# RISK ASSESSMENTS

FIU CONNECT
RISK ASSESSMENTS

ManchesterCF
Financial Intelligence

ARCTIC
INTELLIGENCE

### 2.2.1 Risk Assessment as the Foundation of Proportionality

Supervisors frequently emphasise proportionality in financial crime compliance. Proportionality does not mean reduced standards; it means aligning controls to risk exposure.

Risk assessments provide the evidence base that supports proportionality decisions, such as:

- why enhanced due diligence (EDD) is applied to certain customer segments
- why specific products or services require additional controls
- why specific delivery and transaction channels require additional controls
- why certain jurisdictions trigger enhanced monitoring and/or require additional controls
- why resources are concentrated in particular business or functional areas

Without a defensible FCRA, proportionality arguments lack credibility and are unlikely to withstand supervisory scrutiny. By the same token, applying proportionality in the risk assessment, for example, between risk groups or risk categories or risk factors or risk indicators or controls or assessment units it is important for organisations to document the rationale behind why proportionality was or was not applied.

## 2.3 Statutory v Best-Practice FCRAs

While FCRAs are universally recognised as central to effective compliance, not all risk assessments are created equal. Across jurisdictions, some risk assessments are explicitly mandated by law, while others arise from supervisory guidance, enforcement expectations or recognised good practice.

This chapter clarifies the distinction between statutory (legally required) FCRAs and best-practice (expectation-driven) assessments. It explains how supervisors can interpret these obligations in practice, how refresh cycles and trigger events are assessed and why organisations are frequently sanctioned despite having formally "completed" an FCRA.

For risk and compliance professionals, understanding this distinction is critical. Supervisory enforcement actions consistently demonstrate that meeting the letter of the law is insufficient if the substance of the risk assessment is weak.

### 2.3.1 What is a Statutory FCRA?

A statutory FCRA is one that is explicitly required by law or regulation. In these cases, failure to conduct, maintain or update a risk assessment may constitute a direct breach of legislative obligations.

Across FATF-member jurisdictions, statutory requirements typically arise from:

- AML/CFT legislation
- implementing regulations
- secondary rules or legally binding guidance

Although legislative wording varies, statutory obligations almost always require organisations to:

- identify and assess relevant financial crime risks
- document the FCRA
- have boards sign off on the contents of the risk assessment as it pertains to risk appetite
- keep it up to date

- make it available to supervisors on request

Statutory risk assessments form the legal foundation of a firm's financial crime compliance framework. The major bodies that provide guidance on risk assessments are summarised in Chapter 3.

**Nature, Size and Complexity**

Risk assessments (and controls) must be appropriate and proportionate given the nature, size and complexity of the organisation – here are a few things to consider:

| Nature of Business | Size of the Business | Complexity of the Business |
|---|---|---|
| • What does the business do?<br>• How does it make money?<br>• What products and services are offered?<br>• What types of customer does it serve?<br>• What customer segments does it serve?<br>• How are customers acquired?<br>• What countries does it operate in? | • What is the size of the customer base?<br>• How much revenue is earned annually?<br>• How many staff does the business employ?<br>• How many customers are served?<br>• How many offices/branches are there? | • How many products/services are offered?<br>• What is the nature of products/services?<br>• How many and what channels are used?<br>• How many countries does it operate in?<br>• How regulated is the business?<br>• What is the ownership structure?<br>• What is the governance structure? |

## 2.3.2 Core Financial Crime Risk Domains with Statutory Risk Assessment Obligations

**Money Laundering Risk Assessments**

In most jurisdictions, enterprise-wide money laundering risk assessments are explicitly required under AML legislation; these are commonly combined with terrorist financing and proliferation financing risk indicators.

Failure to maintain a robust money laundering risk assessment is one of the most common grounds for supervisory criticism. Fundamental aspects of money laundering are discussed in more depth in Chapter 4.

**Terrorist Financing Risk Assessments**

Although terrorist financing risk assessments are often combined with money laundering risk assessments, supervisors increasingly expect terrorist financing risk to be assessed in a distinct and explicit manner.

Supervisory findings frequently highlight deficiencies where organisations treat terrorist financing risk as identical to money laundering risk, fail to consider the risks associated with low-value and high-frequency transactions, or overlook geographic and sector-specific terrorist financing typologies.

Best practice and increasingly a supervisory expectation, is that terrorist financing risk is clearly articulated within the enterprise-wide risk assessment, even where overlapping methodologies or data sources are used. A fuller discussion of terrorist financing can be found in Chapter 4.

