AI Auditing Standards, Frameworks, and Review Programs (Global Survey)

Global Standards: International bodies have begun issuing AI governance standards with audit-relevant provisions. In Dec 2023 ISO published **ISO/IEC 42001:2023** ("Artificial Intelligence – Management Systems"), a full management-system standard defining requirements for AI risk assessment, impact assessment, data governance, security and controls. In the USA, NIST released its voluntary **AI Risk Management Framework (AI RMF 1.0)** in Jan 2023, providing guidance to identify and manage AI risks (with a special **Generative AI profile** added July 2024). The OECD (2019, updated 2024) adopted high-level **AI Principles** (5 ethical values and 5 recommendations) as the first intergovernmental standard for trustworthy AI. The IEEE Standards Association is also active: it has launched the **Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)** to define certification criteria for ethical AI, and is developing a suite of "P7000" standards on AI ethics (e.g. transparency, bias, data privacy). These standards are final/published (ISO 42001, NIST RMF, OECD Principles, etc.) or in advanced development (IEEE projects). They are broadly applicable across industries and help shape organizational AI governance and audit controls.

Regional Regulations: Governments are enacting AI-specific laws and guidelines that embed audit requirements. For example, the **EU AI Act** (Regulation (EU) 2021/0106) establishes a risk-based regime for AI systems. High-risk AI providers must maintain a quality management system, document lifecycle controls (testing, validation, risk management, monitoring) and undergo conformity assessments before deployment. (The Act was adopted in 2024 and will enter into force by 2026.) The Act explicitly envisions *standards, conformity assessments, and audits* as oversight tools. In the UK, the Information Commissioner's Office (ICO) issued **draft "AI auditing framework" guidance** (2020) focusing on data-protection and explainability; it advises organizations on governance and technical controls to mitigate AI privacy risks. In the USA, the Executive Branch has issued memoranda (e.g. OMB M-21-06 and M-24-10) requiring all federal agencies to implement AI governance and risk-management (designating Chief AI Officers, maintaining AI inventories, applying NIST RMF, etc.).

Self-Assessment Tools: The EU's High-Level Expert Group on AI released voluntary ethics guidance in 2019, including the **"Assessment List for Trustworthy AI" (ALTAI)** tool (July 2020) – a checklist that translates the seven trustworthiness requirements into concrete self-audit steps. Singapore's regulators have issued model frameworks: the **Model AI Governance Framework** (PDPC/IMDA 2019, updated 2020) offers sector-neutral ethical AI guidelines, and a companion **ISAGO guide** (with WEF) gives organizations a self-assessment checklist. Singapore's IMDA also piloted **AI Verify** (2022–23), a principle-based testing framework and toolkit (covering 11 governance principles) to *validate* AI systems against ethics requirements. These tools are published and mature (frameworks adopted, self-assessment guides online, AI Verify open-sourced in 2023).

Sector-Specific Guidelines

- **Financial Services:** The Monetary Authority of Singapore (MAS) published the **FEAT Principles** (2018) – Fairness, Ethics, Accountability and Transparency – for AI and data analytics in finance. These non-binding principles advise banks to maintain governance frameworks, justify AI models, monitor bias and explain decisions internally and to customers. (MAS later developed a detailed "Veritas" toolkit for measuring FEAT compliance.) Other financial regulators (e.g. OCC, Fed) have signaled that existing risk-management frameworks apply to AI, but MAS FEAT remains the first formal regulator-issued AI guidance for banks.
- **Healthcare:** The World Health Organization issued **"Ethics and Governance of AI for Health"** guidance (June 2021) and updated it in Jan 2024 for generative models. Key recommendations include mandatory **third-party audits and impact assessments** of large-scale AI in healthcare (e.g. large language models), with findings published (including disaggregated outcomes). (These WHO guidelines are advisory, emphasizing patient safety, transparency and human rights in AI.) In addition, medical device regulators (e.g. FDA) are working on AI/ML software guidance, which is at least conceptually aligned with broader trustworthy-AI norms.
- **Government Use:** Several governments require risk assessment and transparency for AI. Canada's **Directive on Automated Decision-Making** (2019) mandates Algorithmic Impact Assessments (AIAs) for federal AI systems and public disclosure of these assessments. This creates an audit trail and registry of government AI use (on an open portal). The UK's Cabinet Office and other governments similarly require Data Protection Impact Assessments for high-risk AI, alongside emerging frameworks for "algorithmic audits" of public-sector AI (e.g. New York City's AI audit law).

Standards Organizations and Professional Bodies

- **ISACA (IT Audit):** In 2024 ISACA released an **AI Audit Toolkit** for auditors. It provides a framework and control catalog that *maps to* existing standards (e.g. COBIT, NIST 800-53, ISO 27001) and incorporates guidelines from the EU AI Act, Singapore's Model AI Framework, MITRE ATLAS and OWASP ML Top Ten. The toolkit (and an upcoming Advanced AI Auditing certification) is specifically aimed at helping IT and internal auditors evaluate AI governance and ethical controls.
- **IIA (Internal Auditors):** The Institute of Internal Auditors updated its **AI Auditing Framework** in late 2023. This multi-part framework guides internal auditors through AI risk domains, best practices, and control points (spanning data, models, operations and outcomes). It is a published framework (available to members) meant to complement general audit methodology when AI is in scope.

