
ENKIDU

— MIOVSKI GROUP —

Data Governance & Ethics — Assessment & Accreditation Criteria

For Machine Learning, Neural Networks, and AI Systems

Version 2.0 · Updated from Criteria Mapping

24 January 2026

Prepared by MIOVSKI GROUP

Classification · Confidential · Draft for Internal Review

Executive Summary

This document establishes comprehensive criteria for assessing and accrediting data governance and ethics practices in artificial intelligence, machine learning, and neural network systems. This version has been updated based on the official criteria mapping spreadsheet which clearly delineates which criteria apply to training data, inference data, or both.

The framework is organized into three major sections:

- **SECTION 1: DATA LIFECYCLE CRITERIA (Stages 1-10)** - Criteria assessed for both training and inference data, with specific application noted for each criterion
- **SECTION 2: DATA OPERATION CRITERIA** - Split into separate Training Operations and Inference Operations subsections with identical criterion codes but different applications
- **SECTION 3: CROSS-CUTTING GOVERNANCE AND ETHICAL CRITERIA** - Organizational-level criteria that apply across all AI systems and data uses, not specific to individual projects

Total Assessment Criteria: 63 unique criteria across all categories

Criteria Distribution

- Training Data Only: 5 criteria (Data Operation - Training)
- Inference Data Only: 10 criteria (5 Data Operation + 5 Data Sharing)
- Both Training and Inference: 36 criteria (Acquisition through Disposition, excluding Operation)
- Cross-Cutting Organizational: 12 criteria (Governance, Documentation, Ethics, Training)

1. Introduction and Framework Foundation

1.1 Purpose and Scope

This framework provides standardized, evidence-based criteria for evaluating data governance and ethical compliance in AI/ML systems. It applies to organizations that design, develop, deploy, or operate AI systems, with particular emphasis on high-impact and high-risk applications that affect individuals' fundamental rights, safety, or well-being.

1.2 Updated Criteria Structure

This version reflects the official criteria mapping which specifies:

- Which criteria apply to Training Data
- Which criteria apply to Inference Data
- Which criteria apply to Both phases
- Data Operation criteria are explicitly duplicated with separate Training and Inference sections
- Cross-Cutting Governance criteria apply at the organizational level, not to specific data or projects

1.3 Regulatory Foundation

- EU AI Act (2024): Risk-based regulatory framework with specific requirements for high-risk AI

systems including data governance (Article 10), documentation, human oversight, and transparency

- Canada AIDA (Bill C-27): Proposed framework for high-impact AI systems emphasizing risk assessment, mitigation, transparency, and accountability
- US Executive Order 14110: Comprehensive approach to AI safety, security, privacy protection, and bias mitigation (rescinded January 2025 but framework remains influential)
- NIST AI Risk Management Framework: Voluntary framework for identifying, assessing, and managing AI risks through Govern, Map, Measure, and Manage functions
- ISO/IEC 42001 & 8183: International standards for AI management systems and data lifecycle management

1.4 Training vs. Inference Distinction

Throughout this framework, criteria are marked as applying to:

Training Data: Data used to develop, train, validate, and test AI models. This includes historical datasets, labeled data, synthetic data, and data used for model tuning and evaluation.

Inference Data: Data used during operational deployment when the AI system is making predictions, recommendations, or decisions in production environments. This includes real-time inputs and operational data.

Both: Criteria that apply to both training and inference data, though implementation details may differ.

2. Data Lifecycle Assessment Criteria

The following criteria assess data governance across the 10 lifecycle stages (excluding Operation, which is covered separately in Section 3). Each criterion indicates whether it applies to Training Data, Inference Data, or Both.

2.1 Data Acquisition

TRAINING DATA AND INFERENCE DATA

This stage covers obtaining data from various sources with appropriate legal rights, consent, and documentation.

Criterion AC-01: Legal Basis for Data Collection

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Documented legal basis for data collection (consent, contract, legitimate interest, legal obligation)
- GDPR Article 6 compliance documentation (where applicable)
- PIPEDA or CCPA compliance evidence (jurisdictional)
- Consent forms, terms of service, or other legal agreements
- Legal review and approval documentation

- Verify legal basis adequacy for intended AI use
- Assess alignment with applicable regulations
- Review consent specificity for AI training/inference
- Evaluate documentation completeness
- Check legal counsel involvement

Criterion AC-02: Data Source Documentation and Provenance

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Complete inventory of all data sources
- Source reliability assessments
- Data provenance documentation (chain of custody)
- Collection methodology documentation
- Timestamp and versioning information
- Verify source inventory completeness
- Assess source reliability evaluations
- Review provenance chain integrity
- Evaluate methodology appropriateness
- Check version control practices

