Framework	Primary Source (URL)	Type	Region	Status	Scope/Definitions	Risk/Applicability
African Union – AI Strategy	https://fpf.org/blog/global/the-african-unions-continental-ai-strategy-data-protection-and-governance-laws-set-to-play-a-key-role-in-ai-regulation/	Continental strategy / policy	African Union	Strategic framework	Digital transformation and responsible AI	Guidance to member states' AI policies
Brazil PL 2338/2023 (AI Bill)	https://artificialintelligenceact.com/brazil-ai-act/	Proposed binding law	Brazil	Parliamentary process ongoing	National framework for AI development and use	Risk-tiered, inspired by EU AI Act
BS 30440 (British Standard on AI Governance)	https://openaccess.city.ac.uk/id/eprint/30857/1/e100749.full%20%281%29.pdf	National standard	UK (global use)	Published 2023	Validation of healthcare AI systems	Risk and benefit in clinical settings
C2PA / Content Authenticity Initiative	https://c2pa.org/	Technical standard / spec	Global	Operational standard	Media provenance, content authenticity	Synthetic media, deepfakes, misinformation
Canada AIDA (Bill C-27)	https://www.360businesslaw.com/canadas-artificial-intelligence-and-data-act-aida-key-developments-objectives-and-future-implications-for-ai-regulation/	Proposed federal law (now stalled)	Canada	Legislative process with major revisions / uncertainty	High-impact AI systems and general-purpose AI	Harms to individuals and biased outcomes
China – Generative AI & Deep Synthesis Measures	https://www.chinalawvision.com/2025/02/digital-economy-ai/deep-synthesis-not-deepfake-how-ai-compliance-works-in-china/	Binding regulations	China	In force	Generative AI and deep synthesis services	Public-facing content and recommendation AI
Colorado AI Act (SB 24-205) - known as CAIA	https://www.naag.org/attorney-general-journal/a-deep-dive-into-colorados-artificial-intelligence-act/	Binding state law	USA – Colorado	Enacted; effectiveness delayed to 2026	High-risk AI systems affecting consumers	Algorithmic discrimination and harm risks
Council of Europe AI Convention	https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence	Treaty-level binding instrument	Council of Europe + observers	Opened for signature 2024	Human rights, democracy and rule-of-law impacts	Public sector and certain private-sector uses
Cyber Resilience Act (CRA)	https://digital-strategy.ec.europa.eu/en/search?search=CRA	Binding law (EU)	EU	Adopted; phased application	Cyber-secure products with digital elements	Risk-based classes of digital products
ENISA - AI/Cypersecurity Guidance	https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation	Guidance	EU	Published/updated	AI threat landscape, good practice	Risk based recommendations
ETSI SAI (Securing AI)	https://www.etsi.org/deliver/etsi_en/304200_304299/304223/02.00.00_20/en_304223v020000a.pdf	Technical standards series	Europe / global users	Published standards	Security of AI and AI-enabled systems	Threats to ML models, data, pipelines
EU AI Act	https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence	Binding law / regulation	EU/EEA	Adopted; phased applicability - but likely to be postphoned for August 2027 enforcement	Risk-based framework for AI systems and models	Prohibited, high-risk, limited-risk, minimal-risk
G7 – Hiroshima Principles & Code of Conduct	https://www.mofa.go.jp/files/100573473.pdf	Political commitment / principles	G7 and partners	In force as non-binding guidance	Trustworthy AI and generative AI governance	Frontier and foundation models
IEEE 7000 – Ethical System Design	https://standards.ieee.org	Ethics standard (IEEE)	Global	Published	Guidance for applying ethical values consistently in systems and AI development.	Cross-sector; applies to AI and non-AI digital systems where values and ethics are material.
IEEE 7001 – Transparency	https://standards.ieee.org	Transparency standard (IEEE)	Global	Published	Standard for transparency of autonomous/intelligent systems; information to stakeholders.	Cross-sector; applies where explainability and communication of system behaviour is required.
ISO/IEC 23894 (AI Risk)	https://standard.com/en-sg/blog/iso-23894/	International guidance standard	Global (ISO/IEC)	Published standard 2024	Risk management for AI systems	Extends ISO 31000 to AI contexts
ISO/IEC 42001 (AIMS)	https://kpmg.com/ch/en/insights/artificial-intelligence/iso-iec-42001.html	International management system standard (certifiable)	Global (ISO/IEC)	Published standard 2023	AI management system for organizations	Risk-based controls for AI lifecycle (9 control objectives & 38 controls)
ISO/IEC 42005 – AI Management System Assessment	https://www.iso.org	Assessment standard (ISO/IEC)	Global	In development / emerging	Guidance for assessing the conformity and effectiveness of an AI management system (AIMS).	Supports organisations seeking assurance, certification or internal audit of their AIMS.
Japan – AI Business Guidelines (METI/MIC)	https://www.meti.go.jp/english/press/2024/0419_002.html	National guidelines	Japan	Issued as non-binding guidance	Governance for AI providers and users	Risk-proportionate obligations
NIS2 Directive	https://digital-strategy.ec.europa.eu/en/policies/nis2-directive	Cybersecurity directive Binding Law	EU	In transposition to national law	Essential and important entities' security	Security measures across lifecycle Network and information system risks; reporting duties
NIST AI RMF	https://www.nist.gov/itl/ai-risk-management-framework	Risk management framework	USA / global adopters	Released v1.0	Governance and risk for AI systems	Focus on trustworthy AI characteristics
OECD AI Principles	https://www.oecd.org/en/topics/sub-issues/ai-principles.html	Voluntary principles / soft law	OECD & adherents	Adopted 2019	High-level principles for trustworthy AI	Applies to all AI systems and actors
Singapore – Model AI Governance	https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework	Voluntary model framework / guidance	Singapore / global adopters	Version 2 and sector playbooks released	Practical governance for AI deployment	Focus on high-impact use cases
South Korea – AI Act / Strategy	https://cset.georgetown.edu/publication/south-korea-ai-law-2025/	Binding law	South Korea	National strategy; AI Act in development	Trusted AI, data, and digital innovation	Risk-tiered, aligned with EU-style approach
UK – Bletchley & Seoul Commitments, AI Safety Summits	https://www.gov.uk/government/publications/frontier-ai-safety-commitments-ai-seoul-summit-2024	Voluntary + program	Global / UK hosted	In force as soft law	Frontier model safety, systemic risks	High-impact foundation models and capabilities
UN Advisory Body Interim Report on AI Governance	https://www.un.org	Global advisory report	Global	Interim / non-binding	High-level recommendations for a global framework for AI governance.	Strategic; informs states and organisations about emerging global governance directions.
