TECHPARK SÜDTIROL / ALTO ADIGE

Bolzano/Bozen, 27st of September 2023

Market research – Open Data Hub – Cyber Security Test

This document concerns a market research for the identification of one or more partners that can support NOI S.p.A. in the analysis of the Open Data Hub project from a Cyber Security point of view. This market research includes activities like, for example, testing (e.g. penetration testing, cyber-attacks, etc.), workshops about specific topics that could emerge during the project, redaction of Cyber Security guidelines, etc.

NOI AG / S.p.A.
A.-Volta-Straße 13A
Via A. Volta, 13A
I-39100 Bozen / Bolzano
T +39 0471 066 600
info@noi.bz.it
PEC: noi@pec.noi.bz.it
www.noi.bz.it

Eintragung im Handelsregister der Handelskammer Bozen
Steuernr. & MwSt.Nr.: 02595720216
Ges.kapital voll eingezahlt: 110.740.000 €

Numero d'iscrizione nel registro delle imprese presso la Camera di commercio di Bolzano
Codice fiscale e part. IVA.: 02595720216
Capitale sociale interamente versato: 172.740.000 €

Project name: IMPACT – Impacting Innovation Through Specialization
Project code: EFRE1048
Project CUP: J57H23000640009

Table of contents

1. Goal of the market research

This chapter aims to explain in more detail about content included in the market research. The aim is to identify one or more partners that can support NOI S.p.A. in the analysis of the Open Data Hub project from a Cyber Security point of view. This market research includes activities like, for example, testing (e.g., penetration testing, cyber-attacks, etc.), workshops about specific topics that could emerge during the project, redaction of Cyber Security guidelines, etc.

1.1 INTRODUCTION

One of the key project of the Tech Transfer Digital of NOI S.P.A. is the Open Data Hub, a cross-border digital platform that helps start-ups, companies and research institutes to develop digital solutions based on real data. It connects data from different data providers and makes this data easily available for data consumers.

More information and details about the Open Data Hub Project can be found on the project website:

https://opendatahub.com/

In particular the most interesting information for this market research are summarized in the "Quickstart" section of the website:

https://opendatahub.com/quickstart/

Finally the source code of the Open Data Hub core and all Open Data Hub applications is collected and released on GitHub in the "NOI Techpark - Südtirol / Alto Adige" organization:

https://github.com/noi-techpark

This Market Research includes the testing of all applications, API, tools and software components related to the Open Data Hub Project. The main Open Data Hub tools. The list of the main Open Data Hub tools is listed in the "Quickstarrt" section of the website, but the final list of applications and tools that must be tested will be defined during the kick-off meeting.

1.2 TASKS AND SERVICES

The task, services and activities included in this market research are:

- Analysis of the existing Open Data Hub infrastructure also considering the future project and infrastructure development. The output of this activity will be a document that includes:
    - the list of possible risk factors of the current architecture.
    - the list of possible risk factors to be considered for the future development of the architecture which will be based on

Infrastructure as a Code technologies (e.g. Kubernetes, Terraform, etc.);
    - the list of actions and countermeasures that the Open Data Hub team should implement to eliminate or reduce to the minimum the risk factors described in the previous points;
    - the guidelines that the Open Data Hub team and contributors will have to follow for future platform developments in order to minimize risks dictated by Cyber Security aspects. This guideline shouldn't be focused only on architectural aspects (e.g. how to implement penetration testing, how to mitigate risks like exposed servers, services, secret management, etc.), but should also contain some procedural guidelines (e.g., frequency and type of tests to be performed, possible guarantees to be requested from suppliers, how to deal with dependabot alerts, etc.).

