GLOBAL RISK ALLIANCE LTD

TRAINING SERVICES

A solutions approach to risk identification and the prevention of revenue loss.

www.global-riskalliance.com

Overview

Global Risk Alliance houses significant expertise on a number of subject areas within the fields of security, corruption, financial crime, cyber-crime and procurement fraud evidenced, for example, by our authorship of the British Standard (BS10501) on implementing procurement fraud controls, co-convenorship of a new International Standard (ISO) on ant-fraud controls, co-authorship of the OECD's flagship report on illicit financial flows in West Africa and provision of training in each of those areas in numerous countries from Austria, Bulgaria and Nigeria to Denmark, Mexico and Singapore.

This knowledge has been drawn from a range of professional backgrounds from academia and law enforcement to government and the private sector and has been maintained through a constant pattern of engagement with national governments and international organisations.

We provide a broad range of training modes to ensure that you maximise your knowledge requirement outcomes. We design our eLearning, virtual or Instructor Led Training courses to meet your requirements at an operational and executive level. Our courses can also be adapted to consider organisation, local, national and international threats.

Courses can be delivered at preferred locations and dates and at a course length that is agreeable to your requirement.

In this way, the training programmes we provide combine an in-depth knowledge, based on experience and evidence, with a pragmatic understanding of the need for there to be practical application of those courses to real world issues and dilemmas. Each of our courses is designed on the assumption of no prior and/or detailed knowledge and based upon the coverage of all relevant issues in an ordered, logical and systematic manner.

Each of our courses is designed to be interactive because we know from our experience that every delegate has something to offer and that every delegate has something to learn and to introduce into their area of operation.

Let us design your eLearning courses. Agree on content, then we design your training programmes using AI that allows for the creation of courses in over 150 different language and in video or SCORM formats.

Talk to us today

To discuss your requirements further, you can contact us at +44(0) 203 0519297 or arrange a virtual call by emailing us at training@global-riskalliance.com.

Course Aim

This course will provide delegates involved in tackling the financial underpinning of corrupt behaviour with the knowledge, concepts and practices necessary to understand and mitigate illicit financial flows.

Who Should Attend

This course is aimed at those who work within departments of agencies charged with identifying, tracing and recovering illicit funds garnered from corrupt behaviour. Thus, it would be value to those working in:

- Audit
- Taxation
- Risk management
- Law enforcement
- Financial Sector
- NGOs
- Private Sector

Duration

2 - 5 Days

Course Objectives

This course aims to increase and enhance delegates' understanding of the typologies of illicit financial movements and of the mechanisms, structures and tools necessary to identify, trace and mitigate the impact of such flows.

It assumes no prior knowledge of the subject but ensures through a high level of interactivity that delegates with any level of experience in the field will be able share and receive the collective knowledge of the group.

Course Outline

- The nature and extent of corruption in general and in the context of delegates' working experience
- International Legislative and Regulatory frameworks such as the UN Convention Against Corruption
- The Illicit Financial Flows Environment including the level of financial corruption globally, so-called 'secrecy' jurisdictions, illicit financial flow circuits and their enablers
- International Legislative, Regulatory and Institutional provisions including sanctions
- National Counter-Financial Corruption strategies
- Creating an effective anti-corruption agency
- Developing and instituting investigative strategies for mitigating financial corruption including operational procedures and asset recovery
- Financial regulation as an illicit financial flow mitigatory practice
- Global, regional and national anti-bribery provisions
- The proactive use of auditing to discover the loopholes of regulatory approaches to tackling illicit financial flows
- Mitigating financial flows including effective tax policy, reducing capital flight and obtaining multi-jurisdictional technical assistance
- The role of the private and public sector in assisting with tackling financial corruption including the role of 'offshore' tax havens and their reduction of financial transparency
- Risk management strategies and concepts based on real-world and real-time threat assessments
- Tackling the normalisation of financial corruption through dedicated training and education programmes
- Enhancing effective political engagement through an understanding of the nature and impact of populist anti-corruption rhetoric and analysis of the legislative process and its created or common blocking mechanisms
- Strengthening public sector transparency including the notion of professional ethics and ensuring ethical practice in procurement
- Utilising the Media and enhancing advocacy to illustrate the nature, extent and impact of financial corruption
- Incorporating technology and innovation in investigative practice

Course Aim

This course will provide those involved at any stage of the process for procuring goods and/or services within their organisations with the knowledge and skillset to identify and mitigate the threat posed by the breadth and multi-layered complexity of procurement fraud.

