network services is defined and implemented."	Not affected	Governance/Process.	IT Operations
should	"The requirements are agreed in the form of SLAs."	Not affected	Contractually.	Purchasing/Supplier Management
should	"Adequate redundancy solutions are implemented."	**Stable**	Redundancy is a structural availability measure, consistent with other redundancy assessments in the catalog.	IT Operations
high	"Procedures for monitoring the quality of network traffic (e.g., traffic flow analyses, availability measurements) are defined and carried out. (A)"	Not affected	Quality/availability monitoring, no reference to safety detection (assessed separately in 5.2.7).	IT Operations

Overall classification: Stable (no degraded/friction element), regardless of the need for protection.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"A procedure for the return and secure removal of information assets from each external IT service is defined and implemented."	Not affected	Governance/Contract Process.	Purchasing/Supplier Management

Level	Requirement (original wording)	Category	Justification	Responsible
should	"A description of the termination process is given, adapted to any changes, and contractually regulated."	Not affected	Contractually.	Purchasing/Supplier Management

Overall classification: Not affected (0 of 2 requirements affected), regardless of protection needs.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Effective segregation (e.g., segregation of customers) prevents access to own information by unauthorized users of other organizations."	**Stable**	Tenant segregation is a structural barrier when implemented correctly (cryptographic isolation, strict access controls) — consistent with the segmentation rating in 5.2.2/5.2.7.	IT Operations
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]"	Not affected	Documentation of the concept; the mechanism strength is already rated above.	Purchasing/Supplier Management

Overall classification: Stable (no degraded/friction element), regardless of the need for protection.

Summary Chapter 5 (total, 15 controls)

Control	Overall classification	Proportion affected
5.1.1	Stable	0/3
5.1.2	Partially degraded	2/6
5.2.1	Not affected	0/6
5.2.2	Stable	0/3
5.2.3	Partially degraded	5/10
5.2.4	Partially degraded	1/8
5.2.5	Partially degraded	3/6
5.2.6	Partially degraded	2/8 → 3/10
5.2.7	Partially degraded	1/4 → 2/5
5.2.8	Partially degraded	1/5 → 3/15
5.2.9	Not affected → from high: Partially degraded	0/3 → 1/6 → 1/9
5.3.1	Partially degraded	1/10
5.3.2	Stable	0/5
5.3.3	Not affected	0/2
5.3.4	Stable	0/2

Chapter 5 is the technically densest chapter and shows the widest range: 4 Consistently stable (cryptography, dev/test/prod separation, network redundancy, client separation — all architectural/cryptographic hard barriers), 9 Partially demoted, 2 Not affected, 1 Dependent on protection requirements (5.2.9, with the extensively justified exception that the very strong Stable addition does not overturn the overall degraded rating in the case of very high protection requirements). Two market-ready Mythos core findings of this chapter: the collapse of the patch gap window (5.2.5, 5.2.6) and the consistently missing obligation to use phishing-resistant authentication (5.1.2, 5.2.7, congruent with 4.1.2).

Chapter 6 — Supplier Relationships (3 Controls, 31 Requirements)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Contractors and partners are subjected to a security risk assessment."	Not affected	Governance/Process.	Purchasing/Supplier Management
must	"An appropriate level of information security is ensured by contractual agreements with contractors and partners."	Not affected	Contractually.	Purchasing/Supplier Management
must	"Where applicable, contractual agreements with clients and customers are passed on to contractors and partners."	Not affected	Contractual, pass-through.	Purchasing/Supplier Management
should	"Contractors and partners are contractually obligated to pass on any requirements regarding an appropriate level of information security to their subcontractors."	Not affected	Contractual cascading.	Purchasing/Supplier Management
should	"Service reports and documents by contractors and partners are reviewed."	**Partially degraded**	Capability decoupling: the audit is based on documents provided by the supplier. AI tools convincingly make fake or embellished reports/evidence easier to create without requiring independent cross-checking.	Purchasing/Supplier Management
high	"Evidence is provided that the information security	**Partially degraded**	The list of examples allows pure self-	Purchasing/Supplier Management

Level	Requirement (original wording)	Category	Justification	Responsible
	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)"		disclosure/attestation to suffice — the same document forgery gap as above, here related to formal evidence. Only very high does this conclude via the obligation to carry out a third audit (see below).	
high	"The supplier's level of compliance with the required evidence is documented, regularly and in case of changes... reviewed and monitored. (C, I, A)"	**Partially degraded**	The test frequency is well formulated with dual actuator; however, the underlying proof-authenticity problem remains regardless of this.	Purchasing/Supplier Management
high	"The supplier's compliance with contractual agreements is checked, documented, regularly and in case of changes... reviewed and monitored. (C, I, A)"	**Partially degraded**	Same reasoning.	Purchasing/Supplier Management
very high	"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-based decision must be made by the organization's management to continue doing business with the	**Stable**	Obliged to carry out an independent third-party audit (TISAX® label or similar) instead of self-disclosure — an on-site audit with interviews and random checks is much more difficult to falsify on a large scale than a submitted document. Closes the gap named at high.	Purchasing/Supplier Management