**Proliferation Financing Risk Assessments**

Proliferation financing risk has received increased supervisory attention following publications released by the FATF in recent years and in response to evolving geopolitical developments.

- behavioural indicators: customer behaviour may indicate trafficking:
  - inconsistent lifestyle compared to stated income
  - victims being escorted to banks or financial institutions
- open-source searches: customer identity and true purpose for transactions can be searched against:
  - court documents
  - news articles
  - publicly available advertisements

By incorporating these components into financial crime risk assessments, risk analysts can better identify, prevent, and disrupt human trafficking activities. This approach ensures compliance with regulatory standards while addressing the unique challenges posed by trafficking-related financial crimes.

## 5.9 Environmental Crime

Environmental crime is a global phenomenon affecting nearly all regions and countries, and has particularly devastating ramifications in developing countries where bad governance, corruption or even violent conflict may be more prevalent[23].

Environmental crime is a complex term, largely due to the many offences falling under its umbrella. While no universal definition of environmental crime exists, it is generally understood to encompass[24]

> *illegal activities harming the environment and aimed at benefitting individuals or groups or companies from the exploitation of, damage to, trade or theft of natural resources, including serious crimes and transnational organized crime.*

Although a range of actors perpetrate offences against the environment, environmental crime is largely driven by transnational organised crime (TOC) groups (sometimes also referred to as organised crime groups or OCGs) who exploit natural resources and destroy habitats for financial gain. TOC groups are attracted by the high profits and low risks associated with the commission of environmental crime offences.

Alongside the rising involvement of TOC groups, environmental crime is increasingly converging with other crimes, such as corruption, drug trafficking, counterfeiting, human trafficking, cybercrime, financing of non-state militias and terrorist groups, and money laundering[25]. For instance, exploiting confusion and ignorance, criminal networks can sustain illegal supply chains in exotic forestry byproducts without being challenged by otherwise competent authorities.

**Environmental Crime Offences**

Environmental crime is a broad term that refers to the exploitation of the world's flora and fauna as well as pollution-related crime. Environmental crime encompasses a number of distinct areas of offences. These categories of offences include[26]:

- illegal trade in ozone-depleting substances (ODS)
- illegal trade and dumping of hazardous waste
- illegal trade in wildlife
- illegal, unreported and unregulated (IUU) fishing
- illegal logging and trade in timber
- illegal extraction and trade in minerals

While it can often be clear where the environmental crime occurred, it is not always clear how the contraband substance got to its destination. Sometimes the substance is sent directly from the source jurisdiction to the destination, in other instances, transit ports are involved.

Understanding transit routes can be a key to unravelling the mystery behind some of these crimes.

Whether sent directly from source jurisdiction to the destination country, or sent circuitously through a transit jurisdiction, there will be a financial footprint left behind.

### 5.9.1 Financial Flows

Criminal activity becomes untenable if criminals cannot easily disguise, move and use the wealth earned from it. Many of the activities outlined in this course are considered by most nations to be predicate offences to environmental crime once the profits are placed into the financial system.

By examining environmental crime through an AML/CFT lens, financial institution employees will be better equipped to spot and report suspicious transactions.

Put simply, environmental crime is inextricably intertwined with financial crime. Taking a "follow the money" approach to the proceeds of environmental crime will help identify the broader criminal support networks that profit from the commission of this crime.

When the amount made by the criminal is small, there is little or no demand for money laundering. For example, a pangolin poacher in a source country can use the amount received for their recent kill as cash to pay for groceries and other daily necessities without attracting attention.

As the pangolin byproducts make their way through transit countries and into destination countries though, the amount of money generated starts to become unwieldly and money laundering becomes increasingly necessary to wash the proceeds.

Once the funds have made their way into the formal financial system, they immediately become more liquid, which makes it harder for authorities to track and seize them.

Assessing financial crime risks related to environmental crime should involve:

- industry and business risk related to industries prone to environmental crimes, such as:
  - forestry and timber trade
  - mining and precious metals
  - waste management and recycling
  - wildlife trade and trafficking
- assess inconsistencies in business operations, such as:
  - boards lacking industry expertise
  - companies with unusually high profit margins compared to peers
- geographic risk related to regions known for environmental crimes, such as[27]:
  - countries with weak environmental regulations
  - areas with high biodiversity and natural resources
  - transit and destination countries for illegal wildlife and timber trade[28]
- corruption hotspots: identify jurisdictions with significant corruption risks that facilitate environmental crimes[29]
- transaction monitoring: look for suspicious transactions or patterns indicative of environmental crimes, such as:
  - large cash transactions tied to high-risk industries
  - payments to shell companies or intermediaries in high-risk regions
  - unusual trade financing arrangements or invoice discrepancies
- supply chain analysis: examine financial flows across the supply chain, from raw material acquisition to final product delivery[30]
- corruption and bribery risks: evaluate risks of bribery or corruption involving government officials, such as:
  - payments to expedite permits or licenses
  - bribes to avoid inspections or enforcement actions
- third-party risks: monitor intermediaries or agents who may facilitate corruption or illegal activities

