JUST FCC — IN THEORY

Understanding the Law, Purpose, Effectiveness and Limits of Financial Crime Compliance

Author: Sil Kingma
Publisher: Brave New Books
ISBN: 9789465549453
First edition: 2026
Language: English

© 2026 Sil Kingma. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, distributed or transmitted in any form or by any means, including electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the copyright holder, except as permitted by applicable copyright law.

Legal Disclaimer

This book is intended for educational, analytical and informational purposes. It provides a general examination of Financial Crime Compliance, with particular emphasis on the European legal framework, regulatory obligations, institutional responsibilities, effectiveness, proportionality and fundamental rights.

Although reasonable care has been taken in preparing this publication, the author and publisher make no representation or warranty as to the completeness, accuracy or continued applicability of the information presented. Laws, regulations, supervisory expectations and judicial interpretations may change over time.

The views, interpretations and conclusions expressed in this book are those of the author and do not necessarily reflect the positions of any financial institution, supervisory authority or other organisation.

Nothing in this publication constitutes legal advice or should be relied upon as a substitute for professional legal assessment of specific circumstances.

Legal reference date: 1 October 2026.

JUST FCC Series

Volume I — *JUST FCC — IN THEORY*
Volume II — *JUST FCC — IN PRACTICE*

Comply with What the Law Requires, Justify What You Choose, and Remain Accountable for What You Do.

JUST FCC — IN THEORY

Understanding the Law, Purpose, Effectiveness and Limits of Financial Crime Compliance

CONTENTS

SERIES FOREWORD
Introducing JUST FCC 5

PREFACE
Understanding Financial Crime Compliance 11

INTRODUCTION
Why Financial Crime Compliance Must Be Understood Before It Can Be Improved 17

PART ONE — ORIGINS AND PURPOSE 31

Question 1 — What Is Financial Crime Compliance? 32

Question 2 — Why Were Banks Given Responsibilities in the Fight Against Financial Crime? 39

Question 3 — How Did Anti-Money Laundering Rules First Develop? 47

Question 4 — What Is the FATF, and Why Does It Matter to Banks? 56

Question 5 — How Has EU Financial Crime Legislation Developed Over Time? 65

Question 6 — How Did Terrorist Financing Become Part of the Compliance Framework? 69

Question 7 — How Did Financial Sanctions and Other Financial Crime Rules Develop? 73

Question 8 — Why Are Banks Expected to Act as Financial Crime Gatekeepers? 78

Question 9 — What Is Financial Crime Compliance Intended to Achieve? 83

Question 10 — Do We Know Whether the Financial Crime Compliance System Works? 88

PART TWO — THE LEGAL FRAMEWORK 95

Question 11 — Which Financial Crime Laws and Regulations Apply to EU Banks? . 96

Question 12 — What Is the Difference Between FATF Standards, EU Law, National Law and Supervisory Guidance? 105

Question 13 — What Changes Under the New EU AML Framework? 115

Question 14 — What Are a Bank's Main AML and Counter-Terrorist Financing Obligations? 127

Question 15 — What Must Banks Do to Identify and Manage Financial Crime Risks? 137

Question 16 — What Customer Due Diligence and Ongoing Monitoring Duties Does the Law Impose? 145

Question 17 — When Must a Bank Investigate and Report Suspicious Activity? 151

Question 18 — What Are a Bank's Obligations Under Financial Sanctions Laws? ... 159

Question 19 — How Do Proliferation Financing Requirements Differ from AML and Sanctions Obligations? 167

Question 20 — Which Other Financial Crime Obligations May Apply, Including Fraud, Corruption, Market Abuse and Tax-Related Reporting? 175

Question 21 — What Governance, Internal Control and Record-Keeping Duties Apply? 183

PART THREE — THE LIMITS OF THE MANDATE 192

Question 22 — How Do Data Protection Law and Fundamental Rights Affect Financial Crime Compliance? 192

Question 23 — Does the Law Require This Action, or Is It Supervisory Guidance or Bank Policy? 202

Question 24 — How Do Banks' General Terms and Conditions Relate to Financial Crime Compliance Obligations and Internal Policies? 211

Question 25 — Can a Bank Refuse, Restrict or Terminate a Customer Relationship on Financial Crime Compliance Grounds? 220