Who Should Attend

This course is aimed at a wide range of people since financial crime impacts upon every sector and at every level since it continues to manifest itself globally. Thus, it would be of value to those working in:

- Supply chain risk management professionals
- Public and private sector
- Risk and Compliance professionals
- Those organisation that are expanding into emerging markets, joint ventures and mergers.
- Accountants and auditors
- Project organisations
- Procurement fraud investigators
- Organisations subject to external sanctions and wish to show a holistic lessons learnt approach

Duration

2 - 5 Days

Course Objectives

This course aims to increase and enhance delegates' understanding of the various procurement fraud threats which impact upon them and the organisations, sectors and regions in which they operate and provide them with the tools necessary to mitigate those threats.

Course Outline

- Nature and scope of procurement fraud
- Manipulation of the procurement process with global case examples provided to illustrate each step in the manipulation process
- Examination and analysis of individual and/or organised crime within the procurement cycle
- Creation of a procurement fraud risk lifecycle within an organization
- Examination and analysis of corruption and bribery methodologies utilized during the procurement cycle
- Examination of the essential components for an effective and robust due diligence process and related procedures
- Collection, collation, exploration and evaluation of the data sources available to profile procurement fraud risk within an organisation
- Creating anonymous procurement fraud reporting vectors including hotlines and whistle-blower protection frameworks
- Exploring the nature and impact of the use of technology and data analytics to identify actual and potential procurement fraud risk
- Procurement fraud typologies from a national, regional and global perspective
- Designing of an organizational risk mitigation framework
- Creation and operation of a rapid and systematic anti-fraud and procurement fraud response
- Creation and management of an effective anti-fraud culture
- Determination of the nature and characteristics of robust corruption controls
- Determination of the tender process with the identification of choke points and areas of vulnerability
- Establishing and monitoring of conflicts of interest
- Obtaining and maintaining an independent quality assurance mechanism
- Identifying and utilising a range of fraud identification and analysis tools and techniques
- Determining and detailing various specialist and technical support functions and personnel

Course Aim

This course will provide a clear and concise anti-corruption roadmap that will provide delegates with a detailed understanding of the concepts, strategies and mechanisms needed to mitigate corruption in their home jurisdiction.

Who Should Attend

This course is aimed at those who work or aim to work in the anti-corruption field and/or wish to gain a firmer understanding of the nature and extent of corruption and the steps necessary to mitigate it. Thus, it would be of value to those in the:

- Public sector
- Private sector
- NGOs
- Academia
- Law enforcement

Duration

2 - 5 Days

Course Objectives

The course aims to examine corruption and anti-corruption in a holistic manner ensuring that every issue that might impact upon the success of an anti-corruption strategy is considered and analysed. It assumes no prior knowledge of the subject but ensures through a high level of interactivity that delegates with any level of experience in the field will be able share and receive the collective knowledge of the group

Course Outline

- The nature and extent of corruption in general and in the context of delegates' working experience
- International Legislative and Regulatory frameworks such as the UN Convention Against Corruption
- The nature and impact of good governance
- The creation and implementation of regulatory architecture and the dangers of under or over-regulation as an anti-corruption tool
- Whistle-blowing protection frameworks
- Assessment of international Legislation such as the Bribery Act and the Foreign Corrupt Practices Act and associated cases
- The nature, dynamics and impact of corruption upon economic development
- The relationship between and impact of humanitarian aid and corruption
- Innovative strategies and tools to mitigate corruption in the developing world
- The role and dynamics of advocacy in raising awareness of, increasing public engagement with and reporting of, and dealing with, corrupt behaviour
- Exploring the role and nature of ethical behaviour as a causative or facilitative factor in corruption
- Evaluating a range of anti-corruption agencies in order to ascertain good and bad practice
- Creating more transparent public sector organisations and institutions including the behaviour of officials and politicians who work within or with those bodies and considering related issues such as elections and lobbying
- Corruption risk identification and assessment
- Anti-corruption strategic planning including consideration of the five pillars of anti-corruption, namely, Prevention, Enforcement & Detection, Consequences, Civil Society and Media
- Exploration of the application of knowledge and experience gained by delegates to the delegates' own jurisdictions and/or organisations

Course Aim

This course will provide those involved in international security with a comprehensive understanding of key transnational threats, their typologies, extent and impact and analyse the strategies and mechanisms necessary to mitigate them

Who Should Attend

This course is aimed at those who work within the security environment, whether in an operational or strategic role within an organisation or sector responsible for, or affected by, key security concerns. Thus, it would be value to those working in:

- Law enforcement
- Government
- Intelligence
- Private sector organisations in general and sectors such as aviation, oil and gas in particular

Duration

2 - 5 Days

Course Objectives

This course aims to increase and enhance delegates' understanding of the various security threats, individually and collectively, which impact upon the organisations, sectors and regions in which they operate and provide them with the tools necessary to mitigate those threats.