United States – OMB/NIST Federal Baseline	https://airc.nist.gov/airmf-resources/playbook/	Guidance and policy baseline + Framework	USA federal government	In effect via OMB, NIST AI RMF	Federal use of AI and safety practices	Impacts on rights, safety, and services
US Executive Order 14110 – Safe, Secure, Trustworthy AI	https://www.whitehouse.gov	Executive order / policy	USA (global influence)	In force	Sets US federal policy direction on AI safety, security, civil rights, labour and competition.	Applies directly to US federal agencies and indirectly to providers engaging with them.

Framework	Lifecycle Controls Definition: A narrative description of which stages of the AI lifecycle the framework actually influences and how. Why it matters: This shows whether a framework is focused on: early design ethics (e.g., IEEE 7000), testing & evaluation (e.g., NIST AI RMF), deployment controls (e.g., EU AI Act), operational safeguards (e.g., CRA), or entire lifecycle consistency (e.g., ISO/IEC 42001). Example: EU AI Act: Focuses on deployment, operation, monitoring, documentation, and risk controls — less on early design. ISO/IEC 42001: Full lifecycle from planning → development → deployment → use → monitoring.	Risk Controls Definition: How a framework expects an organisation to identify, assess, mitigate, monitor, or document risks related to AI. Why it matters: Risk controls are central to ISO 42001 Annex A (A.5–A.10), and reflect how a framework complements AI risk management. Example: ISO/IEC 23894: Complete AI risk management lifecycle. EU AI Act: Pre-deployment risk evaluation + transparency + incident reporting. OECD Principles: High-level societal-risk expectations but no specific processes.
African Union – AI Strategy	Focuses primarily on macro-level planning and design of national and regional AI ecosystems rather than system-level development. It informs how AI projects should be conceived and governed and sets expectations for responsible use, but offers little direct guidance on testing, deployment or operational monitoring at system level.	Risk controls are framed at a strategic policy level. The strategy calls for member states to identify societal, economic, and human-rights risks from AI, promote inclusive and equitable access, and strengthen transparency and accountability. Concrete risk processes are expected to be implemented via national laws, sector rules and management standards, rather than specified directly.
Brazil PL 2338/2023 (AI Bill)	Provides risk-based expectations that affect how AI systems are planned, deployed and used, including impact assessment and rights protections. It has less prescription over the technical development lifecycle, but encourages governance mechanisms and monitoring aligned to the system's risk classification.	Risk controls are risk-tiered for "high-risk" and "very high-risk" systems. The bill requires pre-deployment impact and risk assessment, transparency and information duties to affected individuals and regulators, safeguards proportionate to risk, and monitoring during operation. It also foresees incident reporting, remediation duties, and a clear allocation of responsibilities between providers, deployers, and supply-chain actors.
BS 30440 (British Standard on AI Governance)	Structures governance and assurance activities across the entire lifecycle of AI systems, from initial concept and requirements definition through development, deployment, operation and decommissioning. It reinforces auditability and evidence collection at each stage to support robust assurance and certification.	Risk controls are structured and auditable across the AI lifecycle. Organisations must systematically identify and assess AI-related risks, define and document treatment plans, and embed controls at key lifecycle stages. The standard emphasises evidence-based decision-making, operational monitoring, and traceability so that independent assurance or certification can verify risk posture.
C2PA / Content Authenticity Initiative	Lifecycle focus is strongest at the deployment and operation stages, where content provenance and watermarking controls are implemented to tag, distribute and verify media. It has limited influence on early design, but affects how systems are configured and used in production, and supports ongoing monitoring of misuse or tampering.	Risk controls focus on provenance, integrity and misuse of digital content. The framework mitigates deepfake and synthetic-media risks by requiring provenance metadata, cryptographic signing, tamper-evident chains of custody, and user-facing trust indicators. These controls align with data integrity and transparency obligations and support responsible consumption and redistribution of media.
Canada AIDA (Bill C-27)	Focuses lifecycle requirements on high-impact AI systems, particularly around assessment before deployment, ongoing monitoring and responsible use. It drives governance and compliance activities at planning and operational stages, but does not define detailed software development or testing processes on its own.	Risk controls concentrate on "high-impact systems". Providers must perform impact assessments, implement risk-mitigation measures, maintain records of data and model behaviour, and provide transparency and explanations to regulators and affected individuals. Operational obligations include monitoring, reporting of material incidents or harms, and corrective actions, with clear duties for both providers and deployers.
China – Generative AI & Deep Synthesis Measures	Lifecycle impact is strongest at development, deployment and operation of generative and deep-synthesis services. Requirements influence training data choices, pre-release security and safety testing, user-interface design and ongoing monitoring for harmful or illegal content, with less direct focus on early conceptual design choices.	Risk controls address content and security risks of generative and deep-synthesis services. They require governance of training data, algorithm and model security evaluation, pre-release safety testing, and mandatory labelling or watermarking of synthetic content. Providers must monitor for illegal or harmful outputs, establish complaint channels, and report serious incidents or unlawful generation to authorities.
Colorado AI Act (SB 24-205) - known as CAIA	Lifecycle influence is most visible at deployment and use, where obligations for risk management, impact assessment and consumer protection apply to high-risk AI systems. It implicitly affects earlier planning and development decisions through these obligations, but does not define engineering lifecycle processes in detail.	Risk controls are centred on consumer protection for "high-risk AI systems". Deployers must carry out impact assessments, implement risk-management programmes, and provide disclosures to consumers when automated decisions materially affect them. The Act also requires notice, explanation, and an opportunity to correct, plus documentation, risk monitoring and oversight for systems in use.
Council of Europe AI Convention	Shapes lifecycle governance by requiring human-rights and rule-of-law considerations to be integrated from conception and design through deployment and use of AI systems. It does not describe technical development steps, but frames how impact assessment, safeguards and oversight should operate throughout the lifecycle.	Risk controls are grounded in human-rights, rule-of-law and democracy principles. Parties must identify and mitigate risks to fundamental rights (e.g. discrimination, freedom of expression, due process), ensure transparency, provide effective remedies, and establish independent oversight mechanisms. The Convention does not define technical controls but requires legally robust safeguards and accountability structures in national frameworks.