PART FOUR — EFFECTIVENESS, ACCOUNTABILITY AND FUNDAMENTAL RIGHTS 233

Question 26 — How Do Fundamental Rights Apply to Financial Crime Compliance Decisions? 233

Question 27 — What Does Proportionality Require When a Bank Monitors or Restricts a Customer? 247

Question 28 — When Does Financial Crime Monitoring Become Excessive? 263

Question 29 — How Should Banks Apply Data Minimisation, Purpose Limitation and Retention Rules? 275

Question 30 — How Can Banks Prevent Discrimination in Screening, Monitoring and Risk Classification? 295

Question 31 — What Are the Risks of Profiling, Automated Decision-Making and Artificial Intelligence? 309

Question 32 — When Must a Bank Explain a Financial Crime Compliance Decision to a Customer? 325

Question 33 — How Should Banks Handle Complaints and Challenges to Financial Crime Compliance Decisions? 334

Question 34 — What Remedies Are Available When Financial Crime Compliance Decisions Cause Unjustified Harm? 347

Question 35 — Who Is Accountable for Errors in Financial Crime Compliance Systems? 361

Question 36 — How Should Banks Measure the Effectiveness and Proportionality of Financial Crime Compliance Controls? 374

Question 37 — Can Population-Wide Financial Surveillance Be Reconciled with Fundamental Rights? 387

Question 38 — What Makes Financial Crime Compliance Legally Defensible? 402

FROM THEORY TO PRACTICE 419

Turning Legal Obligations into Proportionate Controls and Defensible Decisions

SERIES FOREWORD

Introducing JUST FCC

Financial Crime Compliance has become an integral part of modern banking. Financial institutions are required to understand their customers, assess financial crime risks, monitor business relationships and transactions, investigate relevant circumstances, report information to competent authorities and comply with applicable financial sanctions. These responsibilities serve important public objectives. They also influence how banks operate, how employees exercise professional judgement and how customers experience access to financial services.

The development of this framework reflects legitimate concerns about money laundering, terrorist financing, sanctions evasion and other forms of financial crime. Banks occupy a distinctive position within the financial system. They maintain customer relationships, process payments and possess information that may help identify the misuse of financial services. Legislators have therefore assigned them preventive responsibilities intended to support broader systems of financial crime prevention, detection and enforcement.

Yet the importance of combating financial crime does not, by itself, establish that every measure adopted in its name is legally required, effective or proportionate.

That distinction lies at the heart of JUST FCC.

Over several decades, Financial Crime Compliance has developed through international standards, European legislation, national laws, supervisory expectations and institutional responses. Banks have translated these requirements into policies, procedures, risk assessments, monitoring systems, investigative processes, reporting arrangements and governance structures. Some practices arise directly from binding legal obligations. Others reflect supervisory guidance, contractual arrangements, institutional risk preferences or decisions about how best to implement applicable requirements.

These different sources of responsibility frequently converge in everyday compliance work. An employee may be required to follow a procedure without necessarily knowing whether its precise form is prescribed by legislation, expected by a supervisor or chosen by the institution. A monitoring control may be treated as established practice even though its contribution to preventing or detecting financial crime has not been independently demonstrated. An additional request for customer information may respond to a genuine legal requirement or identified risk, but it may also reflect an institutional preference whose necessity and scope deserve closer examination.

JUST FCC begins with the proposition that these distinctions matter.

A legal obligation, an operational measure and a demonstrated outcome are three different things. They may be closely connected, but they should not be treated as interchangeable.

A legal obligation establishes what an institution is required to do. An operational measure represents the means through which the institution seeks to fulfil that obligation. Evidence about the measure's operation may demonstrate whether it performs its intended function, while evidence about broader outcomes may be more difficult to obtain. Financial crime prevention depends on the combined activities of financial institutions, supervisory authorities, financial intelligence units, law enforcement bodies and other participants. No individual bank necessarily possesses the information required to establish the wider effects of its preventive activities.

Recognising these distinctions is not an argument against compliance. Banks must fulfil their binding legal obligations, including obligations whose contribution to broader public outcomes cannot be measured precisely. Nor does JUST FCC proceed from the assumption that existing controls are ineffective or unnecessary. Its starting point is that the importance of financial crime prevention makes careful examination of the measures used to pursue it especially necessary.

