iSanctuary

Financial crime training



Specialist modules and a two-week residential programme

Programmes for organisations that prevent, investigate and respond to financial crime.

iSanctuary

Training that connects the whole case

iSanctuary brings together financial investigation, risk advisory and digital-asset expertise. Our training portfolio connects these disciplines to the decisions your people make.

For operational teams

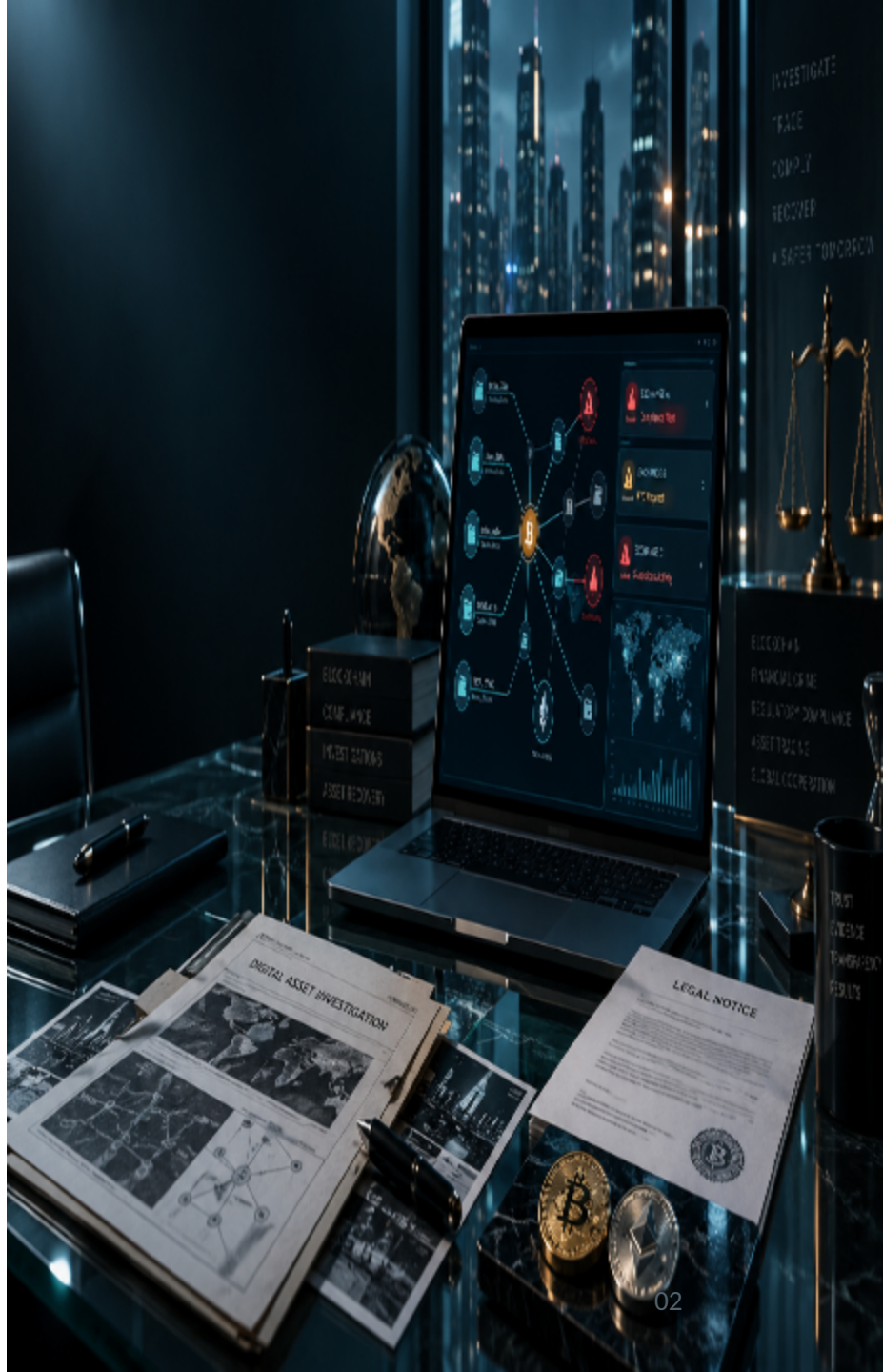
Develop financial lines of enquiry, examine ownership and turn fragmented information into a coherent investigation.

