Digital Risk Assessment Product: Invitation to Tender – November 2022

1. Purpose

The Global Interagency Security Forum (www.gisf.ngo) is looking to develop a modular digital risk assessment product for humanitarian security staff (non-digital experts) working in the humanitarian sector ('humanitarian' describes not-for-profit activities that seek to improve lives and reduce suffering.), to assess, understand, and mitigate the risks manifesting from the interaction of digital with physical and personal security risks. The product will consist of (1) a modular guide that will explain how to assess and mitigate different risks stemming from digital and physical security issues and (2) practical tools that can be included into 'traditional' security risk assessment processes to conduct this digital risk assessment in practice.

2. Background

GISF is an independent network of security focal points that represent humanitarian, development, and human rights NGOs operating internationally (from now on, referred to as NGOs or humanitarian organisations). GISF is committed to improving the safety and security of operations and staff, and strengthening humanitarian security risk management (SRM) to allow greater access for crisis-affected populations. GISF acts as a global reference point for good practice and collective knowledge on humanitarian security risk management and, as such, strives to produce inclusive, collaborative, and innovative research for the whole humanitarian community. The GISF Secretariat is hosted by one of GISF's member organisations: the Mines Advisory Group (MAG).

3. Project Description and Scope of the Work

GISF is launching a new research project on the topic of *Security in a Digital World*, exploring the ways in which SRM in the aid sector is changing in response to the opportunities and risks stemming from the digitalised world we live and work in.

As part of this wider project, GISF aims to publish a modular risk assessment product that helps NGO security focal points (SFPs) understand how to assess and mitigate risks stemming from the interaction of digital with physical and personal security risks (from now on, referred to as digital humanitarian security risks).

1. The product should include a modular guide that focuses on different categories of digital humanitarian security risk and how NGO security focal points can address them. The topics covered should be based on a preliminary structure that will be shared with the consultant and the modules should link digital risks back to 'physical' security issues while providing case studies, practical examples, and templates/tools to address them.
2. The product should also include practical 'tools' that take the user through a coherent digital risk assessment process. Tools should be easy to integrate into 'traditional' security risk assessment processes and address the different risks outlined in the modules.

The product should be useful for 'humanitarian' NGOs across the sector, irrespective of their size or mandate. As the product will be used by non-digital experts (i.e., existing global, regional, and country-level security leads), it should bridge the gap between traditional and digital security tools and processes and be relevant in their line of work. As the product needs to be tailored to different contexts and digital risks are quickly evolving, the product should provide guiding questions helping users identify the answers relevant for their context.

The product will be initially developed in English with the aim to translate it into French, Spanish, and Arabic, subject to capacity and budgetary requirements. However, the consultant is not expected to manage the translations but only assist in identifying individuals who can proofread the translations and ensure they make sense.

This project will be delivered and led by the primary consultant or the consultant team. At the same time, GISF will oversee that the project meets the goals. The work will be supported by a working group comprised of digital and security experts. See below for details.

The consultant or the consultant team is responsible for preparing and delivering the product in line with the project's objectives, as outlined in the ToR. This includes developing and writing the modules and accompanying instructions, identifying (with the input of GISF and the working group) module topics, and liaising with working group members who may support the work on specific modules where necessary and possible. The consultant will also provide feedback to all those working on the product ensuring that the content is coherent and meets the project's objectives, and the feedback of the working group and GISF is incorporated. Moreover, the consultant will develop practical tools that will include the topics identified in the module and that can be included into 'traditional' security risk assessment processes. The consultant will prepare, organise, and lead meetings with the working group and present the product to the GISF membership.

The consultant will also support GISF in identifying and reaching out to organisations to trial the product, and incorporate feedback voiced in response to the piloting phase.

GISF will supervise the consultants' work to ensure the final product meets the project's objectives. This will include reviewing and providing feedback on drafts. GISF can support facilitating engagement with the working group from the administrative side, in terms of setting up meetings. However, the consultant is primarily responsible for ensuring that if working group members contribute to the writing of modules, they are meeting the project objectives and are implementing feedback.

GISF will also be responsible for contracting an editor if necessary and a designer once the product's content has been finalised.

The working group will provide overall oversight of the project, ensuring the final outputs meet the needs of GISF members and the broader aid sector. The working group will provide input into the overall product development, including the initial project outline document, the draft of the modules, and the tools. Members of the working group may contribute to the drafting of modules, where fitting.

Following the second draft of the product, it will be piloted by at least four organisations with different mandates and different sizes. These organisations will be determined by GISF and the consultant. Following the piloting, further changes will be made to the product, if necessary, by the consultant.

Overall, the project aims at:

1. Providing NGOs with an easy-to-understand and practical guide and tools that can be integrated into 'traditional' security risk assessment tools and allows them to assess how physical security risks are impacted by digital risks and vice versa.
2. Identifying and creating specific modules covering elements critical to maintaining and advancing an NGO's security in a digital world.
3. Providing concrete guidance and demystifying processes for organisations looking to improve their understanding and response to the risks they face in a digital world.