The existence of a legitimate objective does not eliminate the need to understand the legal authority, purpose, design and consequences of a particular intervention. Equally, uncertainty about effectiveness does not establish that a measure has no preventive value. A responsible assessment must distinguish what the law requires, what the institution has chosen to implement, what the available evidence demonstrates and what remains uncertain.

This distinction becomes particularly important when Financial Crime Compliance affects customers.

Customer due diligence may require individuals and businesses to disclose sensitive personal, financial or commercial information. Transaction monitoring and investigations may involve extensive processing of personal data. Information requests may impose significant administrative burdens. Transactions may be delayed or restricted, and banking relationships may be refused or terminated. Depending on the circumstances, such decisions can affect a person's or business's ability to participate in ordinary economic life.

These consequences cannot be evaluated solely by establishing that an institution has followed its internal procedures. They require attention to the applicable legal framework, the purpose and necessity of the action, the evidence supporting it and the rights and legitimate interests affected.

Banks are private institutions performing responsibilities that serve public objectives. Their preventive role does not confer unlimited authority to investigate customers, restrict financial activity or impose consequences beyond those permitted by applicable law and contract. At the same time, the protection of customer rights does not remove mandatory obligations concerning customer due diligence, reporting, record-keeping or financial sanctions. The challenge is to understand how these

responsibilities and safeguards operate together without allowing either to obscure the other.

The legal framework also does not determine every aspect of operational implementation. Banks may be required to maintain appropriate monitoring arrangements without being instructed to adopt one universal set of detection scenarios, numerical thresholds or investigative workflows. Within the limits established by law and applicable supervisory requirements, institutions must make choices concerning risk differentiation, information collection, technological systems, investigative procedures and the allocation of resources.

Those choices carry responsibilities of their own.

A measure should not be regarded as necessary merely because it has been used for many years, approved internally or incorporated into a standard procedure. Nor should it be reduced or discontinued solely because it is costly, generates substantial operational activity or imposes burdens on customers. The relevant question is whether the institution can explain how the measure relates to its legal obligations, which risks it addresses, what evidence supports its operation and whether its design remains justified.

JUST FCC approaches these questions through four connected principles.

Legally grounded. Every compliance obligation and intervention should be understood in relation to its applicable legal basis. Binding legislation, international standards, supervisory guidance, contractual provisions and internal policies must be distinguished rather than treated as equivalent sources of authority. Where the law requires a particular action, that requirement must be fulfilled. Where discretion exists, the institution should identify the authority and reasoning supporting its chosen approach.

Evidence-informed. Institutions should distinguish between the activities they perform, the functioning of their controls and the outcomes those controls are intended to achieve. Operational statistics, completed procedures and supervisory compliance findings may provide valuable information, but they do not necessarily demonstrate wider effectiveness. Conclusions should reflect what the available evidence can reasonably establish, while acknowledging material limitations and uncertainty.

Proportionate. Financial Crime Compliance measures should be assessed in relation to their legal purposes, the risks they address and the rights and interests they affect. Where the applicable framework permits discretion, institutions should consider whether the selected measures are appropriately targeted and whether less intrusive or burdensome alternatives can satisfy the relevant requirements. Proportionality is not a justification for disregarding binding obligations; it is a discipline for exercising authority within the limits of the law.

Accountable. Compliance decisions and control arrangements should be capable of explanation, appropriate documentation and review. Responsibilities must be allocated to those with the relevant authority, and material choices should be supported by identifiable legal, factual and risk-based considerations. Accountability

concerns not only whether a procedure was followed, but also whether the institution can justify the decisions and arrangements for which it is responsible.

These principles apply at different levels of a financial institution, although the responsibilities involved are not identical.

An employee reviewing a transaction-monitoring alert must operate within approved procedures, evaluate the available information and determine whether closure, further investigation or escalation is justified. That employee does not ordinarily possess the authority to redesign the bank's monitoring framework, change its risk appetite or disregard mandatory requirements.

Those responsible for designing, approving and overseeing the framework must address broader questions. They must consider whether the arrangements provide adequate coverage of applicable obligations and relevant risks, whether controls operate as intended, whether information processing is appropriately justified and whether material weaknesses or unnecessary burdens require changes. Such decisions may involve management, compliance, legal, privacy, risk management, technology and internal audit functions, each acting within its respective responsibilities.

