A pocket guide to:

Counter-Terrorist Financing (CTF) Risk Assessments

To find out how FCR Compliance can help you to conduct a CTF Risk Assessment, please contact Steve@FCRcompliance.com

FCR Compliance

What is a CTF Risk Assessment?

A Counter-Terrorist Financing (CTF) Risk Assessment focuses on understanding and managing the risk that a firm's products or services could be used to raise, move, or store funds for terrorist purposes.

An effective CTF Risk Assessment starts with identifying where these risks might arise and ensuring that controls are proportionate to the level of exposure.

While closely linked to anti-money laundering (AML) efforts, CTF differs in focus. Money laundering seeks to hide the proceeds of crime, whereas terrorist financing (TF) often involves small and/or legitimate funds used for criminal intent.

Who should carry out a CTF Risk Assessment?

All UK regulated firms are expected to assess their TF risks and maintain effective, proportionate controls to prevent their business from being misused for terrorism-related activity.

Supervisory Focus:

The FCA will not just ask **“What are your risks?”** , it will also ask **“How do you know?”** and **“How do you monitor and respond to change?”**

What is the legal and regulatory framework?

- **Money Laundering Regulations 2017 (as amended):** Firms must identify, assess, and understand their TF risks

- **FCA SYSC & Financial Crime Guide (FCG):** Require proportionate, risk-based policies, controls, and procedures

- **National Risk Assessment (NRA 2025):** Key reference for understanding current and emerging threats

- **Home Office / HM Treasury / FATF:** Issue typology and risk guidance used to evidence awareness

What are the key points in a CTF Risk Assessment?

- Terrorist financing often involves small sums but high consequences

- TF differs from money-laundering — the intent is to fund acts, not conceal profits

- A strong CTF approach demonstrates a living compliance culture, not a static document

- It supports proportionate, defensible control decisions

- It reduces regulatory, reputational, and criminal exposure

How does Terrorist Financing Differ from Money Laundering?

Feature	Money-Laundering	Terrorist Financing
Primary Objective	Conceal or disguise the origin of criminal proceeds	Raise, move, or store funds to support terrorist acts or organisations
Source of Funds	Usually illicit (crime-derived)	Can be legitimate or illicit — salaries, donations, benefits, loans
Transaction Size	Often large sums needing complex layering	Typically small, low-value transactions that appear ordinary
Flow Pattern	Funds move from crime → legitimate system	Funds move from legitimate system → criminal activity

How does Terrorist Financing Differ from Money Laundering?

Feature	Money-Laundering	Terrorist Financing
Visibility in Financial System	Tries to enter and integrate into normal business flow	May exit quickly to fund events, travel, or materials
Detection Challenge	Volume and complexity of layering	Subtle, routine-looking payments — requires behavioural awareness
Risk Focus for Firms	High-value, complex structures, tax-haven exposure	Small payments, online platforms, charities, informal transfers

How does Terrorist Financing Differ from Money Laundering?

Key takeaway:

Standard AML controls are **not enough.**

Firms must demonstrate that they understand their specific terrorist financing risk exposure **and** can detect when funds may be used for terrorist purposes.

Understanding the threat landscape

There are multiple forms of terrorism — each with distinct financial behaviours and control implications, for example:

Typology	Description	Typical funding behaviour
Self-Initiated / Lone Actors	Individuals acting alone	Personal income, small transfers, loans, credit cards, prepaid cards, crypto
Small / Local Cells	Loose domestic networks	Loans, credit cards, informal transfers, local fundraising, membership fees
Overseas Terrorist Fighters	Personal/family funds, remittances, travel payments, online donations	Personal/family funds, remittances, travel payments, online donations

