

EDUCATION THAT MATTER

ETM AI Transformation Infrastructure Standards

Public Draft for Industry Review and Comment

Proposed v0.9-8 | October 13, 2026 | Editorial review copy

First public comment period closes December 15, 2026

Requirements for aligned and accountable AI-enabled operations

Issued by Education That Matter™

For public review. This draft establishes a requirements baseline and does not disclose ETM implementation methods, assessment instruments, scoring logic, or technical control designs.

Document status and use

This document is a public draft issued by Education That Matter™ for industry, practitioner, workforce, education, governance, and enterprise review. It proposes a common infrastructure baseline for preparing, aligning, validating, governing, and continuously improving AI-enabled operations.

The public standard defines required organizational conditions, control objectives, intended outcomes, and evidence expectations. It does not prescribe ETM assessment methods, document matrices, classification instruments, scoring, process-tracing techniques, implementation sequences, training systems, or proprietary control architecture. Organizations may satisfy the requirements through approaches appropriate to their operating context.

Item	Designation
Document title	ETM AI Transformation Infrastructure Standards™
Status	Public Draft for Industry Review and Comment
Version	Proposed 0.9-6 — editorial review copy
Proposed revision date	October 12, 2026 (not yet published)
Canonical publication page	https://educationthatmatter.com/ai-transformation-infrastructure-standards/
Public comment deadline	December 15, 2026
Intended audience	Enterprise leaders, operational leaders, governance and risk professionals, technologists, workforce leaders, educators, and industry specialists
Primary purpose	Define a common requirements baseline for responsible enterprise AI transformation
Normative language	Shall indicates a requirement; should indicates a recommendation; may indicates an option

Public draft notice

This draft is provided for review and discussion. It is not a certification, legal opinion, regulatory determination, or guarantee of AI safety, performance, compliance, or organizational readiness. Organizations remain responsible for applicable laws, regulations, contracts, professional obligations, security requirements, and sector-specific standards.

Intellectual property boundary

© 2026 Education That Matter IP, LLC. All rights reserved. This document is published for review, evaluation, citation, and public comment. The requirements and principles may be cited with attribution to Education That Matter™. No license is granted to modify, rebrand, commercialize, incorporate this document into another standard, or create derivative works without prior written permission.

This public draft defines infrastructure requirements and intended outcomes. It does not disclose ETM's proprietary assessment instruments, maturity or conformance scoring, implementation procedures, validation scripts, governance-control architecture, enforcement mechanisms, technical configurations, or certification methodology.

Document control. The authoritative version, current publication status, comment period, and any corrections or successor versions are maintained at <https://educationthatmatter.com/ai-transformation-infrastructure-standards/>. Downloaded and printed copies are uncontrolled and should be verified against that source.

Executive statement

Enterprise AI transformation cannot be accomplished by installing a platform and applying one operating model everywhere. AI enters a living operating environment made up of people, authoritative information, processes, systems, decisions, controls, and obligations. Those conditions differ by organization, industry, jurisdiction, business function, and individual workflow.

Technology infrastructure and operational infrastructure must advance in parallel. Technical safeguards and operational controls have distinct responsibilities and must work together. This standard establishes a shared requirements baseline while allowing organization-specific implementation.

ETM's position is direct: AI may absorb tasks, but organizations retain responsibility. AI participation must operate within documented authority, validated information, defined human accountability, controlled execution, and evidence sufficient to explain what occurred.

AI transformation also occurs within a broader operating environment. Organizations remain responsible for identifying and governing material impacts that AI-enabled transformation may impose on affected stakeholders, shared resources, infrastructure, services, and external operating conditions. Technology and operational infrastructures operate in parallel within this environment, which can constrain, influence, or destabilize both.

1 Purpose

The purpose of this standard is to help organizations establish the infrastructure needed to introduce, expand, or govern AI without weakening operational stability, decision accountability, information integrity, workforce continuity, knowledge and cognitive diversity, innovation capacity, or institutional trust.

The standard is designed to support organizations at different stages of adoption, from early exploration through enterprise-scale integration. It can inform leadership planning, readiness reviews, procurement requirements, operating-model design, workforce preparation, governance programs, and independent assurance activities.

2 Governing premise

Requirements may be standardized; their application must reflect the organization. Approved documentation, assigned responsibilities, decision authority, and actual execution must remain consistent as AI participation changes.

Standardized baseline	Organization-specific alignment
Required outcomes and control expectations	Industry, regulatory, and jurisdictional obligations
Decision and accountability principles	Business-unit authority and escalation paths
Information integrity requirements	Authoritative sources, repositories, and ownership
Validation and evidence expectations	Workflow-level risk, review, and evidence design
Workforce continuity expectations	Roles, capacity, competencies, and change impacts
Continuous improvement requirements	Metrics, monitoring cadence, and improvement priorities

3 Scope

This standard applies to organizational environments in which AI creates, transforms, recommends, analyzes, classifies, prioritizes, predicts, decides, initiates, or executes work that can affect operations, people, customers, partners, assets, records, rights, safety, compliance, or reputation.