Criterion AC-03: Bias Assessment in Data Collection

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Systematic bias analysis methodology
- Identification of potential selection bias
- Demographic representation analysis
- Historical bias assessment
- Bias mitigation strategies documentation
- Review bias analysis methodology rigor
- Assess bias type identification completeness
- Evaluate mitigation strategy effectiveness
- Verify baseline bias metrics establishment
- Check ongoing monitoring plans

Criterion AC-04: Privacy and Confidentiality Protections

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA)

- Data minimization justification
- Anonymization or pseudonymization procedures
- Sensitive data identification and handling
- Cross-border data transfer mechanisms (if applicable)
- Verify PIA/DPIA quality and depth
- Assess minimization justification adequacy
- Review anonymization technique robustness
- Evaluate sensitive data protections
- Check transfer mechanism compliance

Criterion AC-05: Copyright and Intellectual Property Compliance

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Copyright clearance documentation
- Data licensing agreements
- Fair use analysis (where claimed)
- Attribution requirements documentation
- Third-party IP rights assessment
- Verify copyright compliance thoroughness
- Review licensing terms appropriateness
- Assess fair use justifications (with legal context)
- Evaluate attribution implementation
- Check IP risk mitigation

2.2 Data Ingestion

TRAINING DATA AND INFERENCE DATA

This stage covers importing and processing data with quality validation, standardization, and security measures.

Criterion IN-01: Data Quality Validation

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Automated quality validation rules
- Completeness checks
- Accuracy validation procedures
- Consistency verification
- Outlier and anomaly detection
- Quality metrics and thresholds

- Assess validation rule comprehensiveness
- Review quality metrics appropriateness
- Verify anomaly detection effectiveness
- Evaluate threshold calibration
- Check validation automation coverage

Criterion IN-02: Data Format Standardization

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Standard format definitions
- Schema documentation
- Format conversion procedures
- Data type specifications
- Encoding standardization (UTF-8, etc.)
- Verify format standardization completeness
- Assess schema definition clarity
- Review conversion procedure accuracy
- Evaluate type specification rigor
- Check encoding consistency

Criterion IN-03: Security During Ingestion

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Encryption in transit (TLS 1.3 or equivalent)
- Authentication and authorization controls
- Input validation and sanitization
- Ingestion logging and monitoring
- Rate limiting and abuse prevention
- Verify encryption implementation strength
- Assess authentication mechanism robustness
- Review input validation comprehensiveness
- Evaluate logging and monitoring adequacy
- Check rate limiting effectiveness

Criterion IN-04: Data Labeling and Annotation Quality

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Annotation guidelines and taxonomy

- Inter-annotator agreement metrics (Cohen's kappa, Fleiss' kappa)
- Annotator qualifications and training
- Quality assurance procedures
- Disagreement resolution process
- Review annotation guideline clarity
- Assess inter-annotator agreement levels (typically >0.7)
- Verify annotator qualification standards
- Evaluate QA process effectiveness
- Check disagreement resolution fairness

2.3 Data Integration

TRAINING DATA AND INFERENCE DATA

Criterion IT-01: Data Lineage Tracking

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- End-to-end lineage documentation
- Transformation tracking
- Source-to-destination mapping
- Lineage visualization capabilities
- Impact analysis procedures
- Verify lineage completeness
- Assess transformation documentation quality
- Review mapping accuracy
- Evaluate visualization usability
- Check impact analysis capability

Criterion IT-02: Integration Quality Assurance

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Integration testing procedures
- Cross-source consistency validation
- Duplicate detection and resolution
- Conflict resolution rules
- Integration error handling
- Review testing procedure comprehensiveness
- Assess consistency validation thoroughness
- Verify duplicate detection effectiveness

- Evaluate conflict resolution logic
- Check error handling robustness

Criterion IT-03: Bias Amplification Assessment

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Pre- and post-integration bias analysis
- Correlation-based bias detection
- Representation shift analysis
- Amplification mitigation strategies
- Statistical testing for fairness degradation
- Evaluate bias analysis methodology
- Assess amplification risk identification
- Review mitigation strategy effectiveness
- Verify statistical testing appropriateness
- Check comparative analysis quality

Criterion IT-04: Master Data Management

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Master data definitions and standards
- Entity resolution procedures
- Golden record creation process
- Data stewardship roles and responsibilities
- Master data governance
- Verify master data standard comprehensiveness
- Assess entity resolution accuracy
- Review golden record quality
- Evaluate stewardship role clarity
- Check governance effectiveness