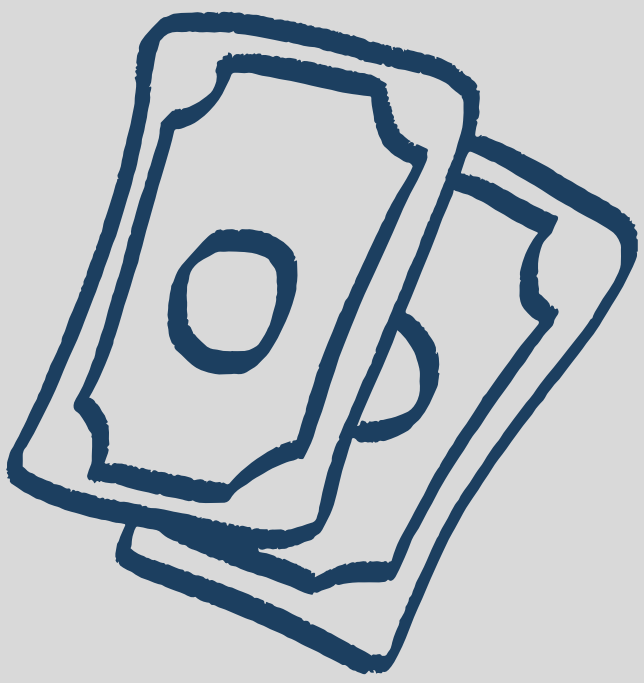
Understanding the threat landscape

Typology	Description	Typical funding behaviour
Decentralised / Networked Groups	Semi-independent affiliates of global movements	Local fundraising, charity misuse, online crowdfunding, commercial profit
Centralised / Territory-Controlling Groups (Daesh, Al-Qaida)	Structured, transactional, revenue-generating	State aid / sponsorship, trade, state revenue, ransom, front companies, layering

Understanding the threats: Self-initiated / lone actors

Vulnerable Sectors:

- Crowdfunding donation platforms
- CASPSs
- Retail banking and other lending
- EMI / PSP
- IVTS / MSB



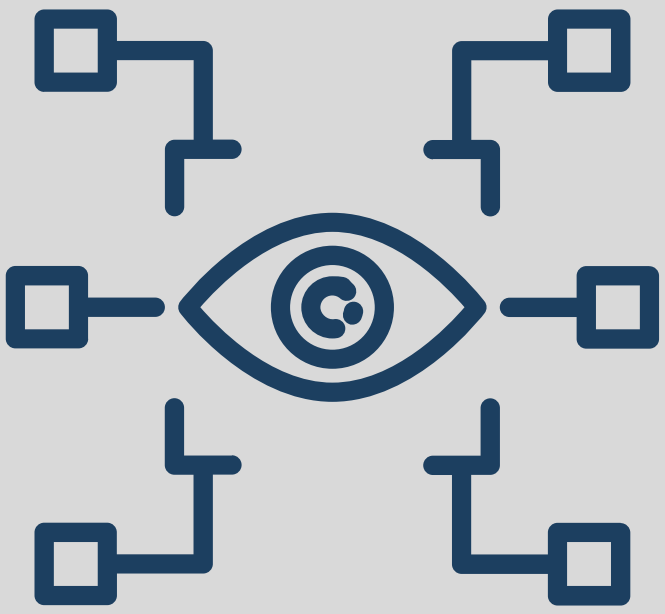
Funding Traits:

- Low-value, self-funded, short-term transactions
- Use of everyday channels (prepaid cards, e-money, crypto)

Understanding the threats: Self-initiated / lone actors

Firm Exposure:

- Micro-payments inconsistent with customer profile
- Sudden changes in payment behaviour or channels



Example Control Focus:

- Behavioural monitoring
- Red-flag rules for new or uncharacteristic payment methods

Understanding the threats: Small / local terrorist cells

Vulnerable Sectors:

- Crowdfunding donations platforms / private donations/ NPO
- EMI / PSP
- VTS / MSB
- CASPS
- Retail banking and other lender
- Wholesale Market / Wealth Management

Funding Traits:

- Community donations, unregistered charities, small business fronts
- Informal systems (hawala, cash couriers)

Understanding the threats: Small / local terrorist cells

Firm Exposure:

- Frequent small inbound transfers from unrelated senders
- Ambiguous charitable or community-group purposes

Example Control Focus:

- Verify legitimacy of customer nature of business
- Enhanced due diligence on small NGOs or cash-heavy operations

Understanding the threats: Overseas terrorist fighters

Vulnerable Sectors:

- Crowdfunding donations platforms
- Retail banking and other lenders
- EMI / PSP
- IVTS / MSB
- CASP

Funding Traits:

- Personal savings, family remittances, travel-linked payments
- Informal transfer systems and crypto increasingly used

Understanding the threats: Overseas terrorist fighters

Firm Exposure:

- Small, repetitive transfers to conflict-adjacent countries
- Sudden withdrawals or ticket purchases inconsistent with profile