# 7. RISK ASSESSMENT FUNDAMENTALS

Financial crime risk assessments (FCRAs) only deliver supervisory and operational value when they are embedded within the compliance value chain. Supervisors increasingly assess not just whether a risk assessment exists, but whether its outcomes are translated into policies, controls, monitoring activities, management information and governance decisions.

This chapter explains how enterprise-wide FCRAs integrate with the end-to-end compliance framework from risk identification through to board oversight. It highlights common disconnects between assessment outputs and operational controls and explains why these gaps are a frequent source of supervisory criticism.

## 7.1 The Compliance Value Chain Explained

The compliance value chain represents the logical sequence through which financial crime risks are identified, mitigated, monitored and governed. While terminology may vary between organisations, the underlying structure is consistent across jurisdictions and supervisory frameworks.

At a high level, the value chain comprises:

- risk identification and assessment;
- policy and control design;
- control implementation and operation;
- monitoring, testing and assurance;
- reporting, escalation and governance;
- review, remediation and continuous improvement.

FCRAs sit at the front of this value chain. When weaknesses exist at this stage, deficiencies propagate through all subsequent layers.

## 7.2 Risk Assessments as the Foundation of Control Design

### 7.2.1 Translating Risk into Controls

Risk assessments identify what could go wrong within an organisation and where exposure to financial crime risk is greatest. Controls determine how those identified risks are mitigated in practice. Supervisors expect there to be a clear and traceable relationship between the risks identified in an FCRA and the controls implemented to manage those risks.

An effective framework clearly demonstrates which risks have been identified, which specific controls are designed to mitigate those risks and how the strength of each control aligns with the severity of the underlying risk. For example, higher-risk customer segments should be subject to enhanced due diligence (EDD) measures, higher-risk products should attract increased transaction monitoring thresholds and higher-risk jurisdictions should trigger additional sanctions screening measures.

Where risk assessments do not meaningfully inform control design, supervisors often conclude that controls are misaligned, disproportionate or insufficiently risk-based.

### 7.2.2 Proportionality and Resource Allocation

Risk assessments are a primary mechanism through which organisations demonstrate proportionality in their anti-money laundering (AML)/counter-financing of terrorism (CFT) frameworks. They support defensible decisions about where specialist resources should be deployed, which business units require enhanced oversight and which risks can be accepted within the organisation's defined risk appetite.

In the absence of a robust and defensible risk assessment, organisations often struggle to justify why resources are allocated unevenly across the business. This can lead to supervisory criticism, particularly where higher-risk areas are not demonstrably prioritised.

## 7.3 Control Implementation and Operationalisation

### 7.3.1 From Policy to Practice

Risk assessments inform not only which controls are required, but also how those controls should operate in practice. This includes defining clear ownership of controls, establishing supporting procedures and workflows, setting escalation thresholds and determining appropriate documentation standards.

Supervisors increasingly assess whether controls are operationally effective rather than merely documented. A well-designed risk assessment supports this evaluation by clearly articulating the specific risks that each control is intended to mitigate.

### 7.3.2 Common Implementation Gaps

Supervisory findings frequently identify controls that exist in policy but either have not been implemented in practice or are applied inconsistently across the organisation. Supervisors also observe business units implementing controls without a clear understanding of the underlying risks they are intended to address, as well as training programs that are not aligned to actual risk exposure. Note, for instance, the repeated enforcement actions taken against Standard Chartered Bank (SCB) in the US and UK for persistent deficiencies in the treatment of identified risks. The particulars of this case are examined in Chapter 13.

These gaps commonly arise where risk assessments are overly abstract, overly generic or disconnected from operational realities, resulting in controls that lack practical relevance or effectiveness.

## 7.4 Roles Within the Risk Assessment Process

FCRAs are not completed by a single function but is an enterprise-wide process that relies on clearly defined roles across the first line, second line, third line, senior management and the board. Each role plays a distinct part in ensuring the FCRA is logical, explainable, defensible and based on accurate data from which to make informed risk-based decisions.