3.1 Included

- Enterprise and departmental AI initiatives, including pilots that may influence real work or decisions.
- Generative AI, predictive AI, embedded AI capabilities, autonomous or semi-autonomous agents, and AI-enabled workflow tools.
- Internal, vendor-provided, open, hosted, and locally operated models and services.
- Human, process, information, technology, governance, evidence, and continuity conditions surrounding AI use.

3.2 Not included

- A universal operating model, technology architecture, product selection, or vendor endorsement.
- A substitute for legal, regulatory, cybersecurity, privacy, safety, records-management, accessibility, labor, or professional requirements.
- ETM’s proprietary assessment, scoring, implementation, validation, enforcement, or certification methodology.

4 Foundational principles

Principle	Expectation
Human accountability	A named human authority remains accountable for material organizational decisions and approved execution.
Authoritative information	AI-enabled work is grounded in information whose source, ownership, currency, status, and permitted use can be established.
Contextual alignment	Requirements are applied to the actual industry, organization, business function, workflow, and risk context.

Principle	Expectation
Separation of responsibilities	Creation, recommendation, evaluation, approval, and execution are separated when risk warrants independent judgment.
Intervention before consequence	Human review occurs early enough to prevent or alter a material action, not merely observe it afterward.
Evidence by design	The organization retains sufficient evidence to reconstruct participation, review, approval, execution, exception, and outcome.
Continuity through change	Roles, knowledge, review capacity, escalation coverage, and operational ownership remain viable as tasks change.
Proportionality	Controls reflect impact, uncertainty, reversibility, affected parties, and the organization's obligations.
Continuous validation	Readiness and control effectiveness are re-evaluated as models, tools, data, workflows, threats, and obligations change.
Provider independence	Governance requirements remain applicable even when a model, vendor, platform, or deployment arrangement changes.
Non-self-authorization	An AI system cannot create, expand, delegate, inherit, validate, or approve its own authority or the authority of another AI system.
Knowledge and cognitive diversity	Human expertise, independent reasoning, relevant perspectives, and innovation capacity remain viable as AI participation expands.
Stakeholder impact accountability	AI-enabled transformation shall account for material operational effects on identifiable internal and external stakeholders whose resources, services, rights, responsibilities, costs, access, safety, or operating conditions may be

Principle	Expectation
	affected.

5 Infrastructure requirements

The following domains define the minimum public requirements baseline. Organizations may add stricter requirements based on sector, jurisdiction, risk, contractual duty, professional practice, or internal policy.

5.1 Leadership accountability and decision authority

LA 1 The organization shall designate accountable executive ownership for AI-enabled operational transformation.

LA 2 The organization shall define who may propose, evaluate, approve, suspend, modify, and retire AI-enabled uses.

LA 3 Decision rights, delegations, thresholds, exceptions, and escalation paths shall be documented at a level appropriate to operational risk.

LA 4 Accountability shall remain assigned when work crosses departments, systems, vendors, or legal entities.

LA 5 Documented decision and delegation authority shall be consistent with assigned operational responsibility and permitted system execution. Material discrepancies shall be resolved or affected execution restricted pending authorized resolution.

Outcome: leaders can identify who owns the decision, who may act, who must review, and who is accountable when conditions change.

5.2 AI literacy and readiness

AR 1 Personnel whose work is affected by AI shall receive role-relevant education on capabilities, limitations, uncertainty, appropriate use, and escalation.

AR 2 Leaders shall understand that fluent output is not evidence of accuracy, authority, completeness, or permission.

AR 3 Readiness decisions shall consider operational capacity, information condition, workforce impact, governance capacity, and the ability to validate and intervene.

AR 4 The organization shall not treat technology availability as proof of operational readiness.

Outcome: people understand the system well enough to use it appropriately, challenge it when necessary, and recognize when work must stop or escalate.

5.3 Information and document integrity

- ID 1 The organization shall identify the authoritative information sources permitted for each material AI-enabled use.
- ID 2 Ownership, approval status, version, effective date, retention status, access rights, and relevant restrictions shall be determinable for governed information.
- ID 3 Documents and records used in AI-enabled work shall be sufficiently structured, current, traceable, accessible, and controlled for their intended use.
- ID 4 Conflicting, superseded, incomplete, unverified, or prohibited information shall be managed before it can drive material execution.
- ID 5 The organization shall define how AI-generated or AI-modified content is identified, reviewed, approved, retained, and superseded.
- ID 6 The organization shall maintain a governed document and information-management environment capable of identifying authoritative, approved, current, superseded, restricted, and retained content.
- ID 7 Documents made available to AI shall include sufficient metadata, ownership, version, approval, effective-date, access, retention, provenance, and lifecycle information to determine whether the content is authorized for the intended use.
- ID 8 AI retrieval, search, generation, and workflow participation shall be designed to prevent superseded, unapproved, conflicting, restricted, or contextually inappropriate content from being treated as authoritative.
- ID 9 Document conversion, restructuring, summarization, extraction, or AI-assisted modification shall preserve source provenance, meaning, approval status, traceability, and applicable controls.
- ID 10 A material change to an authoritative document, its metadata, permissions, lifecycle status, or availability to AI shall trigger review of affected AI-enabled workflows and uses.

