Tool 2 - Context Risk Multiplier Worksheet

The Context Risk Multiplier (CRM) evaluates how the governance environment amplifies or mitigates the real-world risk of deploying an AI system. It ensures that deployment decisions reflect both technical exposure (from Tool 1) and institutional readiness. The CRM converts intrinsic risk into an adjusted risk tier by assessing four factors: Legal Framework, Institutional Capacity, Data Ecosystem, and Public Trust & Transparency.

Even a well-tested model can be unsafe in a weak governance context, while strong safeguards can enable responsible innovation. While developed for social assistance use cases, this tool is adaptable for broader use across social protection pillars.

Sources and Methodology

This diagnostic draws on institutional readiness assessment approaches from multiple frameworks, adapted for social protection contexts:

- **Humanitarian data governance:** The four-factor structure reflects the contextual assessment approach in the *Handbook on Data Protection in Humanitarian Action* (ICRC, 2024), which emphasises that data protection risks must be evaluated in light of institutional capacity, legal frameworks, and the specific vulnerabilities of affected populations. The Handbook's guidance on Data Protection Impact Assessments (DPIAs) and its emphasis on contextual factors (Chapter 5 and Chapter 17.6) directly informs this tool's structure.

- **AI ethics and readiness assessment:** The UNESCO Readiness Assessment Methodology and Ethical Impact Assessment for AI (UNESCO, 2023) provide the foundation for assessing legal and regulatory readiness, institutional capacity, and stakeholder engagement. Key diagnostic questions are adapted from the UNESCO framework's approach to evaluating procurement, governance structures, and human rights safeguards.

- **Humanitarian coordination standards:** The OCHA Data Responsibility Guidelines (OCHA, 2025) and IASC guidance on data governance in humanitarian settings (IASC, 2023) inform the tool's approach to assessing data ecosystem maturity, interoperability, and cross-organisational data sharing arrangements.

- **Human rights impact assessment:** The tool's emphasis on legal basis, appeal rights, and transparency reflects the HRIA methodology described in ICRC (2024, Chapter 17.6.1-17.6.2), which positions contextual factors as essential determinants of whether AI systems can be deployed safely.

- **Social protection data governance:** The assessment of institutional capacity and data ecosystems aligns with the *Data Governance Framework for Digital Social Protection Systems* (DCI, 2025). Specifically, the four factors in this tool correspond to the DCI framework's core pillars (Management, Quality, Access, and Security) and its structural building blocks (Policy & Regulations, Institutions & People, and Technology & Data).

Related Tools

Practioners may also wish to consult:

- UNESCO Readiness Assessment Methodology: https://unesdoc.unesco.org/ark:/48223/pf0000385198
- UNESCO Ethical Impact Assessment: https://unesdoc.unesco.org/ark:/48223/pf0000386276

A note on rating scales: This tool rates institutional readiness as Strong, Moderate, or Weak, where Strong means greatest capacity to manage risk safely. Tool 1 uses a different scale (Low / Medium / High) because it measures intrinsic risk rather than governance capacity. The two scales are combined in the decision matrix described in the companion report (DCI AI Hub, 2026, Section 5.4).

Relationship to the risk framework: This tool examines the remaining two of the five structural sources of risk identified in the companion report (DCI AI Hub, 2026), namely Governance and Institutional Oversight Risks and Market, Sovereignty and Industry Structure Risks, through four diagnostic dimensions. The first three sources, Data Risks, Model Risks, and Operational and Integration Risks, are assessed in Tool 1.

System Information

AI Component / Module:	
Brief Description:	
Version Number:	
Date Assessed:	
Date for Next Review:	

Ratings

Intrinsic Risk Tier (from Tool 1)	□ Low □ Medium □ High
CRM Tier (from Tool 2)	□ Low □ Medium □ High
Final Overall Risk Tier (from Tool 2)	□ Low □ Medium □ High
Narrative Justification	_____

Decision Sign-Off

Role	Name	Signature	Date
Technical Lead			
Programme Lead			
Legal / DPO			

How to use this tool

Step 1 - Gather documents

Collect all relevant documents before starting the assessment. This should include applicable laws and regulations, institutional mandates, internal policies and standard operating procedures, recent audit and evaluation reports, data governance and security documentation, DPIAs or AI Impact Assessments (AIAs), and records of grievance and appeal mechanisms. Where possible, obtain copies rather than relying on verbal descriptions. This ensures that all ratings are grounded in verifiable evidence.

