

Terms of Reference For Institutional Consultancy

Title:	International Institutional Consultancy to Conduct Tajikistan's National Child Online Safety Assessment Using the WeProtect Global Alliance Model National Response Framework (MNRF), with Integrated Analysis of Artificial Intelligence, Emerging Technologies and Child Safeguarding
Consultancy Mode:	National ☐ International ☒
Type of Contract:	Institutional
Mode of Selection:	Competitive ☒ Single Source ☐
Location	Tajikistan
Duration of Contract:	September 2026 – December 2026

1. Background

Children constitute a substantial share of the world's online population. UNICEF estimates that one in three internet users globally is a child, with more than 175,000 children going online for the first time every day. However, safeguards have not kept pace with children's rapidly expanding digital presence. Evidence from the *Disrupting Harm* research programme, led by UNICEF Innocenti in partnership with ECPAT International and INTERPOL, found that between 1 and 20 per cent of children across 13 countries experienced technology-facilitated sexual exploitation and abuse during the previous year. Survivors were significantly more likely to experience self-harm or suicidal thoughts, while only a small proportion disclosed the abuse to formal protection services. These findings demonstrate that child online safety has become an increasingly important child rights, governance and public policy issue requiring coordinated, whole-of-government responses.

At the same time, rapid advances in artificial intelligence (AI) are reshaping children's digital experiences. UNICEF estimates that at least 20 million children across 10 countries have already used artificial intelligence (AI), adopting the technology more than three times faster than adults and often without adequate safeguards¹. AI-generated child sexual abuse material, sexually explicit deepfakes, AI-assisted grooming, algorithmic amplification of harmful content, and misuse of children's personal data are emerging risks that existing child protection systems are often ill-equipped to address. At the same time, AI offers significant opportunities to improve education, accessibility, innovation and public service delivery. Maximising these opportunities while safeguarding children's rights requires child-centred governance, effective regulation and strengthened institutional capacity.

Against this global backdrop, Tajikistan is entering a period of accelerated digital transformation. The Government of Tajikistan has identified digitalization as a strategic national development priority, promoting the modernization of public administration, education, innovation and public service delivery through digital technologies. At the same time, children and adolescents represent a substantial share of the country's population and are among the fastest adopters of digital technologies. As internet connectivity, smartphone ownership and access to digital services continue to expand, growing numbers of children are engaging with online environments from an increasingly early age. Ensuring that children can

¹ ECPAT International, INTERPOL and UNICEF Office of Research – Innocenti (2022). *Disrupting Harm: Evidence on Online Child Sexual Exploitation and Abuse* (13-country research project, 2019–2022). Funded by the Global Partnership to End Violence against Children through Safe Online. Available at: https://www.unicef.org/innocenti/reports/disrupting-harm-country-reports?utm_source=chatgpt.com

safely benefit from these opportunities has therefore become an important national child protection and public policy priority.

National efforts to strengthen child online safety remain at an early stage and are primarily focused on establishing a legislative foundation. Existing legislation, including the Law of the Republic of Tajikistan *On Responsibility for the Education and Upbringing of a Child*, defines certain parental responsibilities related to children's digital use. The National Strategy on Countering Terrorism also recognizes the misuse of digital platforms and online games for promoting violence, extremism, and adolescent recruitment. In addition, draft Rules for Protecting Children from Information Harmful to Their Health or Development are currently nearing adoption. However, preliminary analysis indicates that these measures do not yet provide a comprehensive, child-centred framework for preventing and responding to the full spectrum of online risks affecting children, nor do they establish coordinated institutional mechanisms across sectors.

Recent national evidence reinforces these challenges. Findings from the *Zireh (Shield)* Information Campaign implemented by Asia-Plus Media Group with support from the European Union under the CARAVAN project, documented widespread experiences of cyberbullying, psychological harassment, non-consensual image sharing, online fraud and threatening communications among adolescents, alongside emerging concerns related to AI-generated content and impersonation. The study also found that approximately 80–85 per cent of adolescents had concealed serious online incidents from adults because they feared punishment, restrictions or being judged, while trust in schools as sources of support remained very low. These findings highlight important gaps in prevention, reporting mechanisms, institutional response and trusted support systems for children navigating online environments.