Outcome: the organization maintains an AI-ready document and information-management environment that enables people and systems to distinguish authoritative information from content that is outdated, unapproved, altered, restricted, incomplete, conflicting, or merely credible in appearance.

5.4 Process and workflow alignment

- PW 1 The current operating process shall be understood before AI participation is introduced into material work.
- PW 2 The organization shall identify where AI participates, what input it receives, what output it produces, and what downstream action may follow.
- PW 3 Workflow requirements shall account for normal work, exceptions, failure states, handoffs, dependencies, and recovery.
- PW 4 Local workflow alignment shall preserve applicable enterprise requirements while reflecting the function's actual work and obligations.

PW 5 A process shall not be treated as transformed solely because an AI capability has been added.

PW 6 The organization shall maintain a controlled process for determining whether AI participation materially affects operational processes, documentation, responsibilities, decision authority, information handling, human review, evidence, or continuity.

PW 7 Every controlled document or artifact governing, supporting, authorizing, or providing evidence for an AI-affected process shall receive a documented alignment determination. Revision shall be required where an identified impact makes existing documentation inadequate; AI participation alone shall not require blanket revision.

PW 8 Affected documentation shall be updated or supplemented where necessary, approved by authorized owners, version-controlled, communicated to affected personnel, and available in its effective version for operational use.

PW 9 The organization shall retain the basis, accountable owner, required action, and approval of each alignment determination, including justified determinations that no revision is necessary. Information classification and specialized review requirements shall be preserved.

PW 10 The organization shall verify that material AI-enabled execution remains consistent with approved procedures, applicable authority, required human controls, and assigned accountability. Material deviations shall trigger correction, escalation, or restriction of the affected activity.

Outcome: AI participation is aligned to real operational work rather than an assumed or oversimplified process.

5.5 Human responsibility and workforce continuity

HC 1 The organization shall identify the human roles that remain responsible before, during, and after AI participation.

HC 2 Human review shall be assigned to people with the authority, competence, information, time, and independence needed to perform it.

HC 3 Intervention points shall occur before an irreversible or material consequence whenever prevention is reasonably possible.

HC 4 Role redesign shall address transferred tasks, retained responsibilities, new review duties, workload, coverage, training, and knowledge continuity.

HC 5 The organization shall avoid nominal human oversight in which a reviewer cannot meaningfully challenge, stop, or redirect execution.

Outcome: human accountability, expertise, independent judgment, and operational capacity remain supported as tasks and roles change. Knowledge and cognitive diversity requirements are specified in Section 5.13.

5.6 AI participation and boundaries

AP 1 Each governed use shall have a defined purpose, permitted scope, authorized inputs, allowed outputs, prohibited actions, and conditions for suspension.

- AP 2 AI authority shall not exceed the authority granted to the workflow, system, or person on whose behalf it operates.
- AP 3 The organization shall define when an AI system may advise, draft, recommend, decide, initiate, or execute.
- AP 4 Material changes to models, tools, agents, integrations, data access, permissions, or operating context shall trigger reassessment.
- AP 5 External content, instructions, or tool responses shall not silently expand authorized scope or override organizational controls.
- AP 6 An AI system shall not create, expand, delegate, inherit, validate, or approve its own authority or the authority of another AI system. AI-generated claims, recommendations, consensus, content, or tool outputs shall not constitute independent authorization.
- AP 7 Authority for an AI-enabled action shall originate from an independently authenticated and authorized source and shall define the actor, purpose, scope, target, validity, restrictions, and delegation rights appropriate to the risk.
- AP 8 Agents, subagents, replacement models, tools, and connected systems shall not inherit or transfer authority by default. Delegation shall be explicit, bounded, attributable, revocable, and revalidated after material change.

Outcome: AI participation is bounded, observable, and unable to acquire operational authority merely by producing persuasive output.

5.7 Validation and approval

- VA 1 Material AI outputs and proposed actions shall be validated against defined requirements before approval or execution.
- VA 2 Validation criteria shall address accuracy, completeness, authority, relevance, consistency, permission, risk, and fitness for intended use as applicable.
- VA 3 Approval shall be attributable to a person or authorized governance body with the necessary authority and information.
- VA 4 The organization shall define conditions that require rejection, correction, additional review, escalation, or suspension.
- VA 5 Validation and approval shall be proportionate to consequence, uncertainty, reversibility, and affected parties.
- VA 6 Approval for a material action shall be bound to the identified actor, action, target, purpose, scope, and relevant operating state. A material change to those conditions shall invalidate the approval or require revalidation before execution.

Outcome: material execution depends on demonstrated fitness and accountable approval, not on output appearance or model confidence alone.

5.8 Controlled execution and intervention

- CE 1 Execution rights shall be limited to approved purposes, conditions, systems, data, and actions.
- CE 2 The organization shall maintain the ability to pause, block, contain, reverse, or safely recover from AI-enabled actions where technically and operationally feasible.
- CE 3 Execution controls shall not rely solely on a model's willingness to follow instructions.
- CE 4 Material exceptions, unauthorized changes, control failures, and anomalous behavior shall trigger defined response and escalation.
- CE 5 The organization shall verify that approved controls remain effective in the operating environment.
- CE 6 Missing, ambiguous, stale, self-conferred, or unverifiable authority shall produce a fail-secure result that prevents execution until valid authority is established.
- CE 7 Controls governing material AI-enabled actions shall remain independent of unilateral modification, disabling, or circumvention by the AI systems they govern.
- CE 8 AI may propose changes to governance controls but shall not independently approve, deploy, modify, disable, or remove the controls governing its authority, validation, monitoring, execution, evidence, suspension, or termination.