Scope:

- The digital risk assessment product should be useful to humanitarian organisations, regardless of their size and mandate.
- The product should be designed to be used by non-digital security experts and should bridge the gap between digital, physical, and personal security.
- The modules should cover all the elements critical to maintaining and advancing an organisation's security in a digital world.

Publication format:

- The publication will be composed of multiple modules, with each module focusing on a specific element of humanitarian digital security and an overall descriptive piece explaining the structure and practical tools to use to conduct a digital risk assessment.
- The modules will be based on the knowledge and analysis of digital and security experts.
- The modules will fit together appropriately and coherently to create a comprehensive digital risk assessment guide and tools for humanitarian security leads.
- The modules will also include practical templates on specific risks.
- The product should be easy to understand for staff from different backgrounds and those unfamiliar with technical terms related to digital and cyber security.
- The publication should follow the style of GISF guides, be easy to read, and visually appealing with text being broken down into smaller sections.
- It might be a possibility to digitise the guide and tools in the future in a similar format to the NGO Security Toolbox.

4. Deliverables/Timeframe

Deadline	
28.11.2022	Tender launch
12.12.2022	Confirmation of tender submission
03.01.2023	Invitation to tender submission deadline
09.01.2023	Tender review and vendor selection

13.01.2023	Final requirements agreed with GISF
28.02.2023	The consultant develops draft 1 of the product in accordance with GISF and the working group
14.03.2023	The working group and GISF review draft 1 and provides the consultant with feedback
01.05.2023	Incorporating the working group and GISF's feedback, the consultant develops draft 2 of the product in accordance with GISF and the working group.
15.05.2023	The working group and GISF review draft 2 and provide the consultant with feedback
05.06.2023	Incorporating the working group and GISF's feedback, the consultant develops draft 3 of the product in accordance with GISF and the working group.
16.06.2023	The consultant with the help of GISF create a testing group of NGO security advisors to pilot draft 3 of the guide and tools. Piloting takes place and feedback is provided to the consultant.
15.07.2023	The consultant supports in the the identification and selection of Spanish, French, and Arabic translators and proof-readers of the product.
31.07.2023	Incorporating the feedback of the piloting stage, the consultant develops the final draft of the product in accordance with GISF and the working group.
15.08.2022	Sign-off by GISF with the guidance of the working group
01.09.2023	Edit and design

GISF and the consultant will have regular feedback sessions during this period to monitor progress and make amendments to the tool where necessary. The consultant will also have regular meetings (approximately every 4 weeks) with the working group and GISF to incorporate the working group's feedback and ideas.

5. Confirmation of Tender Submission

All potential vendors are **requested to confirm by 12.12.2022** whether they intend to submit a tender or not. Confirmation should be sent to gisf-research@gisf.ngo, copying in gisf-americasra@gisf.ngo. Failure to confirm by this date may disqualify vendors from consideration of their subsequent tender submission.

6. Tender Submission

Tenders and supporting documents must be submitted via email to gisf-research@gisf.ngo. **Final date for the receipt of tenders is 19.00 pm GMT on January 3rd, 2023.** Only complete

submissions meeting the eligibility requirements will be considered. Tenders shall not exceed 15 pages plus appendices, and should at minimum contain:

- An implementation plan outlining the timeframe and milestones.
- A company/consultant profile focused on information relevant to this tender.
- Detail the experience of proposed team members or consultant.
- Examples of previous similar or relevant products developed.
- A detailed financial proposal including costs for all services provided and a clear explanation of how work is charged.

All costs must be included in the tender offer. The costs are to be specified in pound sterling, excluding VAT. If VAT is applicable, indicate the VAT % to be charged separately (i.e., not included in the price of services). Costs associated with the preparation of the tender will not be reimbursed.

All tender offers must be valid for a minimum of 90 days from the tender submission deadline date.

7. Tender Analysis and Evaluation

GISF will consider several factors when analysing suitable tenders, including:

- Understanding of the product requirements.
- Relevant experience of the company/consultant and/or project team.
- Timeframe for completion.
- Value for money.
- Communication with GISF.

Once tenders have been submitted and received, they will be evaluated by a Tender Committee. The scoring and weighting used to evaluate each tender is outlined in the following table.

	Evaluation Criteria	Maximum Marks
	Tender documents	10%
	Understanding of GISF's requirements	20%
	Proposed design, implementation plan, timeline, and price	40%
	Proposed consultant's or development team's expertise	30%
	Total	100%

At the discretion of GISF, selected vendors may be invited to supply additional information on the contents of their proposal during the evaluation period. If no suitable tender is identified, the invitation for tender may be reopened and advertised on a broader level.

Upon identification of the preferred tender, the selected vendor will meet GISF to finalise the requirements and agree on contract terms.

