



**Appendix: Suggested foundations for a digital service framework in the algorithmic age**

Author: Giulio Coppi, Senior Humanitarian Officer, Access Now

The guiding schema proposed as an appendix to this report is a humanitarian digital service framework; a strategic blueprint for planning and managing risks-driven plans considerate of future algorithmic developments and their impacts on people and systems. This foundational framework is designed to be resource, scale, and tech agnostic. It is proposed to support immediate change, but also to inform further research by operational and academic partners involved in humanitarian logistics and supply chain innovation, and internal reflection by aid groups, digital transformation teams and their boards.

The framework is an adaptation of existing procurement guidance models relevant for algorithmic environments such as the AI adoption across mission-driven organisations by Civic Machines Lab, Risk management framework for procuring AI systems by the Centre for Inclusive Change, the MERL Tech assessment of AI vendors, the WEF AI procurement in a box and the WEF Adopting AI responsibly: guidelines for procurement, AI and procurement primer by New York University, the Responsible AI procurement section of the Scottish AI Playbook, Responsibly buying AI guide by the UK Local Government Association, the relevant sections of the NIST cybersecurity standard, and NetHope's humanitarian AI code of conduct. These resources have been processed by Access Now based on the findings presented above and framed through a customised version of the adaptive risk management (ARM) principles.

The proposed framework also has an operational component which is far from conclusive or final, and may never be. This roadmap offers building blocks for any organisation to modify, customise, and develop through an inclusive multistakeholder process. To ensure this research allows any organisation to take the first steps in the right direction, the language in the framework is presented in a format compatible with immediate integration into training design, job descriptions and terms of reference templates. It might also offer a stepping stone to academic researchers interested in further shaping an ARM-inspired humanitarian digital service framework for volatile and high risk environments by developing on top of this concept the already mentioned dynamic capabilities and microfoundations theories.

This living document is proposed in an editable Sheet format and a printable PDF version to allow for a variety of uses and customization options. Please send any feedback or comment to [un@accessnow.org](mailto:un@accessnow.org)