Sound professional judgement and sound institutional design are complementary responsibilities. Neither can substitute for the other.

The JUST FCC series develops this understanding across two connected books.

JUST FCC — IN THEORY

Understanding the Law, Purpose, Effectiveness and Limits of Financial Crime Compliance

The first book examines the foundations upon which Financial Crime Compliance rests. It considers why banks were assigned preventive responsibilities, how international standards and European legislation developed, what the applicable legal framework requires and what can reasonably be established about the effectiveness of financial crime prevention.

It also examines the boundaries of the bank's mandate. Particular attention is given to the distinction between statutory obligations, supervisory expectations, contractual rights and institutional policies. The analysis extends to fundamental rights, data protection, proportionality, equal treatment, automated decision-making, customer protection, legal remedies and institutional accountability.

The central concern is not simply what banks are required to do, but why particular responsibilities exist, how their legal limits should be understood and what justifies the measures adopted in their name.

By addressing these questions together, *IN THEORY* establishes the legal and analytical foundations necessary to distinguish mandatory compliance from institutional choice, preventive activity from demonstrated effectiveness and legitimate intervention from unjustified intrusion.

This volume deliberately focuses on the legal, conceptual and evidential foundations of Financial Crime Compliance. Practical applications, worked examples, case studies and a structured methodology are addressed in the companion volume, JUST FCC — IN PRACTICE.

JUST FCC — IN PRACTICE

Applying the Law Through Proportionate Controls and Defensible Decisions

The second book examines how those foundations should inform the organisation and execution of Financial Crime Compliance within banks.

It addresses customer due diligence, risk assessment, ongoing monitoring, transaction analysis, investigations, reporting, financial sanctions and related financial crime risks. It also considers the governance, documentation, testing and review of controls, including the responsibilities of those who design, operate, challenge and oversee compliance arrangements.

A central part of *IN PRACTICE* is the JUST FCC method, which provides a structured approach to examining monitoring objectives, identifying applicable legal requirements, assessing relevant risks and determining whether controls remain necessary, appropriately targeted and legally sufficient. The method does not presume that less monitoring is always preferable. It requires institutions to examine whether alternative arrangements can fulfil their obligations without unnecessary intrusion or operational burden.

The book also translates these principles into professional decision-making. Through structured reasoning, practical examples and decision-support tools, it examines how relevant facts can be assessed, uncertainty addressed, decisions documented and matters escalated within the authority assigned to the decision-maker.

The central concern is how banks and their employees can fulfil binding obligations through controls and decisions that are effective, proportionate and capable of justification.

The two books are intended to be read as complementary parts of one approach.

IN THEORY establishes the reasons, legal foundations and boundaries of Financial Crime Compliance. *IN PRACTICE* examines how institutions can translate those foundations into operational arrangements and defensible decisions. The first explains the responsibilities and limits; the second examines their implementation. Neither is complete without the other.

Together, they address a question that runs throughout JUST FCC:

Can a financial institution explain not only what it does in the name of Financial Crime Compliance, but why it is required or justified, what evidence supports it and how its consequences are taken into account?

This question cannot always be answered with certainty. Financial crime risks evolve, legal requirements differ between activities and jurisdictions, and the available

evidence may be incomplete. Some obligations leave little or no room for institutional discretion, while others require judgement about how a legally defined objective should be achieved. Reasonable assessments may differ, particularly where relevant facts are uncertain or competing considerations must be evaluated within the applicable legal framework.

JUST FCC does not propose an alternative legal regime, a universal measure of effectiveness or a formula capable of resolving every compliance dilemma. It does not suggest that banks may disregard obligations because their wider impact is difficult to demonstrate, nor that the existence of those obligations automatically justifies every operational measure adopted to fulfil them.

Its purpose is to make the reasoning behind Financial Crime Compliance clearer, more disciplined and more capable of scrutiny.

Preventing financial crime is a legitimate and important public objective. Pursuing that objective responsibly requires financial institutions to understand the authority they have been given, fulfil the obligations imposed upon them, recognise the limits of their mandate and remain accountable for the choices they make within it.

This is the purpose of JUST FCC: to advance Financial Crime Compliance that is legally grounded, evidence-informed, proportionate and accountable.

PREFACE

Understanding Financial Crime Compliance

Before Financial Crime Compliance can be evaluated or improved, it must be understood.

