TIL ORGANISASJONEN

Etter et stort og omfattende arbeid kan vi endelig dele Røde Kors sitt støtteverktøykonsept for beredskap og aksjoner med hele organisasjonen. Dokumentet som følger er hoveddokumentet («cover letter») som danner grunnlaget for tilbudene fra leverandørene.

Det er viktig at dere forstår at det som beskrives her er våre krav, og ikke nødvendigvis helt likt den endelige løsningen. Denne får vi ikke på plass før etter vi har valgt hvordan støtteverktøyene skal leveres og av hvem til høsten. På tirsdag 30/april sendte vi ut forespørsel om tilbud til et titalls nasjonale og internasjonale og leverandører. Tilbudsprosessen skal etter planen avsluttes i løpet av september. Etter dette starter selve arbeidet med å utvikle og levere systemene.

REQUEST FOR PROPOSAL

Incident Preparedness and Response Management System

Norwegian Red Cross

1. INTRODUCTION

Norwegian Red Cross invites your company (Respondent) to submit a response to this Request for Proposal (RFP). The purpose of this RFP process is to get solution proposals from the market that will allow Norwegian Red Cross to meet requirements for a new incident preparedness and management system.

This RFP's scope covers several areas within an incident preparedness and response management system. The Respondent must be very specific about which part(s) of the application scope he can deliver. The following application scope is included in this RFP and consist of three loosely coupled systems integrated using open APIs.

2. DEFINITIONS & ABBREVIATIONS

AMS	Alert Management System
COTS Application	Commercial off-the-shelf Application
IAM	Identity and Access Management
IC	Incident Commander
ICS	Incident Command System
IPRMS	Incident Preparedness and Response Management System
IPMS	Incident Preparedness Management System
IRMS	Incident Readiness Management System
NRC	Norwegian Red Cross
OIDC	OpenID Connect, an authentication layer on top of OAuth 2.0, which is an authorization framework.
PII	Personal Identifiable Information
RBAC	Role-based access control
RFP	Request-For-Proposal
Respondent	A partner that responds to this RFP
SaaS	Software as a Service. Subscription based software which is centrally hosted

3. ATTACHMENTS

1	Norges Røde Kors årsrapport 2017 (no)
2	Norwegian Red Cross Annual Report 2017 (eng)
3	Norwegian Red Cross RFP Domains and Scenarios
4	Norwegian Red Cross RFP Product Requirements
5	Norwegian Red Cross RFP Roadmap for future releases
6	Norwegian Red Cross RFP Product Pricing - Delivery Method and Service Operation

4. NORWEGIAN RED CROSS

4.1 Introduction

The Norwegian Red Cross is a national association of the world's largest humanitarian aid organization; The International Red Cross and Red Crescent Movement. The organization is in 191 countries and has around the world approx. 100 million members and volunteers. The basic idea of the Red Cross is to prevent and alleviate human suffering, both in local communities and in international conflicts.

Currently, the Norwegian Red Cross has about 130,000 members and 40,000 volunteers divided into different activities. The Red Cross is organized with headquarters in Oslo, 19 district offices and approx. 400 local chapters around the country. The number of employees is more than 700 on a national basis. See also www.rodekors.no for more information (in Norwegian).

The Norwegian Red Cross preparedness structure is organized in three levels: tactical, operational and strategic. The tactical level involves the management of the organization's activities at local level (usually one Norwegian Red Cross local office per municipality), and it is the local office that most often is closest to the location where the incidents take place. Operational preparedness work is organized at district level (usually a Norwegian Red Cross district per county). This level has a more coordinating role if there are more local offices involved and should plan a bit further in time. Strategic preparedness work is primarily at the national level and is rarely involved before further coordination is required between several districts or when an event is of a national scale.

One of Norwegian Red Cross' current main objectives is to strengthen the volunteer work and to support the volunteers work processes by making smart future proof digital solutions and tools available. This can be achieved by:

- Digitalize communication and work processes
- Ensuring that solutions have high standards of ease of use
- Focus on self-service, with no need for user support

"Digital Volunteering" is an internal program that supports the Norwegian Red Cross' digitalization strategy for volunteers, and the "Incident Preparedness and Management System" is one the program's on-going projects that requires one or more IT components.