Strengthening child online safety therefore requires more than legislative reform or isolated interventions. It requires a comprehensive understanding of the capacities, governance arrangements, coordination mechanisms and systemic gaps across the broader child online safety ecosystem, including child protection, justice, education, digital governance, law enforcement, the ICT sector and emerging technologies. Establishing such an evidence base is essential for informing policy reform, prioritising investments and developing an evidence-based National Action Plan on Child Online Safety.

To support this objective, UNICEF, in partnership with the Government of Tajikistan, will undertake the country's first National Child Online Safety Assessment. Rather than applying multiple international frameworks independently, the assessment will be undertaken using a single, integrated assessment framework developed by the selected institution during the inception phase. The framework will draw upon internationally recognised methodologies and normative guidance, with the WeProtect Global Alliance Model National Response Framework (MNRF) serving as the primary systems backbone for assessing national capacity to prevent and respond to Online Child Sexual Exploitation and Abuse (OCSEA).

Building on this foundation, the assessment framework will incorporate additional analytical domains addressing broader child online safety risks, artificial intelligence, digital governance, child rights in digital environments, institutional readiness and technological safeguards, informed by UNICEF's Policy Guidance on AI and Children (Version 3.0, 2025), General Comment No. 25, UNESCO's AI Readiness Assessment Methodology, UNDP's AI Landscape Assessment Methodology and other relevant international good practice.

The integrated framework will enable a single, coherent assessment process that avoids repetitive stakeholder consultations, overlapping analysis and fragmented recommendations, while providing a comprehensive evidence base to strengthen governance, institutional capacity, multi-sectoral coordination and child-centred digital transformation. The assessment will ultimately inform the development of Tajikistan's first National Action Plan on Child Online Safety.

Purpose and specific objectives

The purpose of this consultancy is to generate the first comprehensive national evidence base on child online safety in Tajikistan by assessing the country's capacity to prevent, detect, investigate and respond to Online Child Sexual Exploitation and Abuse (OCSEA), while evaluating its readiness to address emerging artificial intelligence (AI)-enabled risks affecting children.

Page | 3

The assessment will provide a systems-level analysis of national capacities, institutional arrangements, legal and policy frameworks, coordination mechanisms, service delivery and emerging digital risks. The findings will establish a national baseline to inform evidence-based policy reforms, strengthen institutional capacities, support multi-sectoral coordination and guide the development of a National Action Plan on Child Online Safety.

The selected institution will develop, during the inception phase, a bespoke National Child Online Safety Assessment Framework tailored to the Tajikistan context. Rather than applying multiple international frameworks as parallel assessments, the consultancy will develop a single integrated assessment methodology that draws upon existing internationally recognised frameworks and guidance.

The WeProtect Global Alliance Model National Response Framework (MNRF) and Maturity Model will serve as the primary systems framework for assessing national capacities to prevent and respond to Online Child Sexual Exploitation and Abuse (OCSEA). Building on this foundation, the assessment framework will be expanded to examine broader dimensions of child online safety, including artificial intelligence, emerging digital risks, child rights in digital environments, digital governance, prevention, education, institutional readiness and technological safeguards. The integrated framework should be informed, where appropriate, by UNICEF's Policy Guidance on AI and Children (Version 3.0, 2025), General Comment No. 25, UNESCO's AI Readiness Assessment Methodology, UNDP's AI Landscape Assessment Methodology and other relevant international good practice.

The resulting framework shall enable one coherent assessment process, one integrated stakeholder consultation process, one consolidated evidence base and one unified set of recommendations, thereby avoiding duplication of consultations, overlapping findings and fragmented recommendations.

Objective 1. Conduct an Integrated National Child Online Safety Assessment

Using the bespoke National Child Online Safety Assessment Framework developed during the inception phase—with the WeProtect Global Alliance Model National Response Framework (MNRF) and Maturity Model serving as the primary systems backbone—conduct a comprehensive assessment of Tajikistan's child online safety ecosystem. The assessment shall evaluate national capacities to prevent and respond to Online Child Sexual Exploitation and Abuse (OCSEA) and other technology-facilitated forms of violence against children, examining governance, institutional, legal and operational dimensions while identifying systemic strengths, gaps and priorities for strengthening the national response.