2.4 Data Classification

TRAINING DATA AND INFERENCE DATA

Criterion CL-01: Sensitivity Classification

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Classification scheme (Public, Internal, Confidential, Restricted)

- Sensitive data identification (PII, PHI, financial, biometric)
- Special category data under GDPR Article 9
- Classification labeling and tagging
- Access controls aligned with classification
- Review classification scheme appropriateness
- Assess sensitive data identification accuracy
- Verify special category handling
- Evaluate labeling consistency
- Check access control alignment

Criterion CL-02: Regulatory Classification

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Regulatory regime identification (GDPR, HIPAA, CCPA, etc.)
- Data subject categorization (children, vulnerable populations)
- Jurisdictional classification
- Industry-specific regulation mapping
- Classification documentation and tagging
- Verify regulatory identification completeness
- Assess subject categorization accuracy
- Review jurisdictional mapping correctness
- Evaluate industry regulation coverage
- Check documentation quality

Criterion CL-03: Training vs. Inference Data Labeling

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Clear labeling distinguishing training from inference data
- Purpose-based classification
- Retention period differentiation
- Usage restriction documentation
- Phase-specific handling procedures
- Verify labeling clarity and accuracy
- Assess purpose classification specificity
- Review retention differentiation appropriateness
- Evaluate usage restriction enforcement
- Check handling procedure differences

Criterion CL-04: Data Quality Classification

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Quality tier definitions (Gold, Silver, Bronze)
- Quality scoring methodology
- Fitness-for-purpose assessments
- Quality limitation documentation
- Usage guidelines per quality tier
- Review quality tier definition appropriateness
- Assess scoring methodology validity
- Verify fitness assessment rigor
- Evaluate limitation documentation clarity
- Check usage guideline enforcement

2.5 Data Storage

TRAINING DATA AND INFERENCE DATA

Criterion ST-01: Security Controls

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Encryption at rest (AES-256 or equivalent)
- Key management procedures
- Access control mechanisms (RBAC, ABAC)
- Network isolation and segmentation
- Physical security measures
- Verify encryption implementation strength
- Assess key management security
- Review access control granularity
- Evaluate network isolation effectiveness
- Check physical security adequacy

Criterion ST-02: Data Retention and Lifecycle Management

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Retention policy documentation
- Retention period justification
- Automated deletion procedures
- Retention exceptions and approvals

- Lifecycle state tracking
- Review retention policy comprehensiveness
- Assess period justification reasonableness
- Verify automated deletion reliability
- Evaluate exception process rigor
- Check lifecycle tracking accuracy

Criterion ST-03: Backup and Recovery

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Backup strategy and schedule
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Backup testing procedures
- Offsite/cloud backup arrangements
- Disaster recovery plan
- Verify backup strategy adequacy
- Assess RTO/RPO appropriateness
- Review testing frequency and results
- Evaluate offsite protection
- Check DR plan completeness

Criterion ST-04: Audit Logging and Monitoring

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Comprehensive audit logging (access, modifications, deletions)
- Log retention and protection
- Real-time monitoring and alerting
- Anomaly detection capabilities
- Log review and analysis procedures
- Verify logging comprehensiveness
- Assess log protection adequacy
- Review monitoring coverage
- Evaluate anomaly detection effectiveness
- Check log review regularity

Criterion ST-05: Storage Infrastructure Resilience

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Redundancy and high availability design
- Failover procedures and testing
- Capacity planning and monitoring
- Performance SLA definitions
- Infrastructure as Code (IaC) for consistency
- Review redundancy design adequacy
- Assess failover procedure effectiveness
- Verify capacity planning rigor
- Evaluate SLA appropriateness
- Check IaC implementation quality

2.6 Data Maintenance

TRAINING DATA AND INFERENCE DATA

Criterion MA-01: Data Currency Management

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Data refresh schedules and triggers
- Staleness detection mechanisms
- Update procedures and workflows
- Currency requirements by data type
- Outdated data flagging and handling
- Review refresh schedule appropriateness
- Assess staleness detection sensitivity
- Verify update procedure reliability
- Evaluate currency requirement definitions
- Check handling of outdated data

Criterion MA-02: Data Cleansing and Correction

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Error detection mechanisms
- Correction workflows and approvals
- Data quality improvement procedures
- Correction audit trails
- Validation of corrections
- Verify error detection effectiveness
- Assess correction workflow appropriateness

- Review improvement procedure impact
- Evaluate audit trail completeness
- Check correction validation rigor