It assumes no prior knowledge of the subject but ensures through a high level of interactivity that delegates with any level of experience in the field will be able share and receive the collective knowledge of the group.

Course Outline

- Financial Crime and Money Laundering including typologies and financial flows.
- Cybercrime including hacktivism, the Dark Web and intellectual property breaches
- Regulated and Unregulated Drugs Trafficking including typologies, international legislation and regulation, government and law enforcement responses
- Human Trafficking and Human Smuggling
- Trafficking in Endangered species including an exploration of UN conventions and CITES
- Maritime Piracy
- Exploitation and trafficking of movable natural resources including oil, minerals and precious metals
- Border Security and Border Management including the creation of coordinated regional maritime surveillance and intelligence sharing capacity
- Creating Strategic Plans to tackle international security
- International Fight against Terrorism and Organised Crime Networks including the convergence between the two groups and an exploration of the involvement of international agencies
- Creating Strategic Plans to tackle international security
- The application of new technologies in addressing issues of or pertaining to International Security concerns
- The role of intelligence gathering and analysis in tackling international security including agencies, sources of information and the creation of intelligence threat assessments
- Intelligence Led Law Enforcement and Information Sharing including national models, coordination and communication stratagems
- The role and dynamics of anti-corruption as an international security tool

Course Aim

This course will provide those involved in raising cyber awareness for their organisations with a detailed overview of the nature and dynamics of cyber-space in terms of its impact upon personal and corporate security and reputation and how that impact can best be mitigated.

Who Should Attend

This course is aimed at a wide range of people since everyone at both a personal, government or business level are impacted by the connectivity of cyber-space to their daily lives. Thus, whilst it will be of specific relevance to any organisation for whom security issues caused or facilitated by staff members, it will be relevant for anybody who connects at any level to the cyber world. Thus, it would be of value to those working in:

- Law enforcement
- Government
- Private Sector
- Education

Duration

2 - 5 Days

Course Objectives

This course aims to increase and enhance delegates' understanding of the various cyber threats which impact upon them and the organisations, sectors and regions in which they operate and provide them with the tools necessary to mitigate those threats at both a personal and organisational level. It assumes no prior knowledge of the subject but ensures through a high level of interactivity that delegates with any level of experience in the field will be able share and receive the collective knowledge of the group.

Course Outline

- Technological threat environment including the centrality of computer systems and devices, data loss and critical infrastructure disruption
- The information threat environment, including the dangers posed by social engineering (such as the systematic targeting of the users of social networks) and the introduction of mitigating behaviour regarding control of images posted online, the setting of appropriate privacy settings and the avoidance of the placement of personal details, particularly location, on the internet
- The Internet as a cyber target, market and facilitator of crime including the organised crime market in information, identity theft including through malware attacks, cyber-dependent crime underpinned by Crime as a Service (CaaS) such as the use of malware (malicious software), cryptoware (e.g. ransomware) and consideration of the and Dark Web (i.e. illicit commodities sold through illegitimate means)
- The nature and impact of digital disintegration whereby an increasing number of devices are connected online and an increasing number of complex transactions occur on those devices increasing the risk to the devices' owners
- E-commerce and crime – targeting methodologies, cyber security awareness, protocols and policies (passwords, storage and access of data, social networking behaviour of employees)
- Cyber-bullying in terms of its nature, characteristics and impact (from loss of sleep to low self-esteem and in some cases suicide), mitigation (from simply not responding to contacting the Internet Service Provider, School authorities or the police), regulation and legislation
- Cyber-crime investigations and prosecutions with an examination of investigative, evidential, legal and jurisdictional issues including extradition and mutual legal assistance and increasing the digital readiness of law enforcement agencies
- Cyber-Terrorism including the use of the internet (principally social media platforms) for recruitment, propaganda, communication and movement of finances
- Phishing attacks and how to recognise and respond to a common but potentially devastating security risk

Course Aim

This course will provide those involved in identifying and mitigating the threat posed by financial crime a detailed overview of the nature and parameters of such crime (which are necessarily broad in scope) and the tools, processes and mechanisms needed to tackle the complexity of financial crime

Who Should Attend

This course is aimed at a wide range of people since financial crime impacts upon every sector and at every level. Thus, whilst it will be of specific relevance to those individuals who operate in a fraud or financial crime related role, it is also relevant to any member of an organisation since the majority of such crimes are detected by tips from non-specialised but observant personnel. Thus, it would be of value to those working in:

- Law enforcement and Government
- Private Sector
- Banking and Insurance
- Real Estate

Duration

2 - 5 Days

Course Objectives

This course aims to increase and enhance delegates' understanding of the various financial crime threats which impact upon the organisations, sectors and regions in which they operate and provide them with the tools to mitigate those threats. It assumes no prior knowledge of the subject but ensures through a high level of interactivity that delegates with any level of experience in the field will be able share and receive the collective knowledge of the group.