Outcome: governance can affect what happens during execution and is not limited to policy statements or retrospective review.

5.9 Evidence records and traceability

- ER 1 The organization shall retain evidence appropriate to the use, risk, obligation, and retention context.
- ER 2 Evidence should identify relevant inputs, sources, system or model participation, versions, reviewers, decisions, approvals, execution, exceptions, and outcomes.
- ER 3 Records shall be protected against unauthorized alteration and remain accessible to authorized reviewers for the required period.
- ER 4 The organization shall be able to reconstruct a material AI-enabled event sufficiently to support accountability, investigation, reporting, correction, and learning.
- ER 5 Evidence requirements shall be designed before deployment rather than assembled only after an incident.
- ER 6 Evidence for a material AI-enabled action should demonstrate the source and validity of authorization, its applicable limits, and whether execution remained within those limits.
- ER 7 Evidence of alignment shall identify applicable governing documentation and effective versions, relevant review and authorization, observed deviations, and the disposition of corrective actions. Collection and retention shall respect information classification and applicable obligations.

Outcome: the organization can demonstrate how a material result was produced, reviewed, authorized, and executed.

5.10 Risk security privacy and compliance alignment

RC 1 AI-enabled uses shall be aligned with applicable risk, cybersecurity, privacy, legal, regulatory, safety, records, accessibility, labor, procurement, and ethical obligations.

RC 2 Existing controls shall be evaluated for whether they remain effective when AI changes the speed, scale, variability, or autonomy of work.

RC 3 Third-party and supply-chain dependencies shall be evaluated across data use, permissions, service changes, model changes, incident response, continuity, and exit.

RC 4 Material unresolved conflicts between business objectives and governing obligations shall be escalated to authorized decision makers.

RC 5 Compliance evidence shall reflect actual operation, not only policy existence or training completion.

RC 6 Third-party AI participation shall be incorporated into the organization's operational responsibilities, authorization limits, review requirements, change controls, evidence expectations, and continuity arrangements.

Outcome: AI transformation is integrated with the organization's wider obligations and assurance functions.

5.11 Operational health and performance

OH 1 The organization shall establish measures that show whether AI-enabled work is improving or degrading operational health.

OH 2 Measures should address quality, errors, exceptions, rework, cycle time, human workload, intervention, customer or stakeholder impact, continuity, and control effectiveness as applicable. Measures should also address knowledge and perspective diversity, independent human reasoning, shared AI dependencies, and retained innovation capacity where relevant.

OH 3 Efficiency gains shall not be evaluated separately from risk transfer, hidden labor, review capacity, information quality, or downstream correction.

OH 4 Leaders shall receive reporting sufficient to identify systemic weakness, accumulated exceptions, and material changes in operating conditions. Reporting shall identify material deterioration in the knowledge and cognitive diversity conditions defined in Section 5.13 and track corrective action.

Outcome: transformation success is measured by sustainable organizational performance, not adoption volume alone.

5.12 Continuous monitoring and change governance

CM 1 The organization shall monitor material changes in models, tools, agents, integrations, information sources, permissions, threats, workflows, laws, and business conditions.

CM 2 Defined changes shall trigger revalidation, renewed approval, control adjustment, retraining, or suspension.

CM 3 Incidents, near misses, exceptions, user feedback, and performance evidence shall inform corrective action and future design.

CM 4 Retirement or replacement of AI-enabled capability shall include continuity, access removal, record retention, dependency resolution, and communication.

CM 5 The organization shall periodically determine whether the use remains necessary, appropriate, and supportable.

CM 6 Monitoring shall identify related attempts to circumvent authorization or operational controls, including attempts distributed across agents, tools, or workflows.

CM 7 Introduction, modification, expansion, replacement, or removal of AI capability shall undergo an operational-impact determination before controlled implementation. Material changes in permissions, autonomy, integrations, workflow participation, or vendor capability shall be included.

CM 8 Material change shall prompt review of affected processes, controlled documentation, decision authority, operational controls, workforce roles, review capacity, evidence, and continuity. Required updates, validation, and approval shall be completed before affected material execution is authorized.

CM 9 Controlled release shall establish effective versions and communicate relevant changes to affected personnel. Emergency changes shall have defined authorization, temporary limits, timely retrospective review, and recorded resolution of outstanding impacts.

CM 10 Alignment shall be reassessed at a defined, risk-appropriate interval and when incidents, exceptions, control-test results, or other evidence indicate that documentation and actual operation may have diverged.

Outcome: governance remains current as technology and operational conditions evolve.

5.13 Knowledge and cognitive diversity

This domain extends Human Continuity to the preservation of independent human judgment, institutional expertise, varied knowledge, and innovation capacity. Diversity concerns relevant experience, disciplines, contexts, sources, and reasoning. Controls shall be proportionate to the decision or workflow and shall preserve information quality, authorized access, privacy, and applicable obligations.

