Status: Reference Version

This document describes a legal and factual boundary of permissibility. It is not a discussion paper, not a position, not an offer, and not a demand. It serves solely as a reference anchor for classification and delimitation.

PART 1 – BOUNDARY OF PERMISSIBILITY

A. Normative Core – What *ex ante* Means

Ex ante means that a condition must be examined and confirmed as permissible **before** it is executed. What matters is not what can be determined, documented, or corrected afterward, but what is effectively constrained in advance. Measures that take effect only after an impact has occurred do not meet this requirement. They are *ex post* and therefore legally irrelevant for *ex ante* purposes.

Modern laws follow this principle regardless of industry or technology. They require precaution instead of reaction, and verifiability instead of trust. Responsibility does not arise retroactively; it arises **before** a system is used. This responsibility is personally attributable and non-delegable. Neither the use of external providers nor certificates, contracts, or organizational arrangements transfer or shift this obligation.

C-Level Matrix – Impact of an Ex-ante System

No.	C-Level Question	Without Ex-ante (Status quo)	With Ex-ante	Hard Consequence
I	What is considered risk?	Events that occur	Decisions that are made	Risk arises before any damage occurs
II	When does liability start?	After damage has occurred	At the moment a decision is made not to impose limits	Liability is decision-based
III	What do I need to justify?	Why something happened	Why limitation was not applied	The burden of justification is reversed
IV	Is waiting neutral?	Yes	No	Waiting equals a consious risk decision
V	Can I delegate?	Yes (IT, Compliance, Security)	No	Delegation no longer protects
VI	What constitutes gross negligence?	Difficult to delineate	Technically provable	Negligence becomes objective
VIII	What do I defend myself?	Yes	No	Forensics lose weight
IV	Can I delegate?	Yes (IT, Compliance, Security)	Technically provable	No - longer provices protection
VII	What constitutes gross negligence?	Difficult to delineate	Technical limits	Forensics lose relevance
VIII	What do I defend myself?	Nothing	Liability relevance remains	"We got lucky" no longer counts
IX	How long is inaction acceptable?	Unlimited	Time-limited	Time weakens defense
X	What does a courtor regulator see?	Intentions and documentation	Avoidability & decision	Standard is posssibility, not intent
XI	What does the insurer see?	Indeterminate residual risk	Decision risk	Insurability becomes conditional
XII	What does the insurer see?	Diffuse	Decision risk	Clearly attributap e the choice made action

B. Irrelevant Categories – What Does Not Substitute *Ex Ante*

For meeting *ex ante* requirements, it is irrelevant where systems are operated or who provides them. Location, jurisdiction, cloud models, or political control do not change the

user's legal responsibility. Assurances by manufacturers or platform operators are likewise irrelevant. The sole decisive factor is whether the required effect is technically enforced **in advance**.

C. Attribution – Who Is Responsible

An *ex ante*-compliant state exists only if it is determined **prior to execution** whether a condition is permissible or not. This determination must be possible independently of the operational software. Systems that can be modified after the fact, that interpret, or that allow exceptions cannot meet this requirement. Subsequent reviews, audits, or corrections do not replace prior constraint.

D. Technical Reality – Limits of Classical IT

Software-based systems are part of the state being assessed and therefore cannot themselves serve as proof. They change, they drift, and they generate only internal perspectives. *Ex ante*, however, requires that effects be independently observable and demonstrable. Black boxes are permissible only if their effects are fully and permanently verifiable.

Ex ante is not a static state, but a continuous property. Deviations, changes, and context shifts are the norm. A system must be able to represent these changes without relying on subsequent intervention. Decisions about permissibility must not be implicitly made by technology; they must be clearly attributable and traceable.

E. Boundary – Legal Impossibility Without a Different System Class

Without a technical layer that enforces these requirements **prior to execution**, *ex ante* cannot be legally established. Classical IT architectures are not designed for this. They react, they correct, and they document, but they do not constrain in advance. In such structures, *ex ante* remains an assumption, not a demonstrable state.

PART 2 – EXISTENCE AND FACTUAL STATUS

2a. Existence of the System Class

There exists a system class that operates independently of operational software. This system class is published. It is fully documented. It is globally accessible. It is technically verifiable.

The system class is delivered in a functional state. At delivery, it contains no active rules. Rules are activated exclusively by the respective operator. The operator is the sole authority able to enable or disable rules.

Rules are hierarchically organized. Higher-level rules cannot be overridden by lower-level rules. Lower-level rules may only impose stricter constraints. Any weakening of higher-level rules is excluded.

Once rules are activated, no subsequent modification is предусмотрено. There are no updates. There are no patches. There are no exceptions.

After transfer, the licensor has no intervention or control capability. Remote access is not provided. Subsequent rule-setting by third parties is excluded.

The system class does not make its own decisions. It does not interpret rules. It does not learn. It does not optimize.

