VACANCY NOTICE FOR TEMPORARY AGENT SELECTION

Job title (same as on the job description)	**Team Leader – Principal Risk Officer**
Reference	**CLIMA/COM/2026/526347**
Application deadline	03.12.2026 - 12.00 (Brussels time)
Directorate-General (full name)	Directorate-General for Climate Action
Unit	CLIMA.E.TRO – Taskforce for Resilient Operations
Place of assignment	Brussels
Grade range	AD5-11
Domain	CLIMATE
Contract type	Temporary Agent 2a

About us ("We are")

The European Commission is organising an external selection procedure for a temporary agent to fill the post of Team Leader – Principal Risk Officer. The officer will be a part of the taskforce whose main goal is to prepare establishment of a dedicated "secure ETS operations office" by 2028, where all reviewed processes and streamlined administrative tasks will benefit from efficiency gains and financial sector grade information security services. This taskforce will be hosted by the Directorate-General for Climate Action (DG CLIMA) and report directly to the Director for Climate Resilience and Information Management of DG CLIMA.

The taskforce is established with the aim to retain operational excellence and continuity of the ETS (Emissions Trading System) Registry in an evolving and increasingly challenging geopolitical and cybersecurity landscape. The taskforce will enhance the current operating model, by aspiring to ensure maximum compliance with applicable regulations for comparable financial market infrastructures and to minimise exposure of the critical climate information systems to external threats thereby contributing to predictable and stable policies and business continuity.

ETS operations are centralised in a single information system, called the Union Registry. It holds carbon emission allowances in accounts for more than 15,000 operators from the power sector and energy intensive industry, including the aviation sector. Emission allowances are considered financial instruments under MiFID, and the registry offers services similar to the notary and central maintenance services offered by Central Securities Depositories ('CSD').

About the role ("We propose")

The risk management function will form part of ETS Office's second line (of defence), and its mission is to support ETS Office in achieving its goals and delivering its strategy through providing robust, independent oversight of risk-taking activities. We offer an exceptional opportunity to build a modern enterprise risk architecture from the ground up. As a key member of the initial team establishing the future ETS Office in Brussels, you will co-create, design and implement a risk framework tailored to an agile, small-to-mid-size Financial Market Infrastructure (FMI) operating at the crossroads of the European financial and climate policy ecosystems. We offer a unique opportunity to influence the development of a new strategically important systemic pillar in the European market.

The chosen candidate's main task will be to coordinate the strategic design, implementation, and governance of our holistic risk management function. This spans across all pillars of financial risk, operational resiliency, and legal reporting management.

For our organization, this role will be key for the establishment and proper functioning of the future Office. A robust and independently validated risk framework will be instrumental to the future Office's secure operating model. This post will make a key contribution to the credibility of the Office's risk management framework. Main responsibilities include:

- enterprise Risk Management (ERM) and Risk Governance:
    - develop, maintain and implement the ETS Office enterprise-wide risk management framework, risk strategy and Risk Appetite Framework in compliance with relevant frameworks, such as CSDR (Central Securities Depositories Regulation), Digital Operational Resilience Act (DORA) and relevant prudential and financial-market infrastructure requirements and ESMA guidelines;
    - establish appropriate risk policies, methodologies, limits, key risk indicators and escalation mechanisms;
    - define a Reporting framework to regularly report on risk exposure, highlight emerging systemic threats, propose solutions to mitigate and manage identified risks.
- Operational and ICT Risk:
    - in collaboration with the respective services, develop an operational risk framework and oversee risk arising from: IT systems and critical infrastructure; cyber threats and information security; operational incidents and processing failures; human error, fraud and internal process failures; third party providers and outsourcing;
    - define a strategy and oversee operational resilience, business continuity and disaster recovery arrangements, including scenario testing and crisis-management preparedness ensuring the system can resume operations within the strict Recovery Time and Point Objectives (RTO/RPO) required by legislation;
    - conduct risk assessments. Define framework and launch contracts to outsource the periodic assessment of all systems and services. Communicate risk findings to stakeholders, including senior management and governance bodies, providing clear and actionable recommendations;
    - provide independent risk oversight of compliance with applicable digital operational resilience requirements, including DORA where relevant.
- Additional Responsibilities:
    - stay abreast of industry trends and regulatory changes, adjusting risk management strategies as necessary;
    - establish and maintain relationships with internal/external auditors and governance bodies, providing them with the necessary insights for their external assessments;
    - define and evaluate security metrics (KPIs) for security controls on all systems.

Qualifications, experience and skills ("We look for")

We are looking for a Team leader – Principal Risk Officer.

A post-aligned academic qualification is preferred, such as Master's degree or PhD in Finance, Financial Engineering, Economics, Business and Administration, or a highly relevant mathematical discipline. Relevant professional certification such as PRMIA PRM or equivalent would be considered a strong advantage. Prior experience in risk management within a financial institution, Central Securities Depository (CSD), Central Counterparty (CCP), central bank, major custodian, settlement bank, market infrastructure, supervisory authority or comparable systemically important financial institution would be particularly relevant. Quantitative skills and understanding of data structure, system infrastructure and application functionalities would also be required.

Additionally, the ideal candidate should have:

- a minimum of 14 years of relevant professional experience in private and/or public sector financial institutions;

- strong understanding of securities settlement, post-trade infrastructure and financial-market plumbing;

- ability to assess complex risks across technology, operations, financial markets and regulation;

- experience managing large teams and contracts leading to successful ICT operational/risk management initiatives and implementing Internal Control Systems (ICS) to prevent fraud;

- proven experience on ICT oriented risk/audit management or security frameworks such as Certified in Risk and Information Systems Control (CRISC) Certified Information Security Manager (CISM), Certified Information Systems Professional (CISSP), Certified Secure Software Lifecycle Professional (CSSLP), Certified Information Systems Auditor (CISA) or Certified Data Privacy Professional (CDPP) will be considered as a plus;

- experience in the build-out of a comprehensive digital operational resilience framework in strict compliance with the Digital Operational Resilience Act (DORA), establishing proactive ICT risk screening, incident reporting, and threat-led penetration testing.

Other valued qualities: Adaptability as the candidate navigates diverse work environment and maturity levels. Strong organizational and project management skills, staying updated on the latest security threats, and exceptional communication abilities are must-haves. The ability to think creatively and approach challenges from different perspectives is also crucial.

Familiarity with the European Commission environment, including security practices, methodologies and roles (ITSRM, LSO / LISO, CRO, GRC, etc.), will be valued but is not indispensable.

Given the nature of the role, the selected individual will embark on the EU security clearance process. Fluency in English, both spoken and written, is indispensable.

The recruitment grade will be determined in accordance with Article 13 of Commission Decision C(2025)4716, taking account of the candidate's recognised professional experience. In exceptional and duly justified cases, the Authority Authorised to Conclude Employment contracts (AACE) may authorise classification in a higher grade with fewer years of professional experience than normally required under that Article.

How to express your interest?

You should send your documents in a single pdf in the following order:

1. your CV 2. completed application form.

Please send these documents by the publication deadline to CLIMA-E-ARES@ec.europa.eu, Elina.BARDRAM@ec.europa.eu and Javier.CACERES@ec.europa.eu indicating the selection reference CLIMA/COM/2026/526347 in the subject.

No applications will be accepted after the publication deadline.

Eligibility

For eligibility please consult this page with all the information needed.