KD 1 The organization shall identify knowledge and expertise critical to AI-affected operations and maintain arrangements to preserve, transfer, and apply institutional memory, tacit knowledge, and practitioner experience before material role, workflow, or system changes place that knowledge at risk.

KD 2 For material AI-assisted decisions, the organization shall define where independent human analysis is required before exposure to AI recommendations and retain evidence of that analysis or an authorized, documented exception. Human review shall be able to challenge AI framing and consider credible alternatives.

KD 3 The organization shall define source-diversity expectations appropriate to each material use. Validation shall consider relevant primary evidence and independent practitioner or

contextual knowledge where available. Multiple AI outputs derived from common sources shall not be represented as independent corroboration.

KD 4 Material decisions shall include relevant functional, disciplinary, experiential, and contextual perspectives appropriate to the affected parties and operating context. Review shall record credible alternatives, substantive dissent, and their disposition without requiring disagreement or treating every perspective as equally supported.

KD 5 The organization shall periodically review whether shared AI participation is narrowing sources, reasoning, alternatives, or recommendations in material workflows. Apparent consensus shall be evaluated for common AI and source dependencies. Similarity alone shall not establish loss of independent judgment; unresolved material concerns shall receive accountable review and corrective action.

KD 6 The organization shall maintain proportionate opportunities for human-led ideation, experimentation, and knowledge development in which AI does not establish the initial problem framing or solution space. It shall assign accountable ownership, resources, review intervals, and measures sufficient to determine whether human innovation capacity is being sustained.

Evidence expectations: records should identify critical knowledge and its owners, preservation and transfer activity, independent human contributions and their timing relative to AI use, source provenance, relevant perspectives, alternatives and dissent, shared AI dependencies, convergence reviews, human-led experimentation, and corrective-action outcomes. Collection shall be limited to what is necessary for the governed use and shall respect access, classification, privacy, and retention controls.

Outcome: AI-enabled efficiency is supported without avoidable erosion of human knowledge, independent judgment, relevant perspectives, or innovation capacity.

Organizations may develop a Human Knowledge Diversity Index (HKDI) as a local indicator. This draft establishes no validated composite index, universal scoring method, benchmark, or conformance threshold. Any such indicator should disclose its scope, baseline, dimensions, limitations, and review basis; it shall not replace substantive evidence or independent judgment.

5.14 External operational impact and stakeholder transparency

EOI 1 The organization shall identify material external operational impacts arising from AI-enabled transformation, including effects on affected stakeholders, shared resources, infrastructure, services, costs, rights, access, safety, or continuity.

EOI 2 The organization shall identify stakeholders materially affected by the transformation and establish responsibility for determining when engagement, disclosure, consultation, notification, or other communication is appropriate or required.

EOI 3 Information necessary for affected stakeholders to understand material operational impacts shall not be unnecessarily restricted when disclosure is required by law, public obligation, contractual responsibility, governance commitment, or the organization's established transparency requirements.

EOI 4 Confidentiality controls shall distinguish legitimate protection of proprietary, security-sensitive, personal, contractual, or otherwise protected information from restrictions that would materially impair required accountability, oversight, stakeholder participation, or public transparency.

EOI 5 Material external impacts, stakeholder concerns, organizational responses, mitigation actions, commitments, and unresolved conditions shall be documented at a level proportionate to operational significance.

EOI 6 Material changes in external impact, stakeholder conditions, resource requirements, public obligations, or operating assumptions shall trigger reassessment and escalation where established thresholds are exceeded.

Outcome: organizations can demonstrate that material external consequences of AI-enabled transformation are identified, governed, communicated where appropriate, and incorporated into operational decision-making.

5.15 Intellectual property stewardship and AI content rights

Organizations shall establish controls for determining the ownership, provenance, authorized use, and applicable licensing conditions of content incorporated into AI-enabled operations. This requirement family does not presume that all AI access, training, retrieval, or outputs require royalties; legal exceptions and jurisdiction-specific rights remain applicable.

IP 1 — Rights inventory. The organization shall identify material third-party and internally owned works used in AI-enabled workflows, including source, rights holder where known, license or permission status, restrictions, and accountable steward.

IP 2 — Purpose-specific rights assessment. Before material AI use, the organization shall determine whether intended activities—including indexing, retrieval, model training or fine-tuning, redistribution, and commercial output—are authorized by applicable law, license, or other permission.

IP 3 — Authority boundary. Technical accessibility shall not be treated as evidence of permission. Agents and automated tools shall not grant themselves new rights or override usage restrictions.

IP 4 — Contractual controls. Procurement and vendor governance shall address content inputs, retention, model training, subcontractor use, onward disclosure, ownership, output rights, and audit or reporting provisions appropriate to the engagement.

IP 5 — Attribution and integrity. Where legally or contractually required, workflows shall preserve attribution, provenance, notices, and integrity controls; otherwise the organization should apply proportionate traceability practices.

IP 6 — Licensing and remuneration. The organization shall record and fulfill applicable licensing fees, royalties, or other compensation commitments; no automatic royalty is presumed absent a relevant legal or contractual basis.