4.2 Preparedness and Incident Response

To ensure the correct type and amount of incident response capacity is always available (preparedness), a continual process must be maintained and executed. When an incident occurs that requires an immediate and coordinated response, our volunteers and employees must be alerted concurrently as soon as possible. Incident Commander (IC) need to communicate the situation accurately and precisely to all personnel on call, where to meet, which personnel are coming and when. Concurrently, IC starts planning the response, and when personnel arrive, allocate them to response units, assign missions to these units and continue this process until the incidents is resolved. After large scale incidents which affects the community at scale, the Red Cross also delivers on long-term support and services to the community. These services are not part of the scope of the IPRMS-project.

The domains which IPRMS must support, together with scenario descriptions of core workflows, is detailed further in the RPF document "Norwegian Red Cross - RFP IPRMS - Domains and Scenarios.docx"

4.3 Why should you respond to this request?

This project is conservatively estimated to **increase the survival rate** of lost and distressed persons **by at least 1 %**. Using yearly death rate reported by Red Cross alone, this amounts to at least 15 more persons saved from dying over a period of 10 years. By responding to this RFP, you will become an instrumental part of this process by helping us choose the correct delivery method for each critical part of this system delivery.

4.4 Guidelines for the Respondent

Norwegian Red Cross has already spent a considerable amount of time in defining the business processes that the new IPRMS shall support. If the Respondent however, believes that they can deliver required functionality using another approach than the approach described, we urge the Respondent to do so with appropriate documentation.

Scope

The Respondent shall specify which parts of the scope it recommends can be covered by using COTS/SaaS application(s), and which parts of the scope it recommends can be covered by custom development. **The scope is defined in section 6** and describes the requirement document on a high level. For a full description of requirements, see the document "Norwegian Red Cross - RFP IPRMS – Requirements.xlsx". In the event of any deviation between the high-level description in this document and the requirement document, the requirement document takes precedence.

Scoring

Each response will be scored on price and quality, where quality counts more than price.

Delivery method

The Norwegian Red Cross IT department has limited internal development resources, but there is a lot of domain competence and some IT capacity among volunteers. This competence is strategically important for the organization and should be utilized in the IPRMS project.

Recommendations

Additionally, the project group has defined recommendations regards to architecture and development model (if custom development is required). The list below consists of *recommendations* from Norwegian Red Cross and shall not be considered as formal requirements. However, the Respondent should take Norwegian Red Cross' recommendations into consideration when responding to the RFP:

- Use of the Microsoft Azure platform with auto deploy to deliver Infrastructure-as-a-Service (IaaS)
- Use containers/Docker technology to perform the application development, independent on the environment it is managed on
- The principle of microservices opens for independent choices of technology frameworks and programming languages for each service, but it may be advantageous to have a "standard" technology reference to keep complexity of application development and DevOps as low as possible.
- Use Node.js as the primary programming language for backend services (Javascript with library and framework), .NET may be an option for some services
- Use Flutter for cross-platform frontend development, optionally React Native.
- Use MS SQL Server for persistence
- Use Azure DevOps for user stories, system requirements, test scripts, handling of errors and bugs etc.
- Use SharePoint as documentation tool
- Use Github as Git resporitory for source code
- Use Jenkins as open-source automation server

5. PARTNER REQUIREMENTS

5.1 Company information

Norwegian Red Cross requests information about the Respondent as an IT service provider regarding company strategy for the IT service market, financial status, global revenue for IT services, legal party, organization, locations where the Respondent has a presence, subcontractors and partners.