Cyber Resilience Act (CRA)	Targets lifecycle stages from design through deployment for digital and AI-enabled products, with particular emphasis on secure development, configuration and operational security. Post-deployment, it reinforces patching, vulnerability management and monitoring obligations, while having less detailed guidance for concept and ethical design choices.	Risk controls focus on cybersecurity of products with digital/AI elements. Manufacturers must implement secure development practices, vulnerability and patch management, security updates throughout product lifespan, and mandatory reporting of actively exploited vulnerabilities and incidents. CRA also requires documentation such as SBOMs and supports conformity assessment to verify that security risks are handled appropriately.
ENISA - AI/Cypersecurity Guidance	Focuses lifecycle guidance on secure development, deployment and operation of AI systems, including threat modelling, security testing and hardening. It informs how updates, monitoring and incident handling should be managed over time, while relying on other frameworks for broader ethical and governance aspects.	Risk controls provide operational security practices for AI systems. The guidance covers threat modelling specific to AI, robustness and adversarial-attack testing, hardening of models and pipelines, monitoring for anomalous behaviour, and integration with incident-response processes. It emphasises resilience and secure-by-design lifecycle practices rather than general ethics.
ETSI SAI (Securing AI)	Has strong influence on development, testing, deployment and operation stages by specifying security and robustness controls for AI components and systems. It is less about conceptual planning and more about embedding secure-by-design and secure-by-default practices into the AI lifecycle, including updates and decommissioning.	Risk controls are technical and component-focused. ETSI SAI addresses attack-surface reduction, secure training infrastructure, data poisoning prevention, adversarial robustness, verification and validation of AI components, and coordinated vulnerability disclosure. It treats AI as a security-critical component requiring specialised risk analysis and testing alongside traditional ICT security.
EU AI Act	Primarily shapes lifecycle stages from design and development of high-risk systems (through risk management and data governance obligations) to deployment, operation and post-market monitoring. It requires pre-deployment conformity assessment, ongoing oversight and incident reporting, while leaving detailed engineering methods to harmonised standards and technical norms.	Risk controls are built around a mandatory risk-management system for high-risk AI. This includes hazard identification, risk estimation and evaluation, testing and mitigation, quality and governance of training data, detailed technical documentation, and human oversight mechanisms. Post-market monitoring, incident reporting, and corrective actions are required, supported by conformity assessment and enforcement by market-surveillance authorities.
G7 – Hiroshima Principles & Code of Conduct	Provides high-level lifecycle guidance for organisations developing and deploying advanced AI, particularly general purpose and frontier models. It encourages responsible design and evaluation, careful deployment and ongoing monitoring, but leaves implementation details to standards and internal governance frameworks.	Risk controls are articulated as non-binding expectations for advanced and frontier models. They call for systematic risk identification, safety testing and evaluation, measures to prevent misuse, transparency about capabilities and limitations, and ongoing monitoring of deployed systems. Implementation details are intentionally left to internal governance arrangements and technical standards.
IEEE 7000 – Ethical System Design	Strongly targets early lifecycle stages by embedding stakeholder values, ethical analysis and impact considerations into concept development and design decisions. The resulting requirements flow into development and subsequent lifecycle activities, but the standard is primarily about getting the design and governance foundations right.	Risk controls target ethical and societal risk in early lifecycle stages. The standard requires identification of stakeholders and their values, analysis of potential harms and benefits, structured ethical impact assessments, and documentation of value-driven requirements. This process steers design decisions to avoid unacceptable risks and creates traceability of ethical trade-offs for later oversight.
IEEE 7001 – Transparency	Supports lifecycle-wide transparency by defining expectations for information and documentation from design and development through deployment and operational use. It has particular relevance at release and use stages, where users and other stakeholders need clear information about system capabilities, limitations and impacts.	Risk controls address transparency-related risks, such as misunderstanding system capabilities, over-reliance, or misinterpretation of outputs. IEEE 7001 requires clear system documentation, user-facing explanations, disclosure of limitations and conditions of use, and information design that enables informed human oversight. This supports faster detection of misuse or harm and more accountable operation.
ISO/IEC 23894 (AI Risk)	Covers lifecycle-wide risk management, integrating impact and risk assessment into planning, design, development, deployment and operation of AI systems. It guides how risks are identified, analysed, treated and reviewed at multiple stages, complementing ISO/IEC 42001's management system structure.	Risk controls follow a complete AI risk-management cycle: establishing context; identifying AI-specific risks (data, models, human interaction, societal effects); assessing likelihood and impact; selecting treatments; and monitoring residual risk. It provides concrete guidance on integrating risk analysis into AI projects and on re-assessing risks as systems or environments change.
ISO/IEC 42001 (AIMS)	Explicitly addresses the full AI lifecycle by requiring organisations to plan, design, develop, deploy, operate and monitor AI systems within an AI management system. Controls span from early context and risk analysis through operational use, incident handling and continual improvement, making it the most comprehensive lifecycle reference.	Risk controls are embedded in an AI management system. Organisations must perform AI impact and risk assessments (A.5), define lifecycle processes and controls (A.6.2), manage AI-related assets and data (A.4 & A.7), ensure appropriate transparency (A.8), govern responsible use (A.9), and manage third-party risks (A.10). Continual improvement, internal audit, and non-conformity management ensure that risk controls remain effective.
ISO/IEC 42005 – AI Management System Assessment	Covers the lifecycle indirectly by defining how an AI management system—covering planning, development, deployment, operation and improvement—should be assessed. It focuses on evaluating evidence and practices across all stages rather than specifying development methods itself.	Risk controls relate to how an assessor verifies risk management rather than how risks are treated technically. The standard defines criteria and methods to evaluate whether an organisation's AIMS has adequate risk identification, impact assessment, treatment, documentation, operational safeguards, incident management, and supplier oversight. It enables consistent internal and external assessment of AIMS effectiveness.
Japan – AI Business Guidelines (METI/MIC)	Offer lifecycle guidance for organisations planning, deploying and operating AI systems in business contexts. They focus on responsible use, accountability and transparency at deployment and use stages, while giving lighter direction on specific development and testing methodologies.	Risk controls focus on business and consumer impacts. Organisations are expected to identify risks from data and models, prevent unfair discrimination and inappropriate profiling, ensure transparency towards users and impacted individuals, and establish internal governance rules for responsible use. Controls are typically implemented via company policies, risk processes and sectoral standards.
NIS2 Directive	Influences the lifecycle mainly from deployment onwards for AI-enabled systems used by essential and important entities. It requires appropriate security measures, incident detection, reporting and continuity planning during operation, while leaving detailed design and development practices to sectoral and technical standards.	Risk controls address network and information-system security for essential and important entities, including AI-enabled services. Organisations must implement technical and organisational security measures, vulnerability handling, logging and monitoring, business continuity and disaster recovery, and prompt incident detection and reporting. AI systems are treated as part of the broader critical-infrastructure risk surface.