IP 7 — Human authorship and claims. Published work, registration applications, and commercial representations shall accurately distinguish human contributions from AI-generated material when legally relevant.

IP 8 — Exceptions and disputes. Suspected unauthorized use, rights conflicts, takedown requests, and licensing disputes shall be routed to named human authority with proportionate suspension, remediation, and escalation procedures.

IP 9 — Evidence and monitoring. The organization shall retain risk-proportionate evidence of source identification, rights determinations, approvals, contract terms, exceptions, and material changes to use conditions.

IP 10 — Workforce competency. Relevant personnel shall receive role-appropriate instruction on ownership, copyright limitations, licenses, confidential information, AI content handling, and escalation.

Interpretation note. Copyright generally protects original expression rather than abstract ideas, procedures, or methods. Fair use, other exceptions, and AI-training disputes require context-specific legal analysis. These requirements are operational controls, not a legal determination or ETM certification.

5.16 Evidence-Based Trust and Production Validation

Trust shall be established through verifiable evidence, validated methodologies, demonstrated performance, and accountable human governance—not assumptions, unsupported claims, or opinions presented as facts.

Scientific findings remain subject to challenge and revision as evidence develops. Technical validation, operational suitability, and production authorization are distinct responsibilities.

EBT 1 — Organizations shall establish evidence-based criteria for trusting AI-enabled systems within their intended operational context.

EBT 2 — Material claims about AI capability, accuracy, safety, and reliability shall be supported by identifiable, relevant, and verifiable evidence.

EBT 3 — Organizations shall distinguish established scientific findings, validated technical results, assumptions, predictions, and opinions.

EBT 4 — AI-enabled systems shall undergo appropriate testing against documented operational requirements before authorization for production use.

EBT 5 — Validation shall account for intended use, foreseeable limitations, data quality, operating conditions, and material failure scenarios.

EBT 6 — Organizations shall distinguish technology-provider validation from their own responsibility to establish operational suitability.

EBT 7 — Production authorization shall be granted through defined organizational authority and shall not be independently established by the AI system being evaluated.

EBT 8 — Material changes in models, capabilities, integrations, workflows, or operating conditions shall trigger proportionate reassessment of continued operational trust.

EBT 9 — Organizations shall retain appropriate evidence of testing, validation findings, identified limitations, approval decisions, and material exceptions.

EBT 10 — Organizations shall maintain the capability to monitor, challenge, suspend, or withdraw production authorization when evidence no longer supports acceptable operation.

Evidence expectations: documented validation criteria, source and method provenance, testing outcomes, known limitations, responsible approver, authorization scope, material changes, monitoring results, and suspension or reassessment records.

6 Applying the standard in context

Conformance to a common baseline does not require uniform implementation. Organizations should interpret and apply each requirement according to the nature of the work and its potential consequences while preserving the intent of the requirement.

Context factor	Questions for alignment
Industry and regulation	What sector duties, licensing rules, standards, and supervisory expectations apply?
Business function	What responsibilities, expertise, records, systems, and decision rights define the function?
Workflow	Where does AI enter, what changes, who is affected, and what may happen next?
Impact and reversibility	Could the result affect rights, safety, livelihood, finances, access, reputation, or essential operations? Can it be corrected?
Information condition	Are sources authoritative, current, permitted, complete, traceable, and fit for the intended use?
Human capacity	Do reviewers have sufficient authority, expertise, time, independence, and coverage?

Context factor	Questions for alignment
Technology arrangement	What models, agents, integrations, tools, permissions, vendors, and dependencies participate?
Operational maturity	Can the organization document, validate, govern, evidence, monitor, and improve the use reliably?
External operating environment	Who outside the organization is materially affected? What shared resources, infrastructure, services, costs, obligations, disclosure needs, or changing conditions require accountable review?

A requirement may be met through different processes and technologies. The organization should be able to demonstrate that its chosen approach satisfies the requirement in practice and remains effective under foreseeable operating conditions.

7 Organizational adoption expectations

Organizations adopting this standard should demonstrate a defined scope, accountable ownership, justified applicability decisions, remediation of material gaps, and evidence of continuing control effectiveness.

Adoption may be supported by internal programs or qualified providers. Use of ETM products, architecture, proprietary methods, or certification programs is not required to apply this public requirements baseline.

8 Roles in standards adoption

Role titles may vary. The organization should ensure that the following responsibilities are covered without creating conflicts that weaken independent judgment.

Responsibility	Public expectation
Executive accountability	Own transformation outcomes, risk acceptance, resources, and enterprise alignment.

Responsibility	Public expectation
Operational ownership	Define actual work, decisions, exceptions, dependencies, and performance expectations.
Information stewardship	Establish authoritative sources, access, quality, lifecycle, and record status.
Technology and security	Manage architecture, integration, permissions, resilience, monitoring, and technical safeguards.
Legal risk and compliance	Interpret obligations, advise on material exposure, and support accountable decisions.
Workforce leadership	Address role design, capacity, competency, employee impact, training, and continuity. Coordinate knowledge preservation, transfer, and sustained human innovation capacity.
Independent review	Challenge assumptions, validate material conditions, and escalate unresolved concerns. Examine source independence, shared AI dependencies, alternatives, and material convergence concerns.
Users and reviewers	Operate within authorized boundaries, validate work, report exceptions, and intervene when required.
Stakeholder impact coordination	Coordinate material external impact assessment, appropriate engagement and disclosure, confidentiality review, documented commitments, and escalation through accountable operational owners.