Criterion MA-03: Dataset Rebalancing and Augmentation

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Class imbalance monitoring
- Rebalancing strategies (oversampling, undersampling, SMOTE)
- Data augmentation techniques
- Synthetic data generation procedures
- Augmented data quality validation
- Review imbalance monitoring effectiveness
- Assess rebalancing strategy appropriateness
- Verify augmentation technique validity
- Evaluate synthetic data quality
- Check validation methodology

Criterion MA-04: Schema Evolution Management

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Schema change control procedures
- Backward compatibility management
- Migration planning and testing
- Schema version tracking
- Impact assessment of schema changes
- Verify change control rigor
- Assess compatibility management
- Review migration procedure safety
- Evaluate version tracking accuracy
- Check impact assessment thoroughness

Criterion MA-05: Continuous Data Improvement

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Data quality metrics and KPIs
- Feedback loop implementation
- Continuous monitoring and analysis

- Improvement prioritization methodology
- Stakeholder feedback incorporation
- Review metrics and KPI appropriateness
- Assess feedback loop effectiveness
- Verify monitoring comprehensiveness
- Evaluate prioritization methodology
- Check stakeholder engagement

2.7 Data Sharing and Dissemination

INFERENCE DATA ONLY

Per the criteria mapping, Data Sharing and Dissemination criteria apply only to Inference Data, as they relate to operational data sharing in production systems.

Criterion SH-01: Data Sharing Governance

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Data sharing policies and procedures
- Approval workflows for sharing
- Data use agreements and contracts
- Purpose limitation enforcement
- Sharing activity logging and tracking
- Review sharing policy comprehensiveness
- Assess approval workflow rigor
- Verify agreement adequacy
- Evaluate purpose limitation enforcement
- Check activity tracking completeness

Criterion SH-02: Privacy Protection in Sharing

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Anonymization or de-identification procedures
- Differential privacy implementation
- Re-identification risk assessment
- Data aggregation techniques
- Privacy-preserving data sharing methods
- Verify anonymization robustness
- Assess differential privacy implementation
- Review re-identification risk analysis

- Evaluate aggregation appropriateness
- Check privacy-preserving method effectiveness

Criterion SH-03: Third-Party Data Processor Management

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Processor due diligence procedures
- Data Processing Agreements (DPAs)
- Sub-processor approval and management
- Processor audit rights and execution
- Processor security and compliance monitoring
- Review due diligence thoroughness
- Assess DPA comprehensiveness
- Verify sub-processor controls
- Evaluate audit execution
- Check monitoring effectiveness

Criterion SH-04: Training Data Publication and Transparency

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Public documentation of training data sources (EU AI Act Article 53)
- Dataset cards describing characteristics and limitations
- Model cards with training data information
- Copyright and licensing transparency
- Transparency reporting for general-purpose AI
- Verify documentation completeness and accuracy
- Assess dataset card quality
- Review model card comprehensiveness
- Evaluate copyright disclosure
- Check transparency reporting adequacy

Criterion SH-05: API and Interface Security

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- API authentication and authorization
- Rate limiting and throttling
- Input validation and sanitization
- API security testing (penetration testing, fuzzing)

- API versioning and deprecation management
- Verify authentication mechanism strength
- Assess rate limiting effectiveness
- Review input validation comprehensiveness
- Evaluate security testing rigor
- Check versioning strategy

2.8 Data Archival

TRAINING DATA AND INFERENCE DATA

Criterion AR-01: Archival Policy and Procedures

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Archival policy and triggers
- Archival format and standards
- Retrieval procedures and SLAs
- Archival testing and verification
- Cost management for archival storage
- Review archival policy appropriateness
- Assess format longevity
- Verify retrieval capability
- Evaluate testing frequency
- Check cost optimization

Criterion AR-02: Archival Security and Privacy

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Encryption of archived data
- Access controls for archived data
- Long-term privacy preservation
- Integrity verification mechanisms
- Secure archival media management
- Verify encryption robustness
- Assess access control appropriateness
- Review privacy preservation methods
- Evaluate integrity verification
- Check media security

Criterion AR-03: Archival Documentation

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Comprehensive metadata preservation
- Context documentation
- Archival inventory and cataloging
- Search and discovery capabilities
- Documentation of archival decisions
- Verify metadata completeness
- Assess context preservation
- Review catalog quality
- Evaluate search effectiveness
- Check decision documentation

Criterion AR-04: Long-Term Accessibility

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Format migration strategies
- Technology obsolescence planning
- Media degradation monitoring
- Long-term readability assurance
- Archival refresh procedures
- Review migration strategy viability
- Assess obsolescence planning
- Verify degradation monitoring
- Evaluate readability assurance
- Check refresh procedure reliability