The main players typically involved in FCRAs are based on a three-lines-of-defence model:

**First Line of Defence: Business and Operational Functions**

The first line of defence comprises the business units, customer-facing teams, product owners, operations and support functions that own and manage money

# 8. THE FINANCIAL CRIME RISK ASSESSMENT LIFECYCLE

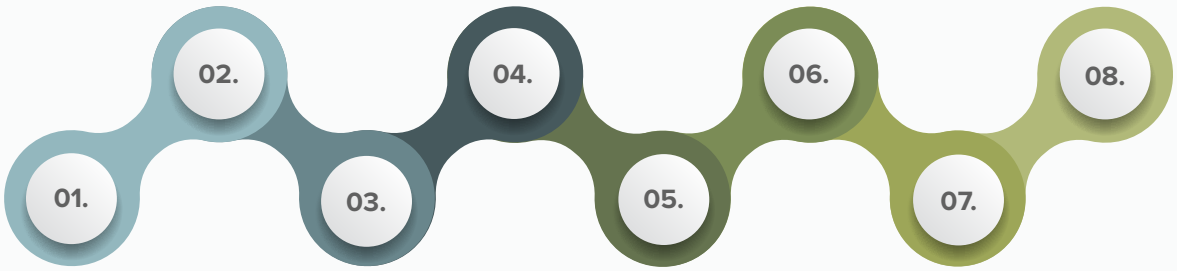
Financial crime risk assessments (FCRAs) are not single events or static documents. Supervisors across Financial Action Task Force- (FATF-) member jurisdictions consistently emphasise that risk assessments must operate as ongoing, cyclical processes that adapt to changes in business activity, customer behaviour, supervisory expectations and the external threat environment.

This chapter examines the full lifecycle of an FCRA from initial scoping and data preparation through to governance, reporting and refresh. It provides a practical framework that risk and compliance professionals can apply regardless of jurisdiction, sector or organisational size.

Understanding the lifecycle is critical for avoiding one of the most common supervisory criticisms: that an organisation has completed a risk assessment, but cannot demonstrate how it is maintained, updated or used over time.

## 8.1 Overview of the Risk Assessment Lifecycle

While organisations may use different terminology or tools, an effective FCRA lifecycle generally consists of the interconnected stages listed atop the next page:




**Data Preparation and Mapping**
Confirm completeness and accuracy of risk and controls mapping. Confirm whether all mapped controls have been tested on schedule. Collate and prepare data, including deciding weightings of inherent risk questions to the inherent risk score.

**Identify Inherent Risks**
Identify inherent risks posed within the following financial crime risk groups: customer, product/service, jurisdiction, delivery channel and transaction.

**Assess Control Effectiveness**
Assess the design and operating effectiveness of controls that are mapped to the inherent risk factors. Effective controls will likely reduce the inherent risk.

**Calculate Residual Risk**
Residual risk is the output of the calculation from inherent risk and control ratings. Since it relies on two data sources, it should be refreshed for accuracy.

**Develop Action Plans**
Based on the residual risk rating, entities should use their Risk Appetite Statement to inform risk-based decisions of whether to avoid (eg, offboard or reject application), mitigate (eg, apply further controls) or accept (eg, within appetite) the risk posed by inherent risk factor.

**Trigger and Time-Based**
Refreshes review the risk assessment annually or ad-hoc in response to defined trigger events (eg, new product offering).

**Track and Monitor**
Report residual risk metrics and new risk factors as part of management information to accountable persons, control owners, risk and compliance governance structures, senior management etc.

**Risk Management**
Oversight and Reporting Board and executive level reporting and discussion in respect of alignment to the organisation's overall risk appetite and adjust as required.

- scoping and planning;
- governance and accountability;
- data preparation and mapping;
- identification of inherent risks;
- assessment of control design and effectiveness;
- residual risk evaluation;
- action planning and risk treatment;
- monitoring, reporting and governance;
- review, refresh and continuous improvement.

These stages are iterative rather than linear. Outputs from later stages often feed back into earlier stages as risks evolve.

## 8.2 Scoping and Planning

### 8.2.1 Defining Scope and Objectives

The risk assessment lifecycle begins with clear and well-defined scoping. Supervisors expect organisations to be able to clearly explain what the risk assessment covers, which legal entities, business units, products and services, channels and countries are included, which financial crime domains fall within scope and how the assessment aligns with applicable supervisory obligations.

Where scoping is poorly defined, risk assessments frequently become either too narrow to be meaningful or so broad that they lack sufficient analytical depth to support defensible conclusions.