This first book of JUST FCC examines the foundations of a system that has become central to European banking. It asks why financial institutions were assigned responsibilities in the fight against financial crime, how those responsibilities developed, what the law requires, what can reasonably be established about the effectiveness of the resulting framework and where the limits of institutional authority lie.

These are not merely historical or theoretical questions. They shape decisions made every day by banks and their employees. They also determine how those decisions should be assessed when they affect customers, involve extensive processing of personal information or raise questions about the necessity and proportionality of preventive measures.

A customer may be asked to explain the origin of funds, provide information about business activities or clarify a transaction. A bank may determine that enhanced due diligence is necessary, that financial activity requires investigation or that a business relationship cannot continue. Each decision takes place within a framework of legal obligations, supervisory expectations, contractual arrangements, institutional policies and professional judgement.

Understanding that framework is essential to understanding the decision.

Financial Crime Compliance has not developed from a single legal instrument or a unified theory of financial crime prevention. Its responsibilities have accumulated over time. Anti-money laundering measures initially focused heavily on the proceeds of serious criminal activity. Subsequent developments incorporated terrorist financing, beneficial ownership, risk-based customer due diligence, ongoing monitoring and more extensive institutional governance arrangements. Financial sanctions developed through partly distinct legal and institutional processes, reflecting foreign policy, international security and other public objectives.

These areas now overlap in the work of financial institutions, but they do not necessarily share the same legal basis, purpose or consequences.

The distinction matters. A duty to identify a customer is not the same as a duty to investigate circumstances that may indicate suspicious activity. An obligation to report information to a competent authority is not equivalent to a prohibition on

making funds available to a person subject to applicable financial sanctions. A bank's contractual ability to terminate a business relationship is not identical to a statutory obligation to do so. The conditions governing each action must be examined under the legal framework applicable to that action.

The first part of this book therefore begins with the origins and purposes of Financial Crime Compliance. It examines why banks became participants in a preventive system that extends beyond their traditional role as providers of financial services. It traces the development of international standards and European legislation, considers the expansion of preventive responsibilities and examines the objectives that the framework is intended to serve.

It also addresses a question that is fundamental but often difficult to answer:

Do we know whether the Financial Crime Compliance system works?

The answer requires care.

Banks can often measure the activities they perform: customers reviewed, alerts generated, investigations completed, reports submitted and sanctions matches assessed. Such information may be important for operational management, institutional oversight and demonstrating aspects of legal compliance. It does not, however, automatically establish how much financial crime has been prevented or how effectively the wider system achieves its public objectives.

A completed investigation may demonstrate that a bank followed an established procedure without establishing whether the investigation contributed to the detection of criminal activity. A report submitted to a financial intelligence unit may fulfil a legal obligation without enabling the reporting institution to determine how the information was subsequently used. A monitoring system may identify transactions that meet defined detection criteria without demonstrating the extent to which money laundering has been prevented.

These limitations do not establish that preventive measures have no value. Nor does uncertainty about wider outcomes justify disregarding binding legal obligations. They demonstrate why claims about effectiveness must reflect the evidence available and the limits of what that evidence can reasonably establish.

The existence of a legal obligation, the operation of a compliance control and the achievement of a preventive outcome are related but distinct matters.

Understanding those distinctions is essential to the JUST FCC approach.

The second part of this book examines the legal framework applicable to banks operating within the European Union. It distinguishes international standards from EU legislation, national implementation, supervisory guidance and other sources that influence institutional practice. It considers the principal obligations concerning financial crime risk management, customer due diligence, ongoing monitoring, the examination and reporting of suspicious activity, financial sanctions, governance and record-keeping.

The legal framework must also be understood in its proper temporal context.

The analysis uses **1 October 2026** as its principal legal reference date. Particular attention is given to the European Union's new anti-money laundering framework, including the distinction between requirements already applicable at that date and provisions of Regulation (EU) 2024/1624 that will generally become applicable on **10 July 2027**, subject to the regulation's specific provisions and exceptions. Readers should distinguish the law in force at the reference date from forthcoming requirements and verify subsequent legal developments when applying the analysis to particular circumstances.

This distinction is important because the adoption of new legislation does not necessarily mean that all of its substantive requirements are immediately applicable. Equally, institutions may need to prepare for future obligations while continuing to comply with the framework currently governing their activities.