Control Focus:

- Incorporate country-risk mapping into transaction monitoring
- Identify travel-linked or destination-based activity

Understanding the threats: Decentralised / Networked Groups

Vulnerable Sectors:

- Crowdfunding donation platforms / online donations
- Wholesale Markets
- Wealth Management
- CASP
- Retail banking and other lenders
- EMI / PSP
- IVTA / MSB

Funding Traits:

- Local fundraising and online crowdfunding
- Use of legitimate fronts or charities
- Crypto wallets for intra-group transfers

Understanding the threats: Decentralised / Networked Groups

Firm Exposure:

- Charities or SMEs sending funds to high-risk jurisdictions
- Online fundraising with vague or shifting purposes

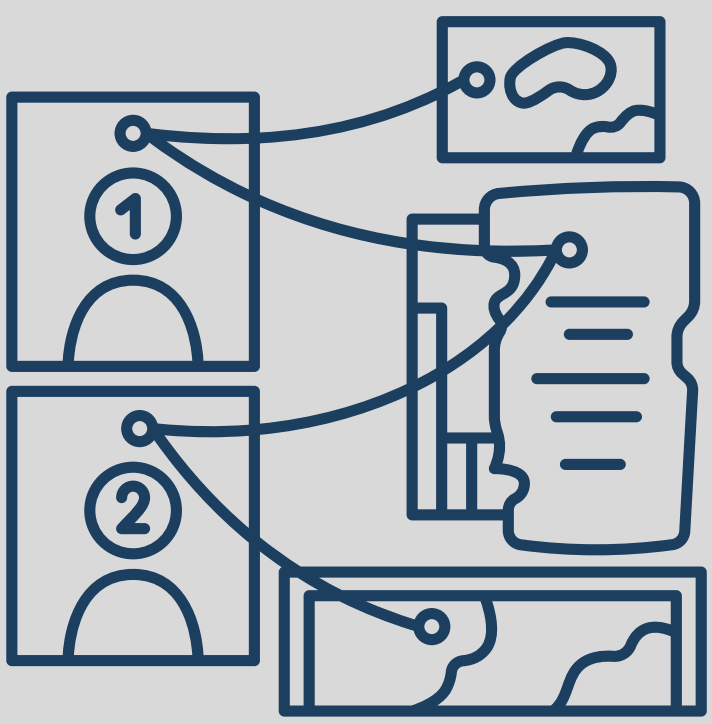
Control Focus:

- Beneficial ownership checks and source-of-funds validation
- Monitor exposure to digital payments and crowdfunding platform

Understanding the threats: Centralised / Territory Controlling Organisations

Vulnerable Sectors:

- Crowdfunding donations platforms / online donations
- IVTS / MSB
- TCSP
- Wealth Management
- Accountancy
- Legal CASP



Funding Traits:

- Diversified income streams: extortion, trade, ransom, smuggling, donations
- Sophisticated money-laundering and sanctions-evasion methods

Understanding the threats: Centralised / Territory Controlling Organisations

Firm Exposure:

- Trade-finance, import/export clients in high-risk jurisdictions
- Complex corporate ownership or shell entities

Control Focus:

- Sanctions screening (including beneficial ownership)
- Trade-based money-laundering controls and document scrutiny

How should you apply proportionate controls?

Core Principle:

Your controls must be commensurate with your firm’s real-world risk exposure.

Proportionality in Practice:

- Match control strength to risk level
- Document how and why each risk was rated
- Avoid “one-size-fits-all” approaches
- Review regularly to reflect emerging threats

Your CTF compliance check list

You should:

Document the understanding of TF risks relevant to your firm

Map your controls to the main terrorist typologies that you are exposed to

Monitor covers small, frequent, or emerging transaction types

Have procedures for identifying and escalating suspicious activity

Your CTF compliance check list

Ensure external intelligence sources are actively monitored and referenced

Ensure your governance and reporting channels are clearly defined

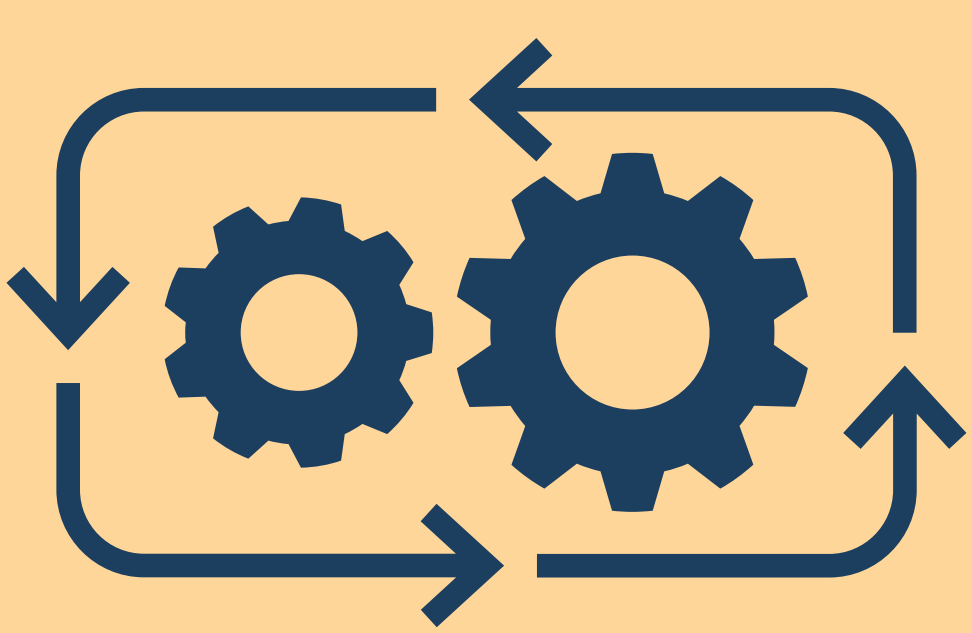
A regular review cycle established and evidenced

Train your staff to recognise TF typologies and behavioural indicators

Tips for best practice

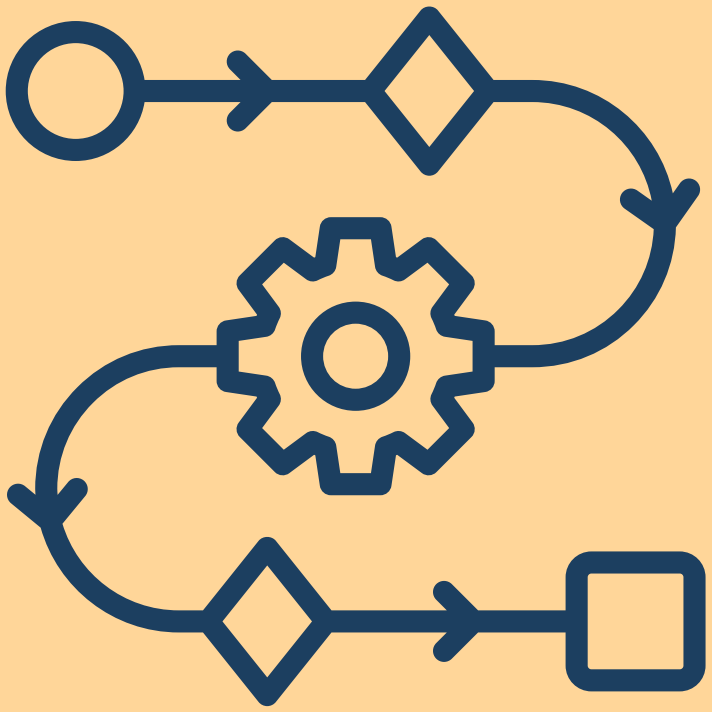
- Tell your risk story: demonstrate real understanding, not just process

- Evidence your reasoning: show how you know each risk and what supports your view



- Scenario test: consider how each terrorist typology could exploit your services

Tips for best practice



- Integrate sanctions and TF controls: one process, shared intelligence
- Train staff: TF differs from ML — ensure awareness of specific red flags
- Stay proportionate: design controls that fit your actual business risk profile