### 8.2.2 Governance and Accountability

Effective planning requires clear governance and accountability arrangements to be established at the outset of the risk assessment process. This includes:

- defining ownership of the risk assessment;
- clarifying roles and responsibilities across business, compliance and risk functions;
- establishing approval pathways and escalation thresholds.

Supervisors increasingly expect organisations to demonstrate clarity regarding who is accountable for producing, reviewing and approving the risk assessment, particularly at senior management and board level.

## 8.3 Data Preparation and Risk Mapping

### 8.3.1 Data Collection and Validation

Risk assessments rely on a combination of internal and external data sources. Typical inputs include customer and transaction data, product and service inventories, geographic exposure information, control inventories and testing results, and external risk sources such as typologies and supervisory guidance. Findings circulated by international organisations like those introduced in Chapter 4 as well as the typologies explored in Chapters 5 and 6 will form part of the external risk inputs.

Supervisors expect organisations to validate the completeness and accuracy of the data used in their assessments. Risk assessments built on outdated, incomplete or unreliable data are routinely criticised during supervisory reviews.

### 8.3.2 Mapping Risks and Controls

At this stage of the lifecycle, organisations map their risk categories and risk factors, identify the risk indicators used to assess exposure and document the existing controls intended to mitigate those risks.

## 8.14 Indicator Design: Quality Over Quantity

### 8.14.1 Characteristics of Effective Risk Indicators

High-quality risk indicators are relevant to the underlying risk, clearly defined and unambiguous, supported by reliable data or evidence, and capable of being assessed consistently across different users and business units.

Indicators that are vague, duplicative or unsupported by data undermine the credibility and defensibility of the risk assessment.

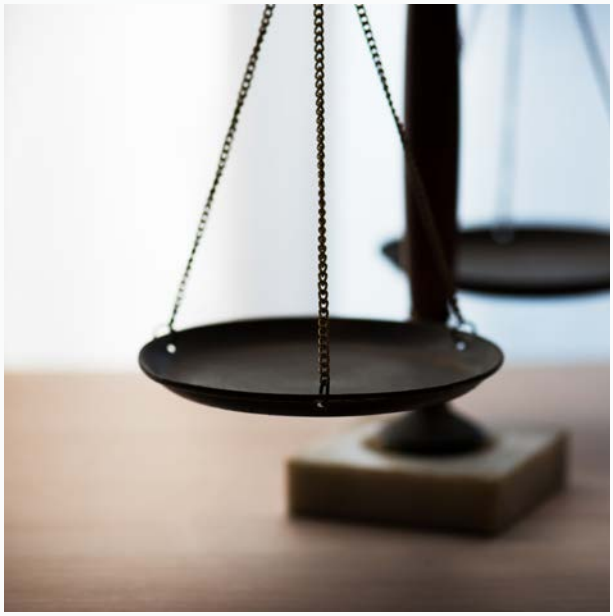
### 8.14.2 Balancing Qualitative and Quantitative Indicators

Most FCRAs rely on a combination of qualitative indicators, such as expert judgment and quantitative indicators, such as metrics, like transaction values and volumes. Supervisors increasingly expect a balanced approach in which qualitative judgment is supported by objective data wherever possible.

Over-reliance on either purely subjective or purely quantitative indicators is often viewed as a weakness. The following sequence illustrates a common challenge for many organisations:

1. firstly, defining the risk indicators that are to be measured;
2. secondly, determining whether a qualitative or quantitative response can be provided based on the availability of data;
3. thirdly, determining how the answer should be treated.

For example, if a risk indicator was “What proportion of our customers are foreign PEPs?” and if the answer was 1%, some organisations may decide to treat this as low risk, whereas others may treat it as medium risk. There are no right or wrong answers, but the key point is explainability and defensibility of the calibration decisions the organisation makes.



## 8.15 Scalability and Enterprise Application

Risk taxonomies and models must be capable of scaling across multiple business units, different jurisdictions and multiple financial crime domains. Scalable frameworks support consistent assessment, comparable reporting and efficient refresh and maintenance processes.

Frameworks that are designed for single-entity or single-jurisdiction use often fail when applied across an enterprise-wide environment. This point is particularly illustrated in the Danske Bank Estonian Branch scandal with is discussed in detail in Chapter 13.

