Single Rulebook Q&A

Question ID	2014_1153
Status	Final Q&A
Legal act	Regulation (EU) No 575/2013 (CRR)
Topic	Operational risk
Article	4
Paragraph	(1)(52)
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Not applicable
Article/Paragraph	-
Date of submission	07/05/2014
Published as Final Q&A	25/07/2014
Disclose name of institution / entity	Yes
Name of institution / submitter	NATIONAL BANK OF ROMANIA
Country of incorporation / residence	ROMANIA
Type of submitter	Competent authority
Subject matter	Operational risk - compliance risk
Question	Does the definition of operational risk include compliance risk?
Background on the question	According to the definition given by CRR to operational risk, legal risk is included in operational risk. The definition of legal risk was implemented into our national legislation by taking into account the provisions regarding legal risk provided by Basel II Accord ("legal risk include, but is not limited to, exposures to fines, or punitive damages resulting from supervisory actions, as well as private settlements"), which generally fits with the definition that will be provided by the EBA draft RTS on AMA assessment methodologies. The definition of legal risk overlaps in a certain degree with the one of compliance risk provided by EBA Guidelines on Internal Governance (GL 44) ("the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices or ethical standards").

Final answer	For the purpose of calculating capital requirements for operational risk and for the purposes of a proper operational risk management, risk arising from an institution's non-compliance with its legal or statutory responsibilities or requirements must be included in the definition of operational risk found in Article 4(1)(52) of Regulation (EU) No. 575/2013 (CRR). A failure to comply with legal or statutory responsibilities/requirements is one of many different categories of operational risk. It is caused by conscious or unconscious failure to implement the requirements of laws, rules, regulations, agreements, prescribed practices or ethical standards. It may result in a regulatory penalty or fine. From the operational risk perspective, the business practices of a bank are governed by its board and senior management, and should operate in a safe and sound manner, with integrity and in compliance with applicable laws and regulations. The classification depends on the underlying area the rule is governing. Thus, if it is due to lack of formal rules and/or failure to comply with rules governing clients, products or business practises, the event could for example be classified under the category 'Clients, Product and Businesses Processes'. Other cases could result in a classification under category 'Execution, Delivery and Process Management' if related to the non-compliance with regulations and internal rules on Anti Money Laundering; under 'Internal Fraud' if it is due to lack of formal rules and/or failure to comply with rules on personal transactions; or under 'Employment Practices and Workplace Safety' if it is due to unsuitable policies for variable compensation.
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2014_1153