Tech stack management	Digital Procurement / Log	ICT / Cybersecurity	Legal / Compliance	Programmes / Digital Protection	Data Protection
<p>(corresponding <a href="#">NIST AI RMF Functions: Map, Manage</a>)</p> <ul style="list-style-type: none"> <li>- Continuously identifies new tech actors and products/services, evaluates and recommends potential changes to current supply sources and participates in the incorporation of research results into the procurement program.</li> <li>- Monitors pricing and cost policies by providers side and their broader supply chain, keeping a comparative analysis to ensure alternative options are mapped and known</li> <li>- Establishes regular contacts with local and community based tech initiatives</li> <li>- Advises requisitioning units and recipient entities on the full range of procurement issues, providing support and guidance at all stages of the procurement cycle</li> <li>- Monitors compliance with ethical standards and BHR frameworks by providers side and their broader supply chain, ensuring red lines and selection criteria are updated on a regular basis</li> <li>- Runs standard due diligence processes and ensures potential providers perform standard assessment checklists</li> <li>- Publishes contract specifications and invitations to tender alongside the various assessments</li> </ul>	<ul style="list-style-type: none"> <li>- Maps out technologies and, products/services used across the organisation and all data pipelines</li> <li>- Continuously monitor data and metadata flows related to internal systems activity by human and agentic users, manages and oversees access controls</li> <li>- Continuously identifies new technologies, and products/services, evaluates and recommends potential supply sources and participates in the incorporation of research results into the procurement program.</li> <li>- Continuously monitor budget items and projected trends</li> <li>- Establishes regular contacts with local and community based tech initiatives</li> <li>- Advises requisitioning units and recipient entities on the full range of ICT issues, providing support and guidance at all stages of the procurement cycle.</li> <li>- Continuously monitors the respect of cybersecurity and data/digital internal policies involving high risk or high priority servers or databases</li> </ul>	<ul style="list-style-type: none"> <li>- Approves and monitors legal documentation and contracts and supports the development of sector-wide protective standards, participates in the inclusion of research results into the procurement program</li> <li>- Continuously monitor financial reports and detect changes in company affiliations or ownership of the providers or their supply chain that might infringe on policies or generate liability</li> <li>- Ensures consistent <a href="#">inclusion into all tech agreements and contracts of contractual safeguards</a> such as AI usage disclosure requirements, clear ownership terms for data and models, provisions for adapting to future regulatory changes, liability clauses for AI errors or failures, exit options that allow safe termination if the system no longer meets the expected needs or radically alter the data policy, among others</li> </ul>	<ul style="list-style-type: none"> <li>- Oversees internal HRRIAs and/or hHRDD+, their filing, and their updates as needed based on the evolving context</li> <li>- Continuously maps digital trends and habits among communities experiencing vulnerability, and participates in the incorporation of research results into the procurement program</li> <li>- Establishes regular contacts with local and community based tech initiatives, and participates in the incorporation of research results into the procurement program</li> <li>- Coordinates regularly with global and local digital rights network for <a href="#">information sharing and joint incident response planning</a></li> <li>- Supports the identification of high risk applications, databases, or datapoints</li> <li>- Creates community feedback channels for AI systems</li> </ul>	<ul style="list-style-type: none"> <li>- Oversees and monitors DP requirements including DPIAs, their filing, and their updates as needed based on the evolving context</li> <li>- Receives complaints and requests from interested individuals on data management and digital practices</li> </ul>	
Crossfunctional objectives	Ensures continuous monitoring of the digital ecosystem and data flows Collaborate with relevant external experts across sectors to keep abreast of emerging trends and best practices				
Example	A humanitarian NGO provides protection services to refugees and runs a locally hosted digital legal assistance system with algorithmic functionalities to provide customized support in advancing refugees' claims to various services. Measures are put in place to ensure network segmentation and segregation, and the NGO has strict data collection policies and only uses vetted data collection systems by a trusted provider.				
Dynamic risk evaluation & mitigation	Digital Procurement / Log	ICT / Cybersecurity	Legal / Compliance	Programmes / Digital Protection	Data Protection
<p>(corresponding <a href="#">NIST AI RMF Functions: Map, Measure</a>)</p> <ul style="list-style-type: none"> <li>- Continuously evaluates risks on the providers side and their broader supply chain using traditional and advanced/automated techniques</li> <li>- Identifies alerts, risks, and concerns involving current and prospective providers, and their products/services, evaluates and recommends potential supply sources and participates in the incorporation of research results into the procurement program.</li> <li>- Continuously evaluates budget and pricing implications of prospective changes made by the providers and their broader supply chain, including medium to long term signals</li> <li>- Monitors compliance with BHR frameworks by providers and their broader supply chain, ensuring any infraction of red lines and selection criteria detected throughout the project/service lifecycle</li> <li>- Regularly update standard due diligence processes and ensures current providers are up to date with their standard assessment checklists</li> </ul>	<ul style="list-style-type: none"> <li>- Continuously identifies alerts, risks, and concerns involving technologies, and products/services, evaluates and recommends potential supply sources and participates in the incorporation of research results into the procurement program.