The third part examines the limits of the bank's mandate.

Financial Crime Compliance obligations do not operate outside the wider legal order. Banks remain subject to applicable rules concerning personal data, contractual relationships, customer protection and the exercise of legal rights. Their preventive responsibilities do not confer unrestricted authority to investigate customers, demand information or restrict access to financial services.

At the same time, these legal boundaries must be understood alongside mandatory obligations that financial institutions cannot simply disregard. A bank may be required to conduct customer due diligence, report relevant information or comply with an applicable financial sanctions prohibition even where doing so creates inconvenience or other consequences for the customer.

The essential task is therefore to distinguish circumstances in which the law requires a particular action from circumstances in which the institution must exercise judgement within the discretion available to it.

These questions become especially important when Financial Crime Compliance decisions affect a customer's ability to participate in economic life. Refusing to establish a banking relationship, restricting access to an account or terminating payment services can affect the ability of individuals and businesses to work, trade, receive income, meet financial obligations or conduct ordinary transactions. The consequences may be particularly serious where practical alternatives are limited.

Such decisions require careful attention to their legal and factual foundations. Where the law mandates an action, the institution must comply with the relevant conditions. Where discretion exists, the bank should be capable of explaining the circumstances relied upon, the risks identified, the legal or contractual authority supporting its decision and the reasons for selecting the measure adopted.

This part also examines a distinction that is easily lost in operational practice:

A bank's internal policy is not the same thing as the law.

Internal policies are essential to organising compliance work. They may establish procedures, responsibilities and risk-management requirements that go beyond the minimum measures expressly prescribed by legislation. Such arrangements may reflect legitimate institutional decisions concerning risk appetite, operational consistency and the design of preventive controls.

Their existence does not, however, transform every institutional preference into a statutory obligation. Nor does the fact that a measure is required by internal policy automatically establish that its consequences for customers are justified under applicable law and contract. Understanding these distinctions is necessary both for employees applying procedures and for those responsible for approving, challenging and reviewing them.

The fourth part extends the examination of the bank's mandate to questions of effectiveness, accountability and fundamental rights.

Financial Crime Compliance can involve substantial interference with personal and commercial interests. Customer information may reveal sensitive aspects of financial behaviour. Monitoring systems may process extensive transaction data. Risk classifications may influence the intensity of scrutiny applied to individuals or businesses. Automated systems may affect how customers are assessed, investigated or subjected to restrictions.

These activities raise questions that cannot be answered solely by referring to the importance of financial crime prevention.

The applicable legal framework may require consideration of privacy, data protection, proportionality, equal treatment, transparency, accountability and effective legal protection. The relevance and precise legal effect of these principles depend on the circumstances and the legal provisions governing the activity concerned. Their application must therefore be examined carefully rather than reduced to general assertions that either security or individual rights should always prevail.

Particular attention is given to the relationship between preventive obligations and the principles of purpose limitation, data minimisation and storage limitation. The book also examines the risks of excessive monitoring, discriminatory treatment, profiling and automated decision-making, including the use of artificial intelligence within Financial Crime Compliance processes.

The analysis extends to the consequences of institutional decisions. Under what circumstances should a bank explain a compliance decision to a customer? What opportunities exist to challenge a decision or seek an appropriate remedy? Who bears responsibility when compliance systems produce errors or unjustified consequences? How should effectiveness and proportionality be understood when evaluating preventive controls?

These questions concern more than operational quality. They address the legitimacy, legal boundaries and accountability of a system in which private institutions perform preventive functions serving public objectives.

The fact that a bank acts in pursuit of a legitimate objective does not mean that every intervention is automatically justified. Equally, the existence of fundamental rights and legal safeguards does not permit mandatory preventive obligations to be ignored. A responsible approach requires an understanding of how these requirements interact, which legal standards apply and where institutional discretion begins and ends.

This is also why effectiveness and proportionality must be considered together without being treated as identical concepts.

A measure may operate as intended while imposing burdens that require separate legal justification. Another measure may appear less intrusive but fail to provide the capability necessary to fulfil a binding obligation. A control may generate substantial activity without reliable evidence of its contribution to the purpose it is intended to serve. These possibilities demonstrate why institutional decisions should be assessed through their legal basis, intended objective, available evidence and consequences rather than through a single operational indicator.

