Business Software Alliance

14 August 2026

BSA RECOMMENDATIONS FOR THE DRAFT ARTIFICIAL INTELLIGENCE ACT

On behalf of the Business Software Alliance (**BSA**),[1] we appreciate the opportunity to provide our recommendations on Thailand's Draft Artificial Intelligence Act (**draft AI Act**) to the Electronic Transaction Development Agency (**ETDA**). BSA has engaged extensively on AI governance issues in Thailand, including submitting comments on the Draft AI Bill in 2023,[2] meeting with the Ministry of Digital Economy and Society, ETDA, and several other government agencies to discuss AI governance and other issues on 7 May 2025, submitting comments on the Draft Principles of the AI Law,[3] and most recently contributing to the ETDA's AI and Copyright Working Group.

BSA is the global trade association of the enterprise software industry. Our member companies are leaders in artificial intelligence, cybersecurity, cloud computing, and other cutting-edge technologies. Close consultation between policy makers and the effected industry and other stakeholders is critical for effective policy making. BSA offers our extensive global experience in technology policy to serve as a resource and we hope that our recommendations below will be helpful to the Government of Thailand as you develop an AI Law that will promote and support AI innovation in Thailand.

Set Definitions in Line with International Understanding

Given that AI systems are developed and deployed in an international context, regulations and standards that apply to AI should operate across different jurisdictions to facilitate and promote further adoption and use of AI technologies. Definitions pertaining to AI should be aligned across jurisdictions to ensure that all stakeholders have a common understanding of AI.

Definition of AI. Section 5 of the Draft Act defines an AI system as a "computer system developed using *artificial intelligence techniques* that is capable of producing various outputs, such as predictions, content generation, recommendations, or decisions, and that may affect physical or virtual environments. Such a system may operate at varying levels of autonomy and may have the ability to adapt after deployment."

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] BSA Comments on Draft Artificial Intelligence Bill, 18 August 2023, at https://www.bsa.org/policy-filings/thailand-bsa-comments-on-draft-bill-on-promotion-and-support-of-national-artificial-intelligence-innovation

[3] BSA Recommendations for Draft Principles of the Law on Artificial Intelligence, 7 June 2025, at https://www.bsa.org/policy-filings/thailand-bsa-recommendations-for-draft-principles-of-the-law-on-artificial-intelligence.

We appreciate that the definition within Section 5 is close to the OECD's definition of AI — "a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment." However, the definition hinges on "artificial intelligence techniques," which is itself undefined, resulting in an unclear scope to the Draft Act.

Recommendation: Replace "developed using artificial intelligence techniques" with the OECD's definition so that an AI system is defined as one that "for explicit or implicit objectives, infers, from the input it receives, how to generate outputs." This will distinguish AI systems from conventional rule-based software and align Thailand's AI governance regime with other jurisdictions adopting the OECD definition.

As discussed in previous submissions, prioritizing international alignment in defining AI-related terms will: (a) reduce discrepancies and conflicts between different legal frameworks, thus promoting compliance; (b) serve as foundation for dialogue and cooperation between governments on AI-related risks; and (c) support the international development of best practices and benchmarks for using AI systems safely, allowing AI systems to be deployed responsibly on a global scale.

Roles and Responsibilities in the AI Value Chain

Chapter 3 imposes obligations on actors that are not defined within Section 5 of the Draft Act. For instance, Section 43 lays out obligations on "developers" of AI systems capable of generating or modifying content, and Section 46 on "platform providers," while Section 45 separately addresses deployers using AI to generate content for public dissemination. As "developer" and "platform provider" are undefined, organizations will find it challenging to determine which role they play.

Clearly defined roles matter because obligations should fall on the entity best positioned to identify and efficiently mitigate the risk of harm. A developer has access to information about training data, known limitations, and intended use cases, but has no insight into how a system is used after deployment; a deployer is best positioned to understand how the system is being used and the risks a specific use presents to individuals. This division is especially significant for enterprise software and cloud services, where a provider may develop, host, and maintain an AI capability while the business customer determines the purpose of use, provides input data, configures the system, and makes any consequential decision. Each party should be accountable for the risks within its effective control, and the AI Act should allocate obligations accordingly.