The assessment shall:

- Assess national capacities across all six WeProtect MNRF capability areas (policy and governance, criminal justice, victim support, prevention, industry engagement and international cooperation);
- Determine the maturity level of each capability area using the WeProtect Maturity Model;
- Assess institutional mandates, governance arrangements and coordination mechanisms supporting child online safety;
- Assess the effectiveness of prevention, reporting, investigation, prosecution, referral and victim support systems for children affected by online harms;

- Assess the legal, regulatory and policy framework governing child online safety, including legislation relating to Online Child Sexual Exploitation and Abuse (OCSEA), child protection, criminal justice, ICT and digital governance, and evaluate its implementation within the national child protection ecosystem;
- Evaluate alignment with the Convention on the Rights of the Child, General Comment No. 25, and other relevant international standards;
- Identify systemic strengths, gaps, implementation bottlenecks and priority areas for policy, institutional and investment reforms.

Objective 2. Assess AI Readiness and Emerging Digital Risks Affecting Children

Building on the integrated National Child Online Safety Assessment Framework, conduct a thematic analysis of Tajikistan's preparedness to protect children's rights in an increasingly AI-enabled digital environment. This objective complements the systems assessment under Objective 1 by examining AI-specific and emerging digital risks that are not comprehensively addressed through the WeProtect Model National Response Framework, while avoiding duplication of evidence collection, stakeholder consultations and analytical findings.

The assessment shall examine:

- AI-enabled risks affecting children, including AI-generated child sexual abuse material (AI-generated CSAM), deepfakes, synthetic media, AI-assisted grooming, algorithmic amplification of harmful content, misuse of children's personal data, manipulative design, and AI-facilitated dependencies;
- The national AI governance ecosystem, including governance arrangements, institutional responsibilities, regulatory readiness, and the emerging legal, regulatory and policy environment for artificial intelligence and digital technologies affecting children;
- Institutional capacity to identify, prevent and respond to AI-enabled harms, including the capacities of relevant government institutions and frontline professionals;
- AI literacy and preparedness among children, caregivers, educators and frontline professionals, drawing on existing evidence and, where appropriate, targeted consultations or small-scale assessments;
- The implications of AI for children's rights, including education, child development, equity, inclusion, participation and digital wellbeing;
- Existing technological safeguards, digital safety infrastructure and innovative technological solutions that could strengthen child online safety;
- Alignment with UNICEF's Policy Guidance on AI and Children and other relevant international standards, including an assessment of legislative, regulatory and policy gaps affecting children in digital environments;
- Recommendations to strengthen child-centred AI governance, including legislative and regulatory reforms, institutional strengthening, technological safeguards and responsible AI implementation.

Objective 3. Develop a National Action Plan on Child Online Safety

Using the findings of the integrated National Child Online Safety Assessment—including the systems assessment and thematic analyses undertaken under Objectives 1–3—develop a prioritised, evidence-based and implementable National Action Plan on Child Online Safety that strengthens Tajikistan's child online safety ecosystem over the short, medium and long term.

The Action Plan shall:

- Translate assessment findings into practical, sequenced and measurable actions;

- Define institutional roles and responsibilities across government, civil society, academia, the private sector and caregivers;
- Identify capacity-building priorities, resource requirements and partnership opportunities;
- Include indicative implementation timelines and monitoring indicators; and
- Ensure alignment with national development priorities, digital transformation strategies, and international child rights standards.

Reference materials (Hyperlinked):

1. [The UNICEF Child Protection Systems Strengthening Approach](#)
2. [Phases of Child Protection Systems Strengthening and Benchmarks for Measurement](#)
3. [High-Priority Child Protection Systems Strengthening \(CPSS\) Interventions](#)
4. [Child Protection Strategy | UNICEF](#)
5. [Legislating for Digital Age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse, UNICEF, 2022](#)
6. [Model National Response Maturity Model](#)
7. [Guidelines for industry on online child protection](#)
8. [Caring for child survivors of sexual abuse](#)
9. [ISO Requirements for child-friendly services for victims of violence](#)
10. [Child Protection in Digital Education](#)
11. [UNICEF Guidance on AI and children \(Version 3.0\)](#)
12. [Committee on the Rights of the Child, General Comment No. 25](#)
13. [UNDP Artificial Intelligence Landscape Assessment Methodology](#)
14. [UNESCO Readiness assessment methodology: a tool of the Recommendation on the Ethics of Artificial Intelligence](#)
15. [When AI becomes a friend: Child rights risks, harms, and regulatory responses to AI chatbots and companions](#) (policy brief and recommendations for businesses 2026)
16. [AI and Child Sexual Abuse and Exploitation: Issue brief](#) (2026)
17. [Artificial Intelligence Governance in Motion: A rapid global review of AI regulation and its implication for children's rights](#) (2025)
18. [Keeping Children Safe Online: Trends in Online Platform Regulation and Emerging Lessons](#) (2025) (policy brief)
19. [New frontiers in child labour: Why digital risks demand urgent attention](#) (2026)
20. [Assessing child rights impacts in relation to the digital environment](#) (2025)