  The results of this activity will be presented to the entire Open Data Hub team in a dedicated meeting.
- Definition of specific guidelines regarding the implementation of periodic intrusion testing. These guidelines should contain indications about the implementation and the frequency of testing.
- Implementation of the first intrusion tests on both Open Data Hub infrastructures (old and new one) that will be used as a test bed to then finalize the guidelines described in the previous point.
  The results of this activity will be presented to the entire Open Data Hub team in a dedicated meeting.
- 3 half day workshops to be organized on request, in case of need of an in-depth analysis of specific aspects or technologies concerning the Cyber Security (e.g. how to deal with dependabot alerts, how to mitigate risks like exposed servers, services, secret management, etc.).
- 40 hours of support to be consumed on request, in case of specific requests regarding Cyber Security aspects that may arise during the development of the Open Data Hub Project.
- Consulting and support for the implementation of a secure CI/CD environment, we mention here below some example activities that should be included in the offer. The service provider can add other optional activities that could be included in this task.
    - Check of the CI/CD pipeline from a cyber security point of view.
    - Define a guideline about how to manage secrets with the technologies in use by the Open Data Hub project.

2. Constraints

In this section are listed and described the constraints that the service provider must follow to work with NOI on this project.

2.1 ECONOMIC EXPLOITATION

Where the creation of material subject to proprietary rights, including copyrights, sui generis data rights, and related rights, including solely of photographs, industrial design, all rights of economic exploitation arising from achieved results are reserved to NOI S.p.A., excepting those expressly excluded when the order is placed.

Further, if the material includes a software development project, all source code from libraries or other modules used in the realization of an assignment and belonging to a third party must be released under an Open Source license (opensource.org/ licenses) in a manner compatible with the scope of the "outbound" software license, without requirement for adaptation, addition, cancellation or requests for permission from third parties on the part of NOI S.p.A. In the absence of any expressly indicated license, the terms of the GNU GPL v3 licence shall apply. The use of material belonging to third parties must be expressly declared at the time of the offer or be easily and immediately understandable from the description of the project. If code is developed during the realization of this assignment, NOI S.p.A. will initiate a Git repository on which the supplier must develop and publish the source code.

If the material consists of data, creative works (drawings, literary works, cinematographic works, figurative art, photographs), industrial design or other material which are subject in whole or in part to the proprietary rights of a third party, the use of such material is permitted provided it is licensed under conditions compatible with the license under which said material will be published, if indicated. If no license is indicated, the material will be subject to conditions compatible with the Creative Commons Zero (CC0) license.

2.2 INVOICING

The invoicing of the activities concluded by the supplier will be sent to NOI S.p.A via electronic invoice only after the outputs produced have been successfully tested by NOI S.p.A. Before to proceed with the testing of the outputs, the supplier must provide to NOI S.p.A.:

- the entire documentation.
- if code development is planned, the code must be uploaded to the Git repository provided by NOI S.p.A.
- in the case of multimedia contents (e.g., photos, videos, illustrations, documents), the service provider must upload it on specific platforms (e.g., Vimeo, Flickr, etc.) and provide the source files or open versions through appropriate file hosting services indicated by NOI S.p.A.

All invoices must include that the transaction is subject to the Split Payment discipline as mentioned in the art.17-ter del DPR 633/197 and must be issued exclusively in electronic format (Unique Office code: T04ZHR3).

2.3 WORK METHODOLOGY

The SFSCON is an event organized by the Tech Transfer Digital of NOI S.P.A. Since the main project of the Tech Transfer Digital is the Open Data Hub, for the development of the SFSCON App the team will follow the same work methodology as in the Open Data hub Project. This paragraph will include more details about the work methodology.

The development of the activities covered by this market survey will follow the agile method (scrum). Two weeks sprint sessions are scheduled, unless otherwise agreed, during the kick-off meeting with the core team of NOI S.p.A.

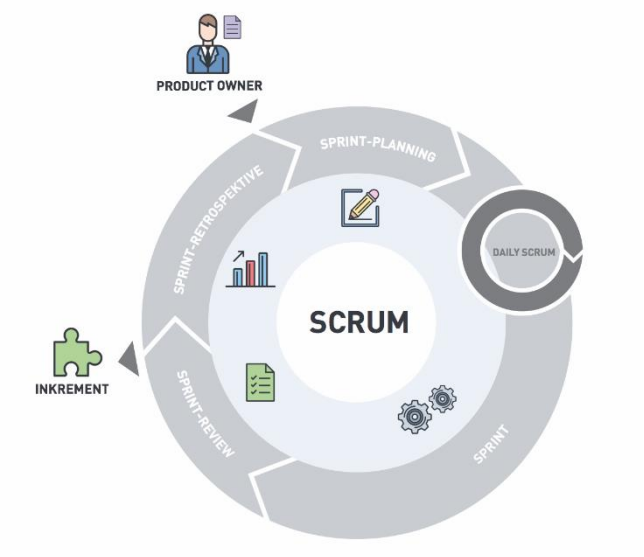

Figure: *the SCRUM methodology.*

The software development will take place in three phases/environments:

- **development environment**: this environment is on supplier's infrastructure and is used during the development of the software components.
- **testing environment**: on infrastructure made available from NOI Techpark. This environment is used to test the new working versions of the software components. For the publication of the new versions a Continuous Integration (Jenkins) pipeline will be developed by the NOI team. For this reason, the new versions of the code will have to be "committed" to a dedicated Git Repository according to the instructions provided by the team of the NOI Techpark.
- **production environment**: on infrastructure made available from NOI Techpark. After the testing phase, as soon as the software produced is

considered sufficiently stable, the software will be integrated into the production environment. Also, this process is managed automatically with Continuous Integration pipelines.

To coordinate the project NOI S.p.A. will use a Kanban Board in GitHub. Each functionality or issue will be described by NOI S.p.A. in GitHub and put on the Kanban Board. The Kanban Board will have the following columns:

- **Backlog:** contains all issues that are on hold and have to be discussed during the next sprint meeting with the supplier;
- **ToDo:** contains all issues that must be concluded in the actual sprint;
- **In Progress** contains all issues where that are working in progress.
- **To Review:** contains all issues that NOI Techpark has to review and that has to be reviewed during the sprint meeting.

All issues in the Kanban, apart from the one in Backlog, have to be assigned to the user that must make the next step (e.g., the issues in ToDo will be assigned to the developer who has to develop the functionality, the issue in To Review will be assigned to the tester, etc.). The supplier will have access to the project Kanban board and will have to check it regularly.

To allow the NOI S.p.A. team to properly review and test the code, for each issue in the ToDo lane the service provider has to send a pull request to the development Branch of the repository at least 5 working days before the sprint meeting.

To allow a better integration of the systems already in use by NOI Techpark it is required to implement all software components, where possible, using the technologies that are already in use by the Open Data Hub (https://opendatahub.com/) project.

2.4 REPOSITORY GIT

The source code must be uploaded to the Git repositories provided by NOI Techpark. During the upload, the service provider must take particular attention to the following aspects:

- do not commit usernames or passwords. NOI Techpark uses GitHub Actions to build the code which implements password ingestion based on special keywords in the source code;
- well document the code describing at least:
    - the general architecture of the system;
    - the list of the licenses of all the libraries used;
    - the installation process;
    - all other useful information for people who want to fork or install and use the project.

As Open Data Hub (https://opendatahub.com/) we have created some boilerplate repositories for the most common project type (es. Java project, Web Component,

.Net Core project, etc.). In case you are starting a new project from scratch, before starting your project please look for the boilerplate that best fits your project and use it to initialize your repository.

2.4.1 Documentation

While you are documenting your code, please consider that the official language of the Open Data Hub is English. So, the entire documentation, including the comments in the code, must be in English. Moreover, you must observe the following guidelines:

- use the right boilerplate of the README.md if exists;
- use only markdown or text (no binaries, no PDF, etc.);
- should be so detailed that a third person, without any connection to the developers can setup the project, run it and develop it further;
- Java Doc and similar tools for other languages should be as complete as possible;
- add the author tags incl. emails;
- README.md should be a good description of the project and should also have usage instructions (boilerplate does not consider that). Mainly because tools like **npm** use it as homepage for each project

In general, the documentation of the project (e.g., readme file, license file, etc.) should be done to allow third parties developers, who do not know anything about the project, to understand the whole project and replicate, install or modify it without the need to contact NOI S.p.A. Therefore, the documentation (README.md) should include also:

- a brief description that allows the user to understand the overall goal and functionalities of the project;
- longer and detailed description that includes also:
    - description of the distinct parts of the repository/application;
    - description of distinct parts of the project (also other repositories, if existing, and a link to them) and how this application is part of the overall project;
    - external services/code/framework/software that are used including their license and copyright information;
- detailed development setup instructions (including testing);
- detailed deployment setup instructions.