Selection and notification of the preferred tender does not guarantee that GISF, MAG, and the selected vendor are engaged in contract for the procurement of the goods and services.

8. Contract Conditions and Payment Terms

Upon confirmation of the successful tender, the chosen vendor will sign MAG's Contract for the Procurement of Services and must comply with MAG's Terms and Conditions and MAG's Policies.

The provision of this work will be undertaken in accordance with MAG's standard payment terms, which is 30 days upon receipt of an invoice. Payment will be made in pound sterling. The maximum budget is 20,000 £.

Payment for services will be in instalments dependent on the successful completion of specific milestones:

- 30% upon the signing of the contract.
- 50% after the submission of the second draft.
- 20% upon submission and signing off of the final draft.

Ownership of the final product will reside with GISF, this includes copyrights and patents associated with the product.

Any questions regarding GISF's requirements or the tendering process should be submitted in email to gisf-research@gisf.ngo.

Annex 1

Preliminary Structure - Digital Risk Assessment Product

Date: 16.11.2022

Note: This preliminary structure is based on topics of concern raised by the working group and the GISF membership. This preliminary structure intends to guide the working group's conversations and to provide the consultant with an overview of relevant issues that should be addressed as part of the product, however, the structure might change and evolve.

What should be included in every module?

- Outlining who, what, why, when, where – introduction to the topics
- Every module should answer what the topic means for 'traditional' security risk management (SRM) and how it could be impacted
- Every module should include examples and case studies of how the digital environment and the physical environment are linked and practical tools/templates

Module 0 - Introductory module

- Aim of the product
- Why is this important
- What is a digital risk assessment and how does this form part of your 'traditional' security risk assessment?
- How can you use this product?

Module 1 - What is your digital environment and how to do a digital risk assessment? Integrating digital security into your security processes.

- Things you start off with in an organisation directly impacting your digital security

    - Hardware (age, model, phone, desktops, laptops, bring your own device - BYOD, …)
    - Software (source: corporations such as Microsoft, own applications, open source, redundancy and patch updates, etc.)
    - Internet connectivity (what providers, bandwidth, VPN, hot spots, free wifi…)
    - Use of online platforms (social media,
    - Smart offices (biometric tools, digital keys, …)
    - IT support and IT regulations and policies (backup policy, password policy, …)
    - Internet connection and setting (ie use of wi-fi, office/home setting, firewall, etc.)
    - Use of information security software to protect user & identity: antivirus, VPN
    - Password and access management
    - Knowledge/skills/maturity level in cybersecurity

-Glossary of IT terms? – defining the terms

-Based on this foundation, vulnerabilities can be identified and how to address them. We could work with checklists. On other points, such as internet connectivity, guiding questions should be provided and/or guiding principles (that might be elaborated in the further modules).

-How does this relate to a context analysis?

-Regular security risk assessment processes and how these topics fit in – questions to ask

Module 2 – Integrating digital risk detection and prevention into your digital processes (more externally focused)

-Some of the main risks impacting humanitarian NGOs (individual basis and organisationally)

- Misinformation/disinformation
- Phishing
- Hacking - targeting of humanitarians online on social media – personal element vs institutional element – indiscriminate element
- Internet access points

-Analysing your threat landscapes and legal landscapes (can you use VPNs everywhere etc?) – how do you include the right questions in your context analysis?

-mitigation measures

Module 3 - Governance, organisational structures, and incident and crisis management

-Duty of care in the digital space

-Do organisations need a cyber manager? What are the different organisational models to manage these issues?

-Who holds the ultimate responsibility for digital security?

-How should an organisation govern itself to protect against digital security threats?

-Where can you look for support or find the right information?

-Case studies and scenarios. Mitigation and response. Reporting and Sharing.

-How is this different from traditional security reporting?

-How do you encourage internal reporting? Who needs to be involved?

-How do you report in the absence of regular communication channels?

Module 4 – Data protection and data hygiene (focused on the organisation)

-Mapping the data you have, where it is, and who has access to it

-Legal basics

-IFRC data play book

-GDPR

-Technical guidance

-Working with partners

Module 5 – Operational issues and confidentiality (focused on the individual); communications technology

-What are the risks?

-Best practices: digital hygiene

- Data detox, settings on smartphone and other devices.
- Where to talk about what and the importance of understanding confidentiality.

-Communications technology – what do you use for travel?

-Person-centred approach and duty of care

-Gender, diversity and adverse environments. Censorship and surveillance.

-Travel

-Comms and internet shutdowns

-Social media

Module 6 – Navigating the humanitarian cyberspace as a sector

-Training

-Inter-agency collaboration and information-sharing

-Case studies of NGOs working together

-Sources of support

Practical Digital Risk Assessment Tool(s)

- Tool(s) that combines all these module elements in one process in one form/tool

<u>Other potential topics:</u>

-Insurance?

-Working with partners