Course Outline

- The nature, scope and impact of Financial Crime including the role and utility of the Fraud Triangle (Incentive, Opportunity and Rationalisation) and perpetrator characteristics
- Impact of market deregulation on the creation of large multinational institutions and the increased globalised risk management vulnerability
- Typologies including investment fraud, mass marketing fraud, insurance fraud, loan and mortgage fraud and money laundering and corruption vehicles
- Real world risk detection and management stratagems including fraud controls, systems and practices.
- Regional focus on fraud including common typologies, typical perpetrators, detection, losses and response
- Identity Theft and Cybercrime including the targeting of organisations and individuals for parcels of information which can facilitate abstraction of customer data
- Bribery and Corruption and their impact upon the facilitation or disguising of financial crime
- The Legislative and Regulatory Framework with a focus upon the most relevant region(s) for delegates and a comparative analysis of other best practice jurisdictions
- Creating an effective and constantly evolving fraud response plan
- Money Laundering as a component of financial crime including the typical three stages of placement, layering and integration,
- Money laundering risks and new technologies (such as internet banking), money laundering risks in structures designed to hide beneficial ownership (such as shell companies) and money laundering and terrorist financing (such as informal value transfer systems)
- Mitigating the money laundering risk through Customer Due Diligence and Enhanced Due Diligence, identifying beneficial owners and Politically Exposed Persons
- Mitigating the money laundering risk through Customer Due Diligence and Enhanced Due Diligence, identifying beneficial owners and Politically Exposed Persons

- Money laundering typologies within a broad geographical context with the identification of key trends and lessons learned from experiencing them
- Anti-money laundering compliance standards
- Anti-money laundering compliance programmes including the determination of risk, policies, training and customer due diligence, suspicious or unusual transaction monitoring and reporting

Course Aim

This course will provide students with the legal knowledge and ethical frameworks for criminal investigation. This includes proper evidence management, investigative techniques while maintaining transparency and accountability. Case preparation and case management, the security of your investigation including protection of whistleblowers.

Who Should Attend

This course is aimed at a wide range of people in both the public and private sector involved in the investigation of corruption and the collection and presentation of evidence. Thus, it would be of value to those working in:

- Government
- Private Sector
- Public Sector
- NGO

Duration

2 - 4 Weeks

Course Objectives

This course aims to increase and enhance delegates' understanding of the investigative process from initial receipt of an allegation or suspicion to the submission of case files and court presentation. This programme provides students with the knowledge and tools for the investigative process. It assumes no prior knowledge of the subject but ensures through a high level of interactivity that delegates with any level of experience in the field will be able share and receive the collective knowledge of the group.

Course Outline

- The foundations and sources of law and the criminal justice system, powers and limits in investigation
- Ethics and human rights, professional conduct and integrity standards
- Whistleblower protections and reporting mechanisms
- Common forms of corruption and associated financial crime in government and business. Root causes and consequences including oversight and accountability mechanisms
- Criminal law basics, legal elements of corruption, bribery and abuse of office
- Arrest, detention, and search procedures specific to corruption cases
- Authorisation requirements for financial investigations
- Evidence handling, chain of custody and anti-tampering safeguards, admissibility of digital and financial evidence
- Investigation planning, scope of cases and resource allocation. Risk assessment and management, crime scene management.
- Interview techniques, cognitive interviewing, recording and legal compliance. Oversight mechanisms, transparency in investigations and audit trails for investigative steps
- Identifying bribery, corruption and abuse of power in government contracts, collaboration with agencies, money laundering detection, tracing illicit financial flows
- Cyber enabled corruption, digital forensics in procurement fraud, tracking electronic bribes and kickbacks
- Mitigating the money laundering risk through Customer Due Diligence and Enhanced Due Diligence, identifying beneficial owners and Politically Exposed Persons
- Case file preparation, structuring and presenting corruption files. Legal and procedural compliance checks
- Court procedures, presenting evidence in corruption trials, police role during trial
- Witness and whistleblower protection, confidentiality protocols and legal protections for informants
- Capstone investigation, simulated corruption case from complaint to trial
- Oversight and integrity review, identifying systemic weaknesses in public sector oversight
- Drafting department wide anti-corruption measures
- Full case presentation and cross examination