NORWEGIAN REFUGEE COUNCIL

KOBLI Legal Aid Platform Cybersecurity Incident Response Operationalization

Terms of Reference

1 Background information

The Norwegian Refugee Council (NRC) is an international humanitarian organization that supports people forced to flee by providing aid, protection, and long-term solutions to displacement.

The Information, Counselling, and Legal Assistance (ICLA) programme enables displaced people to understand, claim, and exercise their legal rights through legal information, counselling, case support, and advocacy.

KOBLI is NRC's digital legal aid platform designed to scale and modernize ICLA services.

At its core is a Legal Case Management system that supports the full lifecycle of legal cases - from intake and registration to follow-up and closure - while ensuring structured workflows, secure handling of sensitive data, and programmatic reporting.

KOBLI handles highly sensitive personal and legal data of displaced populations, making it a high-risk system from a security and data protection perspective.

As the platform scales across countries and introduces features like case management and user-facing portals, the attack surface and potential impact of incidents increase significantly.

Digital ICLA has recently completed a cybersecurity consultancy to establish the foundations of an operational Cybersecurity Incident Response Plan (CIRP) for the KOBLI platform.

The consultancy included a comprehensive gap assessment to:

- Understand the system architecture and threat surface.
- Define the scope of incident response.
- Identify technical and operational gaps.

As a result, a set of CIRP artefacts has been developed to define NRC's target incident response operating model. These artefacts include:

- Incident Detection Catalogue.
- Incident Triage Matrix.
- Incident Severity Classification Model.
- Incident Response Roles & Responsibilities.
- Monitoring & Alerting Requirements.
- Evidence Preservation & Forensics Guidelines.
- Incident Response Playbooks (covering 10 attack scenarios).

These artefacts are custom designed for NRC/KOBLI and form the authoritative basis for incident detection, triage, and response.

2 Purpose of the TOR

At this stage, KOBLI has the basis for an operational incident response protocol, but it still doesn't have SIEM tools or SOC capabilities to perform effective incident response.

The purpose of this ToR is to procure a qualified **Security Operations Center (SOC) / SIEM services provider** to operationalize the CIRP artefacts produced in the previous consultancy and establish a fully functional, continuous incident monitoring and response capability.

The selected provider is expected to:

- Propose a set of **SIEM tools and SOC model** for operationalizing the existing artifacts.

- Integrate said SIEM tools and SOC model with KOBLI for log ingestion, alerting, incident response, management and documentation.
- Provide **24/7 monitoring, detection, and response services** using the proposed tools and platform.
- Operationalize KOBLI's **Detection Catalogue, Triage Matrix, and Playbooks**.
- Deliver **actionable reporting and continuous improvement**.

The end-state objective is a **mature, measurable, and continuously improving SOC capability** aligned with NRC's governance and incident response framework.

3 Scope of Work

The scope of work is structured into three main components:

3.1 Initial Setup and Onboarding

This phase is a one-time implementation activity to establish the SOC platform and integrate with KOBLI.

The service provider shall perform the following:

3.1.1 SIEM Platform Deployment & Integration

- Provision and configure a SIEM platform.
- Integrate all relevant KOBLI log sources, including (but not limited to):
  - Application logs.
  - Authentication/IAM logs.
  - Cloud infrastructure logs (e.g., AWS CloudTrail, WAF, etc.).
  - Database and API logs.
- Ensure reliable log ingestion, normalization, and retention.

3.1.2 Detection Engineering Implementation

- Translate NRC's Incident Detection Catalogue into SIEM correlation rules.

- Map detection rules to the Incident Triage Matrix and severity model.
- Implement alerting logic aligned with S1–S4 severity classification.

3.1.3 Dashboard Configuration

- Configure SOC dashboards in line with KOBLI's Monitoring & Alerting Requirements.
- Provide role-based dashboards for:
    - SOC Analysts (L1/L2).
    - Incident Commander / SOC Lead.
    - Management and Compliance.

NRC approval of the initial setup is required before moving on the next phases.

3.2 Incident Monitoring and Response (Ongoing Services)

This is a continuous service covering **24/7 SOC operations**.

3.2.1 Monitoring & Alert Management

- Continuous monitoring of SIEM alerts and security events.
- Initial triage using NRC's **Triage Matrix.**
- Escalation of validated alerts to L2.

3.2.2 Investigation & Incident Handling

- Perform in-depth investigation of escalated incidents.
- Correlate logs across multiple sources.
- Classify incidents according to KOBLI's **Severity Model (S1–S4).**
- Incident documentation and reporting.

3.2.3 Threat Analysis & Forensics

- Conduct root cause analysis (RCA).
- Perform log, network, and system-level analysis as needed.
- Preserve and document evidence.

3.2.4 Incident Response Support & Coordination

- Recommend and/or execute containment actions such as IP blocking, Account suspension, Access revocation, etc.
- Coordinate with NRC internal stakeholders:
    - Incident Commander.
    - IT / Cloud Operations.
    - Application Owners.
- Support incident response bridge calls for high-severity incidents.

Important: Final decision-making authority remains with NRC (e.g., Incident Commander), in line with defined roles.

3.3 Continuous Improvement & Periodic Maintenance

The provider shall ensure that detection and response capabilities remain effective over time.

3.3.1 Detection Engineering & Tuning

- Periodically review and optimize correlation rules.
- Reduce false positives and alert fatigue.
- Improve detection coverage and quality.

3.3.2 Platform Health & Log Management

- Monitor log ingestion, pipeline health, and data quality.
- Support onboarding of new log sources.
- Ensure continuous availability of monitoring capabilities.

3.3.3 CIRP Artefact Review

- Recommend updates to:
    - Detection Catalogue.
    - Triage Matrix.
    - Response Playbooks.
- Align improvements with evolving threat landscape and operational lessons learned.

4 Key Deliverables

4.1 Initial Setup

- Fully operational SIEM/SOC platform.
- Integrated log sources and data pipelines.
- Implemented correlation rules aligned with NRC artefacts.
- Configured dashboards, alerting, and incident management.

4.2 Incident Monitoring & Response

- 24/7 monitoring and alert handling.
- Incident tickets and escalation records.
- Incident reports (for escalated cases).
- Root Cause Analysis (RCA) reports (for S1/S2 incidents).
- Post-incident review reports.

4.3 Continuous Improvement & Periodic Maintenance

- Periodic detection tuning reports.
- Updated or newly developed correlation rules.
- Recommendations for CIRP artefact updates.

5 Application Process, Requirements & Deadlines

Send applications to: nrc.digitalicla@nrc.no

Application deadline: **31/05/2026 before midnight Oslo time**.

Application requirements:

1. Technical proposal outlining the following:
    a. Consultant's understanding of the assignment and their ability to provide the indicated deliverables.

b. Consultant's understanding of GDPR and a description of their approach in complying with data protection requirements during SOC operations.
c. Proposed deployment model of tools and staff (e.g. on client side or provider side, dedicated or shared staff, etc.)
d. Proposed SLA KPIs.
e. Any other proposed services such as threat hunting, threat intelligence, etc.

2. Financial proposal outlining:
    a. The cost of the initial setup, if any.
    b. Annual cost of the ongoing services.
    c. Estimate of any potential increases in annual cost.
3. Business profile showcasing the consultant's relevant experience. Specifically:
    - Experience in providing SOC operations with list of key clients and services provided.
    - Experience providing incident response for AWS-based applications.
    - Experience with data protection and GDPR compliance.
    - Certifications held by relevant staff members.

www.nrc.no

Norwegian Refugee Council
Postboks 148 Sentrum
0102 Oslo, Norway