**REMIT INFORMATION SECURITY IMPLEMENTATION GROUP (RISIG)**

**Terms of Reference**

1. According to Regulation (EU) No 1227/2011 of the European Parliament and Council on wholesale energy market integrity and transparency (REMIT), the Agency shall establish mechanisms to share information it receives with national regulatory authorities. In particular the Agency shall give access to the information sharing mechanisms only to authorities which have set up systems enabling the Agency to meet the confidentiality, integrity and protection of the received information.
2. In order to support the achievement of this objective, the REMIT Information Security Implementation Group (RISIG) is being established as a standing committee of the REMIT Coordination Group. These Terms of Reference define the responsibilities and tasks of the R ISIG.

**Responsibilities**

1. The RISIG shall contribute to assure a certain common level of policy compliance through common processes within a predefined timeframe based on the requirements and/or guidance provided by ACER. The RISIG’s objectives shall be to provide support, advice and coordination on the following primary information security responsibilities of the Agency under REMIT information security policy:
2. to provide for a forum where ACER and NRAs exchange views on information security and provide mechanisms to inform and consult the national regulatory authorities on further policy development;
3. promote the establishment of common Agency and NRAs information security culture, based on the Agency’s REMIT Information Security Policy, including definition of requirements based on REMIT Information Security Policy and policy compliance assessment;
4. to provide input to the REMIT CG and NRAs for the Agency’s measures taken to prevent any misuse of, and unauthorised access to, the REMIT information shared with the NRAs.

The RISIG shall therefore in particular:

* Prepare assessment procedures and guidelines (including assessment or self-assessment guidelines);
* Review compliance of the NRAs with the Agency's REMIT Information security policies (based on ISO standard 27000);
* Assess gaps regarding compliance of NRAs with existing requirements and confirm validity of the proposed mitigation plans created by NRAs;
* Propose and prioritise policy implementation timelines, based on risk analysis;
* Prepare an annual report on information security policy compliance in the scope of REMIT;
* Propose changes to the Agency’s REMIT Information security policy, when necessary in order to improve on the requirements/guidance and when threats will evolve;
* Review and assess policy amendments (improvements) mentioned in the previous paragraph;
* Foster an information security culture and facilitate the exchange of information security good practices between NRAs and the Agency.

The RISIG shall use The Agency's REMIT Information security policy requirements for compliance assessment and develop guidance specifying how the assessment will be conducted and, should this be necessary, how the requirements in REMIT Information Security Policy have to be implemented.

The RISIG will assess the NRAs’ assessment reports and provide an opinion on possible issues that need still to be mitigated, based on the gap analysis. A mitigation plan will be drafted and proposed by the relevant NRA, based on a ‘minimum contents’ strategy or template, which is assessed and confirmed by the Group.

An awareness raising program will be conducted by the RISIG including but not limited to resolved events/incidents documentation sharing, internal training and distribution of relevant materials/manuals.

The RISIG shall encourage and support activities related to open transfer of knowledge including potential on-site visits from ACER and/or other NRAs to evaluate additional risks or assist otherwise, upon prior authorisation and agreement of the relevant NRA.

**Structure and Governance**

1. The purpose of the RISIG is to establish a common set of activities aimed to enable sufficient and credible monitoring of NRAs’ compliance with the ACER REMIT Information security policy. It will be chaired by the ACER representative. Each of the national regulatory authorities shall nominate at least one senior expert (e.g. NRA information security officer) as a member to participate in the work of the RISIG. External consultants may be co-opted to the RISIG, provided all the confidentiality requirements are met. External consultants shall only be allowed to participate if they are contractually bound to NRA or ACER and have signed a confidentiality statement.
2. The RISIG will meet on a monthly basis in Ljubljana, remote access to the RISIG meetings will be provided, as long as the security of the connection and the confidentiality of the information made available at the meeting can be guaranteed. Intermediate meetings will be organised as necessary to enable the RISIG to fulfil its tasks.