The Respondent as an IT service provider must meet the following minimum requirements:

- Have a solid financial status and meet registration requirements provided by public authorities
- Must respect the human rights
- Must follow rules and regulations for working conditions and social dumping
- Must have zero tolerance for child labor
- Must have zero tolerance for corruption
- Must not be a manufacturer or merchant of weapons, tobacco or pornography – or directly related to any of these

6. SYSTEM REQUIREMENTS

6.1 Incident Preparedness Management System (IRMS, Beredskapsstøttesystem)

The primary goal of the preparedness process is to ensure that Norwegian Red Cross have the right capacity to respond to incidents local government is not capable of handle themselves. The preparedness process is continuously evaluating risks to identify new areas of need, identifying capacity gaps, tracking exception from standards and norms, and ensuring that all personnel is taken care of after each response. The Incident Preparedness Management System must support the execution of all these functions.

6.1.1 Preparedness management

The system shall have functionality to let personnel manage their readiness status and show an overview over which personnel that are available. The personnel must be able to modify their readiness status, and the system must show which personnel who belong to the different alerting lists.

The system shall give users access to contingency plans, checklists of tasks accompanying the contingency plans and to the different municipalities' needs, including all relevant information. Also, the system shall give access to the cooperation plans and agreements between Norwegian Red Cross and the various municipalities.

The system shall have templates for cooperation plans and agreements, and the system should give possibility to create rosters, and inform the user of which human personnel and material resources that can be utilized.

6.1.2 Debrief management

The system shall have functionality for Incident Commander to register the need for debrief after an incident is closed. The Preparedness Manager uses this registration to invite personnel to debrief after an incident. Information supplied about the incident by the Incident Manager is used to determine whom and how to follow up each personnel involved. The system must also support access to information about natural post-reactions, support tracking follow-up status and offer functionality for reporting progress and final remarks.

6.1.3 Resource management

The system delegate resource management by supporting lookup of Personnel information like name, phone, email, address and competence from a PII endpoint.

6.1.4 Exception management

The system shall have functionality for register exceptions from standards and norms, like near-accidents, accidents, reactions and misconduct which need further follow-up. This functionality shall be accessible using an Open API for integration with the Incident Response Management System. Functionality for managing and tracking the handling of each exception shall also be supported.

6.1.5 Security

The system shall support OpenID Connect (OIDC) using an Identity and Access Management (IAM) endpoint provided by us. The token shall only contain the build-in claim "sub" for unique user identification and a custom claim named «roles», which the system uses for RBAC. All other personal identifiable information shall only be accessible through the Personal Identifiable Information (PII) endpoint.

Access to apps shall be secured by pin code or biometry. Access to data shall be secured by RBAC. RBAC must be configurable by us in the system, with ability for fine-grained read and write access to data, views and actions per role. Access shall be validated per-request by testing the existence of role names known by the system in custom claim "roles" in the OIDC ID token generated by an AIM endpoint provided by us.

All network traffic shall be encrypted with https, and Apps shall not allow screen copy.

6.2 Alert Management System (AMS, Varslingssystem)

The system shall have functionality to create and administrate mobilization of personnel by alerting available personnel based on an undesired incident. Preferably by app to app, or web to app. Available personnel must be able to respond to the alert, and the system shall give an overview of which available personnel that have responded to the notification.

6.2.1 Alert management

The system shall have functionality to create, change and delete alert templates. The commander, chiefs and leaders can alert personnel via several channels, with possibility for elevation if no response in one channel. Alerts can be sent based on competence, role, affiliation and/or location filters. Alerts shall contain a meeting point (address and position), and ongoing alerts can be updated. The system must let the commander and chiefs send alerts from an app.

The system gives access to information about who is attending, their position (user-controlled) and when they are coming. Alert history can both be displayed and be exported to external systems.

6.2.2 Alert response

The system shall have functionality to let personnel respond to an alert and change their response. The system must let personnel receive alerts and change their readiness status with an app (third-party or AMS).

6.2.3 Resource management

The system must integrate with Resource Management, i.e. lookup of recipient information like name, phone, email, address and competence from a PII endpoint.

6.2.4 Security

The system shall support OIDC using an IAM endpoint provided by us. The token shall only contain the build-in claim "sub" for unique user identification and a custom claim named «roles», which the system uses for RBAC. All other personal identifiable information shall only be accessible through the a PII endpoint.