Step 2 - Review the evidence and rate each dimension

Examine the collected documentation for the four CRM dimensions: legal framework, institutional capacity, data ecosystem, and public trust. Check for completeness, clarity, and reliability—flag any gaps, uncertainties or outdated sources. If evidence is weak or uncertain, apply the precautionary principle and lean toward a higher-risk rating.

To reach a decision:

- Compare evidence against the rating criteria (Strong / Moderate / Weak).
- Discuss uncertainties openly—consensus is good practice because it surfaces disagreements and helps uncover overlooked issues.
-

The goal is a shared, defensible rating for each dimension based strictly on documented evidence.

Step 3 – Document Justification

For each factor, record a concise but complete narrative explaining why the rating was chosen and which documents were used. Include:

- What evidence was reviewed
- What uncertainties remain
- What real-world impacts were considered
- Why this tier appropriately reflects risk to beneficiaries

Documented justification is mandatory. Ratings without written explanation should be considered invalid. Clear justification ensures traceability, supports audits, and enables learning.

Step 4 –Determine Overall CRM Rating

Use the aggregation rules provided in the last section to combine the four dimension ratings into an overall CRM tier. Enter the final factor ratings, overall CRM rating, evidence sources, and narrative justification into the CRM Summary Box on Page 1 and ensure sign-off from all relevant actors.

Step 5 – Move to next tool and link to the risk register

Continue the risk assessment pathway by moving to Tool 3, the Risk Register. Ensure all risks identified through the CRM assessment are recorded with their mitigation measures, risk owners, and decision implications (Blocking, Pilot Condition, or Monitor) so that the register directly informs the Go/Pilot/No-Go decision in Tool 4.

Step 6 – Reapply When Conditions Change

Repeat the assessment whenever uncertainty increases—such as new data, model retraining, legislative changes, programme rule shifts, or before moving from pilot to scale. Reapplication ensures safeguards stay aligned with evolving risks and that decisions remain transparent and contestable.

Dimension 1 – Legal Framework

This factor assesses whether the legal basis for using AI in social protection is clear, enforceable, and rights-compliant. It considers data-protection law, lawful-processing mandates, appeal rights, authorisation for automated or semi-automated decisions, and regulatory supervision.

Evidence to review

- Data-protection laws (e.g., GDPR-equivalent legislation, sector-specific data rules)
- AI-specific regulations (binding legislation such as the EU AI Act or national equivalents where applicable)
- AI soft law and guidance (national AI strategies, public-sector procurement guidelines for AI, ethical frameworks adopted by government)
- Sector-specific regulations or authorisations for social protection
- Appeal and due-process provisions (including rights to human review of automated decisions)
- Institutional policies aligned to legal mandates
- Cybersecurity laws and regulations applicable to public-sector systems or critical infrastructure
- AI procurement laws, policies, or guidelines (including any pre-approval requirements or certified vendor lists)

Diagnostic Questions

Data Protection & Privacy

- Is the lawful basis for data processing clearly defined?
- Does the data protection framework include enforcement mechanisms, remedies, and a functional supervisory authority?
- Are there specific protections for sensitive data categories processed in social protection (e.g., income, health, household composition)?

Due Process & Appeal Rights

- Are individuals guaranteed the right to challenge or appeal decisions?
- Are there clear limits on automated decision-making?

AI-Specific Regulation & Strategy

- Is the use of AI explicility authorised where relevant?
- Does applicable AI regulation classify this system as high-risk, requiring specific compliance obligations?
- Does the national AI strategy or equivalent explicitly address AI impacts on human rights, including safeguards for dignity, non-discrimination, privacy, and due process in public-sector applications?