## 8.16 Common Supervisory Criticisms

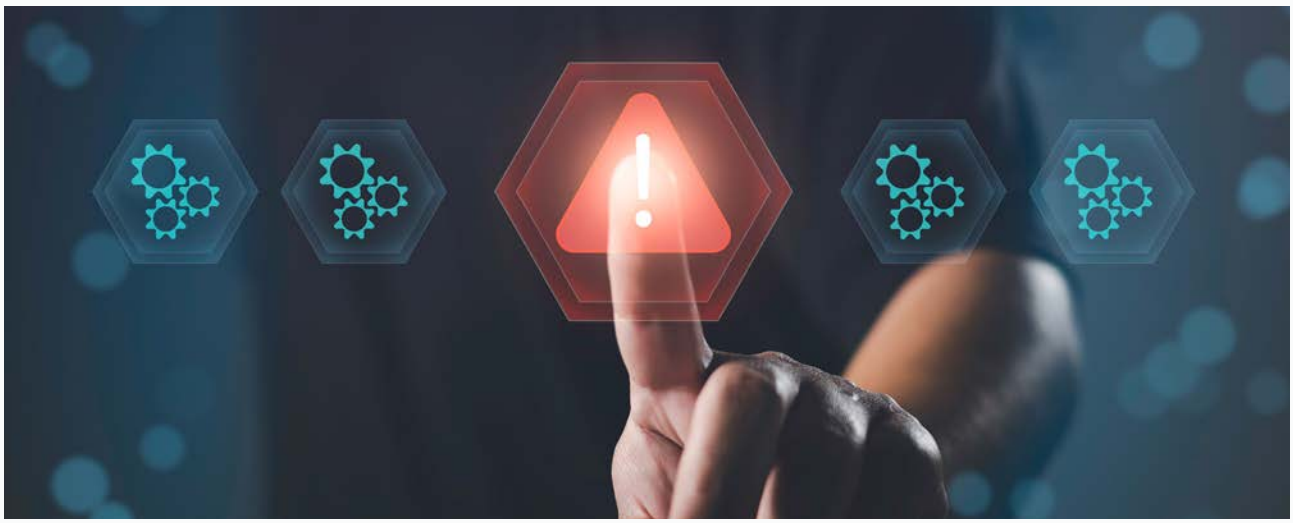
### 8.16.1 Common Lifecycle Failures

Supervisors commonly identify weaknesses across the risk assessment lifecycle, including poor scoping and unclear ownership, inadequate data quality, conflation of inherent and residual risk, lack of evidence supporting control effectiveness and failure to refresh or operationalise risk assessments.

Understanding these common failure points enables organisations to strengthen the maturity and effectiveness of their FCRA lifecycle.

Supervisors frequently identify weaknesses in financial crime risk frameworks, including a lack of clear definitions between different risk layers, inconsistent use of indicators across business units, overly complex models that lack transparency and indicators that do not reflect actual business activity.

Supervisors also commonly note difficulties in explaining how risk conclusions were reached. Addressing these issues is essential to achieving supervisory defensibility and demonstrating a genuinely risk-based approach (RBA).



## Discussion

1. List the interconnected stages of the FCRA lifecycle.
2. Define risk taxonomy.
3. How is the credibility of FCRAs bolstered by the risk taxonomies and models that underpin it?
4. How can organisations avoid supervisory criticism for fragmented, opaque or arbitrary risk assessments?
5. Explain how high-quality, evidence-based risk indicators and transparent aggregation logic are critical to producing explainable and proportionate risk outcomes.
6. What aspects of the FCRA must be scalable across jurisdictions, business lines and financial crime domains to remain effective, consistent and supervisory-ready?

### 10.6.1 What Is a Control?

In a financial crime context, a control is a policy, process, system or activity that is designed to prevent, detect or mitigate the risk of financial crime. Controls may be preventive in nature, such as customer onboarding due diligence; detective in nature, such as transaction monitoring and alert review; or corrective in nature, such as remediation activities following the identification of an incident or breach.

Supervisors expect organisations not only to understand which controls exist within their framework, but also to be able to clearly articulate which specific risks those controls mitigate and how effective the controls are in practice.

### 10.6.2 Control Mapping to Risk

Each material financial crime risk identified through the risk assessment process should be explicitly linked to one or more mitigating controls. Effective frameworks demonstrate clear traceability between risks and controls, avoid gaps in control coverage or over-reliance on a single control and apply control measures that are proportional to the severity of the underlying risk.

Controls that are unmapped or only weakly mapped to identified risks are a frequent source of supervisory concern.

## 10.7 Control Design Effectiveness

### 10.7.1 Assessing Control Design

Control design effectiveness assesses whether a control is capable, in theory, of mitigating the identified risk.

This assessment considers whether the control is appropriately aligned to the underlying risk driver, whether it covers the full scope of the exposure, whether roles and responsibilities are clearly defined and whether supporting procedures are documented and accessible to relevant staff.