Access to apps shall be secured by pin code or biometry. Access to data shall be secured by RBAC. RBAC must be configurable by us in the system, with ability for fine-grained read and write access to data, views and actions per role. Access shall be validated per-request by testing the existence of role names known by the system in custom claim "roles" in the OIDC ID token generated by an AIM endpoint provided by us.

All network traffic shall be encrypted with https and Apps shall not allow screen copy.

6.3 Incident Response Management System (IRMS, aksjonstøttesystem)

Incidents are defined as unplanned situations that requires a coordinated emergency response. The response follows a standardized approach to command, control, and coordination of units performing actions required to resolve the situation. Each action is manually performed asynchronously and decentralized, forming a series of immutable events which combined resolves the situation. This is essentially an eventually consistent append-only log of historical events, which the Incident Response Management System (IRMS) should model accordingly. Hence, incident response requires resilient and fault-tolerant information systems to properly support the response management.

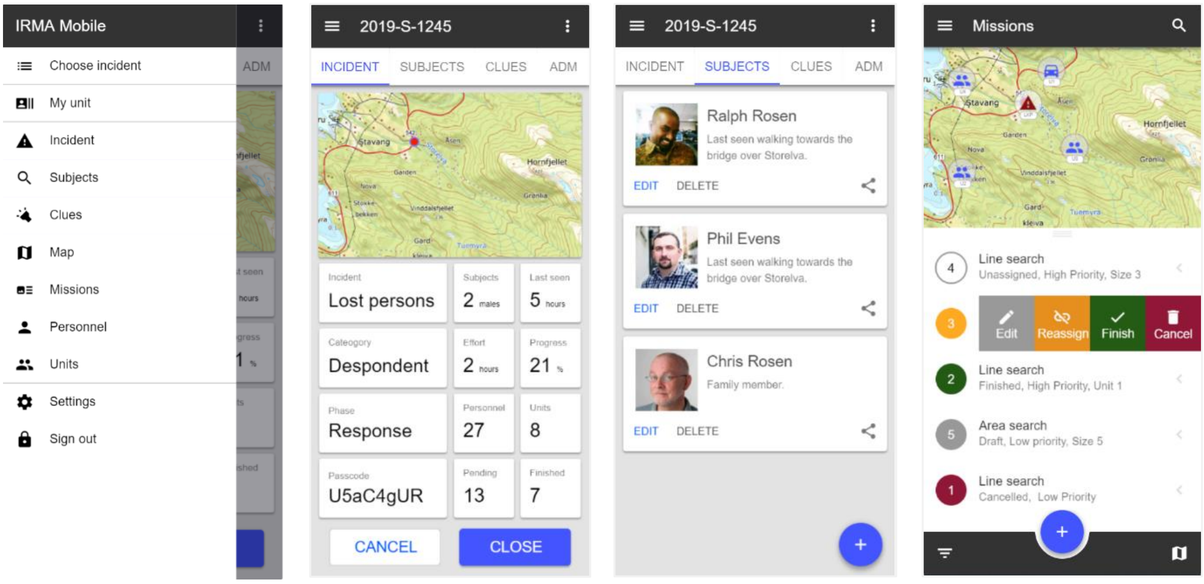
The Ubiquitous Language (taxonomy) of IRMS and the Incident Command System (ICS) overlap on key concepts and design only. The hierarchical composition and coordination of responders differ. IRMS is an opinionated subset of ICS based on best practices and official documentation of managing search and rescue operations in Norway. IRMS defines in practice a simplified and leaner organizational model with only to levels of coordination; Incident and Unit.

NON-FUNCTIONAL NOTE: Internet connectivity on-scene must be assumed to be intermittent and of low bandwidth in general, and non-existing in extraordinary situations. IRMS must therefore be resilient to low bandwidth and intermittent connectivity. Since incident response is inherently distributed in areas of intermittent Internet connectivity, applications based on centralized coordination of concurrent modification of shared states (*Service Orchestration*) suits the domain poorly. The domain is inherently offline in nature, which IRMS shall have first-class support for.

