Hansuke

Week 22
June 2021

Newsletter

NCA publishes its annual threat assessment

The National Crime Agency (NCA) has released the 2021 National Strategic Assessment (NSA) of Serious and Organised Crime. The NSA report has been compiled using intelligence from across law enforcement, government, the third sector and private industry.

The NSA starkly sets out the threat that organised crime poses to the UK. The ransomware attacks and the laundering of dirty money through the UK has caused harm on a massive scale and reputationally damaged UK based institutions.

The past year has seen huge changes in UK society: Covid-19 has changed the landscape and the NSA highlights that organised criminals have adapted their methods to survive. In particular, offenders have turned to online spaces, increasingly using emerging technologies to commit crimes at scale and avoid detection.

Find out more:
NCA's National Strategic Assessment of Strategic and Organised Crime

Firms must keep their fraud risk assessments under constant review. Contact **henryirving@hansuke.co.uk** to discuss further.

FATF issues Terrorist Financing Risk Assessment Guidance

The FATF guidance aims to assist practitioners in assessing terrorist financing risks by providing good approaches, relevant information sources and practical examples.

This report builds on the 2013 FATF guidance on national money laundering and terrorist financing risk assessments, and draws on inputs from over 35 jurisdictions from across the FATF Global Network on their extensive experience and lessons learnt in assessing terrorist financing risk. Recognising that there is no one-size-fits all approach when assessing terrorist financing risk, this guidance provides relevant information sources and considerations for different country contexts.

Find out more:
Terrorist Financing Risk Assessment Guidance

FSI issues Executive Summary on Cyber Resilience Practices

The Financial Stability Institute (FSI), jointly created by the Bank for International Settlements and the Basel Committee on Banking Supervision, has highlighted significant cyber risks exposures in the financial sector. The vulnerability to cyber risks is due to the sector being technology-intensive and highly interconnected via payment systems.

Financial firms must strengthen their cyber resilience, which FSB defines as "the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents".

The new UK Operational Resilience rules and guidance come into force on 31 March 2022. By then, firms must have identified their important business services, set impact tolerances for the maximum tolerable disruption and carried out mapping and testing to a level of sophistication necessary to do so. Firms must also have identified any vulnerabilities in their operational resilience.

Find out more:
Cyber resilience practices – Executive Summary

ICAEW CHARTERED ACCOUNTANTS