NIST AI RMF	Applies across all lifecycle stages via its Govern, Map, Measure and Manage functions, which guide planning, design, testing, deployment and ongoing monitoring. It embeds evaluation and measurement activities into development and post-deployment phases, supporting continuous improvement of AI systems.	Risk controls are organised across the Govern, Map, Measure, Manage functions: 1) Govern sets governance structures, policies and accountability for AI risk; 2) Map identifies system context, stakeholders, data and model risks; 3) Measure covers evaluation, testing, robustness, and metrics; 4) Manage focuses on treatment options, deployment safeguards, monitoring, and incident response. Together they provide concrete, repeatable practices for managing AI risk.
OECD AI Principles	Covers the whole lifecycle at a principle level by promoting human-centred values, robustness and accountability from design to deployment and use. However, it does not specify concrete lifecycle processes, leaving organisations to translate these expectations into their own development, deployment and monitoring practices.	Risk controls are principle-level rather than procedural. They call for identifying and addressing risks to human rights and democratic values, promoting robustness, safety and security, ensuring transparency and explainability where appropriate, and creating accountability frameworks. The detailed processes for risk assessment and mitigation are expected to come from standards and organisational governance.
Singapore – Model AI Governance	Provides practical lifecycle guidance from design and development of AI-driven products and services through deployment, operation and monitoring. It emphasises risk assessment, data governance, transparency and user communication across the lifecycle, helping organisations operationalise high-level principles.	Risk controls are practical and implementation-oriented. The framework encourages structured risk assessment, data management and quality controls, fairness and bias evaluation, transparency artefacts (e.g. explanations and disclosures), and user-communication mechanisms. It also stresses monitoring, review, and human oversight, making it a widely used playbook for operational AI risk governance.
South Korea – AI Act / Strategy	Provides policy-level lifecycle guidance, shaping how organisations plan, design and govern AI systems in line with national strategy. It has clearer implications for deployment and use—particularly around trustworthy use and innovation—while leaving technical development and monitoring approaches to other standards and sector rules.	Risk controls apply especially to designated high-risk AI uses. They include requirements for safety and fairness evaluation, privacy and data-protection safeguards, user transparency, and operational risk controls in critical sectors. The strategy also highlights monitoring, auditing and redress mechanisms, but leaves many implementation details to sectoral regulation and technical guidance.
UK – Bletchley & Seoul Commitments, AI Safety Summits	Provides high-level expectations across the AI lifecycle, encouraging safe design, evaluation and deployment of frontier models. In practice it shapes planning and governance activities and post-deployment monitoring, rather than prescribing detailed development or operational processes.	Risk controls are described as global commitments for frontier-model safety. Signatories endorse safety testing and evaluation prior to deployment, monitoring for misuse and systemic risks, transparency regarding capabilities and limitations, and collaboration with regulators and researchers. Detailed control frameworks are expected to emerge via national policies and technical standards, not the summit texts themselves.
UN Advisory Body Interim Report on AI Governance	Provides macro-level lifecycle guidance by outlining how global governance structures should shape the design, deployment and oversight of AI systems. It remains high-level and conceptual, informing national and organisational thinking about responsible AI across the lifecycle without prescribing technical practices.	Risk controls are framed at the level of global systemic risk governance. The report recommends mechanisms for monitoring global AI risks, protecting human rights, enhancing transparency and accountability, supporting affected communities, and enabling international cooperation. It guides the direction of future treaties, regulations and standards, rather than specifying organisation-level risk procedures.
United States – OMB/NIST Federal Baseline	Applies across the full AI lifecycle for federal agencies: from planning and design of AI use cases, through development and testing in line with NIST practices, to deployment, operation and continuous monitoring. It embeds governance checkpoints and documentation requirements in multiple stages, making it a strong lifecycle reference.	Risk controls define how US federal agencies should manage AI risk. They include impact and rights assessments, documentation of data and models, evaluation and testing aligned with NIST AI RMF, transparency and notice to affected individuals, and human oversight mechanisms. Agencies must also implement operational safeguards, monitoring, and incident-response processes for AI-enabled systems.
US Executive Order 14110 – Safe, Secure, Trustworthy AI	Addresses lifecycle considerations for AI developed, procured or used by US federal agencies, with emphasis on testing and evaluation prior to deployment, safe and secure operation, and continuous monitoring. It influences how safety, security and civil-rights safeguards are built into design choices and operational processes.	Risk controls are aimed at advanced and safety-critical AI across the US federal ecosystem and key private actors. The EO mandates or promotes safety testing and red-teaming, reporting obligations for certain frontier models, civil-rights and anti-discrimination safeguards, worker-impact protections, data-governance requirements, and ongoing monitoring and evaluation. It uses procurement and agency rulemaking to turn these into operational controls.