For compliance functions

Assess higher-risk relationships, identify suspicious activity and decide when further investigation or escalation is needed.

For leaders

Challenge controls, set investigation priorities and oversee a coordinated response across organisational boundaries.



iSanctuary

Who the training is for

Content can be selected around the responsibilities and experience of each group.

01 Financial institutions and regulated businesses

MLROs and compliance teams.
Risk functions and senior managers.

02 Public authorities

Investigators, FIUs and regulators.
Tax authorities and prosecutors.

03 Professional and corporate teams

Law firms and forensic teams.
Internal investigators.
Due diligence specialists.

04 Digital-asset businesses

Exchange, VASP and financial-crime teams working with cryptocurrency activity.

iSanctuary

Six areas of training

35
training topics

01 Financial investigation and asset recovery

9 topics covering financial records, fund flows, assets and concealed ownership.

02 Fraud, bribery and corruption

3 topics covering fraud fundamentals, internal investigations and corruption.

03 AML/CFT, sanctions and compliance

10 topics covering risk, controls, due diligence and financial intelligence.

04 Intelligence, OSINT and due diligence

4 topics covering open sources, analysis and enhanced due diligence.

05 Cryptocurrency and digital assets

5 topics covering blockchain, crypto crime, exchanges and REKTify.

06 Investigation management and professional skills

4 topics covering evidence, governance, interviewing and reports.

iSanctuary

A programme built around your team

Start with the capability you need to improve. We can then discuss the topics, level and delivery approach that fit.

01

Focused modules

Select a subject, from transaction analysis to ownership or crypto fundamentals.

02

A combined team programme

Combine modules around a role, investigation type or organisational priority.

03

Two-week residential programme

Ten days covering strategy, investigative methods and a final group exercise.

Module duration, delivery mode, group size and commercial terms are agreed in the proposal.

iSanctuary

SPECIALIST TRAINING

Financial investigation foundations

01

Financial Investigation Fundamentals

Prioritise financial lines of enquiry and develop a financial investigation strategy.

02

Investigative Accounting

Identify inconsistencies, concealed income and possible financial crime in accounting records.

03

Bank Statement & Transaction Analysis

Reconstruct financial activity and identify transactions requiring further investigation.

Illustrative exercise: Review a set of financial records and prioritise the next lines of enquiry.

iSanctuary

SPECIALIST TRAINING

Tracing funds and recovering assets

01

Tracing Funds

Trace fund flows and identify origin, destination, control and possible intervention points.

02

Asset Tracing & Recovery

Develop asset profiles and assess opportunities for restraint, confiscation or recovery.

03

Complex & Cross-Border Asset Tracing

Plan enquiries across jurisdictions and identify information sources and cooperation routes.

Illustrative exercise: Build a fund-flow narrative and identify information needed to establish control of assets.

iSanctuary

SPECIALIST TRAINING

Corporate structures and concealed ownership

01

Companies & Corporate Structures

Interpret corporate records and connect companies, individuals, transactions and assets.

02

Beneficial Ownership Investigations

Identify ultimate owners and recognise arrangements that obscure ownership or control.

03

Shell Companies, Nominees and Concealed Ownership

Recognise concealed ownership indicators and develop enquiries to resolve them.

Illustrative exercise: Map a layered company structure and record gaps in the ownership evidence.

iSanctuary

SPECIALIST TRAINING

Fraud, bribery and corruption

01

Fraud Investigation Fundamentals

Recognise fraud indicators and build proportionate investigation plans.

02

Internal & Corporate Fraud Investigations

Plan defensible internal investigations while managing evidence and confidentiality.

03

Bribery & Corruption Investigations

Identify corruption indicators, financial relationships and investigative priorities.