Recommendation: Define "developer" in Section 5 as an entity that designs, codes, or produces an AI system, consistent with international usage. Align "platform provider" with the definitions in existing Thai law governing digital platform services, to avoid parallel definitions of the same actors across regimes.

Risk-Based Approach

We support the risk-based approach inherent in the AI Act and recommend that any regulations specify a list of high-risk AI *use cases*. As discussed in our previous submissions, the risks of AI are inherently use-case specific. Any regulations should focus on specific applications of the technology that pose higher risks to the public and must be flexible enough to account for the unique considerations that may be implicated by specific use cases.

The scope of any regulatory obligations should be a function of the degree of risk and the potential scope and severity of harm. Many AI systems pose extremely low, or even no, risk to individuals or

society, while creating potentially significant benefits like helping to organize digital files, auto-populate common forms for later human review, or improve a company's ability to forecast supply chain issues.

Prohibited AI Systems

Section 33 prohibits the deployment of AI systems that affects certain serious risks, including "other risks as announced by the Committee." This permits the Committee to designate additional prohibited categories by announcement, without any guiding criteria or principles within the Draft Act, thus introducing significant ambiguities and uncertainties.

Recommendation: Delete the prohibited risk category in Section 33 and adopt a use-case oriented risk-based approach to regulating AI systems. If the prohibited risk category is retained, this risk tier should be defined by an exhaustive, closed list of specific prohibited practices, objectively defined by the nature of the use and its effect on individuals. The list of prohibited practices should be limited in scope and subject to periodic review through a transparent and consultative process.

High-Risk AI Systems

Section 35 envisages high-risk designation by Royal Decree where deployment of an AI system has an impact on national security, health, the environment, energy, communications and telecommunications, transportation and logistics, or public utilities, and where a controlling or supervisory agency considers it necessary. In effect, each sector regulator may separately initiate the designation of high-risk AI within its own sector.

We are concerned that this decentralized approach will produce inconsistent outcomes and an overly broad interpretation of high-risk AI. Without a common threshold or methodology, the same underlying AI capability may be designated high-risk in one sector but not another or be subject to inconsistent obligations under the same category because they are governed by different regulators. Designation by sector also attaches obligations to kinds or categories of AI systems rather than to specific uses, potentially bringing into scope low-risk or purely protective software simply because it is deployed within a regulated sector. We therefore recommend a different approach that recognizes a specific definition of high-risk use cases. For example, AI systems should only be designated as high-risk if they are used to make consequential decisions to hire, promote, or terminate an individual's employment, or in other contexts, to determine eligibility for credit, healthcare, or housing.

The obligations that follow a high-risk designation under Sections 36 to 40 are extensive. A clear definition creates important predictability and consistency about how these obligations will be applied. This is essential for organizations planning products and services for the Thai market.

Recommendation: Avoid designating entire sectors as high-risk. Instead, clarify that high-risk designations under Section 35 only apply to specifically defined high-risk uses of AI, rather than to categories of AI systems. Such high-risk designations should not apply to all AI systems within a sector. We further recommend issuing a single list of high-risk use cases, maintained by a central authority and updated only after public consultation with the industry. In addition, the AI Act should explicitly recognize that AI tools deployed primarily for cybersecurity, threat detection, vulnerability management, and incident response serve a protective function and should be treated as presumptive low-risk systems, regardless of whether they are deployed within critical information infrastructure (**CII**) or regulated sectors.