Level	Requirement (original wording)	Category	Justification	Responsible
	supplier. A record of this decision exists. (C, I, A)"			
very high	"Contractual obligations with customers regarding transparency of supply chain risks are fulfilled. (C, I, A)"	Not affected	Contractually.	Purchasing/Supplier Management

Overall classification: Partially degraded (1 out of 5 requirements affected by normal protection needs; 4 out of 8 from high; 4 out of 10 incl. very high), regardless of protection needs. In the case of a very high need for protection, the weakness of self-disclosure is explicitly and effectively closed by the third-party audit obligation (TISAX® label) — the overall classification nevertheless remains "partially degraded" because the two monitoring requirements only have to be checked "regularly" at high, regardless of the type of evidence. Practical: actively demand a TISAX® label or equivalent third-party audit from critical suppliers instead of relying on self-disclosures — this is the most effective single lever in this control.
Curing reference: MHC-14 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The non-disclosure requirements are determined and fulfilled."	Not affected	Legally.	Legal Department
must	"Requirements and procedures for applying non-disclosure agreements are known to all persons passing on information in need of protection."	Not affected	Communication/Awareness.	Legal Department
must	"Valid non-disclosure agreements are concluded prior to forwarding sensitive information."	Not affected	Legal gate.	Legal Department
must	"The requirements and procedures for the use of non-disclosure agreements	**Partially degraded**	Time compression: explicitly includes the *operational* procedures	Legal Department

Level	Requirement (original wording)	Category	Justification	Responsible
	and the handling of information requiring protection are reviewed at regular intervals."		for handling information requiring protection (not just the text of the contract) — an outdated handling manual without reference to the occasion is a technical-operational, not purely legal risk.	
should	"Non-disclosure agreement templates are available and checked for legal applicability."	Not affected	Legally.	Legal Department
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."	Not affected	Minimum legal content.	Legal Department
should	"Non-disclosure agreements include provisions for the handling of sensitive information beyond the contractual relationship."	Not affected	Legally.	Legal Department
should	"Options of demonstrating compliance with specifications (e.g., review by an independent third-party or audit rights) are defined."	Not affected	Contractual mechanism.	Legal Department
should	"A process for monitoring the validity period of	Not affected	"In due time" refers to a known expiration date	Legal Department

Level	Requirement (original wording)	Category	Justification	Responsible
	temporary non-disclosure agreements and initiating their extension in due time is defined and implemented."		— a calendar-driven, not a vague periodic trigger.	

Overall classification: Partially demoted (1 out of 9 requirements affected), regardless of protection needs. The only finding in an otherwise purely legal control — specifically concerns the operational handling instructions, not the text of the contract itself.
Curing reference: MHC-10 (see Part II)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"The IT services concerned are identified."	Not affected	Scoping.	Purchasing/Supplier Management
must	"The security requirements relevant to the IT service are determined."	Not affected	Governance.	Purchasing/Supplier Management
must	"The organization responsible for implementing the requirement is defined and aware of its responsibility."	Not affected	Governance/Accountability.	Purchasing/Supplier Management
must	"Mechanisms for shared responsibilities are specified and implemented."	Not affected	Governance.	Purchasing/Supplier Management
must	"The responsible organization fulfils its respective responsibilities."	Not affected	Fulfillment level, no specific mechanism for evaluation mentioned.	Purchasing/Supplier Management
should	"In case of IT services, configuration has been conceptualized, implemented, and documented based on the	Not affected	Documentation.	IT Operations

Level	Requirement (original wording)	Category	Justification	Responsible
	necessary security requirements."			
should	"The responsible staff is adequately trained."	Not affected	Training on responsibilities, thematically separate from phishing awareness from 2.1.3.	Human Resources
high	"A list exists indicating the IT services concerned and the respective responsible IT service providers. (C, I, A)"	Not affected	Inventory.	Purchasing/Supplier Management
high	"The applicability of the ISA controls has been evaluated and documented. (C, I, A)"	Not affected	governance/scoping (the TISAX® applicability check itself).	CISO Function
high	"The service configuration is included in the regular security assessments. (C, I, A)"	**Partially degraded**	Time compression: Periodic instead of continuous inclusion in security assessments leaves configuration deviations in externally operated services undetected between cycles — consistent with the audit cycle finding from 5.2.6.	Purchasing/Supplier Management
high	"Proof is provided that the IT service providers fulfil their responsibility. (C, I, A)"	**Partially degraded**	Capability decoupling: unspecified "proof" without specifying independent verification imports the same document authenticity gap as in 6.1.1.	Purchasing/Supplier Management

Level	Requirement (original wording)	Category	Justification	Responsible
high	"Integration into local protective measures (such as secure authentication mechanisms) is established and documented. (C, I, A)"	**Partially degraded**	Refers to "secure authentication mechanisms" without an explicit phishing resistance requirement — imports the same vulnerability as 4.1.2.	IAM Team