- **IEEE (Standards Assoc.):** The IEEE has led numerous AI ethics standards projects. Its **P7000-series** covers topics like transparency (P7001), algorithmic bias (P7003), data privacy (P7002), etc. Separately, the **Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)** is an initiative to develop certification criteria for ethical AI systems. These efforts are in various stages (some P7000 standards are published, others in draft; ECPAIS is under development), reflecting a long-term push by IEEE to embed ethics into AI assurance.
- **ENISA (EU Cybersecurity):** The EU Agency for Cybersecurity issued AI-related risk guidance, including the "**Multilayer Framework for Good Cybersecurity Practices for AI**" (June 2023). This report offers a scalable cybersecurity risk-management framework for AI systems (three layers: IT/cyber foundations, AI-specific, sector-specific). It is published and intended for national authorities and industry, focusing on *security* aspects of AI. ENISA has also released threat landscape reports and recommendations for securing AI.
- **WEF and Multi-Stakeholder Initiatives:** The World Economic Forum's **AI Governance Alliance** brings together industry, governments and civil society to produce governance toolkits (e.g. the Global Framework for AI risk management, Board governance guidelines). WEF literature (e.g. a Sept 2020 white paper) highlights the need for *integrated AI audit solutions* to track AI models and ensure compliance. (An example WEF analysis calls for enterprise audit software that 1) documents AI usage, 2) checks compliance, and 3) facilitates cross-team collaboration.) The WEF also publishes country risk-readiness indexes and promotes international cooperation on AI governance. These are alliance-driven initiatives (published reports and tools).
- **OECD.AI:** Besides the AI Principles, the OECD's AI Policy Observatory publishes tools and catalogs of frameworks. For instance, it lists a **"Control Audits AI Governance, Risk & Assurance Platform"** (developed in New Zealand) – an enterprise-grade GRC system that integrates ISO 42001 and NIST RMF, with features for policy management, risk assessment, audit trails and compliance dashboards. OECD also hosts case studies on national AI strategies and publishes best-practice recommendations (e.g. OECD's work on AI risk management).

Industry and Private Initiatives

Major consultancies and tech firms have created their own AI audit and governance tools:

- **Deloitte** has a **"Trustworthy AI™ Framework"** (and related publications) aligning AI development with the US *AI Bill of Rights* (2022). It provides a lifecycle roadmap of governance controls to ensure equity, transparency and accountability.
- **PwC** offers a **Responsible AI Toolkit** (2023), a suite of customizable frameworks and checklists covering five dimensions (governance, explainability, bias/fairness,

robustness/security, ethics/regulation). It is aimed at embedding ethical checks and documentation throughout AI projects.

- **EY** publishes guidance on **responsible AI strategy**, framing end-to-end pillars for AI oversight. Its literature notes that EY professionals have built AI governance frameworks and controls to guard against bias and compliance failures.
- **KPMG** rolled out a **"Trusted AI" governance framework** (October 2024) providing an integrated approach to ethical AI design, development and use. (KPMG also released a detailed "Governing Trusted AI" report for business leaders.)
- **Tools and Checklists:** Other market solutions include Singapore's **AI Verify** (principle-based test suite, 2022-23), MITRE's **ATLAS** adversarial resilience framework, and OWASP's ML Top Ten. Many vendors and industry groups offer risk-assessment checklists or auditing "XAI" tools for explainability. In practice, auditors often rely on checklists derived from these sources (e.g. adapting ALTAI, ISO 42001 control objectives, NIST CSF/AI RMF steps).

Components & Tools for AI Audit

Across these standards and programs, common elements include: audit **charters** (defining scope of AI audit), **control checklists**, risk-assessment templates, and continuous monitoring guidance. For example, ISACA's toolkit maps specific controls (e.g. model validation, data quality, transparency) to NIST/ISO controls and regulatory requirements. Singapore's **ISAGO guide** and the EU ALTAI serve as checklist-based audit aids. OECD's Control Audits platform provides workflow and reporting tools. And guidance documents (e.g. EU AI Act, ISO 42001) explicitly call for management reviews and periodic audits of AI systems.

In summary, a growing ecosystem of standards and initiatives now addresses AI audit and assurance. Many are published or piloted (ISO 42001, NIST RMF, EU AI Act, OECD Principles, MAS FEAT, WHO guidance, ICO draft, ENISA reports, ISACA/IIA frameworks, etc.), while others remain in development. Together they cover governance structures, documentation requirements, control objectives, and specific audit tools – forming a foundation for enterprise AI audit programs.

Sources: Authoritative publications by ISO, NIST, EU and national regulators, ISACA/IIA/IEEE, OECD, WEF, ENISA, major consultancies, and other expert bodies. Each citation links to the original source page or document.