2. Scope of work

The selected institution will design and implement Tajikistan's first integrated National Child Online Safety Assessment. Rather than undertaking separate assessments, the institution shall develop a bespoke National Child Online Safety Assessment Framework that synthesises internationally recognised methodologies into a single analytical framework tailored to the Tajikistan context. The WeProtect Global Alliance Model National Response Framework (MNRF) shall serve as the primary systems assessment backbone, complemented by relevant international guidance on child rights, digital governance, artificial intelligence and emerging technologies.

Using this integrated framework, the institution will conduct one coherent national assessment process, comprising a single programme of stakeholder consultations, data collection, analysis and validation. The assessment shall generate one consolidated evidence base and one integrated set of recommendations to strengthen Tajikistan's child online safety ecosystem and inform the development of a National Action Plan on Child Online Safety.

Deliverables	Proposed Tasks	Timeframe
Deliverable 1: Inception Report and Integrated National Child Online Safety Assessment Framework	The selected institution shall: • Develop a bespoke Integrated National Child Online Safety Assessment Framework tailored to Tajikistan, using the WeProtect Global Alliance Model National Response Framework (MNRF) and Maturity Model as the primary systems assessment backbone, complemented by UNICEF normative guidance, General Comment No. 25, UNICEF's Policy Guidance on AI and Children, and other relevant international standards. • Develop the integrated assessment methodology, including the analytical framework, indicators, evidence requirements and data collection methods, demonstrating how the systems assessment and the thematic analysis of AI readiness and emerging digital risks will be implemented through a single, harmonised assessment process. • Prepare stakeholder mapping, consultation strategy, data collection tools, ethical and safeguarding protocols (when relevant), quality assurance arrangements and a detailed implementation workplan. Outputs: • Inception Report • Integrated National Child Online Safety Assessment Framework • Assessment methodology and indicator matrix • Stakeholder engagement plan • Data collection tools	Within 1 month of contract signature (30 September 2026)
Deliverable 2: Integrated National Child Online Safety Assessment Report	Building on the approved Inception Report, the selected institution shall undertake an integrated assessment of Tajikistan's child online safety ecosystem through evidence collection, stakeholder consultations, analysis and validation. The assessment shall synthesize the findings of the systems assessment and the thematic analysis of AI readiness and emerging digital risks into a single, coherent evidence base. The assessment shall examine, as appropriate: • Governance, legal and institutional arrangements, including institutional mandates, coordination mechanisms, national capacities across the WeProtect MNRF capability areas, maturity assessment, alignment with relevant international standards, and legislative, regulatory and policy frameworks governing child online safety; • Prevention, response and support systems, including prevention initiatives, reporting and referral mechanisms, investigation and prosecution capacities, victim support services, multi-sectoral coordination, engagement with	Within 3 months following the start of the contract (30 October 2026)