2.4.2 Licensing and Reuse compliance

In respect to the licensing and copyright information, the service provider must follow the guidelines defined by the Reuse project:

https://reuse.software/

The service provider must provide code where the Reuse linter passes without errors and the licenses must all be compatible with each other.

2.4.3 Pull request (PR)

As mentioned in the previous paragraphs the service provider, before each sprint meeting, will deliver the source code by making a Pull Request to the Development Branch of the repository Git provided by NOI S.p.A. at the beginning of the project. In general, the service provider must observe the following guidelines to make the pull requests:

- at the beginning of each sprint the service provider will open a Pull Request (PR) with a prefix [WIP] as Work in Progress;
- during the sprint, the service provider must regularly push the commits to that PR to allow NOI S.p.A. to monitor the status of the project;
- at the end of the sprint (at least 5 days before the sprint meeting) the service provider will close and send the Pull Request.

NOI S.p.A. will analyze the Pull Request before the meeting and eventually send feedback to the service provider. The minimal requirements for a Pull Request to get accepted are:

- the documentation must exist and be as complete as possible in respect to the status of the project;
- commits must not contain credentials or any other sensible data;
- contributions (e.g., documentation, comments, etc.) must be in English;
- merge conflicts must be resolved by the contributor;
- all Continuous Integration verifications must pass;
- Pull Request branches should have a linear history, that is, they should not contain merge commits.

During the development cycles the pull request comments and in general the issues and the dedicated Kanban board on GitHub (original repository) must be tracked by the service provider. The discussion about issues, pull requests, and other specific comments on the code development will be managed on GitHub in the project repository and NOT through email. That also involves moving user stories to the corresponding column in the Kanban and assigning them to the right user.

2.4.4 Commits

These paragraphs contain some guidelines that the service provider should follow while implementing the project:

- commits should contain a single thing/feature, not be too big and specially they should not be a combination of unrelated features or bug-fixes;
- each commit must be described: present tense and active (e.g., "Add logging to commons" not "commons will get logging now" and not "Added logging").

2.4.5 Deployment

For the deployment of the project NOI S.p.A. will use its CI/CD infrastructure, for this reason it is important that the service provider includes in the documentation of the project the information about how the application should be deployed or updated by a CD pipeline. Therefore, the documentation should point out the following things:

- What parameters must be configured? Which ones are secrets and which are not?
- What services must be used? (e.g., PostgreSQL database, S3, etc.)
- What steps must be made to package the application/project so that it can be copied to the server?
- What steps must be made on the server after deploying? (ex. Database migrations executing with special command)
- What must be adjusted on the server only once? (ex. cron job, shared folder).

2.4.6 Testing

All projects should include unit tests and the minimal requirements for the service provider are:

- setup a test infrastructure;
- write unit tests to cover the most key features;
- the minimal test coverage should be 20%;
- tests should cover own business logic (even if minimal) and not third-party API's / libraries.

Finally, a test-driven development is appreciated.

2.4.7 API development

In case that within the project it is foreseen also the development or the change of APIs, the service provider should observe the following guidelines:

- all API calls must be documented in the README.md;
- Swagger UI should be used;
- in case of errors the API should return to the consumer valid and descriptive error messages;
- the API should be RESTful, if possible, but, in case of need, other formats will be considered. In case of non RESTful APIs the service provider should present to NOI S.p.A. enough documentation to allow NOI S.p.A. to decide whether to go on with the modern technology or stick to RESTful;
- the API must include also:
    - Response codes,
    - HTTP methods,
    - validity errors,
    - logging: JSON format for production and plain-text for local development written to stdout.