9 Conformance and assurance direction

This public draft does not establish certification or authorize organizations to claim ETM conformance. A future conformance framework may define scope, evidence expectations, assessment criteria, reviewer qualifications, finding levels, remediation requirements, renewal, and use of marks.

Until a conformance framework is formally released, organizations may state that they are reviewing or aligning their practices to ETM AI Transformation Infrastructure Standards Public Draft v0.9-5. They should not imply ETM assessment, certification, approval, or endorsement of their organization, product, or AI use.

9.1 Evidence expectations

Evidence should be current, attributable, relevant to the stated scope, and sufficient to demonstrate operation. Policy documents alone may be insufficient where a requirement concerns actual workflow, review, execution, intervention, records, monitoring, or outcomes.

Evidence of operational alignment should demonstrate consistency among approved documentation, accountable authority, and actual execution. An alignment determination is distinct from an information-security classification; restricted information shall remain subject to its applicable access and handling controls.

10 Public review questions

ETM invites substantive comment from enterprise leaders, operational experts, workforce professionals, educators, technologists, governance practitioners, legal and risk professionals, researchers, public-interest participants, and industry specialists.

Comments for the first public review period should be submitted by December 15, 2026, through the public comment form at <https://educationthatmatter.com/ai-transformation-infrastructure-standards/#public-comment>. Submissions may be attributed by name and organization or submitted without public attribution. ETM may consolidate similar comments and will publish material dispositions with a future candidate standard.

- Do the requirements establish a credible cross-industry baseline without imposing a single operating model?
- Which requirements need clearer language, boundaries, definitions, or evidence expectations?
- What sector-specific overlays may be necessary?
- Are workforce continuity and human accountability sufficiently represented?
- Do the requirements adequately address agentic systems, tool use, changing permissions, and controlled execution?
- What unintended burden, ambiguity, or implementation conflict should be addressed before a candidate standard is issued?
- What independent review and conformance safeguards would support trust in a future assessment framework?

- Does the draft establish a sufficiently clear and enforceable non-self-authorization boundary for agents, subagents, tools, replacement models, and AI-enabled workflows?
- Do the operational documentation and change-control requirements establish clear outcomes without prescribing a proprietary assessment or implementation method?
- Do the knowledge and cognitive diversity requirements preserve independent judgment and innovation capacity while allowing proportionate, context-specific implementation?
- Do the external operational impact and stakeholder transparency requirements adequately address affected parties, disclosure obligations, legitimate confidentiality, evidence, and escalation?

11 Standards development path

Proposed revision 0.9-6 dated October 12, 2026 adds a terminology clarification in Section 12 concerning AI and references to superintelligence or Super Intelligence (SI) in external communications. It does not change any control requirement or establish a new technology classification. Revision 0.9-5 dated October 4, 2026 adds Section 5.13 Knowledge and cognitive diversity with requirements KD 1 through KD 6. It expands Human Continuity, operational-health monitoring, role responsibilities, terms, evidence expectations, and public-review questions. Existing requirement identifiers remain unchanged. Revision 0.9-4 strengthened operational documentation alignment, documentation-to-execution consistency, third-party operational responsibility, and AI change-impact requirements. Refinement dated October 4, 2026 adds Stakeholder impact accountability and Section 5.14 requirements EOI 1 through EOI 6, strengthening external operational impact, affected-stakeholder accountability, appropriate transparency, legitimate confidentiality, and external change-impact requirements. The draft version remains 0.9-5; existing requirement identifiers remain unchanged.

Stage	Purpose
Public Draft v0.9-5	Present the initial cross-industry requirements baseline for review and comment.
Public and practitioner review	Collect structured feedback from affected disciplines, sectors, and organizational roles.
Candidate Standard	Resolve material feedback, clarify requirements, and publish the proposed v1.0 baseline.
Standard v1.0	Issue the adopted requirements baseline with governance for maintenance and revision.

Stage	Purpose
Conformance framework	Define authorized evidence, assessment, reviewer, remediation, renewal, and claims requirements separately from the public standard.
Sector and function overlays	Develop compatible guidance for higher-risk or specialized operating environments without changing the core baseline.

Proposed revision 0.9-8 dated October 13, 2026 adds Section 5.16 Evidence-Based Trust and Production Validation (EBT 1–EBT 10). This editorial release candidate retains the prior v0.9-7 requirements and requires approval before public publication.

Proposed revision 0.9-7 dated October 13, 2026 adds Section 5.15 Intellectual property stewardship and AI content rights (IP 1–IP 10). This revision is an editorial release candidate based on the supplied proposed v0.9-6 master and requires approval before public publication.

12 Terms

Terminology clarification — AI and external references to superintelligence

ETM uses Artificial Intelligence (AI) as the primary technical and operational term throughout these Standards. AI is used here in its applicable organizational and technical context, including AI-enabled systems, models, agents, and capabilities.