Regulatory Oversight

- Do regulators have supervisory or enforcement authority over AI systems and data processing?

AI Procurement Governance

- Are there laws or policies governing procurement of AI systems for public services, including requirements for testing and documentation?
- Is there a pre-approval or vetting process before AI systems can be acquired?
- If vendor certification exists, does it address ethical and rights dimensions, or only technical requirements?

Cybersecurity & Critical Infrastructure

- Do cybersecurity laws or critical infrastructure protection regulations apply to this system?
- Are there mandatory security standards, certifications, or incident reporting obligations?

Note: This dimension assesses whether cybersecurity legal obligations exist and apply. Compliance with security standards and controls is assessed in Dimension 3 (Data Ecosystem).

Rating Table

Rating	Criteria	Tick
Strong	Clear, comprehensive, and enforced data-protection law with functional supervisory authority and specific protections for sensitive data; applicable cybersecurity and critical infrastructure requirements identified and documented; AI procurement guidelines exist and require impact assessment, transparency, auditability, and ethical provisions in contracts; explicit authorisation for AI use; national AI strategy addresses human rights safeguards; appeal rights fully operational; active regulatory oversight applicable cybersecurity and critical infrastructure requirements identified and documented, AI procurement guidelines exist and require impact assessment, transparency, and auditability provisions in contracts,	☐

Moderate	Legal basis exists but enforcement is inconsistent; data protection authority exists but has limited capacity; general IT procurement rules apply but lack AI-specific requirements; appeal mechanisms function with gaps; some ambiguity in authorisation; AI strategy exists but does not specifically address rights safeguards; limited regulatory oversight.general IT procurement rules apply but lack AI-specific requirements;	☐
Weak	Legal basis unclear or absent; no functional data protection authority or enforcement mechanisms; no clarity on whether cybersecurity regulations apply or what they require; no procurement framework addresses AI specific risks; standard IT procurement used without adaptation; no sensitive data protections; appeal rights weak or missing; no authorisation for AI; no AI strategy or strategy silent on human rights; no effective regulatory supervision.no clarity on whether cybersecurity regulations apply or what they require; no procurement framework addresses AI specific risks; standard IT procurement used without adaptation;	☐

Evidence Log

Evidence Reviewed	
Evidence Gaps	
Assumptions/Notes	

Dimension 2 – Institutional Capacity

This factor evaluates whether institutions have the staffing, oversight structures, accountability lines, and resources to govern AI responsibly. It aligns with the **"Institutions and People" building block of the DCI Framework (DCI, 2025),** considering operational readiness, auditability, budget, and clarity of responsibility.

Evidence to review

- Organisational charts; mandates of oversight bodies
- Internal audit reports
- Budget allocations for data and digital functions
- Training records; performance evaluations of MIS or data teams
- Incident-response procedures
- Stakeholder engagement records or consultation reports
- AI/algorithmic impact assessment reports or capacity
- Staff competency frameworks or AI literacy training records

Diagnostic Questions

Accountability & Governance

- Are accountability roles clear from programme to technical to legal units?
- Is there cross-functional collaboration between technical teams and sector specialists who understand social protection contexts and risks?
- Have impacted stakeholder groups been identified, and are they involved in AI system development, deployment, or oversight?

Audit & Oversight

- Do independent audits occur regularly?
- Does the institution have the capacity to conduct AI impact assessments (AIAs) or Data Protection Impact Assessments (DPIAs)?

Staffing & Competence

- Do staff have the competence to understand AI system outputs, limitations, and failure modes—not just sufficient numbers?
- Is there evidence that staff exercise independent judgment rather than defaulting to algorithmic recommendations (automation bias)?
- Are AI/data literacy training programmes in place for staff who interact with or oversee AI systems?

Resources & Response

- Are resources available to respond when system issues arise?