SECURITY NOTE: Personal data shall be automatically removed from the system within a predefined amount time after an incident is closed. This includes information stored on mobile devices and desktop computers. Before removal, necessary aggregation of data for statistical purposes shall be performed. This implies that when an incident is reopened, personal data about Subjects and Personnel are no longer available. To minimize the operational costs of lost data after reopening, placeholders shall be kept ensuring that statistics are stable across status transitions between closed and reopened (for example number of subjects and personnel). The details about which data to delete and keep shall be landed as part of the delivery.

6.3.1 Baseline for minimal usability

We have developed a concept design for the smartphone form-factor to make it easier for the Respondent to evaluate scope and complexity of IRMS requirements. It is based on UI components from Material Design and developed using Framer X.



Incident: Lost persons | Subjects: 2 males | Last seen: 5 hours
Category: Despondent | Effort: 2 hours | Progress: 21 %
Phase: Response | Personnel: 27 | Units: 8
Passcode: U5aC4gUR | Pending: 13 | Finished: 7

Ralph Rosen — Last seen walking towards the bridge over Storelva.
Phil Evens — Last seen walking towards the bridge over Storelva.
Chris Rosen — Family member.

4 Line search — Unassigned, High Priority, Size 3
3
2 Line search — Finished, High Priority, Unit 1
5 Area search — Draft, Low priority, Size 5
1 Line search — Cancelled, Low Priority

Figure 1 Concept design for the smartphone form factor of the IRMS mobile app (IRMA)

The concept design forms a baseline for minimal acceptable usability, and should not be considered final, complete or limiting. Respondents can offer other design if it has equal or better usability than our baseline design. Figure 1 shows three views from the design.

A walkthrough of a high-fidelity prototype is available at: https://vimeo.com/333304880.

NOTE: This is only a prototype for evaluating design concepts and the code is not optimized for running on mobile devices. The final product delivered to us shall be “jank”-free on all form-factors.

6.3.2 Incident control (hendelsesstyring)

The system shall have functionality to create, change, close and reopen incidents. Each incident should contain a list of clues describing the situation, including persons (subjects), vehicles (objects) and general information. All information about the incident and the situation that followed, shall be managed by the incident.

DOMAIN NOTE: There is a one-to-many relation between Incident and Operation in the domain which we have not described any independent functional requirements for. This relationship models different operational phases, operations which are closed without any resolution, and then reopened, which in practical terms often implies a clean start. This RFP simplifies this relation to a 1-to-1 operation with the ability to reopen a closed incident, together with the associated operation, continuing where the last effort ended. The system though, should internally model incident and operation as different entities.

6.3.3 Mission control (oppdragsstyring)

The system shall have functionality to create, edit, cancel and finish (archiving) missions. Each mission shall consist of a planned extent for the execution formed by geometries like points, polylines and polygons.

The system must also provide functionality for indication priority which the Operations Section Chief and Team Leaders uses to determine the order to execute. The mobile app shall notify each Team Leader when a mission is assigned, modified and removed from the units’ backlog of missions. Team Leader shall also have the option to self-assign missions using the mobile app. Functionality for assigning to and moving missions between Units shall also be supported.

Before each mission is registered as finished, functionality for registering a mission report shall be supported. All tracking sources associated with the units directly or transitively though Personnel and Transports allocated to the unit, shall be used to automatically add traces associated with the mission to the mission result extent.

6.3.4 Resource control (ressursstyring)

The system shall have functionality to show the position of personnel in real-time together with a callsign or phone number they can be reached on. If they have given consent to provide such information. All personal information shall be imported from one central source in the Norwegian Red Cross’ IT platform thought a PII endpoint, and the users shall bare able to modify their own personal data from the system.

The system shall have a live overview, listing mobilized and redundant personnel’, and it shall be possible to add and remove personnel’ to units.

6.3.5 Task control (oppgavestyring)

The system shall have functionality to create, edit, cancel and complete tasks. Tasks shall be assignable to Units and tasks, and follow the conventions for general task management, including start-date, due-date, progress and notifications. Each list of tasks shall be personal. Task assigned to others shall be visible to the author.