External communications, including governmental communications, may use terms such as “superintelligence,” “Super Intelligence,” or the abbreviation “SI.” ETM recognizes such terminology when relevant to a cited source or governing instrument but does not treat it as a universal synonym for AI, a defined technical capability threshold, or a binding legal classification solely because it appears in a communication.

Where an applicable law, regulation, binding directive, procurement instrument, or contract establishes a specific definition or terminology, organizations shall interpret and apply that terminology within the instrument’s applicable scope. Such usage does not automatically amend the terminology or requirements of these Standards.

Terminology changes alone do not modify the responsibilities for human decision authority, information stewardship, workforce preparedness, validation, controlled execution, accountability, or evidence retention. Operational obligations are determined by the system’s actual capabilities, use context, risks, and applicable requirements.

Term	Meaning
Accountable human authority	A person or authorized governance body with the mandate and responsibility to approve, reject, suspend, or direct a material decision or action.
AI enabled operation	Work in which AI creates, transforms, recommends, analyzes, predicts, decides, initiates, or executes part of an organizational process.
Authoritative information	Information whose source, ownership, approval status, currency, integrity, permitted use, and applicability can be established for the intended purpose.
Conformance	Demonstrated satisfaction of stated requirements within a defined scope under an authorized assessment framework.
Execution	An action that changes a system, record, transaction, communication, access state, physical condition, service, or decision outcome.
Human continuity	The sustained availability of human authority, expertise, institutional memory, tacit knowledge, workforce capacity, independent judgment, knowledge and cognitive diversity, innovation capacity, intervention, and accountability as work changes through AI.
Material	Capable of meaningfully affecting people, rights, safety, finances, compliance, operations, assets, reputation, or institutional obligations.
Operational alignment	Consistency among approved operational documentation, assigned responsibility, decision authority, controls, and actual AI-enabled execution within the organization's context.

Term	Meaning
Operational health	The organization's capacity to perform reliably, responsibly, and sustainably while managing change, exceptions, dependencies, and accountability.
Runtime governance	Controls and accountable decisions that remain capable of influencing AI-enabled work while it is operating, including intervention before material consequence.
Validation	A documented determination that information, output, action, or control is fit for its intended use against defined requirements.
Authority provenance	Verifiable evidence that an authority grant originated from an authorized grantor and remains valid for the identified subject, purpose, scope, target, duration, restrictions, delegation, and revocation state.
Non-self-authorization	The requirement that an AI system cannot create, expand, delegate, inherit, validate, or approve its own authority or the authority of another AI system.
AI affected process	An operational process whose information, tasks, responsibilities, authority, controls, evidence, or continuity is materially influenced by AI participation or change.
Alignment determination	A documented decision on whether AI affects the adequacy of controlled operational documentation and whether revision, new documentation, or other corrective action is required.
Controlled operational documentation	Approved information governing or supporting organizational work, maintained with accountable ownership, effective versions, authorized access, and change control.
Knowledge diversity	The availability and use of relevant knowledge

Term	Meaning
	from varied sources, disciplines, experiences, generations, and operating contexts.
Cognitive diversity	Variation in relevant human reasoning, problem framing, interpretation, and approaches to solving problems.
AI convergence	Increasing similarity of sources, framing, reasoning, or recommendations associated with shared AI participation; a review signal that does not by itself demonstrate harm or a lack of independence.
Independent human reasoning	Human analysis developed without the AI recommendation under review establishing its initial framing or conclusion.
Innovation capacity	The ability to develop, test, challenge, and apply new ideas while retaining human expertise and independent inquiry.
Tacit knowledge	Practical knowledge acquired through experience that may not be fully expressed in formal documentation.
Human Knowledge Diversity Index	A proposed organizational indicator of knowledge and cognitive diversity conditions; no validated score or universal threshold is established by this draft.
External operating environment	The communities, utilities, suppliers, governments, public infrastructure, markets, and other stakeholder conditions within which technology and operational infrastructures operate.
Affected stakeholder	An identifiable person, group, organization, or public body whose resources, services, rights, responsibilities, costs, access, safety, or operating conditions may be materially affected by AI-enabled transformation.
Superintelligence / Super Intelligence (SI)	Terminology sometimes used in external discourse for advanced or hypothetical AI capabilities. Not adopted as a synonym for AI or as a distinct compliance category by these

Term	Meaning
	Standards unless an applicable governing instrument defines it.
Artificial Intelligence (AI)	Primary technical and operational term used by ETM for the AI-enabled systems and capabilities within the scope of these Standards.

Intellectual property stewardship — Organizational processes for identifying rights holders, applicable permissions, authorized purposes, restrictions, and evidence governing use of content.

AI content rights determination — A documented evaluation of whether a proposed AI-enabled use is authorized under applicable law, contract, license, or permission, including applicable exceptions.

Content provenance — Available information about the origin, custody, version, rights status, and modifications of content used in a workflow.

13 Attribution and contact

Citation: Education That Matter™. ETM AI Transformation Infrastructure Standards™ Proposed Public Draft v0.9-8. October 13, 2026. (Editorial review copy; not an official published edition.)

Official publication page: <https://educationthatmatter.com/ai-transformation-infrastructure-standards/>

Parent site: <https://educationthatmatter.com>