Data Localization

Section 50: In-country Processing Requirement

Section 50 authorizes the Committee to prescribe any service within a state agency or a critical information infrastructure organization, for the purposes of "maintaining the security of data of national importance", to deploy an AI system whose processing is located in Thailand. The provision neither defines what constitutes "data of national importance" nor defines the services concerned or the risk levels of the services that could mandate localization of AI system processing. This data localization mandate appears to conflict with the AI Law's broader objectives by threatening confidence in the legal stability of Thailand's business environment for AI development and adoption. Data localization requirements are antithetical to successful AI development, integration, and deployment because they threaten the ability to integrate information sources into cutting edge AI tools, while also raising cybersecurity risk, adding to regulatory uncertainty and increasing compliance burdens without any tangible benefit.

Cross-border data transfers underpin the global economy and are vital to the security of networks and information systems. Data localization requirements do not ensure information security and are likely to have the opposite effect of reducing information security. Such requirements can frustrate efforts to implement effective security measures, protect data, and defend critical networks, just as they can impede business innovation and limit services available to consumers. This concern is especially acute for AI-driven cybersecurity tools, which rely on correlating telemetry, logs, and threat indicators across a global customer base to detect and respond to novel threats. A Thailand-only processing requirement would prevent AI-driven security tools from drawing on threat intelligence first observed elsewhere, directly undermining the cybersecurity and robustness objectives the Draft Act itself identifies as risk-management criteria for AI systems.

Data localization requirements have a chilling effect on AI investment as they restrict state agencies and critical information infrastructure organizations from fully benefiting from cutting edge technology and services available in the global marketplace. Data localization restrictions prevent these organizations from using world leading information technology and cloud computing solutions from service providers that offer their services from outside of Thailand. Such services frequently provide best-in-class security capabilities. Restrictions on international data transfers are also resource-intensive for government authorities to manage.

Recommendations:

- Remove the in-country AI-system processing requirement in Section 50.
- If retained, limit it to a published list of government use cases with a direct national security nexus, each supported by a risk assessment, and subject to periodic review.
- Allow trusted cross-border processing and resilience arrangements that support interoperable data transfer frameworks such as the Global Cross-Border Privacy Rules (**CBPR**) System. Permit offshore AI processing such as offshore remote administration and technical support, cross-border transfer of logs and threat intelligence for incident response, encrypted backup and disaster recovery, or transfer of aggregated or de-identified data for model improvement.

Sections 48-49: Designation of AI Businesses Subject to Contract Control

Sections 48-49 would permit the Committee to designate providers of AI development services, AI system services, and "data processing services to any artificial intelligence system" supplied to government agencies or CII entities as subject to "contract control," and to prescribe mandatory terms across seven categories, including the transfer of data abroad. BSA offers the following observations and concerns.

First, the reach of Section 48 is broad, covering "critical information infrastructure entities," which comprise eight sectors under the Cybersecurity Act B.E. 2562 (2019), from banking and finance to public health, plus any area the NCSC later prescribes. Combined with an undefined reference to AI-related "data processing services," contract control could potentially impact much of the technology supply chain serving Thai banks, hospitals, airlines, and utilities, including cloud-delivered cybersecurity products such as AI-driven threat detection and response and security operations platforms, which are themselves AI-enabled and process telemetry and threat data on behalf of CII entities. Mandated contract terms restricting cross-border data transfer for these services could directly impair their ability to detect and respond to threats, since effective AI-driven security depends on aggregating and correlating data across a global customer base rather than within a single jurisdiction.

Second, Section 49's second paragraph deems a contract to contain prescribed clauses that may not be known at the time of contract negotiation. The European Union, by contrast, addresses AI procurement through non-binding model clauses that public buyers adapt case by case.

Third, as regards cross-border data transfers and other topics specified in Section 49, Thailand already regulates these matters under the Personal Data Protection Act and the Cybersecurity Act. Prescribing fixed contract terms under the AI Law on the same subjects could create conflicting rules across multiple government authorities.

