NORWEGIAN REFUGEE COUNCIL

KOBLI Legal Aid Platform Cybersecurity Incident Response Plan (Tactical) - Consultancy

Terms of Reference

1 Background information

The Norwegian Refugee Council (NRC) is an international humanitarian organization helping people forced to flee. Through its programmes, NRC addresses immediate humanitarian needs, prevents further displacement, and supports durable solutions. One of NRC's key programmes is Information, Counselling, and Legal Assistance (ICLA), which enables people affected by displacement to claim and exercise their rights through information provision, legal counselling, individual case assistance, collaborative dispute resolution, capacity building, and advocacy.

Traditional legal aid services in the humanitarian context have largely depended on in-person delivery. These models are resource-intensive and often limited by geographic, security, or time constraints, while the legal needs of displaced populations continue to grow. In response to these challenges, NRC launched a digital transformation initiative in 2018 to explore how technology could expand the reach and efficiency of ICLA services.

This initiative began under the Dream Design Deliver (DDD) framework, facilitated by NetHope in partnership with Microsoft and Accenture. The DDD process started with a strategic visioning session in Oslo in June 2018, followed by a user-centered design process involving ICLA teams in Kenya, Iraq, and Ukraine. In 2020, key design concepts were tested in a pilot project in Colombia using off-the-shelf digital tools.

After completing the design phase in late 2020, NRC procured a software development partner to build a bespoke digital platform. Development began in 2021, with Lebanon selected as the lead country for field collaboration.

The resulting platform, named KOBLI (derived from the Norwegian verb *å koble*, meaning "to connect"), includes three core digital components:

1. **Content Management System (CMS)** – A backend system used by ICLA teams to publish and manage legal content. It enables country programmes to launch standalone legal information websites, set up chatbots, and integrate content with social media platforms. This allows for timely and localized dissemination of legal information to displaced populations.
2. **Legal Case Management System (LCM)** – A workflow tool used by NRC caseworkers to manage individual legal cases. It supports the full case lifecycle, from initial intake and registration through follow-up and closure, and allows for structured documentation, secure data handling, and programmatic reporting.
3. **User Portal** – A secure digital interface for beneficiaries that allows individuals to access the status of their legal cases, communicate directly with NRC caseworkers, and use self-help tools to obtain relevant legal information and documents.

Together, these components enable NRC to extend the reach and effectiveness of ICLA programming, especially in contexts where access to in-person services is limited.

The first version of KOBLI was delivered by the end of 2021 and underwent several rounds of quality assurance, including penetration testing, code audits, and user feedback. The platform was officially launched in May 2022, starting with a limited rollout in Lebanon. Since then, deployment has expanded to several additional countries.

As of mid-2025:

- The Legal Information Platform (CMS + Digital Access (DA) Platform) is live in Ukraine, Lebanon, Jordan, Iraq, Egypt, and Moldova. None ICLA programs have also been using the CMS module, for example, Ukraine Cash Team, Sudan Cash Team, and Education team in MENA.
- The Legal Case Management (LCM) system is used by ICLA teams in Jordan and Uganda in 2025, and it is intended to expand to Ukraine later this year.
- The User Portal is currently being piloted in Syria, where it will allow users to store sensitive legal documents securely in the cloud.

KOBLI is developed as a proprietary digital platform, owned by NRC. The source code and underlying architecture are fully under NRC's control. The platform is hosted on NRC-managed servers and maintained by a third-party vendor contracted directly by NRC.

2 Purpose of the Consultancy

The KOBLI digital legal aid platform has grown significantly since its launch, with several NRC country offices now actively using its core modules to deliver legal information and manage legal aid cases. This growth results in a need for a comprehensive cybersecurity incident response plan that is tailored to KOBLI but also integrates with NRC's existing incident and data breach response procedures.

Following are the main objectives of this consultancy:

1. Produce a set of tactical response playbooks and supporting documents and templates to guide the KOBLI team in detecting, responding to, and documenting cyber security incidents.
2. Establish clear roles and responsibilities and escalation paths.
3. Train relevant staff on incident detection, response, escalation, and documentation protocols.
4. Perform a full review of the current KOBLI SLA and propose changes to include incident response in its scope.
5. All above documents and procedures must align with the following documents:
    - NRC Incident Taxonomy.
    - Overarching Incident Management SOP.
    - Data Breach Management Procedure.

3 Scope of Work

3.1 Inception

The consultant should start with reviewing existing infrastructure, system, and process documentation, meet with the development team, then conduct stakeholder interviews to understand Digital ICLA operations, context, and NRC's incident response framework.

Moreover, the consultant will examine the current KOBLI SLA to determine needed changes.

The result of this phase is an inception report that outlines the next steps.

In the inception report, the consultant will include the following:

1. A risk assessment which illustrates identified attack vectors.
2. A proposed list of attack types that will be the focus of the response playbooks.
3. A proposal of how KOBLI's incident response will integrate with existing NRC incident response.
4. An overview of proposed key changes in the SLA to include incident response in the scope.
5. A proposal of any additional documents deemed necessary by the consultant.

