Questionnaire
Public

Helsinki, 04/06/2024

Preliminary Market Research – Questionnaire regarding services to support ECHA's Chief Information Security Officer (CISO) activities in the domain of information security

Introduction

The European Chemicals Agency in Helsinki (hereinafter "ECHA"[1]) is inviting you to reply to this questionnaire by **30/06/2024 by 18.00 Helsinki time (EET)**, via e-mail addressed to the functional mailbox procurement@echa.europa.eu.

This questionnaire is meant for market consultation conducted by ECHA in order to better appreciate the current market offering on services related to information security, as described below.

In accordance with the principles of non-discrimination, equal treatment and transparency, the invitation to participate in this market consultation has been published on the website of ECHA, including the questionnaire.

Important: Before answering the questions, please read carefully the background information provided below.

ECHA will preserve the confidentiality of the information provided in response to this questionnaire. Your data will be processed in accordance with ECHA's privacy rules.

1. General Information

- The information included in this questionnaire is only indicative; it is meant to give context for the respondents to provide their answers, but does not commit or bind ECHA, i.e., with regard to any procurement launched by the Agency in the future.
- The responses do not bind the respondents in any way. The information to be collected through this questionnaire will not be considered by ECHA in the evaluation of request to participate or tenders submitted during an eventual procurement procedure launched by the Agency.
- The identity of the companies that will respond to this questionnaire will not be disclosed to any third party, except to the European Court of Auditors, the European Anti-Fraud Office or, for the processing of personal data, the European Data Protection Supervisor if requested for the performance of audits and checks.
- The responses to be provided in the free text fields of this questionnaire should be clear and standalone, i.e., without web links to documents or websites.
- No further interviews are planned to take place with the respondents. Therefore, we kindly invite you to provide as much information as you feel relevant for ECHA to assess best the market situation.

[1] https://echa.europa.eu/

2. Background Information

2.1 Presentation of the contracting authority

ECHA is an EU decentralised agency, managing the technical, scientific and administrative aspects of several EU Regulations and Directives in the area of chemical safety.

ECHA's legal basis includes the following items:

Legislation	Tasks under grant, cooperation, service level and other agreements
Regulation on Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)	EU Observatory for Nanomaterials (EUON)
Classification, Labelling and Packaging Regulation (CLP)	EU Chemicals Legislation Finder (EUCLEF)
Biocidal Products Regulation (BPR)	Occupational Exposure Limits (OELs)
EU Prior Informed Consent (PIC) Regulation	Instrument for Pre-accession Assistance (IPA) – support to accession countries
EU Persistent Organic Pollutants (POPs) Regulation	IUCLID for EFSA
Waste Framework Directive (SCIP database)	Partnership for the Assessment of Risks from Chemicals (PARC)
Drinking Water Directive	
8th Environmental Action Programme	
Cross-border Health Threats Regulation	
Batteries Regulation	

ECHA's mandate is to:

- Carry out technical, scientific, and administrative tasks related to the implementation of the EU's chemicals legislation and policy
- Provide transparent, independent and high quality scientific opinions and decisions, which shall serve as the basis for the drafting and adoption of Union measures
- Collaborate and partner with EU bodies and Institutions, Member State authorities, as well as third countries and international organisations
- Provide tools, advice, and support to industry, with a particular focus on SMEs, in fulfilling their duties under chemical legislation
- Ensure that relevant, reliable, and objective information is available for the public and interested parties.

2.2 Security context in the Agency

The European Union has recently adopted **EU cybersecurity regulation**[2] which purpose is to ensure high common level of security in EU public administration. This means setting up formal internal risk-management, governance control and control framework that contains cybersecurity maturity assessment, risk management measures and

[2] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (https://eur-lex.europa.eu/eli/reg/2023/2841)

cybersecurity plan among other things.

Increasing understanding of the potential impact of risks on the **business functions** and strengthening the relationship between senior management and information security and business continuity function is also being worked on to show the benefits for business how it could enable and support them better in their work.

Another important area for information security in ECHA is securing the migration to **public cloud** and maintaining at least the same overall security level. This includes strategic and architecture work for information security as well as ICT support for business continuity in addition to the traditional design and implementation of security measures, controls and procedures.