RESPONSE NOTE: This is optional functionality**.**

6.3.6 Maps

The system shall have functionality to let all users have access to access base-maps (bottom layer) and overlays of operational data like planned missions, Units and traces. These layers shall be available online and offline. Maps shall support editing operations for points, polylines and polygons, grouping and snapping to other geometry objects. Each user shall have the option to switch between base-maps and turn overlays on and off, display grid based on chosen coordinate system, display a map scale and in chosen coordinate system.

Maps shall support choosing a position in the map and searching for objects with location data. Commander and Chiefs shall be able to export maps with high resolution to pdf.

6.3.7 Tracking (sporingstyring)

The system shall have continuous tracking of personnel and units, including:

- automatic start and stop
- automatic update of last known position
- importing and exporting of traces
- show length of traces
- show real-time and historical data

Additionally, the system shall have functionality for importing traces from GPS, and personnel shall be able to send their current real-time position from the action team app.

6.3.8 Messaging (meldingsutveksling)

The system shall have functionality to send messages (text and images) to units and personnel. The messages must be able to be changed and deleted, and therefore, each message must have a unique ID.

6.3.9 Decision support (beslutningsstøtte)

The system shall have functionality to give Commander, Chiefs and leaders access to search and rescue procedures using an internal IPMS endpoint. This endpoint provides with a stable internal API which is implemented as an Open Host Service. The Open Host Service implements the provided IPMS API and translates it into the internal API which IRMS consumes. This allows for multiple integrations of IPMS solutions without changing IRMS.

6.3.10 Situation sharing (deling av situasjonsbilde)

The system shall have functionality to let commander, chiefs and other leaders see where units are located (in real time and historically). Commander and chiefs can share incident status and aggregated incident statistics.

Additionally, the system shall have functionality to share aggregated incident data with external parts (police, media and others).

6.3.11 Exception handling (avvikshåndtering)

The system shall have functionality to register exceptions, by using IPMS endpoint.

6.3.12 Logging (loggføring)

The system shall have functionality to automatically log all events in the system. The system shall also have functionality to let Commander and Chiefs insert, update and remove incident and communication log entries.

6.3.13 Reporting (rapportering)

The system shall have functionality to automatically create reports after an operation is finished and give authorized users access to them. The system shall also have functionality to automatically register the number of working hours carried out by each volunteer and have the possibility to export activity data to external systems. Access to exception forms shall be provided to the user by a link from the system.

6.3.15 Security

The system shall support OIDC using an IAM endpoint provided by us. The token shall only contain the build-in claim "sub" for unique user identification and a custom claim named «roles», which the system uses for RBAC. All other personal identifiable information shall only be accessible through the a PII endpoint.

Access to apps shall be secured by pin code or biometry. Access to data shall be secured by RBAC. RBAC must be configurable by us in the system, with ability for fine-grained read and write access to data, views and actions per role. Access shall be validated per-request by testing the existence of role names known by the system in custom claim "roles" in the OIDC ID token generated by an AIM endpoint provided by us.

All network traffic shall be encrypted with https and Apps shall not allow screen copy.

7. PLAN FOR THE RFP

DATES	ACTIVITY
2019.04.30	RFP published in Mercell
2019.05.31	Submission deadline
2019.06.21	Initial feedback
2019.08.20 – 2019.08.30	Respondent presentations
2019.08.26 – 2019.09.13	Dialogue and negotiations with relevant suppliers
2019.09.27	Norwegian Red Cross intention to give final feedback to Respondents
2019.10.07	Indicated timeframe for start-up project

8. HOW TO RESPOND TO THE RFP

- The deadline for responding to RFP is set to **31.05.2019.**
- Norwegian Red Cross requests the response to be uploaded in Mercell by all respondents that can get access. All others must use our single point of contact (see below).

RESPONSE NOTE: The respondent can choose to respond to the full RFP scope OR parts of it.

8.1 Response formats

The response is expected in the following format(s).