Framework	Transparency/Docs Definition: What documentation, disclosures, explainability, or information artefacts the framework requires or recommends. Examples: IEEE 7001: Strongest transparency standard; defines user-facing disclosures. EU AI Act: Requires technical documentation, model information, instructions for use. NIST AI RMF: Requires documentation for measurement, monitoring, testing, governance.	Cybersecurity Linkage Definition: How the framework relates to AI security, cybersecurity requirements, model robustness, red-teaming, or ICT product security. Examples: ENISA AI Security Guidance: Strong linkage; cybersecurity-first framing. CRA: Security obligations for software/AI products. ISO/IEC 42001: Security included, but not the main focus	Human Oversight Definition: Whether the framework imposes or recommends human oversight, human-in-the-loop mechanisms, governance roles, or human accountability. Examples: EU AI Act: Requires human oversight for high-risk systems. OECD Principles: Human-centric values and oversight expectations. IEEE 7000: Emphasises stakeholder involvement and ethical review.	Incident Handling / Reporting Definition: Requirements or expectations for incident detection, reporting, post-incident analysis, or corrective action. Examples: EU AI Act: Mandatory reporting for serious incidents & corrective actions. ISO/IEC 42001: Clause 10—non-conformity and continual improvement processes. NIST AI RMF: Encourages incident logging, analysis, resilience mechanismS	Assurance Route Definition: How compliance or conformity with the framework is demonstrated: certification self-declaration third-party assessment audit regulatory inspection Examples: ISO/IEC 42001: Certification. CRA / NIS2: Regulatory enforcement + conformity assessment. OECD principles: Non-binding; no assurance route.	Enforcement Definition: Whether the framework is binding, legally enforceable, or voluntary. Examples: EU AI Act: Legally binding; penalties. Executive Order 14110: Government directive; enforced via procurement & agency policy. IEEE 7000/7001: Voluntary standards. UN Advisory report: Non-binding
African Union – AI Strategy	Calls for transparency and accountability	Tied to AU cyber and data strategies	Human rights and inclusion focus	Promotes mechanisms to address harms	Regional coordination and peer learning	Non-binding at AU level
Brazil PL 2338/2023 (AI Bill)	User information, algorithmic transparency	Security and data governance requirements	Duty of human supervision for critical uses	Mechanisms to address rights violations	Future conformity schemes and certifications	National authorities, administrative sanctions
BS 30440 (British Standard on AI Governance)	Clinical validation documentation	Security as part of validation evidence	Clinical governance and sign-off	Post-market surveillance and reporting	Basis for conformity assessment schemes	Via healthcare regulators and procurement
C2PA / Content Authenticity Initiative	Visible provenance indicators and manifests	Crypto signing, secure supply chain for assets	Publisher and platform review	Revocation of certificates, takedown workflows	Conformance to C2PA spec, vendor attestations	Voluntary; platform policy based
Canada AIDA (Bill C-27)	Public notices and documentation obligations	Secure handling of data and models	Accountable person and governance roles	Reporting of material incidents to regulator	Compliance program and documentation	Administrative monetary penalties, offences
China – Generative AI & Deep Synthesis Measures	Watermarks, labelling of synthetic content	Tied to Cybersecurity and Data Security Laws	Provider responsibility and manual review	Reporting to CAC and other regulators	Security assessment filings, audits	Regulator fines, service suspension
Colorado AI Act (SB 24-205) - known as CAIA	Notices to consumers, disclosures to AG	Data protection and security safeguards	Human review of consequential decisions	Obligations to address and report violations	Documentation supporting "reasonable care"	Attorney General enforcement, civil penalties
Council of Europe AI Convention	Impact assessments, documentation obligations	Security where needed to protect rights	Meaningful human control over AI decisions	Remedies and redress mechanisms required	National implementation and oversight bodies	Domestic law plus Council of Europe monitoring
Cyber Resilience Act (CRA)	Security documentation, SBOM, update policies	Core security baseline for connected products	Manufacturer responsibility and governance	Mandatory reporting of actively exploited flaws	Conformity assessment, CE marking	Market surveillance, fines, product withdrawal
ENISA - AI/Cypersecurity Guidance	Security evidence expectations	Aligns with NIS2	Operational responsibility	Under NIS2 frameworks		Indirect via NIS2/CRA references
ETSI SAI (Securing AI)	Security documentation and testing artefacts	Complements existing cyber standards	Operational security responsibilities	Guidance on vulnerability management	Basis for testing and certification schemes	Via adoption in regulation and procurement
EU AI Act	Technical documentation, logs, user information	Robustness, resilience, secure operation	Human-in-the-loop / over-the-loop controls	Serious incident reporting to authorities	Conformity assessment, CE marking, notified bodies	Market surveillance, significant administrative fines
G7 – Hiroshima Principles & Code of Conduct	Information sharing, transparency to users	Secure design and operation of AI	Human responsibility for outcomes	Cooperation on serious incidents and misuse	Voluntary codes of conduct	Peer pressure and domestic follow-up
IEEE 7000 – Ethical System Design	Requires explicit documentation of value decisions, stakeholder input and ethical trade-offs.	Indirect; focuses on ethical risk rather than classic cyber risk.	Strong emphasis on stakeholder engagement and governance of ethical decisions.	Encourages documenting and learning from ethical issues and harms.	Self-assessment or third-party review using IEEE 7000 process guidance.	Voluntary standard.
IEEE 7001 – Transparency	Central focus on transparency artefacts, documentation and user-facing information.	Limited; focuses on transparency rather than security controls.	Supports informed oversight by making system behaviour and limitations understandable.	Supports post-incident analysis through better documentation and information flows.	Self-assessment or external review against IEEE 7001 transparency requirements.	Voluntary standard.
ISO/IEC 23894 (AI Risk)	Risk registers and documentation	Considers security as key risk dimension	Roles in risk ownership and review	Lessons-learned and risk re-assessment	Supports audits and certifications indirectly	Voluntary; adopted via policy or contracts
ISO/IEC 42001 (AIMS)	Documented policies, roles, processes	References to 27001 and security controls	Governance structure and accountability	Non-conformity and corrective-action process	Third-party certification possible	Market/contractual, not regulatory
ISO/IEC 42005 – AI Management System Assessment	Emphasises evidence, documentation and records for AIMS assessment.	Indirect; via controls inherited from ISO/IEC 42001 and related standards.	Focuses on roles and competence for assessors and governance bodies.	Looks for evidence that incidents and non-conformities are managed within the AIMS.	Supports internal audits and third-party conformity assessments of an AIMS.	Voluntary but may underpin certification schemes.
Japan – AI Business Guidelines (METI/MIC)	Information provision to users and regulators	Security and resilience requirements	Organizational governance and human checks	Notification and remediation expectations	Self-assessment and possible certification	Relies on soft-law and sector regulators
NIS2 Directive	Incident notifications, security documentation	Core EU cyber baseline for critical sectors	Management accountability and board duties	Mandatory incident reporting and response	Supervisory audits and inspections	Administrative fines and orders
NIST AI RMF	Documentation of risks and controls	Integrates with NIST cyber frameworks	Roles, responsibilities and training	Feedback loops and incident learning	Supports audits, procurement questionnaires	Non-binding; adopted via policy/contract
OECD AI Principles	Calls for transparency and explainability	Security and robustness as key pillar	Human-centred values and oversight required	Encourages mechanisms to remedy harm	Non-binding; guides national frameworks	Implemented via domestic regulation/standards
Singapore – Model AI Governance	User communication, model documentation	Security and robustness of AI systems	Escalation paths and human-in-charge	Guidance on issue management and recovery	Self-assessment, pilots, potential certifications	Non-binding; adopted via industry codes
South Korea – AI Act / Strategy	Documentation, explainability for critical uses	Strong link to cyber and data security regime	Human-in-the-loop for high-impact uses	Regulatory reporting obligations emerging	Certification and sandbox mechanisms	Supervisory authorities and sectoral regulators
UK – Bletchley & Seoul Commitments, AI Safety Summits	Model cards, risk reports to regulators/peers	Secure model training and access control	Board-level accountability for AI safety	Information sharing on critical vulnerabilities	Voluntary reporting, independent research review	Non-binding; relies on reputational pressure
UN Advisory Body Interim Report on AI Governance	Promotes transparency, participation and information sharing at international level.	Addresses security and safety at a conceptual level.	Strong focus on human rights, inclusion and global equity in AI governance.	Encourages mechanisms for accountability and remedy, but not detailed.	Non-binding; may influence future treaties, standards and soft-law instruments.	None directly; relies on adoption by states and organisations.