JUST FCC does not begin from the assumption that more monitoring is necessarily better, or that less monitoring is necessarily preferable. It begins with the requirement to understand what is legally necessary, what is institutionally chosen and what can reasonably be justified.

The book is organised into four parts:

Part One — Origins and Purpose examines the historical development, objectives and effectiveness of Financial Crime Compliance.

Part Two — The Legal Framework explains the principal legal obligations governing Financial Crime Compliance in European banking and distinguishes the different sources of authority.

Part Three — The Limits of the Mandate examines the boundaries of banks' preventive responsibilities, including the relationship between legislation, supervisory expectations, internal policies, contractual rights and decisions affecting customer relationships.

Part Four — Effectiveness, Accountability and Fundamental Rights examines the legal safeguards, institutional responsibilities and principles governing the justification and consequences of preventive measures.

Together, these parts move from the reasons financial institutions were assigned preventive responsibilities to the legal conditions under which those responsibilities must be exercised and the standards by which their implementation can be assessed.

The question-and-answer structure is intended to make complex issues accessible without presenting them as simpler than they are. Some questions can be answered by identifying a clear legal requirement. Others require distinctions between overlapping legal regimes, careful interpretation of applicable provisions or an assessment of evidence that remains incomplete. Where the law leaves room for institutional judgement, the discussion identifies the considerations relevant to a

defensible decision rather than suggesting that every situation admits a single universally applicable answer.

This book is written for professionals working in Financial Crime Compliance, including those involved in customer due diligence, transaction monitoring, investigations, compliance, legal affairs, risk management, governance and oversight. It is also intended for readers seeking to understand how financial crime prevention affects the relationship between financial institutions, public authorities and customers.

The analysis does not replace applicable legislation, supervisory requirements, institutional procedures or legal advice concerning individual circumstances. Its purpose is to provide the conceptual and legal understanding necessary to interpret those requirements accurately and assess the responsibilities arising from them.

The second book, **JUST FCC — IN PRACTICE**, builds on this foundation. It examines how financial institutions can translate legal obligations into operational controls and professional decisions, including the design and execution of customer due diligence, monitoring, investigations, reporting, governance and control evaluation. It also develops the JUST FCC method for assessing whether monitoring arrangements remain legally sufficient, appropriately effective and no more intrusive than necessary within the discretion permitted by law.

The relationship between the two books is deliberate.

IN THEORY establishes the legal foundations, purposes, boundaries and principles of accountability. *IN PRACTICE* examines how those foundations can be translated into the systems, procedures and decisions through which banks fulfil their responsibilities.

Operational practice cannot be assessed adequately without understanding the legal mandate on which it rests. Equally, an understanding of the mandate acquires practical significance when it informs the design of controls, the exercise of professional judgement and the treatment of customers.

The central message of this first book is therefore straightforward.

Financial Crime Compliance should not be understood solely as a collection of procedures that banks must perform. It is a system of legally defined responsibilities, preventive objectives, institutional choices and consequential decisions. Understanding the relationships between those elements is the starting point for evaluating whether the system is being applied lawfully, effectively, proportionately and responsibly.

The first responsibility is to understand the mandate. Only then can its implementation be properly assessed.

INTRODUCTION

Why Financial Crime Compliance Must Be Understood Before It Can Be Improved

Financial Crime Compliance has developed into one of the most extensive and consequential areas of responsibility within the European banking sector. Financial institutions are required to establish the identity of their customers, understand the nature and purpose of business relationships, assess financial crime risks, monitor financial activity, investigate circumstances that may indicate money laundering or terrorist financing, report relevant information to competent authorities and comply with applicable financial sanctions and other legal restrictions. These responsibilities influence almost every stage of the relationship between a bank and its customers, from the initial decision to establish an account to the monitoring of ongoing transactions and the circumstances in which particular services may be restricted or a business relationship terminated. Their implementation requires substantial investments in technology, specialist personnel, information management, investigative capacity and institutional governance. For the professionals responsible for carrying out these activities, Financial Crime Compliance is often experienced as a continuous sequence of operational requirements, customer reviews, monitoring alerts, investigations, reporting decisions and supervisory expectations. The familiarity of these activities can, however, obscure questions that are fundamental to understanding their legal and institutional justification. Why were banks assigned these responsibilities in the first place? What precisely are they required to achieve? Which elements of contemporary compliance practice follow directly from binding legal obligations, and which have developed through supervisory interpretation, institutional risk preferences or operational choice? What evidence exists that the resulting arrangements contribute to the prevention or detection of financial crime? And how should the exercise of preventive responsibilities be reconciled with the rights and legitimate interests of the individuals and businesses affected by them? These questions are not peripheral to compliance practice. They concern the authority under which banks act, the purposes their activities are intended to serve and the standards by which their decisions and institutional arrangements should be assessed.