Rating Table

Rating	Criteria	Tick
Strong	Clear accountability and governance structures with cross-functional collaboration between technical and sector-specialist teams; impacted stakeholder groups identified and meaningfully involved in oversight; well-staffed information system, data, and oversight units with demonstrated competence to understand AI outputs, limitations, and failure modes; staff exercise independent judgment with safeguards against automation bias; AI literacy training in place; proven capacity to conduct DPIAs and AIAs; routine independent audits; dedicated budget; functional incident-response procedures.	☐
Moderate	Accountability structures exist but inconsistently applied; some cross functional collaboration but limited integration between technical and programme teams; stakeholder involvement is ad hoc or consultative only; staffing sufficient but overstretched or with uneven AI literacy; some risk of automation bias due to limited understanding of system limitations; DPIA/AIA capacity exists but not routinely applied; audits irregular or lack independence; resource constraints affect monitoring.	☐
Weak	Unclear or missing accountability structures; technical and programme teams operate in silos with little collaboration; no stakeholder involvement; insufficient staffing or staff lack competence to critically assess AI outputs; high risk of automation bias; no capacity to conduct DPIAs or AIAs; no AI literacy training; no audit cycles; no dedicated budget; reliance on single technical focal point; no escalation path.	☐

Evidence Log

Evidence Reviewed	
Evidence Gaps	
Assumptions/Notes	

Dimension 3 – Data Ecosystem

This factor assesses whether data quality, documentation, control, and security are sufficient to support responsible AI. It examines data provenance, interoperability, metadata standards, governance policies, localisation, and safeguarding measures.

Evidence to review

- Data quality assessments; metadata documentation
- Interoperability standards
- Data localisation arrangements • Security certifications (e.g., ISO 27001 or SOC 2)
- Data Protection Impact Assessment findings (see ICRC, 2024)

Diagnostic Questions

Data Quality

- Does the data meet established quality standards for completeness, accuracy, currency, consistency, validity, and uniqueness? (Refer to Pillar 2: Quality in the DCI Data Governance Framework (2025) for detailed assessment guidance.)

Documentation & Provenance

- Are metadata and documentation sufficient to track data lineage, sources, and transformations?

Interoperability

- Are interoperability standards and data-sharing agreements in place across relevant systems?

Sovereignty & Control

- Is the data hosted within national jurisdiction or under a hosting arrangement with clear, enforceable data localisation provisions?
- Does the government retain ownership and control of encryption keys, access credentials, and backup data?
- Are contractual audit rights in place that allow independent inspection of vendor-controlled systems, data processing, and model behaviour?

Security

- Are security controls certified (e.g., ISO 27001, SOC 2) and independently tested?

Risk Assessment

- Does the DPIA identify unresolved data-related risks?

- Does the data meet the six DCI quality dimensions? (Refer to Pillar 2: Quality in the DCI Data Governance Framework (2025) for assessment definitions). Completeness: Is all necessary data present? Accuracy: Does the data correctly reflect reality? Currency: Is the data up to date? Consistency: Is the data uniform across databases? Validity: Does the data follow defined formats/rules? Uniqueness: Are there duplicate records?

Rating Table

Rating	Criteria	Tick
Strong	High-quality, validated data meeting established quality standards with documented provenance; interoperable systems with standardised metadata and clear data-sharing agreements; local or sovereign control over hosting and encryption with enforceable audit rights over vendor system; robust, certified security controls; DPIA completed with no unresolved data risks.	☐
Moderate	Data generally reliable but unevenly documented; partial interoperability; mixed control over hosting; security adequate but not externally certified; DPIA completed but some data risks remain partially addressed...	☐
Weak	Low-quality, outdated, or inconsistent data; fragmented systems with limited interoperability; vendor control over core datasets; no contractual audit access; encryption keys held by vendor; unclear hosting jurisdiction , weak or untested security controls; no DPIA conducted or significant unresolved data risks.	☐

Evidence Log

Evidence Reviewed	
Evidence Gaps	
Assumptions/Notes	

Dimension 4 – Public Trust & Transparency

This factor considers how openly the institution communicates about AI use, protects user rights, and ensures meaningful engagement with affected groups and civil society.