Overall classification: In case of normal protection needs Not affected (0 of 7 requirements affected). If there is a high need for protection, three additional requirements are added (regular inclusion in security assessments, independently verifiable proof of responsibility, secure authentication integration) — overall classification is **partially downgraded** (3 out of 12). Practical: only applies to service provider relationships for assets with high/very high protection needs; in the case of normal protection needs, there is no Mythos-specific additional need.
Curing reference: MHC-10, MHC-03, MHC-14 (see Part II)

Summary Chapter 6

Control	Overall classification	Proportion affected
6.1.1	Partially degraded	1/5 → 4/10
6.1.2	Partially degraded	1/9
6.1.3	Not affected → from high: Partially degraded	0/7 → 3/12

Consistent chapter pattern: Supplier security relies heavily on submitted documents/self-disclosures, whose falsification protection is reduced by AI tools. TISAX® explicitly concludes this in the case of very high protection requirements (6.1.1) via the obligation to carry out an independent third-party audit — the most effective single lever in the entire chapter.

Chapter 7 — Compliance (2 Controls, 6 Requirements)

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Legal, regulatory, and contractual provisions of relevance to information security (see examples) are determined at regular intervals."	Not affected	Pure legal situation scan: Legislation does not change at the pace of an automated attack — periodic observation is appropriate here, not relevant to time compression.	Legal Department
must	"Policies regarding compliance with the provisions are defined, implemented, and communicated to the responsible persons."	Not affected	Governance/Communication.	Legal Department
should	"The integrity of records in accordance with legal, regulatory, and contractual provisions and business requirements is considered."	Not affected	governance level (taking into account), no specific technical mechanism has been identified.	Legal Department

Overall classification: Not affected (0 out of 3 requirements affected), regardless of protection needs.

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

Level	Requirement (original wording)	Category	Justification	Responsible
must	"Legal and contractual information security requirements regarding the procedures and processes in the processing of	Not affected	Legally.	Legal Department

Level	Requirement (original wording)	Category	Justification	Responsible
	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 persons involved."	Not affected	Legal/Communication.	Legal Department
must	"Processes and procedures for the protection of personally identifiable information are considered in the information security management system."	Not affected	ISMS/Data Protection Governance Linkage.	Legal Department/CISO Function

Overall classification: Not affected (0 out of 3 requirements affected), regardless of protection needs.

Summary Chapter 7

Control	Overall classification	Proportion affected
7.1.1	Not affected	0/3
7.1.2	Not affected	0/3

Chapter 7 is completely Not Affected — a clean example of controls that are originally legal/regulatory outside the Mythos scope.

Phase 1 completed: Overview of all 7 chapters

Distribution per chapter (overall classification dominant, normal need for protection)

Chapters	Controls	Stable	Partially degraded	Pure friction	Not affected
1. IS Policies and Organization	14	0	10	0	4 (of which 1 will be demoted from high)
2. Human Resources	4	0	2	0	2 (1 of which will be stable from high)
3. Physical Security	3 (+1 without requirements)	0	2	0	1 (becomes stable from high; in addition, 1 of the 2 degraded controls [3.1.4] from high also becomes stable, see there)
4. Identity and Access Management	4	0	2	1	1 (will be demoted from high)
5. IT Security/Cyber Security	15	4	8	0	3 (of which 1 will be demoted from high)
6. Supplier Relationships	3	0	2	0	1 (will be demoted from high)
7. Compliance	2	0	0	0	2
Total (45 Controls)	**45**	**4 (9 %)**	**26 (58 %)**	**1 (2 %)**	**14 (31 %)**

Classification of the distribution

TISAX® contains a single pure friction case (4.1.2, password-only authentication without a second factor) — practically all other controls, even severely affected, do not completely lose their core effect, they degrade to "partially demoted". The Standfest share is comparatively low at 9% — the "Information Security" module is predominantly formulated in a process/organization-heavy way (many governance requirements without a concrete technical mechanism). The Standfest portion is almost entirely focused on Chapter 5 (cryptography, segmentation, client separation, redundancy) — where TISAX® explicitly sets technical/architectural requirements.

Recurring Pattern Categories (Phase 2 Preview)

Across all chapters, the 26 partially-degraded and the one pure friction finding can be assigned to four to five recurring causes, which are condensed into clusters in phase 2:

1. **Periodic instead of event-related review** (time compression) — concerns policy reviews, software releases, access rights reviews, log evaluation, vulnerability/patch management, system/service audits, backup concept review, supplier monitoring. By far the most common single finding.
2. **Patch gap window collapse** — risk assessment and patch speed without taking into account AI-accelerated exploit development (5.2.5, 5.2.6).
3. **Lack of obligation for phishing-resistant authentication** — consistently in authentication and remote access controls (4.1.2 — here as Pure Friction on the Pure Password Factor, otherwise degraded as Partial —, 5.1.2, 5.2.7, 6.1.3).
4. **Document/evidence falsification by AI** (capability decoupling) — recruitment process (2.1.1), supplier evidence (6.1.1, 6.1.3), compliance documentation.
5. **Signature-based detection** (capability decoupling) — Malware protection (5.2.3).

These five clusters cover the most common, but not all, of the needs that are affected.