2.9 Data Disposition and Retirement

TRAINING DATA AND INFERENCE DATA

Criterion DR-01: Secure Data Deletion

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Secure deletion methods (cryptographic erasure, overwriting)
- Multi-location deletion (backups, replicas, caches)
- Deletion verification and certification
- Hardware disposal procedures
- Deletion audit trails

- Verify deletion method effectiveness
- Assess multi-location coverage
- Review certification validity
- Evaluate hardware disposal security
- Check audit trail completeness

Criterion DR-02: Right to Erasure Compliance

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Erasure request handling procedures
- Identity verification for requests
- Erasure completion timelines
- Exception handling (legal obligations, public interest)
- Communication with data subjects
- Review request handling efficiency
- Assess identity verification robustness
- Verify timeline compliance
- Evaluate exception justifications
- Check communication clarity

Criterion DR-03: Model Decommissioning

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Model decommissioning procedures
- Training data retention decisions upon decommissioning
- Inference data cleanup procedures
- Decommissioning documentation
- Stakeholder notification
- Verify decommissioning procedure completeness
- Assess data retention decision appropriateness
- Review cleanup thoroughness
- Evaluate documentation quality
- Check stakeholder communication

Criterion DR-04: Documentation of Disposition

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Disposition decision documentation

- Certificates of destruction
- Chain of custody through disposition
- Regulatory compliance evidence
- Disposition audit records
- Review decision documentation completeness
- Assess certificate validity
- Verify chain of custody integrity
- Evaluate compliance evidence
- Check audit record quality

Criterion DR-05: Legacy System Data Migration or Disposal

TRAINING DATA AND INFERENCE DATA

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Legacy system inventory
- Migration vs. disposal decision framework
- Data extraction and transformation procedures
- Legacy system decommissioning plan
- Validation of migrated data
- Verify inventory completeness
- Assess decision framework reasonableness
- Review extraction procedure accuracy
- Evaluate decommissioning plan
- Check validation thoroughness

3. Data Operation Criteria

Per the criteria mapping spreadsheet, Data Operation criteria are duplicated with separate sections for Training Operations and Inference Operations. Each section contains the same five criteria (OP-01 through OP-05), but they are assessed and applied differently based on whether the AI system is in the training phase or inference phase.

3.1 Data Operation - Model Training

TRAINING DATA ONLY

These criteria assess data governance during active model training operations, including experimentation, hyperparameter tuning, and iterative model development.

Criterion OP-01: Data Quality Monitoring (Training)

TRAINING DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Continuous data quality monitoring during training

- Quality degradation detection
- Data distribution drift monitoring
- Quality alerts and notifications
- Root cause analysis for quality issues
- Assess monitoring comprehensiveness
- Verify degradation detection sensitivity
- Review drift monitoring effectiveness
- Evaluate alert mechanism timeliness
- Check root cause analysis capability

Criterion OP-02: Model Performance Monitoring (Training)

TRAINING DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Training, validation, and test performance tracking
- Overfitting and underfitting detection
- Performance metric logging across experiments
- Model comparison and selection procedures
- Performance degradation alerts
- Verify performance tracking completeness
- Assess overfitting detection effectiveness
- Review metric logging consistency
- Evaluate comparison methodology rigor
- Check alert calibration

Criterion OP-03: Human Oversight Procedures (Training)

TRAINING DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Human review checkpoints in training workflow
- Expert review of model behavior
- Training decision approval procedures
- Escalation procedures for concerns
- Documentation of human decisions
- Review checkpoint adequacy
- Assess expert review depth
- Verify approval procedure rigor
- Evaluate escalation effectiveness
- Check decision documentation

Criterion OP-04: Bias and Fairness Monitoring (Training)

TRAINING DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Ongoing bias assessment during training iterations
- Fairness metrics calculation (demographic parity, equalized odds, etc.)
- Performance disparity analysis across groups
- Bias mitigation intervention documentation
- Trend analysis over training runs
- Evaluate bias assessment frequency
- Assess fairness metrics appropriateness
- Review disparity analysis thoroughness
- Verify mitigation effectiveness
- Check trend analysis insights

Criterion OP-05: Real-Time Data Validation (Training)

TRAINING DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Input data validation before training batches
- Schema compliance checking
- Range and constraint validation
- Corrupted data detection and handling
- Training pipeline monitoring
- Verify validation coverage
- Assess schema checking rigor
- Review constraint validation
- Evaluate corruption detection
- Check pipeline monitoring

3.2 Data Operation - Model Inference

INFERENCE DATA ONLY

These criteria assess data governance during operational deployment when the AI system is making predictions, recommendations, or decisions on production data.