United States – OMB/NIST Federal Baseline	Public inventories, impact documentation	Alignment with FedRAMP, NIST security	Agency accountability and human review	Incident reporting to oversight bodies	Internal controls, audits, inspector general	Administrative enforcement via OMB oversight
US Executive Order 14110 – Safe, Secure, Trustworthy AI	Requires reporting, disclosures and documentation for certain AI models and uses.	Strong linkage to model safety, red-teaming and critical-infrastructure security.	Calls for protection of civil rights and worker protections in AI deployments.	Includes expectations for incident reporting, evaluations and independent testing.	Implemented through agency policies, guidance and procurement requirements.	Governmental oversight and procurement-based leverage rather than a single regulator.

Framework	Cross-border/Data Definition: Relevance of the framework to cross-border data flows, international cooperation, or multi-jurisdiction AI rules. Examples: CRA, EU AI Act: Strong cross-border implications within the EU market. Singapore Model Framework: Global adoption; cross-border guidance. UN report: International governance considerations.	Sector Focus Definition: Whether the framework is: cross-sectoral public-sector specific safety-critical consumer rights–based cybersecurity / product security focused Examples: CRA: ICT products (security). EU AI Act: All sectors with risk tiers. NIS2: Essential and important sectors. OECD Principles: Cross-sectoral.	Technical Requirements Definition: The degree of technical detail the framework prescribes (e.g., model evaluations, robustness testing, documentation formats, transparency artefacts, etc.). Examples: ETSI SAI: High-technical detail for secure AI. NIST AI RMF: Detailed testing & measurement guidance. OECD Principles: Low technical detail.	Governance Notes Definition: A synthesised explanation of the framework's governance relevance — particularly how it can support AI management systems, regulatory compliance, or risk governance. Examples: "Useful complement to ISO/IEC 42001 Annex A.5 and A.7." "Helps define oversight structures for high-risk use cases." "Supports transparency governance for public-sector agencies."
African Union – AI Strategy	Data governance and cross-border flows	Development, public services, innovation	High-level; no specific controls	Platform for converging national AI laws
Brazil PL 2338/2023 (AI Bill)	Interacts with LGPD privacy regime	Economy-wide with specific high-risk sectors	Details to be set by secondary regulation	Positions Brazil within global AI governance
BS 30440 (British Standard on AI Governance)	Supports global procurement of AI in health	Healthcare AI	Detailed validation and evidence criteria	Blueprint for sector-specific AI standards
C2PA / Content Authenticity Initiative	Global interoperability across ecosystems	Media, news, creative industries, platforms	Signing, verification, manifest processing APIs	Key building block for watermarking and provenance
Canada AIDA (Bill C-27)	Interaction with CPPA and cross-border rules	Cross-sector high-impact AI	High-level; to be detailed in regs	Early comprehensive AI bill; now a reference case
China – Generative AI & Deep Synthesis Measures	Controls on cross-border data and models	Online platforms and service providers	Content filters, watermarking, logging	One of the earliest binding gen-AI regimes
Colorado AI Act (SB 24-205) - known as CAIA	Covers use affecting Colorado residents	Credit, employment, housing, key services	Documented testing, bias and safety checks	First comprehensive US AI consumer law at state level
Council of Europe AI Convention	Cooperation among parties and adequacy links	Public functions and rights-relevant domains	Principle-based; tech-neutral	First global-open AI treaty centred on rights
Cyber Resilience Act (CRA)	Applies to products placed on EU market	Horizontal across digital/IoT products	Security controls aligned with EU standards	Important baseline for AI-enabled hardware/software
ENISA - AI/Cypersecurity Guidance	EU context	Operators of essential servies		
ETSI SAI (Securing AI)	International applicability of ETSI standards	Horizontal; telecom and digital services	Detailed security controls for AI components	Key technical layer under CRA and AI Act
EU AI Act	Applies extraterritorially for EU-placed AI	Cross-sector with sectoral listings in Annex III	Detailed high-risk system requirements	Anchor for many global AI compliance programs
G7 – Hiroshima Principles & Code of Conduct	Interoperable governance among G7 states	Advanced AI developers and platforms	High-level; implemented locally	Bridges EU, US, Japan and others on frontier AI
IEEE 7000 – Ethical System Design	Addresses global ethical considerations rather than jurisdiction-specific rules.	Cross-sector.	Process-oriented; not prescriptive on algorithms but on value-driven engineering.	Useful complement to ISO/IEC 42001 Annex A.2–A.5 for value-driven AI governance.
IEEE 7001 – Transparency	Supports consistent disclosure practices across jurisdictions.	Cross-sector.	High-level requirements for transparency mechanisms and information design.	Aligns strongly with ISO/IEC 42001 Annex A.7–A.9 for information and use.
ISO/IEC 23894 (AI Risk)	Applicable across jurisdictions and sectors	All industries using AI	Methodological rather than technical specs	Pairs naturally with ISO/IEC 42001 and NIST AI RMF
ISO/IEC 42001 (AIMS)	Supports cross-jurisdictional compliance	Any organization using or providing AI	Process-oriented, technology-neutral	Central standard for AI governance programs
ISO/IEC 42005 – AI Management System Assessment	Global applicability wherever ISO/IEC 42001-based AIMS are implemented.	Cross-sector.	Process-focused; assessment criteria rather than technical model requirements.	Natural companion to ISO/IEC 42001 for organisations aiming at formal AIMS assurance.