Pattern formation and gap analysis (phases 2 and 3)

Analysis unit: The chapter summaries count 26 controls with an overall rating of "Partially degraded" and 1 control with "Pure friction" (27 of 45) — this number refers to the overall classification per control with *normal* protection requirements and does not reflect several simultaneous causes of findings per control (e.g. 4.1.2: both lack of phishing resistance and pure time compression, depending on the protection requirement level). 4 additional controls (1.2.2, 4.1.1, 5.2.9, 6.1.3) are inconspicuous when the need for protection is normal, but degrade at high/very high and do not appear in the number of 27, although they contain individual affected requirements. The pattern formation therefore works at the level of the **74 individual affected requirements** (73 Partially Degraded + 1 Pure Friction) via **31 distinct controls**, parsed from the document text using the same extraction procedure as the priority table in the appendix. This value was corrected from the original 71 to 72 during the revision and to 74 with version 1.1: The former compact index had not included one of the two affected requirements (should level, evaluation criteria) in Control 1.4.1, although Chapter 1 itself already correctly showed this as partially demoted; Version 1.1 adds two more individual findings from Control 1.6.3, which result from the primary source-based reassessment of the editorial catalogue duplicates there (see Methodology, Data Quality Note).

Methodological approach: The eight clusters were formed inductively from the 74 individual findings, not derived from a predefined category grid. Each individual finding was first considered individually on the basis of its justification from chapters 1–7; only recurring causal patterns (e.g. "periodic instead of occasion-related") were then combined into a named cluster. The cluster number eight is thus an empirical result of this concrete analysis, not a methodological requirement — a different TISAX® module or a different catalog of requirements could lead to a different cluster number.

Cluster Overview

Cluster	Finds	Controls	Chapters	Dominant criterion
1. Periodic instead of event-related review	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	Time compression
2. Patch Gap Window Collapse / Ransomware Resilience	9	4 (1.3.4, 5.2.5, 5.2.6, 5.2.8)	1, 5	Time compression
3. Lack of phishing-resistant authentication	10	6 (4.1.1, 4.1.2, 4.1.3, 5.1.2, 5.2.7, 6.1.3)	4, 5, 6	Capability Decoupling /

Cluster	Finds	Controls	Chapters	Dominant criterion
				Time Compression
4. AI-powered identity and document forgery	11	5 (2.1.1, 2.1.3, 3.1.1, 6.1.1, 6.1.3)	2, 3, 6	Capability decoupling
5. Signature-based detection vs. AI malware	5	1 (5.2.3)	5	Capability decoupling
6. Aggregation resistance	4	4 (1.6.1, 1.6.3, 5.2.4, 5.2.7)	1, 5	Aggregation resistance
7. Autonomous AI agents undermine approval processes	4	2 (1.3.3, 1.3.4)	1	Capability decoupling
8. Lack of automation in the reaction	4	1 (1.6.2)	1	Time compression
Individual findings (no recurring pattern)	8	6 (1.2.2, 1.4.1, 1.6.3, 3.1.4, 5.1.2, 5.3.1)	1, 3, 5	—

Cluster 1 (Periodic Review) is by far the largest and covers four out of seven chapters — the time compression gap is not an individual phenomenon of individual departments, but a structural pattern across the CISO function, IT operations, IAM and purchasing.

Gap analysis against six frames of comparison

Methodology: For each cluster, it is checked whether NIST CSF 2.0, BSI C5:2026, DORA, CRA, NIS2 Directive/DVO and ISA/IEC 62443-2-1:2024 already close the same structural gap. This is a comparison at the level of regulatory/normative attitudes (maturity level of best practice), not a statement about whether a company is formally subject to these six frameworks — DORA addresses financial companies and their critical ICT service providers, CRA addresses manufacturers of products with digital elements, NIS2 addresses essential/important entities of certain sectors. The classification is based on a web research from July 2026 on the publicly available texts and secondary sources; it does not replace a certification exam specific to the clause.

Legend: ✓ = addresses the gap explicitly and with a binding deadline/method · **~** = mitigates the gap, but does not close it completely · ✗ = shares the same structural gap · **n/a** = outside the material scope of the framework

Cluster	NIST CSF 2.0	BSI C5:2026	DORA	CRA	NIS2-RL/DVO	ISA/IEC 62443-2-1:2024
1. Periodic review	~	~	✓ (Registration)	n/a	~	~
2. Patch Gap/Ransomware	~	~[2]	~	✓ (Disclosure)	~	~
3. Phishing-resistant Auth	~	n/a[1]	~	n/a	~	~
4. Document forgery	✗	n/a[1]	✓ (Suppliers)	n/a	~	n/a[1]
5. Signature-Based Recognition	~[1]	n/a[1]	n/a[1]	n/a	n/a[1]	~[1]
6. Aggregation resistance	~	n/a[1]	n/a[1]	n/a	n/a[1]	~
7. Autonomous AI Agents	✗	✗	✗	✗	✗	✗
8. Automation Obligation Reaction	~	~	✓ (factual)	~ (factual)	~	~

[1] For these cells, it was not possible to verify a sufficiently specific, citable individual specification in the search; Classification is cautious/tendentious, not clause-sharp.