Illustrative exercise: Scope an internal allegation and prepare an evidence-led investigation plan.

iSanctuary

SPECIALIST TRAINING

Money laundering and risk assessment

01 Money Laundering Fundamentals

Recognise money-laundering typologies in financial and commercial activity.

02 Advanced Money Laundering Investigations

Analyse complex laundering methods and develop financial and evidential enquiries.

03 AML/CFT Frameworks & International Standards

Understand how international AML/CFT standards shape regulation and enforcement.

04 AML/CFT Risk Assessment

Assess AML/CFT risks and translate them into proportionate controls and priorities.

Illustrative exercise: Assess a laundering scenario and explain the risk factors that matter most.

iSanctuary

SPECIALIST TRAINING

AML controls and higher-risk relationships

01 **AML Compliance for Regulated Businesses**

Assess an AML control framework and identify areas for improvement.

02 **Customer Due Diligence and KYC**

Apply risk-based CDD and recognise when further investigation or controls are needed.

03 **PEPs, Sanctions & High-Risk Relationships**

Identify PEP and sanctions exposure and determine appropriate escalation and EDD.

04 **Suspicious Activity Identification & Reporting**

Identify meaningful suspicious activity and develop clear assessments.

Illustrative exercise: Review an onboarding file and draft an escalation rationale for a higher-risk relationship.

iSanctuary

SPECIALIST TRAINING

Financial intelligence and sanctions

01 **Financial Intelligence Units & Financial Intelligence**

Understand how financial intelligence becomes an investigative or regulatory lead.

02 **Sanctions Investigations**

Identify evasion indicators and develop financial, corporate and open-source enquiries.

Illustrative exercise: Combine corporate and financial information to identify possible evasion indicators.

iSanctuary

SPECIALIST TRAINING

Intelligence, OSINT and due diligence

01 OSINT Fundamentals for Investigators

Plan ethical OSINT enquiries and assess source reliability and investigative value.

02 Advanced OSINT for Investigations

Combine open sources to identify relationships, business interests and assets.

03 Intelligence Analysis & Case Development

Identify intelligence gaps and translate analysis into a coherent case strategy.

04 Enhanced Due Diligence

Investigate higher-risk relationships and produce defensible integrity and risk assessments.

Illustrative exercise: Corroborate an online finding and distinguish verified facts from unresolved intelligence.

iSanctuary

SPECIALIST TRAINING

Cryptocurrency investigation foundations

01

Cryptocurrency Fundamentals for Investigators

Interpret basic blockchain activity and identify investigative opportunities.

02

Cryptocurrency Investigations & Blockchain Analysis

Trace digital-asset movements and develop transaction, attribution and investigative leads.

03

Crypto-Enabled Fraud & Financial Crime

Recognise crypto-enabled crime typologies and identify appropriate responses.

Illustrative exercise: Interpret a transaction sequence and identify possible investigative leads.

iSanctuary

CRYPTOCURRENCY AND DIGITAL ASSETS

Exchanges and on-chain intervention

01

Investigating VASPs and Currency Exchanges

Identify service providers that may support attribution, information gathering and recovery.

02

REKTify: On-Chain Investigation & Intervention

Understand how notification, markers and monitoring support wider investigation and recovery.

Illustrative exercise: Identify where exchange engagement or on-chain notification may support a wider investigation.

iSanctuary

SPECIALIST TRAINING

Investigation management and professional skills

01 Evidence Handling and Case Management

Maintain defensible analytical records and communicate findings objectively.

02 Financial Crime Governance & Senior Oversight

Assess governance and the information, assurance and challenge needed for effective oversight.

03 Investigative Interviewing

Prepare structured interview strategies and use financial and other evidence effectively.

04 Writing Effective Investigation Reports

Write reports that distinguish evidence, analysis, findings and recommended action.

Illustrative exercise: Turn mixed case material into an objective report for a senior decision-maker.

iSanctuary

Learning through application

The residential outline combines academic sessions with case studies and operational investigation methods.

01 Context and judgement

Examine policy, regulation and the responsibilities of different organisations before applying them to decisions.

02 Financial and intelligence analysis

Work through the relationship between transaction records, corporate information and investigative hypotheses.