Recommendations:

- Delete Sections 48-49 outright to remove the requirement for contract controls.
- If retained, amend Sections 48-49 so that contractual controls are replaced with non-binding guidelines rather than mandatory terms. These guidelines should protect commercial freedom of contract, respect standard commercial operating models, and not retroactively alter existing enterprise service agreements. If retained as mandatory, define "data processing services to any artificial intelligence system" and limit designation to a published list of nationally sensitive functions.
- Clarify that any terms or guidelines regarding cross-border data processing under Section 49(1) must recognize and permit globally accepted legal data transfer mechanisms, including Binding Corporate Rules (**BCRs**), Standard Contractual Clauses (**SCCs**), and the Data Privacy Framework (**DPF**). Base any prescribed terms on internationally recognized instruments, such as the ASEAN Model Contractual Clauses or EU SCCs, binding corporate rules, Global CBPR System certification, and ISO/IEC standards.
- Publish designation criteria, give notice and reasons, provide administrative review, and bound the Section 49(7) power to the stated purpose of Section 48.

Strict and Joint Liability

Section 62 imposes joint liability for damage arising from violations of the Act, regardless of intention or negligence, subject to only two defenses. The provision appears to create joint liability regardless of an entity's role — and does not require that a party's own act or omission caused the damage. It also has no cap or proportionality mechanism, leaving exposure open-ended. Further, it is unclear how a deployer's compliance with its duties under Section 37(4) affects its liability where the cause of damage lies upstream.

We are concerned that this liability scheme will deter investment in, and deployment of, AI systems in Thailand, including by Thai enterprises and by public-sector organizations that the Draft Act's promotion measures are intended to benefit. A no-fault, joint, and uncapped civil liability regime is also difficult to reconcile with the risk-based approach that underpins the rest of the Draft Act because this liability scheme exposes all AI systems to the same unlimited, no-fault liability, regardless of whether an AI system is used for a high risk or low risk activity.

The Draft Act already establishes a comprehensive supervisory framework, under which the Office may order corrective measures, seek court-ordered suspension or recall, and impose administrative fines. Regulatory enforcement through this designated supervisory channel provides a consistent, expert, and proportionate mechanism for securing compliance. Layering a broad private civil liability regime on top of that framework risks inconsistent outcomes and duplicative exposure for the same conduct.

Recommendation: Remove the liability regime under Section 62. Damages for AI-related harm remain available under Thailand's existing civil law, which already provides for compensation based on fault.

Should the liability provision be retained, we recommend replacing blanket joint and strict liability with proportionate fault-based liability based on a shared responsibility framework between providers and deployers. Each party should be responsible only for its own acts and omissions, and for the information and systems within its own control. Regulatory obligations and liabilities should be allocated according to the level of control, visibility, and decision-making authority exercised by each participant across the AI lifecycle. Developers should be responsible for matters within their control, such as model design, documentation, testing, and communication of capabilities and limitations. Deployers should bear responsibility for how AI systems are used within specific operational contexts, particularly in high-risk use cases. This distinction is especially important for foundation models and general-purpose AI systems, including open-weight models, which may ultimately be adapted by third parties for use cases that were neither intended nor foreseeable by the original developer.

A clear allocation of responsibilities promotes accountability while ensuring that obligations remain practical and proportionate. Imposing blanket liability "regardless of intent or negligence" entirely contradicts the shared responsibility model, holding cloud platform providers strictly liable for how endpoint applications are prompted, governed, or deployed by the customer—matters over which providers have no visibility or control. Liability must track the specific operational breach committed by the respective party to, ensure fairness and create the correct incentives for every actor in the AI value chain. Contractual risk allocation between providers and deployers should also remain enforceable.

Further, organizations that act responsibly in developing or deploying AI should be protected. The Act should provide an express safe harbor against civil and administrative liability, or at minimum treat as evidence of due care, for organizations that implement a risk management program aligned with internationally recognized frameworks, such as the NIST AI Risk Management

Framework or ISO/IEC 42001, or compliance with the standards and certification mechanisms established under the Draft Act itself. This would reinforce the Draft Act's own promotion of standards, certification, and good practices by giving organizations a concrete compliance incentive to adopt them.