[2] Applies only to the vulnerability deadline half of the cluster: C5:2026 OPS-25.01AC requires a defined, monitored, CVSS-bound deadline framework for remediation of vulnerabilities, mandatory from audit periods from June 1, 2027 — this structural requirement is confirmed by several secondary sources. The specific CVSS-staggered example deadline values in the criteria catalogue itself, on the other hand, could not be verified directly on the BSI primary document (the PDF full text was technically not extractable); a verified secondary source gives different values. They are therefore deliberately not quantified here. The ransomware/backup immutability half (Control 5.2.8) remains open even under this more cautious classification: The OPS-06 to OPS-09 criteria require encryption, RTO/RPO alignment, monitoring, and regular restore tests, but never immutability/WORM — the term "immutable" appears in the entire criteria catalog only in the context of container images (OPS-26), not in backups.

The most important individual findings:

Cluster 2 (patch gap/ransomware) is the clearest closed case in terms of vulnerability deadline aspect, but not in terms of backup immutability: BSI C5:2026 (binding from audit periods from June 1, 2027) requires a defined and monitored, CVSS-bound deadline framework for remediation of vulnerabilities in criterion OPS-25.01AC (see footnote 2 for the sources of the exact deadline values). This is exactly the clarification that the vague TISAX® formulations lack — "adequate patch management" without speed SLA (5.2.5, should) and "appropriate timeframe" (5.2.6, must) — and independently confirms that the patch gap collapse diagnosed here is not a special case of this analysis, but was treated as a regulatory gap by a German supervisory authority as early as 2026. This does not apply to backup immutability: The C5:2026 criteria OPS-06 to OPS-09 (Data Backup and Recovery) require encryption, RTO/RPO alignment, monitoring and at least annual restore tests, if tightened daily — the term "immutable" appears in the entire catalog of criteria only in the context of container images (OPS-26), not in backups. In this respect, the vulnerability diagnosed in Control 5.2.8 also remains open vis-à-vis C5:2026. In addition to a 24-hour notification of actively exploited vulnerabilities to ENISA, the CRA obliges manufacturers, with a follow-up report after 72 hours and a final report 14 days after a remediation is available — binding from 11 September 2026. This concerns the disclosure obligation for one's own product, not the internal patch management of the IT environment, but it is a precedent for clock-bound rather than vaguely formulated deadlines.

Cluster 3 (phishing resistance) shows a finer nuance: NIS2 Art. 21(2)(j) is the first EU law ever to require multi-factor or continuous authentication by name — thus closing the "no second factor at all" gap. However, the AITM relay vulnerability (real-time phishing overrides OTP/push) remains because neither NIS2 nor the other five frameworks explicitly prescribe phishing-resistant procedures (FIDO2/WebAuthn) in the core text. So far, this clarification only exists in secondary technical guidelines (e.g. NIST SP 800-63B, AAL3) — TISAX® ISA 2027 thus shares this gap with the majority of the benchmarks, not just with itself.

Cluster 4 (Falsification of documents) shows a robust ranking among the benchmarks themselves: DORA Art. 30(3) — sector-specific reference framework for financial firms and their critical ICT service providers, see methodology above — requires an unrestricted right of audit and access and explicitly clarifies that certifications submitted "support, but not replace" one's own audit. NIS2 Art. 21(2)(d)/(3) in conjunction with NIS2-DVO No. 5.1.4 also requires a documented supplier assessment with contractually anchored audit rights or access to test reports — with proportionality ("where appropriate") instead of DORA's unrestricted claim, but without standard certificates (ISO 27001, SOC 2 Type II, TISAX® Assessment, CSA STAR) being allowed to expressly replace these audit rights. TISAX® ISA 2027 remains the weakest of the three requirements with pure self-disclosure/attestation. For the personnel process (2.1.1: Deepfake identity in the application process), there is no equivalent in any of the six frameworks — this part of the cluster remains completely TISAX® original.

Cluster 7 (Autonomous AI Agents) is the only cluster where all six benchmarks share the same gap as TISAX® ISA 2027 — and this is even proven by current research, not just assumed: Neither NIST AI RMF nor ISO/IEC 42001 nor the EU AI Act contain a reference to "agent"/"agentic"/autonomous AI systems so far. NIST has recognized this itself and launched

the "AI Agent Standards Initiative" in February 2026 (937 responses received in response to a Request for Information); an "AI Agent Interoperability Profile" has been announced for Q4 2026 at the earliest — so not yet available according to the status of this analysis. The finding diagnosed here (1.3.3, 1.3.4: AI assistants call up external services/packages independently without a human ever submitting the specific tool for approval) is therefore not a TISAX® peculiarity, but a gap on the front line of regulation as a whole. A second, narrower NIST approach is also still in the draft stage: The NIST Cyber AI Profile (NIST IR 8596) published a first draft in December 2025 with a comment period until the end of January 2026; according to NIST's own project page, the status of the work at the time of this analysis is "Reviewing Comments" — a final text is not available, and an explicit agent reference claimed by secondary sources could not be verified against the NIST primary text (see Part II, MHC-13, Section 2). At this point, the MHC catalogue in Part II deliberately goes beyond pure TISAX® diagnosis (see section "Original additions beyond TISAX®" below).