Criterion OP-01: Data Quality Monitoring (Inference)

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Real-time input data quality monitoring
- Production data quality metrics

- Quality degradation alerts in production
- Out-of-specification data handling
- Quality trend analysis and reporting
- Assess real-time monitoring effectiveness
- Verify metrics appropriateness for production
- Review alert responsiveness
- Evaluate out-of-spec handling
- Check trend analysis frequency

Criterion OP-02: Model Performance Monitoring (Inference)

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Prediction accuracy monitoring in production
- Model drift detection (data drift, concept drift)
- Performance degradation alerts
- A/B testing and challenger models
- Performance SLA tracking
- Verify accuracy monitoring comprehensiveness
- Assess drift detection sensitivity
- Review alert threshold appropriateness
- Evaluate A/B testing methodology
- Check SLA compliance

Criterion OP-03: Human Oversight Procedures (Inference)

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Human-in-the-loop decision points
- Override mechanisms for automated decisions
- Escalation procedures for high-risk predictions
- Human review sampling strategy
- Documentation of human interventions
- Review oversight adequacy for risk level
- Assess override mechanism accessibility
- Verify escalation trigger appropriateness
- Evaluate sampling strategy coverage
- Check intervention documentation

Criterion OP-04: Bias and Fairness Monitoring (Inference)

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Continuous fairness monitoring in production
- Disparate impact analysis on production decisions
- Protected characteristic performance tracking
- Fairness degradation alerts
- Bias incident response procedures
- Evaluate monitoring frequency and coverage
- Assess disparate impact analysis rigor
- Review performance tracking comprehensiveness
- Verify alert sensitivity
- Check incident response effectiveness

Criterion OP-05: Real-Time Data Validation (Inference)

INFERENCE DATA ONLY

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Input validation for all production requests
- Adversarial input detection
- Out-of-distribution (OOD) detection
- Input sanitization and security
- Validation failure handling and logging
- Verify validation completeness
- Assess adversarial detection capability
- Review OOD detection effectiveness
- Evaluate sanitization robustness
- Check failure handling appropriateness

4. Governance and Ethical Criteria

Per the criteria mapping, these criteria apply at the organizational level across all AI systems and data uses. They are not specific to individual projects, training data, or inference data. These criteria assess the overall organizational maturity and commitment to responsible AI.

SCOPE: ORGANIZATIONAL-LEVEL ASSESSMENT, NOT PROJECT-SPECIFIC

4.1 Organizational Governance

Criterion GV-01: AI Governance Structure

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Formal AI governance framework

- Clear roles and responsibilities (AI Ethics Board, Data Governance Committee)
- Board-level oversight of AI risks
- Escalation procedures for ethical concerns
- Governance charter and operating procedures
- Assess governance framework comprehensiveness
- Verify role clarity and authority
- Review board engagement depth
- Evaluate escalation mechanism accessibility
- Check operating procedure effectiveness

Criterion GV-02: Risk Management Framework

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Formal AI risk assessment methodology aligned with NIST AI RMF
- Risk register covering AI-specific risks
- Risk appetite and tolerance statements
- Continuous risk monitoring and updates
- Integration with enterprise risk management
- Review methodology alignment with NIST AI RMF
- Assess risk register comprehensiveness
- Verify risk appetite operationalization
- Evaluate monitoring frequency
- Check ERM integration effectiveness

Criterion GV-03: Compliance Management

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Regulatory landscape monitoring
- Compliance obligation mapping
- Policy and procedure documentation
- Compliance testing and auditing
- Regulatory change management
- Verify monitoring comprehensiveness
- Assess obligation mapping completeness
- Review documentation quality
- Evaluate testing frequency and rigor
- Check change management responsiveness

4.2 Documentation and Transparency

Criterion DC-01: Technical Documentation

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Comprehensive system documentation standards
- Model cards for all deployed models
- Dataset cards for training datasets
- Architecture and design documentation
- Version control and change documentation
- Review documentation standards adequacy
- Assess model card quality and completeness
- Verify dataset card comprehensiveness
- Evaluate architecture documentation
- Check version control practices

Criterion DC-02: Explainability and Interpretability

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Explainable AI (XAI) techniques and tools
- User-facing explanation mechanisms
- Technical explainability capabilities
- Counterfactual explanation support
- Explanation validation and testing
- Verify XAI technique appropriateness
- Assess user explanation clarity
- Review technical capability depth
- Evaluate counterfactual quality
- Check validation rigor