A control may be well designed on paper but still fail to reduce risk if it is not properly implemented or embedded in day-to-day operations.

### 10.7.2 Common Design Weaknesses

Supervisors frequently identify design weaknesses such as controls that do not address the underlying risk drivers, excessive reliance on manual processes in higher-risk areas, unclear ownership or accountability and controls that are outdated or misaligned with current business activities.

These design weaknesses undermine the credibility of residual risk conclusions and weaken the overall effectiveness of the financial crime framework.

## 10.8 Operational Effectiveness

### 10.8.1 What is Operational Effectiveness?

Operational effectiveness assesses whether a control is implemented as designed, operates consistently over time and produces the intended risk mitigation outcome. This assessment focuses on execution in practice rather than on the stated intent or existence of the control.

### 10.8.2 Evidence of Operational Effectiveness

Supervisors increasingly expect assessments of operational effectiveness to be supported by objective evidence. Such evidence may include results of:

- control testing
- quality assurance findings
- internal audit reports
- monitoring metrics and trend analysis
- incident or breach data

Assertions that controls are effective without supporting evidence are a common supervisory red flag.

### 10.8.3 Frequency and Scope of Testing

Control testing should be risk-based, with higher-risk controls tested more frequently than lower-risk controls.

Testing should be sufficiently granular to identify weaknesses, documented in a consistent manner and capable of being repeated over time.

Testing programs that are static, overly generic or checklist-driven often fail to identify emerging issues or deteriorating control performance.

## 10.9 Combining Design and Operational Effectiveness

Controls can generally be categorised into one of four states:

1. controls that are well designed and operating effectively
2. controls that are well designed but operating ineffectively
3. controls that are poorly designed but operating consistently
4. controls that are poorly designed and operating ineffectively

Supervisors expect organisations to recognise and distinguish between these states. In particular, controls that operate consistently but are poorly designed do not meaningfully reduce risk, regardless of the level of operational discipline applied.

| Control Design | Control Performance | Control Effectiveness |
|---|---|---|
| Control design refers to the process of assessing whether a control is “fit for purpose” and addresses the risk | Control performance refers to the process of assessing whether the control is operating effectively | Control effectiveness refers to the process of assessing just how effectively a control is operating |

## 10.10 Calculating Residual Risk

### 10.10.1 What is Residual Risk?

Residual risk is the level of financial crime risk that remains after mitigating controls have been applied. It represents the organisation’s actual exposure to financial crime risk and is a critical input into governance, oversight and decision-making processes.

Residual risk should not be treated as a mathematical artefact, a justification exercise or a default “low” outcome. Instead, it must reflect a realistic and evidence-based assessment of control performance.

The ING case illustrates how mis-classifying or concluding that certain risks are residual risks can result in improper management of the risks. Dimensions of this case are discussed further in Chapter 13.