Deliverables	Proposed Tasks	Timeframe
	industry and ICT stakeholders, and existing research, monitoring and data systems; • Artificial intelligence, emerging technologies and digital risks, including AI-enabled risks affecting children, AI governance and regulatory readiness, institutional capacity, AI literacy, technological safeguards, digital safety infrastructure, child rights implications, and opportunities for the safe, ethical and responsible use of AI to strengthen child online safety. Based on the findings, the assessment shall identify systemic strengths, implementation gaps and priority areas for strengthening Tajikistan's child online safety ecosystem and provide consolidated recommendations to inform the National Action Plan. Based on the findings, the assessment should identify key strengths, systemic gaps, implementation challenges and priority areas for strengthening Tajikistan's child online safety ecosystem and provide practical recommendations to inform national policy and programming. Outputs: • Integrated National Child Online Safety Assessment Report; • WeProtect Maturity Assessment and scoring matrix; • Integrated analysis of governance, legal, institutional and operational capacities; • Thematic analysis of AI readiness, emerging digital risks and child-centred AI governance; • Consolidated recommendations informing the National Action Plan on Child Online Safety.	
Del 4: National Action Plan on Child Online Safety	Based on the findings of the Integrated National Child Online Safety Assessment, the selected institution shall develop a comprehensive, prioritised and implementable National Action Plan to strengthen Tajikistan's child online safety ecosystem. The Action Plan shall: • Translate the assessment findings into a coherent set of strategic priorities and practical actions to strengthen child online safety, including the prevention of and response to Online Child Sexual Exploitation and Abuse (OCSEA) and other technology-facilitated forms of violence against children; • Integrate measures to strengthen child-centred AI governance, address AI-enabled risks, promote responsible innovation, and support the safe, ethical and rights-based use of emerging technologies;	Within 4 months following the start of the contract (20 December 2026)

Deliverables	Proposed Tasks	Timeframe
	- Define short-, medium- and long-term priorities, with clear sequencing of interventions; - Identify practical, feasible and cross-sectoral interventions requiring collaboration across government institutions, civil society, academia, development partners and the private sector; - Clearly define institutional roles, responsibilities and coordination arrangements for implementation; - Identify resource requirements, capacity-building priorities, implementation arrangements, financing opportunities and strategic partnerships; - Ensure alignment with national development priorities, existing sectoral strategies and relevant international child rights standards and commitments. Outputs - National Action Plan on Child Online Safety; - National stakeholder validation workshop; Final National Action Plan incorporating stakeholder feedback; - Implementation, monitoring and evaluation framework, including indicative priorities, timelines and responsibilities.	

3. Methodology

The detailed methodology for this assignment will be proposed by the selected institution as part of its technical proposal, building on the requirements outlined in this Terms of Reference. The proposed approach may be further refined following the selection and onboarding of the institution. UNICEF will review the proposed methods, and the final agreed methodology will be documented in the inception report.

The methodology should be grounded in the application of the WeProtect Model National Response Framework (MNRF) and Maturity Model as the primary systems assessment framework, and should reflect a mixed-methods, participatory, and evidence-based approach, including desk review, stakeholder consultations, and facilitated self-assessment processes.

The proposed methodology should demonstrate how the Integrated National Child Online Safety Assessment Framework will draw upon the WeProtect MNRF and relevant UNICEF normative guidance and international good practice on child rights, digital governance and artificial intelligence. While the WeProtect MNRF should serve as the primary methodological backbone for assessing national capacities to prevent and respond to OCSEA, the assessment should also incorporate additional analytical domains examining AI governance, AI-enabled risks affecting children, technological safeguards, and opportunities for the safe, ethical and child-centred use of AI. The methodology should clearly explain how these analytical domains will be integrated into a single, coherent assessment process and evidence base.

The selected institution should demonstrate a robust and structured approach to engaging key stakeholders throughout the assignment, working in close collaboration with the Inter-agency Working Group, including representatives of the President's Administration, Agency for Innovations and Digital Technologies, the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Finance, the Ministry of Education and Science, the Ministry of Health and Social Protection, the Prosecutor General's Office (if applicable), and the Office of the Human Rights Commissioner. The methodology should describe how these stakeholders will be meaningfully engaged throughout the assignment, including assessment design (where appropriate), data collection, validation of findings, and development of recommendations.

The methodology should indicate whether and how AI will be used in the implementation of the assignment and how associated opportunities and risks will be managed.

The primary working languages for the assignment will be Russian for engagement with government counterparts and English for communication with UNICEF. The selected institution will be expected to provide regular written updates via email and participate in weekly virtual coordination meetings with UNICEF focal points throughout the duration of the assignment.

Ethical considerations

The assignment shall be conducted in accordance with the UNEG Ethical Guidelines and, where applicable, UNICEF's Procedure for Ethical Standards. Should children be involved in the data collection or otherwise, ethical clearance should be sought by the review team. Consultations with adult institutional stakeholders do not, in themselves, require ethical clearance; clearance applies where the assignment involves research with human subjects, in particular any direct engagement with children.