Criterion DC-03: Algorithmic Impact Assessments

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Algorithmic Impact Assessment (AIA) methodology
- Fundamental rights impact analysis
- Stakeholder consultation procedures
- AIA documentation and publication
- Periodic reassessment triggers

- Review AIA methodology comprehensiveness
- Assess fundamental rights analysis depth
- Verify stakeholder consultation breadth
- Evaluate documentation quality
- Check reassessment frequency

4.3 Ethical Principles and Accountability

Criterion ET-01: Fairness and Non-Discrimination

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Formal fairness policy and principles
- Protected characteristic identification
- Fairness metrics and thresholds
- Discrimination remediation procedures
- Regular fairness auditing
- Review fairness policy comprehensiveness
- Assess protected characteristic coverage
- Verify metric selection appropriateness
- Evaluate remediation effectiveness
- Check audit frequency and independence

Criterion ET-02: Transparency and Accountability

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Transparency commitments and disclosures
- Individual rights procedures (access, rectification, erasure, explanation)
- Contestation and appeal mechanisms
- Accountability assignment for AI decisions
- Public transparency reporting
- Verify transparency commitment clarity
- Assess individual rights responsiveness
- Review contestation mechanism effectiveness
- Evaluate accountability clarity
- Check transparency reporting quality

Criterion ET-03: Human Rights Impact

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Human rights impact assessment methodology
- Vulnerable population protection measures
- Human rights risk identification
- Mitigation and remediation procedures
- Stakeholder engagement on human rights
- Review impact assessment methodology
- Assess protection measure adequacy
- Verify risk identification thoroughness
- Evaluate mitigation effectiveness
- Check stakeholder engagement quality

Criterion ET-04: Environmental Sustainability

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Carbon footprint measurement of AI systems
- Energy efficiency optimization
- Sustainable infrastructure choices
- Environmental impact reporting
- Green AI research and implementation
- Verify measurement methodology
- Assess optimization efforts
- Review infrastructure sustainability
- Evaluate reporting transparency
- Check green AI commitment

4.4 Training and Awareness

Criterion TR-01: Staff Training and Competency

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- AI ethics and governance training programs
- Role-specific competency requirements
- Training effectiveness assessment
- Continuous learning and development
- External training and certification support
- Review training program comprehensiveness
- Assess competency requirement appropriateness
- Verify effectiveness measurement

- Evaluate continuous learning culture
- Check external support availability

Criterion TR-02: Organizational Culture

ORGANIZATIONAL LEVEL

EVIDENCE REQUIRED · PRACTITIONERS

ASSESSOR GUIDANCE

- Ethical AI culture and values
- Speak-up and whistleblower mechanisms
- Reward and recognition for ethical behavior
- Leadership commitment and role modeling
- Cross-functional collaboration on ethics
- Assess culture embedding depth
- Verify speak-up mechanism accessibility
- Review reward alignment with values
- Evaluate leadership commitment
- Check collaboration effectiveness

5. Assessment Methodology and Scoring

5.1 Two-Role System

This framework serves two distinct roles:

- Data Ethics and Lineage Practitioners: Collect and document evidence for each criterion
- Data Ethics and Lineage Assessors: Evaluate evidence and assign compliance scores

5.2 Compliance Level Scoring (0-5 Scale)

Each criterion is scored on a six-point scale:

- 0 Not Observed** No evidence of the practice or control. Criterion not addressed.
- 1 Initial/Ad Hoc** Minimal, informal implementation. Inconsistent practices. Significant gaps exist.
- 2 Developing** Basic implementation with some documentation. Key elements present but gaps remain.
- 3 Defined/Managed** Well-defined, documented, and consistently implemented. Meets baseline regulatory requirements.
- 4 Measured/Optimized** Comprehensive with active monitoring and continuous improvement. Exceeds baseline requirements.
- 5 Leading Practice** Exemplary, industry-leading implementation. Innovative approaches with demonstrated effectiveness.