NRC approval of the inception report is required before moving on the next phase.

3.2 Incident Response Artifacts

Once the inception report is approved by NRC, the consultant should then develop the actual response artifacts which include at minimum:

#	Artifact	Purpose
1	Detection Metrics & Thresholds Catalog	Defines exactly what to monitor, including metrics, log sources, thresholds, and alert logic.
2	Attack Detection & Triage Matrix	Helps correlate alerts with potential attack types and map to ATT&CK techniques. Guides initial classification decisions.
3	Incident Classification and Severity Matrix	Assigns a severity level to each attack type based on business impact. Guides response urgency and escalation paths.
4	Incident Response Playbooks	Provide step-by-step response guidance for each attack scenario, including containment, eradication, investigation, and recovery. Those playbooks must consider any 3rd-party tools used as part of KOBLI and include response steps related to them where applicable.
5	Post-Incident Report & Lessons Learned Templates	To standardize after-action reports and integrate findings into future metrics/playbooks.
6	Roles, Responsibilities & Escalation Guide	To determine who does what in case of an incident and how it is escalated.
7	New KOBLI SLA	A modified version which includes incident response in the scope.

Additional notes:

- In addition to the above artifacts, the consultant may suggest additional or alternative artifacts based on their initial assessment and business needs of KOBLI.
- It is preferable that the above artifacts are based on the MITRE ATT&CK framework where applicable.
- Suggested Incident Response Playbooks include:
    1. Unauthorized access to client account.
    2. Unauthorized access to staff account.
    3. Suspicious AWS or bastion host activity.
    4. S3 exposure due to misconfiguration.
    5. MongoDB compromise.
    6. Phishing attack on staff account.
    7. Denial of service attack.
    8. Ransomware attack.
- The consultant may add to/remove from the above list as needed.

3.3 Staff Training

The consultant should train relevant staff on:

1. Detecting attacks using the Attack Detection & Triage Matrix.
2. Prioritizing incident response based on the Classification and Severity Matrix.
3. Executing the response playbooks.
4. Documenting incidents based on the documentation templates.

The consultant will handover the artifacts and other documents after the training.

3.4 Complete Timeline

Dates (TBC)	**Activity**
5th September	ToR finalized and approved
16Th September	Public Webinar on TOR (https://kobli.no/en/page/cirp-webinar)
30Th September	Call for proposal and tender process closes
1st – 15th October	Bid Evaluations and Interviews
15th October	Contract signed & Consultancy Starts
TBD	Inception phase
TBD	Development of Artifacts
TBD	Staff Training & Handover
On Successful Handover	Contract ends

4 Optional Phase Two – Implementation Support

In addition to the scope of work described above, the consultant is requested to include in their proposal a separate financial offer for a potential follow-up engagement (Phase Two).

Phase two would involve supporting the implementation of the playbooks and other documents. Activities in this phase could include (but are not limited to) support in setting up monitoring, attack simulations, or further capacity building.

While a decision on Phase Two will be made after the completion of Phase One and internal review, we request that the consultant include quotation for daily rates of their team members with different expertise that will be potentially required for phase two of this project.

5 Management & Budget of the review

This consultancy is being launched by the Global ICLA team at NRC Head Office. The maximum budget for this work is USD 20,000.

6 Deliverables

The expected minimum deliverables for this consultancy include:

1. Inception report.
2. Detection Metrics & Thresholds Catalog.
3. Attack Detection & Triage Matrix.
4. Incident Classification and Severity Matrix.
5. Incident Response Playbooks.
6. Post-Incident Report & Lessons Learned Templates.
7. Roles, Responsibilities & Escalation Guide.
8. Revised SLA with incident response in scope.
9. Presentation and training (1 or more workshops) to relevant staff.
10. Any other artifacts the consultant deems necessary.

7 Application requirements

Interested consultants or firms must submit a complete proposal that includes the following:

1. Relevant Experience and Similar Work: The proposal must demonstrate that the consultant or firm has conducted similar assignments.
   - For each assignment: a brief summary, timeframe, client name, and the consultant's role.
   - Links to final reports or deliverables (if public or shareable) are encouraged.

2. CV(s) of Consultant(s)
    - CVs of all proposed team members, highlighting their specific experience with cyber security incident response planning.

3. Two Financial Proposals
    - Separate proposals for phases one and two.
    - Detailed budget, indicating daily rates, expected number of days, and any other associated costs.

4. Legal and Administrative Information
    - Company registration number or consultant tax ID.

8 Application process and deadlines

Application Deadline: Before midnight 30th September 2025 (Oslo Time)

Webinar Session to discuss TOR (Optional): 16th September 2025 at 2:30pm (Oslo Time) (sign-up here and you will receive the zoom link: https://kobli.no/en/page/cirp-webinar)

Selection Process: 1st October – 15th October.
Submit completed applications to nrc.digitalicla@nrc.no

NORWEGIAN
REFUGEE COUNCIL

www.nrc.no

Norwegian Refugee Council
Postboks 148 Sentrum
0102 Oslo, Norway