The following guiding principles shall be applied throughout the assignment:

- Privacy and confidentiality
- Informed consent
- Harm and benefits
- Conflict of interest

The reviewers will explain to participants the purpose and intended use of the assessment and make it explicitly clear that participation is voluntary and that participants may withdraw at any time. Throughout the process, the reviewers should be sensitive to local beliefs, customs and cultural practices and conduct the assignment with integrity, professionalism and respect for all stakeholders.

4. Work plan

The assignment will be carried out over a period ranging from September 2026 to December 2026. The bidders are expected to suggest a work plan with logical sequencing of the key deliverables and activities for this assignment as part of the application, which can be refined at the inception stage.

5. Deliverables and payment schedule

The consultancy will produce the following deliverables:

Deliverables	Timeframe	Payment schedule
1. Inception Report and Integrated National Child Online Safety Assessment Framework	30 September 2026	25%
2. Integrated National Child Online Safety Assessment Report	30 November 2026	50%
3. National Action Plan on Child Online Safety	20 December 2026	25%

UNICEF reserves the right to withhold all or a portion of payment if performance is unsatisfactory if work/output is incomplete, not delivered, or for failure to meet deadlines.

6. Management and supervision

The contracted institution will work under the direct supervision of the Child Protection Section. The Child Protection Officer will serve as the contract manager for this assignment.

The consulting institution should work collaboratively with the Inter-agency Working Group, including representatives of the President's Administration, the Agency for Innovations and Digital Technologies, the Ministry of Justice, the Ministry of Internal Affairs, the Ministry of Finance, the Ministry of Education and Science, the Ministry of Health and Social Protection, the Prosecutor General's Office (where applicable), and the Office of the Human Rights Commissioner.

7. Reporting requirements

The selected institution shall submit all deliverables electronically in accordance with the agreed workplan. UNICEF and relevant government counterparts will review each deliverable and provide consolidated feedback prior to its finalisation and acceptance.

8. Qualification requirements/specialised knowledge/experience required to complete the task

The proposed assignment requires a multidisciplinary team of highly qualified technical experts capable of delivering the assignment in accordance with the purpose and scope of work described in this ToR. Previous successful experience with UNICEF is an asset.

- The company must demonstrate at least five years of experience in delivering assignments of a similar nature and complexity.
- The company must demonstrate capacity to manage multidisciplinary assignments involving multiple technical workstreams and deliver high-quality outputs within agreed timelines.
- Experience in advising or working with multilateral institutions (e.g., UNICEF, World Bank, IMF, UNDP) and/or governments is an asset.
- The company must be able to provide a sufficient number of qualified national and international specialists to deliver the required services, including:

1. Legal Experts: With background in criminal law, industry regulations, and child protection laws in multiple jurisdictions. These are typically distinct legal specialties, so the team should collectively cover criminal, regulatory and child-protection law, with demonstrated capacity for comparative legal analysis rather than transposing a single jurisdiction's model.

2. Technical Experts: knowledgeable about digital forensics, AI and cybercrime investigation, and online safety tools, child protection and social services providers.

3. Child Protection Specialists: expertise in Child Protection case management and specialised social work services, multisectoral case management, child friendly services for victims of violence. Required minimum professional experience for each specialist – 5 years.

- The company must demonstrate experience in conducting complex national or multi-sectoral assessments using internationally recognised assessment frameworks, including the WeProtect Model National Response Framework (MNRF) or comparable frameworks.
- The Company must have demonstrated ability to work with government agencies, particularly in the areas of law enforcement and child protection.
- Fluency in English is required for reporting and communication. Russian-speaking capability is an asset.

4. AI Governance and Child Rights Specialist: demonstrated expertise in artificial intelligence governance, responsible AI, digital rights, children's rights in digital environments, AI risk assessment and safeguarding frameworks.

9. Request for submission

1. A technical proposal with proposed methodology/approach to the assignment, managing the project, showing understanding of the scope of work and work plan (no price information should be contained in the technical proposal).
2. A copy of the organization's profile.

3. The proposed technical team (each) curriculum vitae (CV).
4. A sample of previous work (at least 3 sample products/reports relevant to this assignment) undertaken in the last two years
5. Financial proposal (separate envelope/e-mail).

Evaluation process and methods

The evaluation methodology is based on a highest combined score (based on the 70% technical offer and 30% price weight distribution).