</li> <li>- Keeps abreast of product pipeline updates, and upcoming system updates/upgrades and their possible impacts on the data lifecycle</li> <li>- Continuously monitor expenses and costs and detect variations and anomalies</li> <li>- Regularly test the respect of internal rules and policies by known systems featuring advanced or enhanced algorithmic components.</li> </ul>	<ul style="list-style-type: none"> <li>- Continuously identifies alerts, risks, and concerns involving leadership or corporate profiles among the current or prospective providers;</li> <li>- Evaluates alerts, risks, and concerns involving legal language proposed by current or prospective vendors, or modifications to such language and participates in the incorporation of research results into the procurement program</li> <li>- Continuously monitor financial reports and detect changes in company affiliations or ownership of the providers or their supply chain that might infringe on policies or generate liability</li> </ul>	<ul style="list-style-type: none"> <li>- Continuously identifies risks on programme and people using traditional and advanced/automated techniques</li> <li>- Coordinates with global and local digital rights network for risk mapping and information sharing</li> <li>- Evaluates and participates in the incorporation of research results into the procurement program</li> </ul>	<ul style="list-style-type: none"> <li>- Continuously evaluates data risks on systems and people using traditional and advanced/automated techniques;</li> <li>- Takes action to investigate concerns about data protection issues both reactively upon receiving claims and requests, or proactively as a result of its own monitoring activity</li> <li>- Evaluates and participates in the incorporation of research results into the procurement program</li> </ul>	
Crossfunctional objectives	Ensures that risk assessments are always current and reflective of the latest data. Collaborate with relevant external experts across sectors to keep abreast of emerging threats and patterns of risk Provides constant monitoring to detect anomalies and deviances presenting potential risks or threats to the digital ecosystem, to data, or to users				
Example	Recently, ICT and procurement teams have received information through their trusted partners network about an increasing number of algorithmic systems being introduced as a result of investments-driven pushes fuelling data harvesting practices. Suddenly, the cybersecurity team notices that following a major update imposed by their data collection system provider, a new functionality for enhanced performances is transmitting (or attempting to transfer) data and metadata to the provider's cloud instead of only storing data in the dedicated locally hosted digital legal assistance system.				
Integration with decision making	Digital Procurement / Log	ICT / Cybersecurity	Legal / Compliance	Programmes / Digital Protection	Data Protection
<p>(corresponding <a href="#">NIST AI RMF Functions: Govern</a>)</p> <ul style="list-style-type: none"> <li>- Regularly report to the organisation board or digital transformation board about emerging and prospective issues with tech providers, partners, or other providers;</li> <li>- Conducts market research to keep abreast of digital market developments; researches and analyzes statistical data and market reports on the global digital market situation, production patterns and availability of products and services possibly affecting the success of the digital strategy.</li> </ul>	<ul style="list-style-type: none"> <li>- Regularly report to the organisation board or digital transformation board about emerging cyber risks and situations needing attention</li> <li>- Conducts private tech sector research to keep abreast of digital developments; researches, analyzes and reports on data and operational trends involving the global cybersecurity situation</li> <li>- Monitors and reports on tech development patterns possibly affecting the success of the digital strategy.</li> </ul>	<ul style="list-style-type: none"> <li>- Regularly reports on critical emerging issues emerging from financial reports and changes in company affiliations or ownership of the providers or their supply chain that might infringe on policies or generate liability</li> <li>- Supports the framing of all decisions in line with compliance and legal requirements, including to donors</li> </ul>	<ul style="list-style-type: none"> <li>- Regularly report to the organisation board or digital transformation board about emerging cyber risks and situations needing attention emerging from direct programme implementation or sectoral information sharing</li> <li>- Regularly reports on emerging challenges in implementing internal policies as part of programming</li> </ul>	<ul style="list-style-type: none"> <li>- Regularly report to the organisation board or digital transformation board about emerging data protection risks risks and situations needing attention</li> </ul>	
Crossfunctional objectives	Integrates risk evaluations into strategic planning and operational decisions Provides up to date and risk-specific metrics to accompany a forward-looking reflection on ways to improve the digital architecture				
Example	The different teams brief the digital transformation board and the leadership of the NGO on the incident, their response to it, and the results of their engagement with the provider. The new functionality cannot be removed as it is now fully embedded in the product architecture through several critical dependencies. The integrated team suggests the replacement of the provider with the best scoring alternative pre-identified by the procurement team.				