Local Representative

Section 3 applies the draft Act to acts affecting people within Thailand regardless of where processing activities are carried out, and Section 40 requires foreign providers of high-risk AI systems to appoint an in-country coordinator.

Recommendation: Remove the requirement for foreign providers of high-risk AI systems to appoint an in-country coordinator and replace it with a requirement to appoint a person, wherever located, authorized to respond to individuals and businesses under Thailand on their obligations within the AI Act. If an in-country coordinator requirement is retained, we strongly recommend removing the phrase "without any limitation of liability" from Section 40, Paragraph 2. The provision should instead align liability with the provider's specific role under a shared responsibility framework.

Content Authenticity

BSA supports the development and deployment of reliable content authentication and provenance mechanisms that help users identify the history and origin of AI-generated content. We support efforts by the Content Authenticity Initiative (**CAI**)[4] — a global cross-industry coalition supported by over 4,500 members — to promote the adoption of the Coalition for Content Provenance and Authenticity (**C2PA**) technical standard commonly known as Content Credentials.[5] Anyone, including governments, can use the openly available C2PA standard to incorporate digital provenance information into their products and processes. This open standard enables creators and developers to embed verifiable provenance metadata indicating how the AI-generated content was created, the date it was made, and any edits that were made along the way. This standard will help consumers decide what content is trustworthy and promote transparency around the use of AI. The C2PA standard will be useful to support compliance with Section 43(3), which requires developers to embed machine-readable marks in accordance with international standards or standards announced by the Committee. To ensure practical implementation, Section 43 obligations must rely on open international frameworks and be tailored to consumer-facing generative outputs rather than automated operational data.

Recommendation: Recognize the C2PA standard as the accepted baseline for machine-readable marks under Section 43(3) and refrain from developing a Thailand-specific content authentication standard, which would limit interoperability and increase compliance burdens. Furthermore, the Act should clarify that machine-readable marking, provenance, and disclosure duties under Section 43 apply strictly to consumer-facing generative AI outputs (e.g., deepfakes, synthetic media, public-facing text), should not require visible or physical marks, and expressly exclude machine-to-machine telemetry, automated security log summaries, system alerts, threat intelligence feeds, and B2B enterprise operational outputs.

[4] Content Authenticity Initiative at https://contentauthenticity.org/

[5] C2PA Specifications at https://c2pa.org/specifications/specifications/2.1/index.html

Transition Period

Section 2 provides that Chapters 3, 4, and 5 come into force 180 days after publication of the Act in the Government Gazette. However, the obligations in those Chapters depend on subordinate instruments that will follow the Act, including the Royal Decrees designating high-risk AI systems under Section 35, the risk-management guidelines the Office may announce under Section 36, and the standards to be announced by the Committee. As drafted, the 180-day period may expire before organizations know which systems are covered and what compliance requires.

Extending the implementation timeline is essential to ensure an effective and practical compliance framework. A phased approach will allow organizations to understand, plan, and operationalize their obligations in line with the final implementing measures. Allowing sufficient time for industry and regulators to align on definitions, criteria, and procedures will promote more consistent and meaningful compliance while supporting Thailand's goal of developing and deploying trustworthy and responsible AI.

Recommendation: Phase in compliance obligations under the Act by providing a minimum transition period of 12–18 months after the publication of the relevant implementing measures, including any Royal Decree designating high-risk AI systems and the associated guidelines and standards. A phased implementation will give organizations sufficient time to prepare, allocate resources, and build robust governance frameworks that align with both domestic requirements and international best practices.

Conclusion

BSA thanks the ETDA for considering our recommendations on the draft Act and hope that our comments will assist in developing the AI Law. We reiterate our support for ETDA and our wish to act as a resource on international developments and best practices for AI governance policy. Additionally, we would like to continue the discussion with ETDA following our last meeting in May 2025. Please do not hesitate to contact me at waisanw@bsa.org to make arrangements. Thank you once more for your time and consideration.

Yours sincerely,

Wong Wai San
Director, Policy – APAC