Each interested institution is requested to submit in a one page brief a proposed approach for such assignment along with a copy of the organization profile, the proposed technical team curriculum vitae, expected budget as well as a sample of previous works undertaken in the last two years.

After the opening, each proposal will be assessed first on its technical merits and subsequently on its financial value price. The proposal with the best overall value, composed of technical merit and price, will be recommended for approval. UNICEF will set up an evaluation panel composed of technical and procurement staff and their conclusions will be forwarded to the internal UNICEF Contracts Review Committee or other relevant authorities. The evaluation panel will first evaluate each response for compliance with the requirements of this Terms of Reference. Responses deemed not to meet all of the mandatory requirements will be considered non-compliant and rejected at this stage without further consideration. Failure to comply with any of the terms and conditions contained in these Terms of Reference, including provision of all required information, may result in a response or proposal being disqualified from further consideration.

The overall weighting between technical and price evaluation will be based on the predefined criteria. The technical component will account for 70% of the total points allocated and the financial component (commercial evaluation) will account for 30% of the total points allocated.

Technical evaluation:

The proposals will be evaluated against the following technical criteria:

The Technical Proposals will be evaluated against the following:		
REF	CATEGORY	POINTS
1	Experience of the Firm and Key Personnel Institution:	40
A	Demonstrated experience (at least five years) in child protection, child online safety, Online Child Sexual Exploitation and Abuse (OCSEA), children's rights in digital environments, digital governance or related fields. Proven experience in conducting national or multi-sectoral assessments, policy analysis, baseline studies or systems strengthening initiatives.	20
B	Experience working with government institutions, multi-sector stakeholders, and inter-agency coordination mechanisms including demonstrated experience facilitating multi-sector stakeholder consultations, validation processes and consensus-building involving government institutions and development partners. Demonstrated experience applying international assessment frameworks, including the WeProtect Model National Response Framework (MNRF), the Convention on the Rights of the Child (CRC), UNICEF normative guidance, or other internationally recognised child protection, digital governance or human rights frameworks.	10
C	Qualified multidisciplinary team demonstrating complementary expertise across (i) domain expertise in child protection, child online safety and OCSEA; (ii) assessment expertise in governmental, institutional and legislative legislative analysis; and (iii) technological expertise in digital technologies, cybersecurity and artificial intelligence.	10

	The proposed team should include, at a minimum: • Team Leader (child protection, policy and/or systems strengthening) • Child Online Safety/OCSEA Specialist • Legal and/or Public Policy Expert with experience in legislative and institutional analysis • Technical Specialist with expertise in digital technologies, AI governance and child rights in digital environments.	
2	Proposal Description (Proposed methodology and approach):	30
A	Quality, clarity, and feasibility of the proposed methodology. Demonstrated understanding of the WeProtect MNRF and Maturity Model and their application within an integrated National Child Online Safety Assessment Framework. Strong and practical approach to: • evidence collection and analysis; • stakeholder engagement and multi-sector consultation; • validation and consensus-building; • institutional, governance, legal and technological analysis; • responsible and ethical use of AI throughout the assignment; and • a participatory, child-centred and evidence-based assessment process.	20
B	Detailed workplan, implementation approach and milestones demonstrating realistic sequencing of activities, efficient delivery of the integrated assessment, and timely production of high-quality deliverables.	10
Total Technical		70

Only Proposers obtaining a minimum of 49 points in Technical Criteria evaluation will be considered for the Financial Evaluation.

Commercial evaluation:

The price/cost of each of the technically compliant proposals shall be considered only after evaluation of the above technical criteria. A maximum 30 points assigned to the financial proposal will be allocated to the lowest financial proposal. All other price proposals will receive scores in inverse proportion according to the following formula:

Score for price proposal A = (Maximum score for price proposal * Price of lowest priced proposal)/Price of proposal A.

As a result of the financial evaluation, the points of each proposal will be taken into further consideration in the final evaluation.

The bidders should ensure that all pricing information is provided in accordance with the following:

- The currency of the proposal shall be in USD for international companies and in Tajik Somoni for the local Proposers and invoicing must be in the same currency.
- All prices/rates quoted must be exclusive of all taxes as UNICEF is a tax-exempt organization

REQUEST FOR INFORMATION

Any request for information or question should be forwarded to dushanbe@unicef.org