Flexible risk governance	Digital Procurement / Log	ICT / Cybersecurity	Legal / Compliance	Programmes / Digital Protection	Data Protection
(corresponding <a href="#">NIST AI RME functions</a> : Manage, Govern)	<ul style="list-style-type: none"> <li>- Oversees adherence to contractual agreements, recommends amendments and extensions of contracts, and advises concerned parties on contractual rights and obligations;</li> <li>- Prepares a variety of procurement-related documents, contracts, communications, guidelines, instructions to reflect eventual changes in the global digital market developments</li> <li>- Makes sure business and human rights (BHR) framework-related red lines and selection criteria applicable to providers are updated on a regular basis</li> </ul>	<ul style="list-style-type: none"> <li>- Supports the development of revised and updated internal guidance on data collection and accompanying training materials</li> <li>- Supports the revision of internal policies and contract templates</li> </ul>	<ul style="list-style-type: none"> <li>- Regularly supervises the revision of internal policies and contract templates, to make sure they are compliant with relevant regulatory frameworks</li> <li>- Supports negotiations with existing providers to improve or implement protecting clauses and terms, but also penalties and termination clauses, and remedy options for impacted individuals</li> </ul>	<ul style="list-style-type: none"> <li>- Makes sure internal policies are informed by and centred onto human rights and protection considerations</li> <li>- Regularly reports on emerging challenges in implementing internal policies as part of programming</li> </ul>	<ul style="list-style-type: none"> <li>- Supports the revision of existing and upcoming policies, processes, and contracts with most protective data protection standards</li> </ul>
Crossfunctional objectives	Supports changes to the digital transformation governance framework Makes sure the legal, policy, and procurement documents are regularly revised and update				
Example	Procurement, legal and compliance teams revise the internal policies and the contract templates with the new provider to include clauses for preventing the introduction of algorithmic systems outside of the oversight of the NGO, and with “opt out consent” as a requirement, with accompanying penalties and termination clauses, and remedy options for impacted individuals in case of future breaches to the agreement. Negotiations to include similar clauses and conditions are started with all pre-existent tech and data providers. Internal guidance on data collection and accompanying training materials are revised and updated.				
Incident management	Digital Procurement / Log	ICT / Cybersecurity	Legal / Compliance	Programmes / Digital Protection	Data Protection
(corresponding <a href="#">NIST AI RME functions</a> : Measure, Manage)	<ul style="list-style-type: none"> <li>- Oversees implications for contractual agreements, and manages the non technical coordination with providers</li> <li>- Plans exit strategy from service provision if appropriate;</li> </ul>	<ul style="list-style-type: none"> <li>- Lead incident response protocol</li> <li>- Provides timely updates and suggests pathways for resolution</li> <li>- Supervises incident impact assessments</li> </ul>	<ul style="list-style-type: none"> <li>- Makes sure incident response respects the most protective ethical practices and is compliant with legal requirements</li> <li>- Monitors and supports legal and compliance requirements for mandatory disclosure</li> </ul>	<ul style="list-style-type: none"> <li>- Continuously monitors potential impacts on people, making sure incident response has protection and human rights at the centre</li> <li>- Supports the Data Protection team in ensuring communications on the incident are properly shared with affected individuals and all relevant stakeholders</li> </ul>	<ul style="list-style-type: none"> <li>- Oversees compliance with data protection incident handling procedures, and existing applicable legal frameworks</li> <li>- Makes sure internal and external communications on the incident are inspired by best operational and ethical practices and compliant with legal requirements on disclosure</li> </ul>
Crossfunctional objectives	Supports incident response efforts centred on protection and human rights considerations Provides timely guidance to all actors not involved in the response to mitigate impact				
Example	Measures are put in place to ensure the data collection system is isolated from the local server and staff is advised to stop using the data collection tool. Procurement engages with the provider to ask for the deactivation of the new algorithmic functionality, and with the other teams try to understand if and to what extent the provider has obtained access to sensitive data. Programmatic teams in coordination with the DPO try to understand if personal data have been impacted, and plan the outreach to the data owners.				
Impact mitigation & remedy	Digital Procurement / Log	ICT / Cybersecurity	Legal / Compliance	Programmes / Digital Protection	Data Protection
(corresponding <a href="#">NIST AI RME functions</a> : Manage)	<ul style="list-style-type: none"> <li>- Leads the exit strategy from a contract if appropriate;</li> <li>- Oversees adherence to contractual agreements, recommends amendments and termination of contracts, and advises concerned parties on contractual rights and obligations;</li> <li>- Shares lessons learned and incident reports with network of digital procurement experts</li> </ul>	<ul style="list-style-type: none"> <li>- Leads implementation of technical mitigation measures</li> <li>- Connects with local, regional, and global digital rights organisations to ensure affected individuals have access to appropriate mitigation support if these are beyond the mandate of the organisation</li> </ul>	<ul style="list-style-type: none"> <li>- Evaluates legal avenues for action against actors responsible if applicable</li> <li>- Monitors the respect of ethical, legal and compliance requirements on incident response, mitigation, and remedy</li> </ul>	<ul style="list-style-type: none"> <li>- Monitors post-incident effects and impacts on affected individuals and communities</li> <li>- Connects with local, regional, and global digital rights organisations to ensure affected individuals have access to appropriate mitigation support if these are beyond the mandate of the organisation</li> </ul>	<ul style="list-style-type: none"> <li>- Monitors post-incident effects and impacts on affected individuals and communities</li> <li>- Monitors the respect of ethical, legal and compliance requirements on incident response, mitigation, and remedy</li> <li>- Ensures proactive follow up to all active cases</li> </ul>
Crossfunctional objectives	Contributes to concrete actions for impact mitigation Facilitates access to remedy by any affected individual				
Example	While the procurement team leads the transition from one provider to another together with the ICT team, programmatic teams in coordination with the DPO inform all affected external individuals and entities, explaining the incident and expected consequences. Teams also explain to impacted individuals the options for remedy available to them, and explain how to obtain further help or protection through digital rights organisations.				