Cluster 5 (signature-based detection) and cluster 6 (aggregation resistance) could not be verified with comparable precision: The research did not find a sufficiently specific, citable individual requirement for behavior-based/AI-supported malware detection or the explicit obligation to deliberately detect fragmented attack chains in any of the six frameworks. ISA/IEC 62443-2-1:2024 mentions "behavioral analytics" and "continuous monitoring for anomaly detection" in secondary sources as an extension compared to the previous version, without a sharp, citable obligation being derived from this. These two clusters are therefore ranked more cautiously (~ instead of ✓) than the others.

Individual findings outside the clusters

8 Requirements across 6 controls could not be assigned to a recurring pattern: 1.2.2 (role separation undermined by AI dual role), 1.4.1 (outdated probability of occurrence assumptions in the risk methodology — both at the level of the assessment itself and the underlying evaluation criteria, 2 requirements), 1.6.3 high (AI-orchestrated scenarios not provided for in crisis planning, including the second version of the catalogue, which is editorially doubled, 2 requirements), 3.1.4 (PIN/password as a fallback option in the absence of an encryption obligation), 5.1.2 must (non-specific measures for remote access without a minimum standard), 5.3.1 (re-identification of pseudonymised data through AI-supported correlation). For individual findings without a recurring pattern, a six-frame gap analysis is not conclusive; they remain anchored in chapters 1–7 with their complete justification and are incorporated directly into the MHC catalogue (phase 4) as independent individual measures.

Classification for phase 4

Cluster	Classification	Recommendation for MHC
1. Periodic review	Partially addressed industry-wide	The CSF continuity principle (DE. CM) and NIS2 language ("away from periodic snapshots"), but condense TISAX-specific® into a single

Cluster	Classification	Recommendation for MHC
		occasion-related basic principle — 12 affected controls do not need 12 different formulations
2. Patch Gap/Ransomware	Patch deadlines solved industrywide, backup immutability still open	Closely follow the BSI C5:2026 principle for patch deadlines (defined, CVSS-bound deadline framework instead of "adequate"/"appropriate"); Backup immutability requires a separate MHC specification despite C5:2026 check
3. Phishing-resistant Auth	Partially addressed industry-wide	NIS2 already names MFA/Continuous Authentication as a suitable measure; the phishing resistance specification (FIDO2/WebAuthn) must be provided by the MHC itself, no framework already prescribes it bindingly
4. Document forgery (suppliers)	Partially addressed industry-wide	DORA principle (sector-specific: financial sector) "Certificate does not replace own examination" can be adopted
4. Document forgery (personnel and access, incl. 3.1.1)	TISAX® original	No comparative framework relevant — independent MHC development necessary (deepfake verification in the recruitment and access process)
5. Signature-Based Recognition	Predominantly original	Starting point for IEC 62443-2-1 behavioural analysis, but essentially an independent MHC formulation
6. Aggregation resistance	Predominantly original	No framework found with a strict specification — independent MHC development
7. Autonomous AI Agents	Universally unsolved	Greatest chance for a genuinely upstream MHC contribution — even NIST is only at the beginning here (result Q4 2026 at the earliest)
8. Automation Obligation Reaction	Industry-wide factually addressed	DORA principle (sector-specific: financial sector) can be adopted: hard deadline instead of soft duty effectively enforces automation without requiring it literally

Cluster 8 and the patch deadline half of Cluster 2 are the "easiest" cases for Phase 4 — the solution already exists outside of TISAX® and just needs to be adopted; the backup immutability half of cluster 2, on the other hand, requires an independent formulation despite testing. Cluster 7 is the most valuable single finding of this analysis: a gap that no relevant framework currently

fills, whereby an MHC contribution here actually describes new ground instead of merely reflecting existing practice.

Original additions beyond TISAX®

With one exception, the MHC catalogue in Part II is consistently derived from a specific TISAX® requirements report of this document (see Methodology, "What this analysis is — and what is not"). In one topic, this line is deliberately and explicitly crossed: the protection of AI agents.

Reason: Cluster 7 shows that TISAX® ISA 2027 only touches AI agents in two places (1.3.3, 1.3.4 — unchecked tool/service integration) and that this gap is not closed by any of the six benchmarks from Phase 3. A comparison with the OWASP Top 10 for Agentic Applications (ASI01–ASI10, as of June 2026) — a community-based threat taxonomy developed specifically for AI agents — shows that MHC-13, originally derived from Cluster 7, covered only one of these ten threat categories completely and two others partially covered. Seven categories remained unaddressed — not because they are irrelevant for companies, but because TISAX® ISA 2027 does not address them specifically enough at any point to derive an independent finding.