Security **awareness raising** has also been identified as focus area for example in internal audits and the campaign have been enhanced but it requires continuous further development. ECHA has expanded the number and amount of subject matter in the training courses as well as started conducting phishing simulations, but the threat landscape is constantly changing and the awareness raising efforts need to be adapted to the emerging threats

2.3 Scope of the market consultation

The European Chemicals Agency in Helsinki (ECHA) is analysing the possibility to procure management and development services to support its Chief Information Security Officer (CISO).

The CISO support services are expected to support ECHA's information security and business continuity programme including data protection. The expected services include ongoing assessment of the adequacy of our security vision, strategy and operating model and achievement of related security goals by:

- Analysing emerging risks and development of the threat landscape and providing advice on risks related to the organisation,
- Communicating risk and value, and building stronger relationships with senior management and business functions by demonstrating how security can enable and support business objectives and initiatives,
- Providing best practices in the fields of information security and business continuity as well as data protection, relevant surveys and research regarding CISO priorities and concerns, and technologies,
- Comparing service provider and vendors and provide insight on what is available in the market to ensure that ECHA is on the right path.

3. Questions

1. Please provide a description of the coverage of your service offering for Information security support services in the following domains:

    a. **Organisational** controls focus on the policies, procedures, responsibilities and other organisational-level measures necessary for effective information security including:

        i. The information security policy and other core policies as well as regulatory compliance with EU regulations;
        ii. Defined responsibilities for management and the people responsible for operating the information security management system day to day i.e. governance, risk and compliance (GRC) framework;

iii. Contact with authorities and other relevant groups;
iv. Threat intelligence and monitoring and vulnerability management;
v. Classifying and labelling information;
vi. Identity and access control; and
vii. Asset management and maturity assessment.

b. **People**, particularly employees, are a critical part of the information security equation including:
i. Pre-employment screening;
ii. Staff awareness and training;
iii. Contracts and NDAs (non-disclosure agreements) including supply chain security;
iv. Remote working; and
v. Reporting security events and incident response.

c. **Physical** controls focus on the physical environment of the information security management system. This is every bit as important as the digital environment for ensuring information security including:
i. Security perimeters and secure areas;
ii. Clear desks and screens;
iii. Supporting utilities;
iv. Secure cabling; and
v. Equipment maintenance.

d. **Technological** controls are what most people think of when they think about information security including:
i. Zero trust architecture including malware protection;
ii. Backups as well as disaster recovery, failover and business continuity including business impact assessment;
iii. Logging and monitoring including Security Operations Centre (SOC) services;
iv. Network security and segregation; and
v. Development and coding practices.

e. **Data Protection** controls focuses on the measures and controls in place to protect personal data and privacy including:
i. Data protection regulations;
ii. Data handling and storage procedures;
iii. Data transfer methods; and
iv. Rights of the individual (such as the right to access, correct, or erase personal data).

f. Any other domain(s) your services cover not mentioned above.

2. Please provide a description of the coverage of your service offering for Chief Information Security Officer (CISO) support services in the following <u>types</u>:

a. **Research library** and **market research** on the topics/areas including the volume; e.g., number of articles;
b. **Templates and tools** on the topics/areas including the volume e.g. number of templates and tools;
c. Regular meetings (virtual or in person) with **contact point** with wide coverage and extensive experience on the domains mentioned above including the breadth and length of expertise/experience of such contact point;

   d. **Interactions** (virtual meetings or in writing) with subject matter **experts** who have, e.g. written the research library and/or templates and tools including the volume of experts;
   e. **Events** (virtual or in person) such as seminars, conferences or summits on the on the topics/areas including the number of such events annually.
   f. Any other type(s) your services cover not mentioned above.

3. What is your level of interest in **submitting an offer** if ECHA decides to launch competition under the ECHA Dynamic Purchasing System (DPS); i.e., would you consider applying to the DPS in advance of launching the competition and then submitting the offer?

4. What would be your preference on the **duration** of the contract; e.g., renewable every 12 months or something else?

5. What would be your preference on the **price model** of the service offering for Chief Information Security Officer (CISO) support services in the abovementioned domains and types, e.g. is it annual subscription on named individual user or depending on the usage or coverage of the domains and/or types of services for example with separate line items?

6. Would you be in a position, and willing to disclose **a price range** for your service offering for Chief Information Security Officer (CISO) support services?

7. Any other feedback/remarks?

END OF QUESTIONNAIRE