### 10.10.2 Linking Inherent Risk and Controls

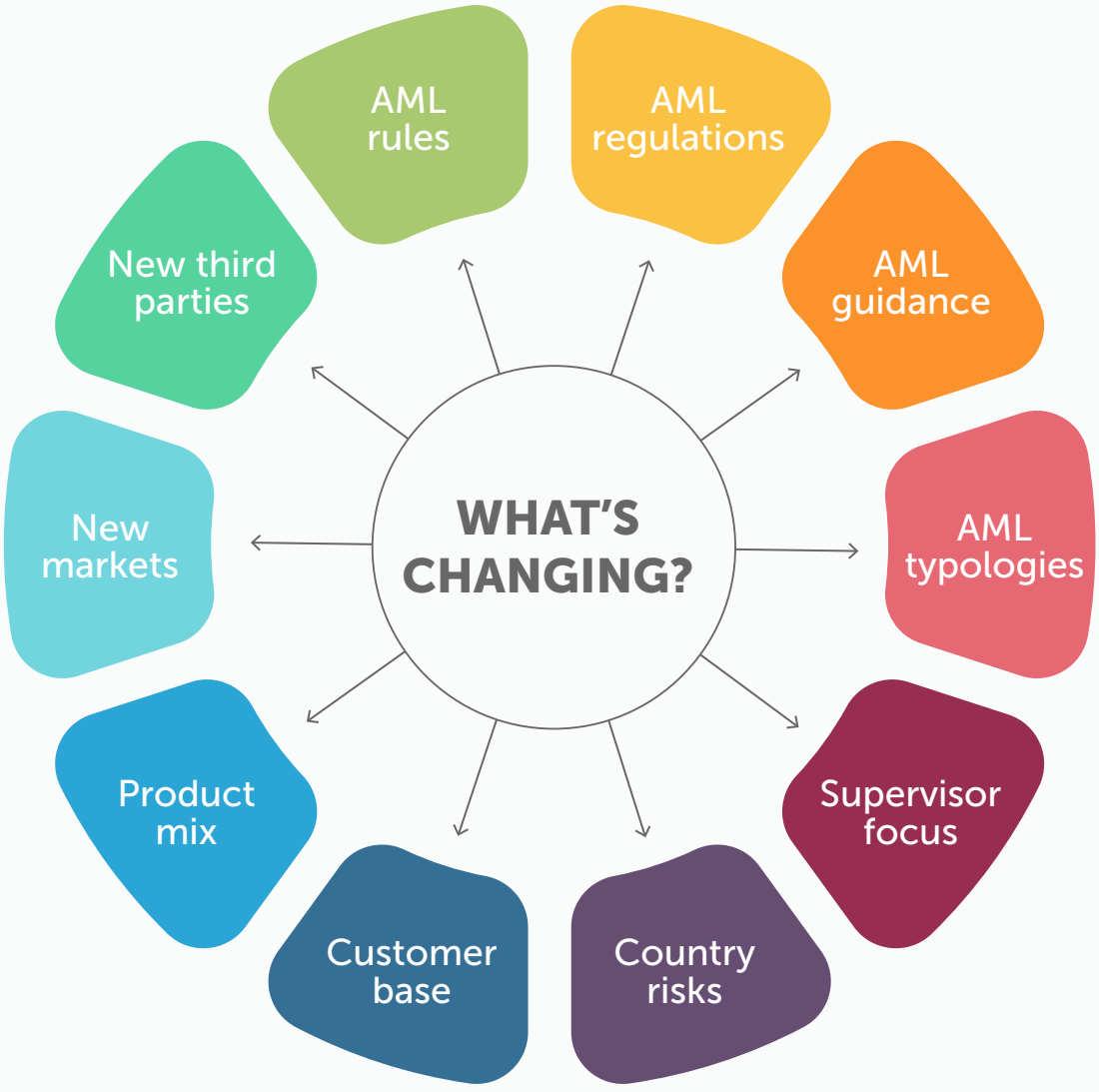
Assessing residual risk requires organisations to understand the severity of inherent risk, assess the strength and effectiveness of mitigating controls and clearly explain how those controls reduce, or fail to reduce, the underlying risk.

Supervisors frequently criticise assessments where residual risk is consistently rated as low despite high inherent risk and weak or poorly evidenced controls.

## 10.11 Residual Risk and Risk Appetite

Residual risk conclusions must be assessed against the organisation's defined risk appetite, risk tolerance and risk limits. Where residual risk exceeds appetite or tolerance, organisations are expected to implement remediation actions, escalate issues to senior management or the board and consider risk avoidance where mitigation is not feasible.

Failure to act on excessive residual risk is a recurring theme in supervisory enforcement actions.



## 10.12 Failures in Putting Assessments into Practice

Supervisors frequently identify weaknesses in financial crime risk appetite frameworks. These weaknesses include:

- vague or generic appetite statements
- failure to reflect appetite in day-to-day decision-making
- inconsistent application across business units
- lack of escalation when risk exceeds tolerance
- poor evidence of board and senior management engagement

The list does not stop there. When organisations put assessments into practice, other weaknesses identified by supervisors include:

- effectiveness assessments that rely on opinion rather than evidence
- failure to distinguish between control design and operational effectiveness
- residual risk ratings that lack clear rationale

- absence of linkage between residual risk and remediation actions
- overly optimistic conclusions that are unsupported by data

Addressing these issues is critical to achieving supervisory defensibility and demonstrating effective governance of financial crime risk.

## Discussion

1. How does the organisation's risk appetite anchor its decision-making response to financial crime?
2. Distinguish risk tolerance from risk appetite. How does defining risk tolerance and risk limits operationalise appetite?
3. How does proportionality inform decisions about which customers require EDD?
4. In a financial crime context, what is a control and what is it designed to do?
5. In your own words, differentiate between control design, control performance and control effectiveness.
6. Compare inherent risk and residual risk. How can an organisation determine if it is willing to accept the level of risk posed by risks that remains after mitigating controls have been applied?

Other FIU CONNECT modules include:

- FIU CONNECT (Terrorist Financing)
- FIU CONNECT (Fundamental AML)
- FIU CONNECT (Human Trafficking)
- FIU CONNECT (Critical Thinking)

For more information visit manchestercf.com.

ManchesterCF
Financial Intelligence