03 Coordinated decisions

Consider evidence, information-sharing and the roles of investigators, prosecutors and regulated firms.

04 A final strategic exercise

Bring the programme together in mixed groups and defend a coordinated response to a senior panel.

iSanctuary

Two-week residential programme

Ten days covering financial-crime strategy, investigative practice and cooperation between public and private organisations.

10

training days

Week one

Threats, policy and regulation. Risk and governance. AML and due diligence. Fraud and corruption. Information and data protection.

Week two

Financial investigation and accounting. Corporate intelligence and OSINT. Asset tracing and recovery. Digital assets. An integrated strategic exercise.

Dates, venue, accommodation arrangements and final faculty are agreed separately.

iSanctuary

Day 1 / Week one

The Financial Crime Landscape: Threats, Policy & Regulation

01

Session focus

The programme opens with the major financial-crime threats and the international AML/CFT architecture. Academic sessions explore policy and regulation alongside the different roles of industry, public authorities and prosecutors.

Learning outcomes

- Understand the contemporary financial crime landscape and major emerging threats.
- Understand how international standards translate into national regulation and enforcement.
- Compare the roles and responsibilities of public- and private-sector organisations.
- Assess how policy and regulatory developments affect financial crime strategy.

iSanctuary

Day 2 / Week one

02

Risk, Governance & Organisational Response

Session focus

Participants examine risk assessment, accountability and control frameworks. Case studies explore organisational failures and how management sets priorities, allocates resources and oversees the response.

Learning outcomes

- Apply risk-based approaches to financial crime.
- Assess the effectiveness of governance and control frameworks.
- Understand the responsibilities of management in overseeing financial crime risk.
- Translate identified threats and vulnerabilities into proportionate responses.

iSanctuary

Day 3 / Week one

AML & Due Diligence

03

Session focus

Participants explore KYC, enhanced due diligence and beneficial ownership alongside PEPs, sanctions and suspicious activity. Sessions consider how regulated firms and public authorities use financial intelligence to support action.

Learning outcomes

- Evaluate CDD and EDD approaches.
- Identify higher-risk relationships, ownership structures and financial crime indicators.
- Understand suspicious activity identification and reporting.
- Assess how financial intelligence can be developed, shared and converted into investigative or regulatory action.

iSanctuary

Day 4 / Week one

04 Fraud, Bribery, Corruption & Complex Financial Crime

Session focus

The programme examines fraud, bribery, corruption and money laundering. Case studies explore how companies, nominees and professional intermediaries can conceal illicit activity across organisations and jurisdictions.

Learning outcomes

- Recognise common and emerging fraud, corruption and money-laundering typologies.
- Understand how complex financial crime schemes operate across organisations and jurisdictions.
- Develop proportionate prevention, detection and investigative responses.

iSanctuary

Day 5 / Week one

Regulation, Information & Data Protection

05

Session focus

Academic sessions examine the collection, use and sharing of financial-crime information. Participants consider privacy, data protection and evidence preservation alongside cooperation between public and private organisations.

Learning outcomes

- Understand key legal and regulatory considerations affecting financial crime work.
- Assess the implications of data protection and privacy requirements.
- Understand opportunities and constraints around information-sharing.
- Identify effective approaches to public-private and inter-agency cooperation.

iSanctuary

Day 6 / Week two

06 Financial Investigation & Accounting

Session focus

Participants examine accounting records, bank statements and transaction data. The day connects financial hypotheses with the development, documentation and preservation of material that may support enforcement or criminal proceedings.

Learning outcomes

- Understand the financial investigation lifecycle.
- Interpret financial and accounting information from an investigative perspective.
- Develop and prioritise financial lines of enquiry.

iSanctuary

Day 7 / Week two

Corporate Intelligence & OSINT

07

Session focus

Participants combine corporate information, beneficial ownership analysis and OSINT. The day explores how multiple sources can explain individuals, business interests, assets and networks, including considerations across jurisdictions.

