Counter Terrorism Financing Policy[1]

Foreword

RUSI is committed to conducting its business according to all relevant laws and regulations, as well as ensuring it complies with its obligations and manages the risks it is exposed to adequately. Given that RUSI conducts projects in high-risk areas where terrorist organizations and individuals are present, a policy to properly address terrorism financing risks is required.

The policy's main objective is to prevent RUSI's funds from inadvertently reaching the hands of terrorist organizations and/or individuals, as well as complying with the Charity Commission's guidelines on how non-profit organisations need to protect themselves from potential terrorist abuse.

Application

This policy is mandatory for all of RUSI's employees, contractors and subcontractors and should be abided by even if there are contractual obligations, policies or procedures which contradict the guidelines established herein.

What is terrorism financing?

As there is no definition of terrorism, a terrorist organisation or terrorism financing, which is commonly accepted by the international community, for the purposes of this policy the following definitions, based on those established in the Terrorism Act of 2000 of the United Kingdom, will apply:

Terrorism: The action or threat of action designed to influence the government or intimidate the public or a section of it through the use of violence against a person, property, and the endangerment of a person's life, the creation of serious risks to the health and safety of the public and/or the disruption of an electronic system.

[1] This policy does not form part of any employee's contract of employment, and it may be amended at any time.

Terrorist Organisation: A terrorist organisation is any group of people who as a common objective plan to engage or do in fact engage in acts of terrorism, regardless of their size or effectiveness.

Terrorism Financing: The action of inviting others to provide funds, receiving funds or giving funds with the knowledge or suspected knowledge that said funds will be used for terrorism purposes.

Third party risk management and terrorism financing prevention

RUSI's first line of defence to prevent any dealings with terrorist organisations or individuals is adequate knowledge of the third parties with which it engages. "Third parties" refers to employees, subcontractors, and partners. "Adequate knowledge" entails subjecting all third parties to a basic due diligence procedure which will include the following:

- Sanctions screenings to verify the third party has no known ties to terrorist organisations. Said screening will include the following sanctions lists:

    1) The UK's Consolidated List of Designated Individuals and Entities
    2) The UK's Financial Sanctions Targets
    3) The United Nations' Security Council's Terrorist List
    4) The United States' Office of Foreign Assets Control List of Sanctioned Individuals and Entities

In addition, all third parties that act as partners or suppliers for RUSI in contracts with a value equal to or greater than £1,000 or which regardless of the value of the contract are headquartered in high-risk areas[2] or jurisdictions under increased monitoring as per the FATF[3], will be required to provide the following documents:

- A bank letter or recent bank statement to verify that the third party has a bank account in a known financial institution and has successfully undergone KYC procedures in financial entities.
- A Subcontractor Information & Due Diligence form which needs to include the general information of the individual or company (such as name, place of residence, tax ID number, banking information, main shareholders or holding company and main economic activity/main source of income). This form will also include a declaration whereby the third party establishes that all funds to be received/given come from a licit source or will be given a licit purpose.

[2]https://www.gov.uk/government/publications/money-laundering-advisory-notice-high-risk-third-countries--2

[3]https://www.fatf-gafi.org/publications/high-risk-and-other-monitored jurisdictions/documents/increased-monitoring-march-2022.html

Once all documents and information are received, the Risk and Compliance Manager will verify it and if successful, the third party will be entered into RUSI's database to undergo periodic sanctions screenings. All third parties will be required to update their information yearly to ensure that RUSI's database remains accurate, and no major changes have occurred since the onboarding process was completed.

No funds may be accepted or paid unless a third party has undergone an adequate due diligence process and has been approved by the corresponding areas.

Red flags and management of alerts

If a potential third party is flagged during the due diligence process the need for an enhanced due diligence process will be triggered. This process will include verifying key individuals (i.e., main shareholders, general manager, CEO, CFO, etc.) in the organisation to ensure they have not been included in the sanctions lists set out above. If there is an alert in relation to an individual a general online verification will be made to verify any negative press or concerning behaviour in social media. Approval of any individual or organisation who has triggered an alert in the initial due diligence process will require approval from the COO to be onboarded.

If after conducting the enhanced due diligence it is concluded that the third party appears to have links with terrorist organisations through funding, involvement in terrorist attacks or by having defended terrorist acts publicly, it will be rejected immediately.

Any attempts of terrorist organisations or individuals to obtain funding or give funds to RUSI will be considered a serious incident and will have to be reported to the following authorities in accordance with RUSI's Whistleblowing Policy:

- The UK Financial Intelligence Unit as per Part 7 of the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000.
- The Police
- The Charity Commission

No cash policy

In addition to the controls described above, RUSI has a strict no-cash policy by which payments to subcontractors and suppliers will only be made via bank transfer. All funding/donations will need to be transferred via a reputable financial entity as well and acceptance of any form of crypto currency is strictly prohibited. In rare cases where payment by bank transfer is not possible then any alternative arrangement must be discussed with and expressly approved by the Chief Operating Officer or in her absence the Head of Finance.

Version control

Author	First drafted	Approval date and approving body	Latest update
Andrea Plazas	19/10/2022	15/12/2022 – Approved by Senior Management	05/09/2023