Evidence to review

- Published DPIAs or AIAs; User-rights notices
- Public communication materials
- Grievance and appeal statistics
- Stakeholder consultation reports
- Civil-society feedback or monitoring reports

Diagnostic Questions

Transparency & Disclosure

- Are DPIAs or AIAs published and accessible to the public?
- Are changes in AI use communicated transparently and proactively?
- Are beneficiaries clearly informed when AI plays a role in decisions affecting them?

User Rights & Agency

- Are beneficiaries informed of their rights in relation to AI-assisted decisions?
- Can users opt out of AI-assisted processes and request a fully human-led pathway?
- Can users challenge/request correction of AI system outputs that affect them?
- Are plain-language explanations provided when AI contributes to adverse or high-impact decisions?

Grievance & Redress

- Do grievance channels show active use and documented follow-up?
- Are grievance mechanisms accessible across multiple channels (including non-digital options)?
- Are response times tracked and reported?

Stakeholder Engagement

- Is there structured, ongoing engagement with civil society on AI governance?
- Are affected communities consulted during AI system design, deployment, or review?
- Is feedback from beneficiaries and civil society systematically incorporated into system improvements?

Rating Table

Rating	Criteria	Tick
Strong	DPIAs or AIAs routinely published; clear user-rights communication including the role of AI; beneficiaries can opt out of AI-assisted processes or request human review; users can challenge or correct AI outputs; explanations provided for adverse decisions; high grievance uptake with documented follow-through; active engagement with civil society.	☐
Moderate	Transparency present but irregular; user-rights information limited in reach; opt-out or human-review pathways exist but are not well communicated or are difficult to access; grievance channels functioning but underused; engagement occasional.	☐
Weak	No publication of DPIAs or AIAs; minimal or no communication of user rights or AI's role; no option to opt out or request human review; no mechanism to challenge AI outputs; g	☐

Evidence Log

Evidence Reviewed	
Evidence Gaps	
Assumptions/Notes	

Putting It All Together: Overall Risk Classification

Once each of the four dimensions of institutional readiness has been assessed, the Context Risk Multiplier (CRM) brings them together into a qualitative rating of overall context readiness. This rating (Strong, Moderate, or Weak) reflects the extent to which an institution's legal, organisational, and data-governance safeguards can reliably manage the risks identified in the intrinsic assessment.

Legal Framework	**□ Strong □ Moderate □ Weak**
Institutional Capacity	**□ Strong □ Moderate □ Weak**
Data Ecosystem	**□ Strong □ Moderate □ Weak**
Public Trust & Transparency	**□ Strong □ Moderate □ Weak**

Add the ratings for each factor as determined in the Worksheet above, then use the table below to determine the relevant CRM tier:

CRM Rating and interpretation	Aggregation rule	Effect on Risk Tier	Tick
Strong - Institution has proven governance and oversight capacity	• Three or four factors are Strong, **AND** • No factors are weak	Lowers overall risk tier	☐
Moderate - Some safeguards exist but capacity gaps remain	• Mixed patterns, not satisfying the overall criteria for Strong or Weak	Keeps risk tier unchanged	☐
Weak - Weak or missing governance foundations	• Two or more factors are Weak, **OR** • One Weak factor and no Strong factors	Raises risk tier by one level	☐

Look back on the intrinsic risk rating from Tool one, and determine the overall risk level by adjusting intrinsic risk up or down using the CRM Tier. A rating of Strong on the CRM lowers the risk tier; a moderate CRM rating keeps the intrinsic risk tier unchanged; and a CRM rating of Weak raises the overall risk tier by one level relative to the intrinsic risk tier.

Summary Ratings

Intrinsic Risk Tier (from Tool 1)	**□ Strong □ Moderate □ Weak**
CRM Tier (from this Tool)	**□ Strong □ Moderate □ Weak**
Final Overall Risk Tier	**□ Strong □ Moderate □ Weak**