Learning outcomes

- Analyse corporate structures and beneficial ownership.
- Recognise shell companies, nominees and mechanisms used to conceal control.
- Use OSINT and corporate intelligence to develop and corroborate intelligence.
- Integrate multiple information sources into a coherent intelligence picture.

iSanctuary

Day 8 / Week two

08

Asset Tracing, Recovery & Cross-Border Investigations

Session focus

The day explores fund tracing through accounts, corporate structures and different jurisdictions. Case studies examine the legal and operational steps that connect intelligence and asset tracing with intervention and recovery.

Learning outcomes

- Trace complex movements of funds and identify concealed assets.
- Understand domestic and cross-border asset-tracing strategies.
- Identify intervention, freezing and recovery opportunities.
- Understand the importance of cooperation between investigators, prosecutors, financial institutions and overseas authorities.

iSanctuary

Day 9 / Week two

Digital Assets & the Future of Financial Crime

09

Session focus

Participants examine wallets, transactions, exchanges and crypto-enabled crime. The programme introduces blockchain analysis and REKTify, including notification and monitoring that may support a wider tracing or recovery strategy.

Learning outcomes

- Understand blockchain, wallets, exchanges and digital-asset transactions.
- Recognise crypto-enabled financial crime typologies.
- Understand REKTify and its use cases.
- Explain how blockchain analysis supports tracing, attribution and investigation.
- Assess VASPs, exchanges and on-chain intervention in tracing and recovery.

iSanctuary

Day 10 / Week two

10

Integrated Strategic Exercise

Session focus

Mixed public and private-sector groups take different stakeholder roles in a complex financial-crime scenario. Each group develops a coordinated strategic response and presents its recommendations to a senior panel.

Learning outcomes

- Integrate financial, regulatory, intelligence and investigative information.
- Make proportionate decisions with incomplete information.
- Balance legal, regulatory, operational and reputational considerations.
- Explain how leadership and cooperation affect outcomes across organisations.
- Develop a coordinated strategy and defend recommendations.

iSanctuary

The integrated strategic exercise

On Day 10, participants work in mixed public and private-sector groups on a complex financial-crime scenario.

01

Stakeholder perspectives

Participants take different organisational roles and consider the information, responsibilities and constraints each role brings.

02

Decision-making under uncertainty

Groups weigh legal, regulatory, operational and reputational considerations with incomplete information.

03

A coordinated response

Each group develops a financial-crime strategy, presents it to a senior panel and defends its recommendations.

The scenario and panel arrangements form part of the agreed programme.

iSanctuary

ILLUSTRATIVE EXERCISE

An example of applied learning

Illustrative scenario for a tailored programme

The situation

A higher-risk customer has connections to a layered corporate structure. Financial records raise questions about payments and digital-asset transfers.

The task

Assess ownership, prioritise fund-tracing enquiries and identify what further information each stakeholder needs.

The decision

Present a proportionate response, explain the limits of the available material and record the basis for escalation or further investigation.

This is a suggested training exercise, rather than a client case or a promised course assessment.

iSanctuary

What participants should take back

The selected modules determine the learning outcomes. A combined programme can help teams develop:

01 **Better enquiry plans**

A clearer rationale for which financial, corporate and intelligence questions to pursue.

02 **More defensible analysis**

A consistent distinction between source material, inference, findings and remaining gaps.

03 **Stronger escalation decisions**

A documented basis for due diligence, reporting and investigative action.

04 **Clearer communication**

Reports and recommendations that senior managers and partner organisations can understand and challenge.

iSanctuary

Planning your training

A scoping discussion gives us the information needed to propose an appropriate programme.

01

Your priorities

The operational problem, financial-crime risks or capability gaps you want the training to address.

02

Your participants

Roles, experience, number of delegates and any differences in learning needs.

03

Your context

Sector, jurisdictions, relevant systems and the types of cases or decisions participants encounter.

04

Practical arrangements

Preferred dates, delivery mode, location and budget range. We agree the final syllabus and commercial scope in the proposal.

iSanctuary

Discuss your training needs

Tell us who you need to train and what you want them to do better.

isanctuary.io

Focused courses. Tailored team programmes. Residential training.