Procedure: Part II expands MHC-13 with four additional minimum standards — (a) agent identity/NHI governance, (b) basic hardening against prompt injection, (c) kill switch, (d) continuous reassessment of released components — and adds a new, standalone MHC-16 (multi-agent integrity) for threats that require a multi-agent communicating architecture. The catalogue thus covers eight of the ten OWASP-ASI categories (ASI01, ASI02, ASI03, ASI04, ASI05 via MHC-13; ASI06, ASI07, ASI08 via MHC-16). Two categories remain unaddressed even after this expansion: ASI09 (Human-Agent Trust Exploitation) and ASI10 (Rogue Agents) — this is deliberately named openly here instead of tacitly treating as solved.

Why this labeling is important: The methodological value of MRIS lies in the fact that each classification can be traced back to a concrete, citable TISAX® requirement text (see Methodology, "Reproducibility"). The additions described here do not meet this criterion — they are the author's professional judgment based on external threat research (primarily OWASP), not a diagnosis distilled from a TISAX® requirement text. This section as well as MHC-13 and MHC-16 (each section 9) in Part II therefore consistently indicate which part is TISAX-derived® and which is original, so that both categories are not mixed. The "74 individual findings across 31 controls" of the core analysis (see Management Summary) remain unaffected by this expansion.

Regulatory outlook: At the time of this analysis, the NIST Cyber AI Profile (NIST IR 8596) is still in the draft stage (status "Reviewing Comments", see Cluster 7 above) and was at no time citable enough to derive a TISAX-comparable® requirement from it. If NIST IR 8596 or a future TISAX® ISA release explicitly addresses agent security, the content originally added here would have to be reviewed and, if necessary, converted into a TISAX-derived® classification.

Appendix: Priority Table and Standard Cross-References

This appendix contains two supplementary overviews to chapters 1–7: a priority table of all individual findings requiring action including MHC reference for implementation, as well as the assignment of each control to ISO 27001/27017, ISA/IEC 62443-2-1 and NIST CSF 2.0 as preliminary work for the gap analysis in phases 2 and 3.

SGA Addendum: 10 of the 330 reported requirements (level "SGA") were subsequently added and were not part of the original 320 requirements count of Phase 1 — affected: 1.1.1, 1.2.1, 1.2.2, 1.5.1 (4), 1.5.2 (2), 1.6.2. They apply regardless of the need for protection, exclusively for Simplified Group Assessment.

Standard cross-references per control

Control	Reference to other 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-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

Control	Reference to other standards (ISO 27001/27017, ISA/IEC 62443-2-1, NIST CSF 2.0)
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, EN. 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
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

Control	Reference to other standards (ISO 27001/27017, ISA/IEC 62443-2-1, NIST CSF 2.0)
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

Priority table: Individual findings requiring action

This table replaces the former "Compact index per requirement". Instead of all 330 requirements assessed, it shows only the 74 individual findings with a need for action (category Partially degraded or Pure friction), each with an abbreviated designation and direct reference to the responsible MHC entry in Part II. they are given in full text and justification in chapters 1–7.

Control	Short name	Category	Curing reference
1. IS Policies and Organization			
1.1.1	Policy review without reference to an occasion ("periodic")	Partially degraded	MHC-10
1.2.1	ISMS effectiveness test without reference to the occasion	Partially degraded	MHC-10
1.2.2	Separation of roles only enforced organizationally, not technically	Partially degraded	Individual measure
1.3.1	Asset inventory maintenance without reference to an occasion	Partially degraded	MHC-10
1.3.3	AI agent can call external services without sharing	Partially degraded	MHC-13
1.3.3	Release sampling without ongoing detection	Partially degraded	MHC-10
1.3.4	AI Coding Assistant downloads software packages without approval	Partially degraded	MHC-13

Control	Short name	Category	Curing reference
1.3.4	Same gap in special software (maintenance tools)	Partially degraded	MHC-13
1.3.4	Repository protection: signature verification not mandatory	Partially degraded	MHC-13
1.3.4	Software release check without reference to the occasion	Partially degraded	MHC-10
1.3.4	Patch status known, but no response speed required	Partially degraded	MHC-09
1.4.1	Risk assessment continues to assume close attacker circles	Partially degraded	Individual measure
1.4.1	Same gap at the level of the evaluation criteria	Partially degraded	Individual measure
1.5.1	Policy compliance review without reference to the occasion	Partially degraded	MHC-10
1.5.1	Requirements compliance check without reference to the occasion	Partially degraded	MHC-10
1.5.1	Group-wide audit plan without trigger for new sites	Partially degraded	MHC-10
1.6.1	Reporting does not detect fragmented attack steps	Partially degraded	MHC-05
1.6.2	Incident processing purely human, no automation obligation	Partially degraded	MHC-11
1.6.2	Same gap in reporting response	Partially degraded	MHC-11
1.6.2	Response time targets without automation obligation to meet	Partially degraded	MHC-11
1.6.2	Escalation mechanism itself remains humanly supported	Partially degraded	MHC-11
1.6.3	Crisis detection designed for gradual, not rapid escalation	Partially degraded	MHC-05
1.6.3	Crisis plan update without reference to the occasion	Partially degraded	MHC-10
1.6.3	Crisis scenarios without AI-orchestrated multiple attacks	Partially degraded	Individual measure
1.6.3	Crisis scenarios without AI-orchestrated multiple attacks (editorial	Partially degraded	Individual measure