Japan – AI Business Guidelines (METI/MIC)	Interoperability with EU and OECD principles	Cross-sector, with focus on industry and gov	Implementation-oriented checklists	Important Asia-Pacific reference framework
NIS2 Directive	EU-wide cooperation and information sharing	Energy, transport, health, digital and more	High-level security outcomes, not specific	Important dependency for AI systems in scope
NIST AI RMF	Globally compatible, technology-neutral	Any sector using AI	Framework outcomes; no prescriptive tech	Widely used baseline; referenced in US policy
OECD AI Principles	Supports interoperability among members	Cross-sector	Principles-level; no detailed controls	Reference for many later AI regulations
Singapore – Model AI Governance	Designed for interoperability with global rules	Finance, healthcare, government and more	Implementation examples, not strict specs	Widely cited practical playbook for companies
South Korea – AI Act / Strategy	Interoperability with global partners	Industry, public sector, innovation hubs	Forthcoming detailed technical standards	Explicitly benchmarked to EU AI Act and OECD
UK – Bletchley & Seoul Commitments, AI Safety Summits	International cooperation on frontier AI safety	General-purpose and frontier model developers	Evaluation benchmarks, safety testing protocols	Sets direction for future binding regulation
UN Advisory Body Interim Report on AI Governance	Explicitly focused on cross-border, multilateral governance of AI.	Cross-sector, societal level.	No technical prescriptions; principle-level guidance.	Useful for horizon-scanning and aligning national / organisational strategies.
United States – OMB/NIST Federal Baseline	Limited; mainly domestic federal context	Federal agencies and contractors	Use of NIST standards and testing methods	Baseline for federal AI procurement and use
US Executive Order 14110 – Safe, Secure, Trustworthy AI	Influences global providers that serve US markets or collaborate with US agencies.	Public sector and critical private sectors.	High-level expectations for testing, evaluations and safety practices.	Key reference for organisations interacting with the US public sector on advanced AI.

Framework	Lifecycle – Plan/ Design Definition: Does this framework provide concrete, operational guidance for this phase? Activities that determine whether and how an AI system should be built, including problem framing, requirements, ethical assessment, stakeholder input, and governance setup. Examples of activities: Problem definition & use-case selection Ethical/value analysis (IEEE 7000) Stakeholder impact identification Initial risk/impact assessment (ISO 23894, ISO 42001 A.5) Governance & accountability setup Data strategy definition High score: Framework explicitly dictates planning methodology, ethical design, or governance obligations	Lifecycle – Develop/ Test Definition: Does this framework provide concrete, operational guidance for this phase? Technical and procedural controls during system development, training, evaluation, verification, and validation—covering models, data, algorithms, pipelines, and pre-release testing. Examples of activities: Dataset preparation, data governance, data quality checks Model training, feature engineering, pipeline design Red-teaming, adversarial testing, robustness assessment Verification and validation (BS 30440, ETSI SAI) Secure development practices (ENISA, CRA) High score: Frameworks that prescribe operational technical controls or testing methodologies.	Lifecycle – Deploy/ Release Definition: Does this framework provide concrete, operational guidance for this phase? Controls required before and at the moment the system is placed into production. Examples: Conformity assessment (EU AI Act) Model cards, transparency disclosures (IEEE 7001, Singapore Model) Security configuration for release (CRA, ENISA) Governance approvals Release documentation and sign-off High score: Framework prescribes pre-deployment checks, approvals or release requirements	Lifecycle – Operate/ Use Definition: Does this framework provide concrete, operational guidance for this phase? Controls governing the correct, safe, compliant use of an AI system in live operations. Examples: User guidance & limitations Operational security configuration (CRA, NIS2, ENISA) Logging, traceability, audit records Human oversight setup (EU AI Act, OECD Principles) Interface-level transparency High score: Framework requires specific duties for operators, deployers, or system users.	Lifecycle – Monitor/ Improve Definition: Does this framework provide concrete, operational guidance for this phase? Post-deployment monitoring, safety evaluation, incident detection, metrics review, continuous improvement, and end-of-life (EOL) processes. Examples: Post-market monitoring (EU AI Act) Safety evaluation and metrics (NIST AI RMF "Manage") Incident reporting (EU AI Act, EO 14110, NIS2) Vulnerability management & patching (CRA) Ethical review loops (IEEE 7000) High score: Framework imposes clear ongoing monitoring or feedback obligations.	ISO/IEC 42001 Alignment Purpose: The score - and text - shows how closely each external framework (law, standard, principle, guideline) aligns with the requirements, controls, structure, and intent of ISO/IEC 42001:2023 – AI Management System (AIMS). Think of it as. **"How much does this framework support, reinforce, or map into ISO/IEC 42001 implementation (Clauses and Annex A controls)?"** 3) strong / structural: Provides comprehensive governance, risk, lifecycle, documentation, and oversight requirements that match the structure of ISO/IEC 42001 2) partial / thematic: Contains specific themes or requirements that align with parts of ISO/IEC 42001 1) weak / contextual: Provides general principles, values, or ethics; supports governance thinking, but does not define processes, roles, controls, or lifecycle requirements; useful context but not implementable as AIMS controls 0) not really aligned / out of scope: The framework does not address management systems, governance, or AI lifecycle controls; no meaningful mapping to ISO/IEC 42001 clauses or Annex A controls.	AINNOLAB Priority Weight (1–5) Purpose: This score expresses how important a given framework is for an organisation's AI governance, compliance, or readiness work — from AINNOLAB's perspective. Think of it as: **"How central is this framework for organisations trying to be compliant, trustworthy, and audit-ready?"** 5) Core backbone: Foundational frameworks that most organisations must (or should) align with; high regulatory or assurance value 4) Important / High-impact: Highly influential, often jurisdictional or technical frameworks that matter in many governance programmes 3) Strategic / Useful: Adds important guidance but not mandatory or universally needed 2) Contextual: Relevant for specific geographies, sectors, or emerging governance areas 1) Peripheral: Soft-law or advisory frameworks that offer insight but are rarely binding or essential	Maturity Focus (1–5) Purpose: Shows which AI maturity level an organisation needs to reach for the framework to make sense or be useful. Think of it as: **"How mature must your AI governance be to meaningfully use this framework?"** **Scale** ***(using AINNOLAB's 5-level maturity model:*** 5) Best-in-Class: Strong AIMS + risk + audit; certification-ready frameworks become essential 4) Embedded: AI is operational; most regulatory and technical frameworks become relevant 3) Developing: Organisation is building consistent governance; principles and some standards start to matter 2) Reactive: Organisation is piloting AI; light-touch principles relevant 1) Limited: Basic awareness only; framework not needed until later	Maturity Focus – Narrative
African Union – AI Strategy	High	Medium	Low	Medium	Medium	1 Contextual reference only; can complement an AIMS but does not define management system requirements.	3	2	Strategic reference for policy direction and capacity building across AU member states.
Brazil PL 2338/2023 (AI Bill)	Medium	Medium	High	High	Medium	2 Partial thematic alignment with ISO/IEC 42001 governance, risk and documentation expectations.	3	3	Emerging but influential Latin American AI bill for risk-based governance.