5.3 Criticality Weighting

Each criterion is assigned a criticality level:

- Critical (C): 40% weight - Score <3 blocks deployment
- High (H): 30% weight - Score <2 requires remediation plan
- Medium (M): 20% weight - Score <2 triggers improvement roadmap
- Low (L): 10% weight - Continuous improvement focus

5.4 Overall Accreditation Levels

- Level 5 (Exemplary): Overall score ≥4.5, no critical criteria <4, organizational excellence
- Level 4 (Advanced): Overall score ≥4.0, no critical criteria <3, strong performance
- Level 3 (Proficient): Overall score ≥3.0, no critical criteria <3, meets all regulatory requirements
- Level 2 (Developing): Overall score ≥2.0, remediation plan required for gaps
- Level 1 (Non-Compliant): Overall score <2.0, immediate remediation required, deployment may be blocked

6. Implementation Guidance

6.1 Practitioner Workflow

- Scoping: Identify AI system and determine applicable criteria (training/inference)
- Planning: Create evidence collection plan with timeline
- Evidence Gathering: Collect documentation, interview stakeholders, test systems
- Documentation: Complete evidence templates for each criterion
- Gap Identification: Note areas where evidence is lacking
- Quality Review: Self-review for completeness before submission
- Submission: Submit evidence package to assessors

6.2 Assessor Workflow

- Evidence Review: Examine submitted evidence for completeness and quality
- Verification: Validate evidence through sampling, testing, or interviews
- Scoring: Assign 0-5 scores based on evidence and guidance
- Documentation: Record findings, rationale, and recommendations
- Calibration: Peer review of scores for consistency
- Reporting: Generate assessment report with scores and findings
- Follow-up: Track remediation of identified gaps

6.3 Reassessment Triggers

- Annual reassessment for all deployed high-risk systems
- Material system changes (new data sources, algorithm changes, use case expansion)
- Regulatory changes affecting the AI system
- Significant incidents or bias discoveries
- Transition from pilot to production deployment

Appendix A: Criteria Summary by Phase

Quick reference showing which criteria apply to which phase:

Training Data Criteria

- All criteria in Stages 1-6 (Acquisition through Storage)
- Data Operation - Model Training (OP-01 through OP-05)
- Data Maintenance (MA-01 through MA-05)
- Data Archival (AR-01 through AR-04)
- Data Disposition and Retirement (DR-01 through DR-05)

Inference Data Criteria

- All criteria in Stages 1-6 (Acquisition through Storage)
- Data Operation - Model Inference (OP-01 through OP-05)
- Data Maintenance (MA-01 through MA-05)
- Data Sharing and Dissemination (SH-01 through SH-05)
- Data Archival (AR-01 through AR-04)
- Data Disposition and Retirement (DR-01 through DR-05)

Organizational (Cross-Cutting) Criteria

- Organizational Governance (GV-01 through GV-03)
- Documentation and Transparency (DC-01 through DC-03)
- Ethical Principles and Accountability (ET-01 through ET-04)
- Training and Awareness (TR-01 through TR-02)

Appendix B: Glossary

Training Data

Data used to develop, train, validate, and test AI models during the model development lifecycle.

Inference Data

Data used during operational deployment when the AI system makes predictions, recommendations, or decisions.

Data Lifecycle

The complete journey of data from acquisition through disposition, encompassing 10 stages.

High-Risk AI System

AI systems that pose significant risks to health, safety, or fundamental rights (per EU AI Act definition).

Bias

Systematic errors or unfairness in AI outputs resulting in discriminatory treatment based on protected characteristics.

Fairness Metrics

Quantitative measures of fairness such as demographic parity, equalized odds, or predictive parity.

Data Drift

Changes in the statistical properties of input data over time, potentially causing model degradation.

Concept Drift

Changes in the relationship between inputs and outputs over time, requiring model retraining.

Model Card

Structured documentation describing a model's characteristics, intended use, limitations, and performance.

Dataset Card

Structured documentation describing a dataset's characteristics, collection methods, and known limitations.

Differential Privacy

Mathematical framework for limiting privacy loss when analyzing datasets.

Explainability (XAI)

The capability to provide understandable explanations for AI system decisions and behaviors.

Appendix C: References

- European Union. (2024). Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act).
- Government of Canada. (2022). Bill C-27, Digital Charter Implementation Act, 2022 (AIDA).
- Biden Administration. (2023). Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.
- NIST. (2023). AI Risk Management Framework (AI RMF 1.0). NIST AI 100-1.
- NIST. (2024). Generative AI Profile. NIST AI 600-1.
- ISO/IEC. (2023). ISO/IEC 42001:2023 - Information technology — Artificial intelligence — Management system.
- ISO/IEC. (2024). ISO/IEC 8183:2024 - Information technology — Artificial intelligence — Data lifecycle framework.
- European Commission. (2016). General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679.
- Office of the Privacy Commissioner of Canada. Personal Information Protection and Electronic Documents Act (PIPEDA).
- State of California. (2018). California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA).

Document Version History:

Version 1.0: Initial comprehensive framework

Version 2.0: Updated based on official criteria mapping spreadsheet with explicit Training/Inference/Organizational distinctions