Control	Short name	Category	Curing reference
	catalogue duplicate, see data quality note)		
1.6.3	Communication strategy without a shortened reaction window	Partially degraded	MHC-05
1.6.3	Communication strategy without a shortened reaction window (editorial catalogue duplicate, see data quality note)	Partially degraded	MHC-05
1.6.3	Contingency plan evaluation without reference to the occasion	Partially degraded	MHC-10
2. Human Resources			
2.1.1	Identity verification vulnerable to deepfake applicant identity	Partially degraded	MHC-15
2.1.1	Live interview vulnerable to real-time deepfake	Partially degraded	MHC-15
2.1.1	References/certificates easier to falsify	Partially degraded	MHC-15
2.1.3	Awareness training designed for outdated phishing identifiers	Partially degraded	MHC-15
3. Physical Security			
3.1.1	Access control vulnerable to AI-powered pretense	Partially degraded	MHC-15
3.1.1	Visitor registration vulnerable to fake legitimation	Partially degraded	MHC-15
3.1.4	Encryption of mobile devices not mandatory	Partially degraded	Individual measure
4. Identity and Access Management			
4.1.1	Blocking of lost ID cards not immediate/automated	Partially degraded	MHC-03
4.1.2	"State of the art" does not enforce phishing resistance	Partially degraded	MHC-03
4.1.2	Password strength ineffective against real-time phishing	Pure friction	MHC-03

Control	Short name	Category	Curing reference
4.1.2	Privileged accounts: simple 2FA without phishing resistance is enough	Partially degraded	MHC-03
4.1.2	Options list allows fulfillment without phishing resistance	Partially degraded	MHC-03
4.1.2	Two-factor example without phishing resistance obligation	Partially degraded	MHC-03
4.1.3	Account review without reference to an occasion	Partially degraded	MHC-10
4.1.3	Possession factor (SMS-OTP) vulnerable to SIM swapping	Partially degraded	MHC-03
4.1.3	Account review in customer systems without reference to the occasion	Partially degraded	MHC-10
4.2.1	Access rights review without reference to the occasion	Partially degraded	MHC-10
4.2.1	Shorter test interval remains periodically without reference to the cause	Partially degraded	MHC-10
5. IT Security/Cyber Security			
5.1.2	Transport protection without mandatory minimum encryption standard	Partially degraded	Individual measure
5.1.2	Remote access: VPN protects transport route, not authentication	Partially degraded	MHC-03
5.2.3	Signature-based malware protection against AI variants weak	Partially degraded	MHC-05
5.2.3	Virus scanner example signals signature recognition	Partially degraded	MHC-05
5.2.3	Same signature recognition limit for file verification	Partially degraded	MHC-05
5.2.3	Full testing periodic and signature-based — double weakness	Partially degraded	MHC-05
5.2.3	Encrypted content bypasses gateway inspection	Partially degraded	MHC-05
5.2.4	Log check fails to detect fragmented attack patterns	Partially degraded	MHC-05

Control	Short name	Category	Curing reference
5.2.5	Vulnerability assessment underestimates shortened exploit window	Partially degraded	MHC-09
5.2.5	Patch management without a mandatory speed SLA	Partially degraded	MHC-09
5.2.6	Appropriate timeframe indefinite	Partially degraded	MHC-09
5.2.6	Audit cycle leaves patch gap open between audits	Partially degraded	MHC-09
5.2.6	Scan frequency only periodically even at very high	Partially degraded	MHC-09
5.2.7	Detection of lateral movement without behavioral basis	Partially degraded	MHC-05
5.2.7	Remote Access Risk Imports Authentication Vulnerability from 4.1.2	Partially degraded	MHC-03
5.2.8	Emergency plan update without reference to the occasion	Partially degraded	MHC-08
5.2.8	Backup protection without immutability (integrity)	Partially degraded	MHC-08
5.2.8	Same gap, confidentiality page	Partially degraded	MHC-08
5.2.9	Backup concept review without reference to the occasion	Partially degraded	MHC-10
5.3.1	Test data: no re-identification-resistant anonymization required	Partially degraded	Individual measure
6. Supplier Relationships			
6.1.1	Supplier reports without independent cross-checking	Partially degraded	MHC-14
6.1.1	Self-disclosure/attestation sufficient as proof	Partially degraded	MHC-14
6.1.1	Test Frequency Good, Proof Authenticity Problem Remains	Partially degraded	MHC-14
6.1.1	Same proof-authenticity gap in contract review	Partially degraded	MHC-14
6.1.2	NDA handling procedure without reference to the occasion	Partially degraded	MHC-10

Control	Short name	Category	Curing reference
6.1.3	Service provider configuration periodically instead of continuously checked	Partially degraded	MHC-10
6.1.3	Unspecified proof without independent verification	Partially degraded	MHC-14
6.1.3	Authentication mechanisms without phishing resistance obligation	Partially degraded	MHC-03