2.4.8 Access Control List (ACL) management

In case that the project foresees Access Control List management, the service provider should observe the following guidelines:

- every login to a webapp needs ACL;
- the passwords must be complex enough to be secure;
- Oauth 2.0 standard is required Session management for webapps should be present, logout after an inactivity time (the length of the inactivity time depends on the single projects and must be agreed with NOI S.p.A.)

As an Access Management tool NOI S.p.A. uses Keycloak (https://www.keycloak.org/) instance. More details are available at the following links:

https://github.com/noi-techpark/documentation#oauth

2.4.9 Dockerization

NOI S.p.A. is using Docker (https://www.docker.com/) to automate the deployment of the application and we strongly recommend to:

- use docker for local development;
- keep local docker setup, staging and production as similar as possible (these will be provided and updated by the NOI S.p.A. team);
- use environmental variables to configure different stages (i.e., .env files).

2.5 WORKING PLACE AND HOUR

2.5.1 Working Hours

The execution of the works that involve collaboration with the staff of NOI Techpark or other entities involved in the project must be carried out within a timeframe ranging from 9.00 to 12.00 and from 15.00 to 17.00. Depending on the needs, different times may be agreed via email between the service provider and the entities involved.

2.5.2 Working Place

The meetings that will be agreed during the project will take place, according to the needs of the project team, online or in the NOI Techpark offices:

- Via Alessandro Volta, 13, Bolzano.

Any expenses that the supplier will have to incur to reach these locations will not imply an additional cost for NOI Techpark. In any case, any travel costs that the supplier will have to incur to ensure the natural performance of the project activities (e.g., extraordinary coordination meetings, interventions that require presence on site, development activities to be carried out in agreement with the one or more entities / suppliers involved in the project, etc.) cannot be billed to NOI Techpark.

3. Request to the supplier

3.1 PROJECT INFORMATION

The supplier must include in all documents (e.g., offer, invoice, etc.) the following information:

Project name: IMPACT – Impacting Innovation Through Specialization
Project code: EFRE1048
Project CUP: J57H23000640009

3.2 OUTPUTS

The service provider should produce the following documentation:

- Document "Analysis of the existing and future Open Data Hub" including:
  - the list of possible risk factors of the current architecture;
  - the list of possible risk factors to be considered for the future development of the architecture;
  - the list of actions and countermeasures that the Open Data Hub team should implement to eliminate or reduce to the minimum the risk factors described in the previous points;
  - the guidelines that the Open Data Hub team and contributors will have to follow for future platform developments in order to minimize risks dictated by Cyber Security aspects. This guideline shouldn't be focused only on architectural aspects (e.g. how to implement penetration testing, how to mitigate risks like exposed servers, services, secret management, etc.), but should also contain some procedural guidelines (e.g., frequency and type of tests to be performed, possible guarantees to be requested from suppliers, how to deal with dependabot messages , etc.).
- Document "Periodic intrusion testing guideline" that includes the indications about the implementation and the frequency of testing.
- Document "Intrusion testing results" that includes:
  - the list of all problems identifies;
  - The list of countermeasures that should be implemented to remove or reduce to the minimum the risks related to the identified problems.
- Document "Secure CI&CD Environment" that includes the indications about:
  - Result of the check of the CI/CD pipelines that includes all possible risks, possible improvements and optimizations to be implemented.
  - Guideline about how to implement CI/CD pipeline inline with cybver security aspects (e.g., how to manage secrets, etc).
  - Any other aspect that has to be considered to implement a secure CI/CD environment.
- For each workshop the slides and the documentation presented must be provided.

The output to be produced for each activity on request will be agreed via email on top of the need of NOI S.P.A.

4. Documentation

To participate in this market research, we kindly ask you to provide the following documentation:

- a short company description that includes also a list of references in similar projects;
- a short description of the team that will be assigned to the project including a short description of the competences of each team member;
- the cost estimation for each single task described in the chapter 2 of the present document.;
- the hourly rate of each team member included in the project team.

5. Contacts

The service providers who are interested in participating in this market research will have to present their estimation by the **9th of October 2023.**

In case of any question please contact:
Stefano Seppi
Email: s.seppi@noi.bz.it