The system class exists independently of use, recognition, or evaluation. Its existence is not dependent on market adoption, operation, or distribution.

2b. Formal Notification (Timing & Addressees)

The system class was formally disclosed to insurers and reinsurers on 25 November 2025. The transmission was made in writing and documented.

By 15 December 2025, a formal written notification was provided to the competent supervisory and regulatory authorities. The transmission was documented.

On 22 December 2025, the system class was formally disclosed in identical form to central industry and critical infrastructure (KRITIS) associations. The transmission was made in writing and documented.

No further determinations regarding reactions, assessments, or classifications are available.

PART 3 – REALITY OF EFFECTS AND DECISIONS

3.1 Where Risks Are Actually Assessed

Risks are not decided in discourse. They are assessed where liability, damage, and failure are actually borne. This assessment takes place independently of public debate, political objectives, or professional conviction.

3.2 Standard of Risk Assessment

Insurers and reinsurers evaluate conditions based on predictability and constrainability. Decisive is whether effects are technically excluded or limited **in advance**. Subsequent controls, organizational measures, or declarations of intent are not decisive for this purpose.

This assessment follows its own standards. It is not aligned with market standards, certifications, or industry practice. It is not the result of negotiation, but of risk examination.

Risk Matrix – Effect of an Ex-ante System

No.	Risk Category	Currently Insured	Impact of an Ex-ante System	Rationale / Mechanism
I	Property & Infrastructure Risks	Yes	Indirect	An ex-ante system does not prevent natural events, but it reduces consequential damage by eliminating operational errors, escalation effects, and uncontrolled system reactions.
II	Business Interruption (BI / CBI)	Yes	Yes (strong)	Behavior is constrained in advance, preventing unplanned cascades and enabling faster containment with a clearly defined start and end of loss.
III	Civil Liability	Yes	Yes	Ex-ante enforcement creates technical attribution of actions and eliminates indeterminate organisation-failure.
IV	Management & Corporate Officer Liability (D&O)	Yes	Yes (strong)	Decisions are explicitly modeled and cryptographically authorized, shifting liability from omission to consciously approved action.
V	Regulatory & Supervisory Risks	Yes (indirectly)	Yes (indirectly)	Effectiveness and compliance are technically enforced rather than asserted or retrospectively argued.
VI	IT & Cyber Risks	Yes (fundamental)	Yes (fundamental)	External attacks cannot introduce new system behavior, eliminating entire damage paths.
VII	Data Protection & Privacy Risks	Yes	Yes	Access and processing exist only if explicitly pre-authorized, preventing implicit or emergent
VIII	Operational & Organizational Risks	Yes	Yes (fundamental)	Processes are no longer interpretive but technically fixed and non-ambiguous.
IX	Supply Chain & Deperidency· Risks	Yes	Partial	Components cannot expand behavior, the supply chain affects availability only.
X	Legal, Litigation & Defense Costs	Yes	Yes	Clear evidentiary conditions reduce litigation duration, settlement pressure, and uncertahity.
XI	Reputational Risks	Yes (indirectly)	Yes	No unreselved incidents, no ambiguous attribution of fault, and no escalation narralives.
XIII	Financial Consequential Risks	Yes	Yes (fundamental)	Fewer unplanned violations and clearly bounded loss exposure.
XIII	Accumulation & Systemic Risks	Yes (very strong)	Yes (very strong)	Homogeneous, emergent losses become structurally impossible, inualidating accumulation assumptions.
XIV	Evidence & Proof Risks	Yes	Yes (direct)	Evidence is inherent rather than reconstructed, eliminating forensic uncertainty.
XV	Residual & Model Risks	Yes	Partial	Ex-ante enforcement reduces unknowns‘but cannot fully eliminate incorrect or incomplete models.
XV	Residual & Model Risks	Yes	Partial	Ex-ante enforcement reduces unknowns but cannot fully eliminate incorrect or incomplete models.

3.3 Public Responsibility Beyond Discourse

Independently of this, decisions in the public sector are subject to additional scrutiny. Public officials do not act solely politically, but within a legally binding framework of responsibility. Public statements, programs, and funding decisions have effect even when technical prerequisites have not been conclusively clarified.

3.4 Transitional Phases and Record Status

In transitional phases without formal guidelines, the documented factual status gains particular importance. It influences which assumptions can be considered known and which cannot. This also affects decisions on the allocation of funds, funding programs, and procurement.

3.5 Audit Reality

Audit institutions such as courts of auditors do not evaluate objectives, but traceability, diligence, and the foundations of decisions. Decisive is whether information recognizable at the time of the decision was taken into account. The existence or non-existence of technical prerequisites is part of the record, not of political evaluation.

This decision reality exists regardless of whether it is publicly addressed. It operates in the background and unfolds its effects outside of discourse.

Note: This document does not describe an implementation and does not constitute a recommendation. It marks a boundary of permissibility and serves factual classification purposes only.