Section	Title	No response	Respond with RFP template	Respond via attachment
1-4		X		
5.1	Partner requirements			X
6	System requirements		X	
7-10	(misc. information)	X		
11	Customer references			X
12	Pricing		X	
13	Roadmap for future releases		X	
14	Delivery method and Service Operation		X	

8.2 Response templates

No RFP responses shall be submitted inline in this RFP document.

All RFP responses shall be submitted in the following documents:

- Norwegian Red Cross - RFP IPRMS – Requirements (attached MS Excel document)
- Norwegian Red Cross - RFP IPRMS - Product Pricing, Delivery Method and Service Operation (attached MS Excel document)
- Norwegian Red Cross - RFP IPRMS - Roadmap for future releases (attached MS Word document)
- SaaS and COTS suppliers must add documentation of their proposal, e.g. system documentation with screen images, access to the solution, or video demonstration of the solution.

Optionally, and used ***as sparingly as possible***, the Respondent may also attach supplementary information outside of the above-mentioned documents, in Respondent-chosen document formats, if there is a crystal-clear reference as to which section in this RFP document the Respondent-attached supplementary information belongs.

8.3 Language

All proposal and contractual documents are to be in English or Norwegian. Scandinavian speaking representatives should be present in all workshops with Norwegian Red Cross.

9. NORWEGIAN RED CROSS FOR CONTACT FOR THE RFP

The single point of contact for all users that cannot use-Mercell, is:

Beate Lien
Title: Project Manager, IKT

Contact info:
E-mail:
beate.lien@redcross.no

Postal address:
Norwegian Red Cross
Att: Beate Lien
Postboks 1, Grønland
0133 OSLO
NORWAY

10. COMMERCIAL & LEGAL ISSUES

10.1 Norwegian Red Cross reservations

Norwegian Red Cross reserves the right to recall the RFP in its entirety or in part, and to, at any time or for any reason, without any further explanation, stop the process, put the process on hold or change the process.

The respondent acknowledges by receiving this RFP that they will not hold Norwegian Red Cross responsible for any expenses, loss or inconvenience suffered.

This RFP is only a request for information about potential products / services and no contractual obligation on behalf of Norwegian Red Cross whatsoever shall arise from the RFP process.

This RFP does not commit Norwegian Red Cross to pay any cost incurred in the preparation or submission of any response to the RFP, or any subsequent follow up that may apply.

10.2 Potential RFP & contract

It is the intention of Norwegian Red Cross to conduct the RFP/commercial process later in 2019. A detailed plan for this process will be determined after this RFP process is concluded.

11. CUSTOMER REFERENCES

Norwegian Red cross requests information on the Respondent's experience with working in similar or relevant cases. Norwegian Red Cross would also like an understanding of the following:

1. Competence profiles of personnel within the following areas:
    a) Experience with working in an agile development team
    b) Experience with working within the platform/development framework defined in section 4.2
    c) Experience with other relevant customers
    d) Other relevant experience

2. Implementation of suggested COTS/SaaS products:
    a) Experience of implementing solutions
    b) Other relevant customers where solution has been implemented recently

12. PRODUCT PRICING

The proposed solution must specify both initial implementation / development cost, and management cost, including all updates and basic support for the first 5 years.

13. ROADMAP FOR FUTURE RELEASES

There must exist a roadmap for future releases of the solution proposed by the vendor. This should be described in attachment. The respondent describes this in their own chosen format

14. DELIVERY METHOD AND SERVICE OPERATION

Scoring of proposed delivery method will be based on the sourcing strategy laid down by the ICT unit, which is an operationalization of the ICT unit's mandate. Specifically following the governing model, which defines the two main principles "cloud before data center" and "SaaS and COTS over custom software". In practical terms, if products score equally on price and quality but have different delivery methods, the products that are delivered as SaaS and COTS will be chosen over development of custom software.

The respondent shall use the form "Norwegian Red Cross - RFP IPRMS - Product Pricing, Delivery Method and Service Operation" to describe chosen delivery method and application management.