Governance and Oversight: Senior Management

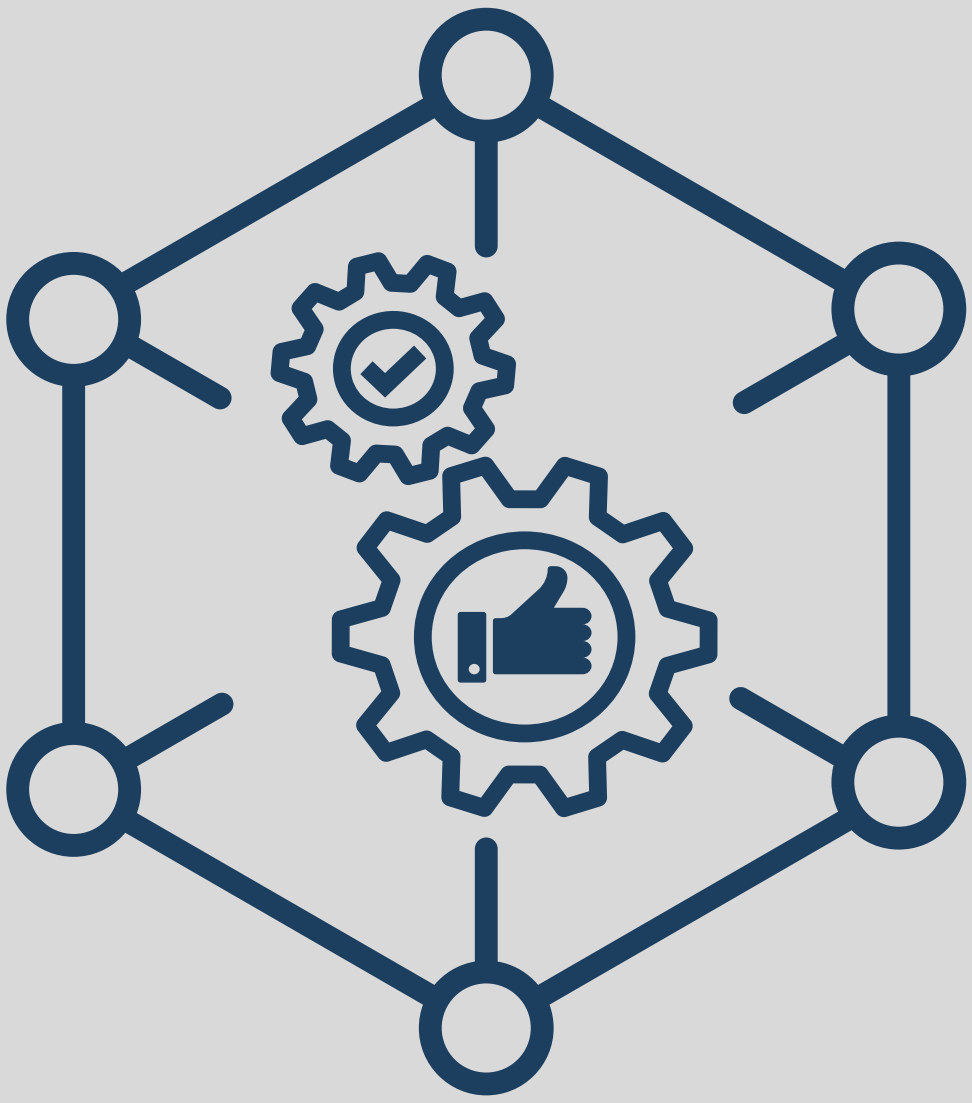
Your Senior Management team should:

- Approve and oversee TF risk approach
- Receive periodic updates on emerging risks and control performance
- Allocate sufficient resources and ensure accountability

Your MLRO / Compliance Function are responsible for:

- Maintaining up-to-date risk documentation
- Leading typology and emerging-risk reviews
- Reporting to management and regulators as required

In summary:



- **Know your risks** — grounded in sources such as the NRA 2025 typologies
- **Evidence your knowledge** — data, intelligence, and reasoning
- **Apply proportionate controls** — matched to real exposure
- **Monitor change** — threats evolve quickly
- **Be audit-ready** — documentation and governance are key

Need support?

If you need support running or reviewing your CTF Risk Assessment, please contact FCR Compliance.

steve@fcrcompliance.com

Steve Lockwood

Steve is one of FCR Compliance's founders. He has been a financial crime specialist for over 20 years.

Steve started his career in law enforcement investigating organized crime money laundering, he then moved to the UK Financial Conduct Authority (FCA) as an investigator in Enforcement and then as a specialist supervisor in the Financial Crime Supervision team. Here he conducted reviews of regulated firms' financial crime compliance programs.

Since 2017 Steve has been helping clients to assess, develop and remediate their Financial Crime compliance programs.

FCR Compliance