BS 30440 (British Standard on AI Governance)	High	High	High	High	High	3 Detailed UK-focused requirements that extend ISO/IEC 42001 and map across Annex A.	5	5	Very relevant for organisations seeking rigorous AI assurance and auditability.
C2PA / Content Authenticity Initiative	Low	Medium	High	High	Medium	1 Contextual alignment with Annex A.7 (data) and A.8 (information to interested parties) for provenance and integrity.	3	3	Developing
Canada AIDA (Bill C-27)	Medium	Medium	High	High	Medium	2 Aligns with Annex A.5 (impact), A.8 (information) and A.9 (use) for high-impact AI systems.	4	3	Important for organisations deploying systems in or into Canada.
China – Generative AI & Deep Synthesis Measures	Medium	Medium	High	High	High	2 Partial alignment with Annex A.5 (impact), A.7 (data), A.8 (disclosures) and A.9 (use) for generative AI.	4	3	Highly relevant for organisations serving Chinese users or operating Chinese platforms.
Colorado AI Act (SB 24-205) - known as CAIA	Medium	Medium	High	High	Medium	2 Aligns with Annex A.5 (impact), A.8 (information) and A.9 (use) for high-risk AI obligations.	4	3	Important for providers and deployers serving Colorado consumers and regulators.
Council of Europe AI Convention	High	Medium	High	High	High	2 Strong thematic link to Annex A.3 (internal organisation), A.5 (impact) and A.8–A.9 (rights-respecting use).	5	4	Anchors AI governance in human-rights law for CoE member states and observers.
Cyber Resilience Act (CRA)	Medium	High	High	High	High	2 Aligns with ISO/IEC 42001 Annex A.4 (resources), A.6.2 (lifecycle), A.7 (data) and A.10 (third-party) for ICT/AI products.	4	4	Critical for EU product manufacturers and operators using AI-enabled components.
ENISA - AI/Cypersecurity Guidance	Medium	High	High	High	High	2 Supports Annex A.4 (resources), A.6.2 (lifecycle), A.7 (data) and A.10 (third-party) for cyber risks	4	4	Key reference for AI security-by-design in EU environments, and future certification schemes.
ETSI SAI (Securing AI)	Medium	High	High	High	High	2 Supports Annex A.4 (resources), A.6.2 (lifecycle), A.7 (data) and A.10 (third-party) from a security viewpoint.	4	4	Key technical companion for AI security and resilience work.
EU AI Act	High	Medium	High	High	High	3 Broad structural alignment with ISO/IEC 42001 clauses 4–10 and Annex A for high-risk and GPAI systems.	5	5	Central regulatory reference for most EU-focused AI programmes, especially high-risk deployments.
G7 – Hiroshima Principles & Code of Conduct	High	Medium	Medium	High	High	2 Partial thematic alignment with ISO/IEC 42001 governance, risk and documentation expectations.	4	3	Useful benchmark for GPAI and frontier-model providers, complementing binding obligations.
IEEE 7000 – Ethical System Design	High	High	Medium	Medium	High	2 Complements Annex A.2–A.5 by embedding values and ethics into AI system requirements and design.	4	4	Strengthens value-sensitive design and ethical risk treatment within an AIMS.
IEEE 7001 – Transparency	High	High	High	Medium	High	2 Aligns strongly with Annex A.7 (data), A.8 (information) and A.9 (use) for transparency artefacts.	4	4	Enhances explainability, documentation and communication capabilities in AI governance.
ISO/IEC 23894 (AI Risk)	High	High	High	High	High	3 Deep alignment with Annex A.5 (impact and risk) and related planning and treatment activities.	5	5	Primary AI risk-management reference tightly coupled to ISO/IEC 42001.
ISO/IEC 42001 (AIMS)	High	High	High	High	High	NA	5	5	Backbone standard for AI management; reference point for AINNOLAB services.
ISO/IEC 42005 – AI Management System Assessment	High	High	High	High	High	3 Directly supports Annex A and clauses 9–10 by defining assessment approaches for an AIMS.	5	5	Crucial for internal/external assessment and certification-oriented programmes.
Japan – AI Business Guidelines (METI/MIC)	High	Medium	Medium	High	High	2 Partial thematic alignment with ISO/IEC 42001 governance, risk and documentation expectations.	3	3	Important soft-law benchmark for Japanese and Japan-facing organisations.
NIS2 Directive	Medium	Medium	High	High	High	2 Aligns with Annex A.4 (resources), A.6.2 (operational security) and A.10 (supplier relationships).	4	3	Baseline cyber-governance directive for essential/important entities using AI-enabled systems.
NIST AI RMF	High	High	High	High	High	3 Clear crosswalk to ISO/IEC 42001 through Govern/Map/Measure/Manage functions.	5	4	De facto risk-management standard, especially in US and multinational contexts.
OECD AI Principles	High	Medium	High	High	High	2 Partial thematic alignment with ISO/IEC 42001 governance, risk and documentation expectations.	4	3	Foundational high-level benchmark for trustworthy AI, especially for organisations at Developing or Embedded levels.
Singapore – Model AI Governance	High	High	High	High	High	3 Practical mapping to Annex A.3–A.5 and A.7–A.9 for governance, risk and documentation.	5	4	Widely used implementation playbook; strong model for embedded AI governance.
South Korea – AI Act / Strategy	High	Medium	Medium	High	High	1 Contextual reference only; can complement an AIMS but does not define management system requirements.	3	3	Relevant for organisations operating in or with South Korean markets and ecosystems.
UK – Bletchley & Seoul Commitments, AI Safety Summits	High	Medium	Medium	Medium	High	1 Contextual reference only; can complement an AIMS but does not define management system requirements.	3	3	Strategic direction and soft-law commitments; relevant for organisations monitoring global AI safety expectations.
UN Advisory Body Interim Report on AI Governance	High	Medium	Low	Medium	Medium	1 Contextual reference only; can complement an AIMS but does not define management system requirements.	3	2	Strategic, global-level guidance useful for horizon scanning and policy alignment.
United States – OMB/NIST Federal Baseline	High	High	High	High	High	3 Strong mapping to ISO/IEC 42001 clauses 4–10 via governance, risk, measurement and management functions.	5	4	Key reference for public-sector AI risk management and for vendors to US federal agencies.
US Executive Order 14110 – Safe, Secure, Trustworthy AI	High	Medium	High	High	High	2 Thematically aligned with Annex A.3 (internal roles), A.5 (impact), A.7–A.9 (data, information, use).	5	4	Sets strong expectations for AI safety and security for US federal ecosystem and beyond.

if questions: Info@ainnolab.com