BSA

AI Component- Paper

Draft Guidelines on Classification of High-Risk Systems
Abandon AI Act's Risk-Based Approach

September 2026

The AI Act is founded on a risk-based approach. The Draft Guidelines on Classification of High-Risk Systems abandon this approach. Instead, the Draft Guidelines treat any AI system as high risk if other entities in the AI supply chain combine that system with high-risk tools. It also treats general-purpose AI systems as high-risk if any potential downstream high-risk usage is not prevented. These fundamental changes are at odds with the Act and should not be made through secondary guidance. Significant revisions are needed to avoid gutting the Act's risk-based approach.

Key Concerns:

- **The Draft Guidelines abandon the Act's risk-based approach in two ways**. Under Article 6 of the AI Act, whether a system is high risk is based on its use. Systems referred to in Annex III are *not* high risk when they do not pose a significant risk of certain harms — including if the AI system is intended to perform a narrow procedural task or a preparatory task. The Draft Guidelines gut this risk-based approach in two areas:

- **First, for complex AI systems,** Paragraph 75 of the Draft Guidelines states that even if an AI system on its own "may be exempt" from high-risk classification under Article 6(3), that exemption does not apply if it is integrated into a complex system and "the overall system's configuration and functioning influence key aspects of the decisions made with the AI system's support in the context of the high-risk use case." Paragraph 90 compounds this by stating that a component cannot benefit from the Article 6(3) filter — even if it performs a narrow procedural task — once it is part of a complex system.
  - Under the Draft Guidelines, a company that develops a low-risk AI system may be subject to high-risk obligations if another company farther down the supply chain integrates that low-risk system into a high-risk tool. That makes the low-risk developer into a high-risk developer — based on the decisions of third parties down the supply chain that the initial provider does not control. That is at odds with the AI Act, which puts this responsibility onto the company that takes a low-risk system and puts it to a high-risk use. The final Guidelines should follow the allocation Article 25 already establishes, rather than layering residual liability onto an upstream provider.

- **Second, for general purpose AI systems, the Draft Guidelines similarly undermine the Act's risk-based approach.** Paragraphs 11–12 deem a GPAI system's intended purpose to encompass high-risk uses wherever those uses are "feasible and reasonably foreseeable," and treat the system as high-risk unless the provider consistently prevents every such use. Because a GPAI system is by nature capable of serving many purposes, no provider can technically foreclose every foreseeable high-risk use — so this converts the Act's intended-

purpose test into a capability test and collapses the distinction between general-purpose and high-risk systems on which the Act is built.

- **The Draft Guidelines are inconsistent with the Act's regulation of the AI supply chain.** Article 25 already provides the mechanism for shifting responsibility when a system's risk profile changes after it leaves the original provider. Under Article 25:
  - a third-party that substantially modifies an existing high-risk system becomes the provider of that system (Article 25(1)(b))
  - a third party that changes the intended purpose of a system in a way that makes it high-risk likewise becomes the provider (Article 25(1)(c))

In both cases, the Act recognizes that the third party that makes the substantial modification or changes the intended purpose should be solely responsible, as provider, for the resulting high-risk system. The Draft Guidelines' treatment of the original provider as responsible for that system, or for the modified portion of it, cannot be reconciled with the allocation of responsibility established by Article 25.

In addition to being inconsistent with the Act, the Draft Guidelines also create confusion about which entity is actually accountable for a high-risk system's compliance, by splitting responsibility between the party that made the change and an upstream provider that has no involvement in that change — and no visibility into or control over it. Regulators and end-users are better served by the single, identifiable and accountable provider that Article 25 already assigns, rather than extending liability to a party that has no role in creating the risk.

Recommendations:

High-risk classification should be consistent with the Act — and based on a system's intended purpose, not on how other companies reconfigure or integrate it downstream.

To do this, the Draft Guidelines should be revised to:

- **Preserve the risk-based approach to upstream components in complex AI systems.** A low-risk AI system should not become high-risk merely because a downstream actor incorporates it into a complex high-risk AI system. The final Guidelines should align its discussion of complex AI systems, including paragraphs 75-76 and 90, with Article 25 of the Act and the obligations it assigns across the AI supply chain.

- **Preserve intended purpose as the test for general-purpose AI systems.** The sentence in Paragraph 12 providing that a GPAI system is high-risk "where such uses are feasible and reasonably foreseeable" should be removed.

- **Create clear guidance for companies.** The Draft Guidelines contain a range of vague and unclear standards that would make it difficult for companies to comply, even if the Guidelines were consistent with the Act. For example, Paragraph 76 alone contains multiple unworkable standards, including a focus on components that "*contribute* to a high-risk purpose" and are not "*genuinely* separable" from the system. Similarly, the concept of "material influence" in Paragraphs 76 and 90 lacks a reliable boundary point — and could extend to an entire business process or platform, rather than to components specifically designed to materially affect the relevant decision. Any boundaries included in the final Guidelines must be workable in practice.