The starting point for JUST FCC is that the existence of a legal obligation, the implementation of a compliance measure and the achievement of the public objective associated with that measure are related but analytically distinct matters. A bank may be legally required to establish customer due diligence arrangements, maintain appropriate monitoring procedures or report specified information to a competent authority. It may demonstrate that these obligations have been implemented through documented policies, trained employees, functioning information systems, completed investigations and records of decisions. Such evidence can establish important

aspects of legal compliance and organisational performance, but it does not necessarily demonstrate the extent to which the measures concerned have prevented financial crime, contributed to successful investigations or reduced the misuse of financial services. A customer due diligence process may accurately establish the identity and ownership structure of a customer without revealing whether that customer will subsequently engage in criminal activity. A transaction-monitoring system may identify patterns of financial behaviour considered relevant to particular risks without establishing whether the wider prevalence of money laundering has decreased. A report submitted to a financial intelligence unit may fulfil a statutory reporting obligation without enabling the reporting institution to determine whether the information ultimately contributed to an investigation, prosecution or other enforcement outcome. These distinctions do not diminish the importance of fulfilling legal obligations. They establish the limits of what can reasonably be concluded from evidence that an obligation has been implemented or that an operational process has been completed. Understanding those limits is necessary before meaningful claims can be made about the effectiveness of Financial Crime Compliance.

The difficulty of evaluating Financial Crime Compliance is not merely a technical problem arising from incomplete statistics or imperfect performance indicators. It reflects the institutional structure of financial crime prevention itself. Legislators establish obligations intended to address public risks, supervisory authorities assess the adequacy of institutional arrangements, financial institutions operate preventive controls, financial intelligence units receive and analyse information, and law enforcement authorities investigate suspected criminal conduct within their respective mandates. Each participant performs a different function and possesses only part of the information potentially relevant to evaluating the system as a whole. Banks may have detailed records of customer reviews, monitoring alerts, investigations, reports and decisions concerning financial sanctions. Public authorities may possess information about the subsequent use of financial intelligence, criminal proceedings, asset recovery or enforcement action. Even where information from these different stages can be connected, the relationship between a particular compliance activity and a wider public outcome may remain difficult to establish. Financial crime is frequently concealed, criminal methods evolve and preventive measures may influence behaviour in ways that are not directly observable. A reduction in detected activity may indicate successful prevention, displacement to other channels, changes in reporting practices or weaknesses in detection. An increase in identified cases may reflect improved controls, greater criminal activity or a combination of both. These circumstances make it difficult to determine what would have happened in the absence of a particular preventive measure. They do not make evaluation impossible, but they require a disciplined distinction between what has been observed, what may reasonably be inferred and what remains uncertain.

The importance of this distinction was illustrated by the Netherlands Court of Audit's report *Gevolgen groot, opbrengsten onbekend*, published on 11 March 2026, which examined the Dutch approach to combating money laundering in the banking sector. The report drew attention to the substantial resources devoted to anti-money laundering activities and to significant limitations in the available information about their results. According to the figures discussed in the report, the costs reported by the banks examined had increased to approximately €1.6 billion in 2024, with around 13,000 full-time equivalent staff involved in anti-money laundering activities. The

report also identified consequences for customers and businesses, including burdensome information requests, difficulties obtaining or maintaining banking services and concerns relating to unequal treatment. These findings are important not because they demonstrate that anti-money laundering obligations are unnecessary or that the measures implemented by banks have failed, but because they expose a fundamental difficulty in assessing a system whose activities, costs and burdens can be measured more readily than its ultimate contribution to preventing financial crime. The resources devoted to compliance may be substantial, and the consequences for customers may be significant, while reliable evidence about the overall preventive benefit remains incomplete. This creates a legitimate need for closer examination of the relationship between institutional effort, public objectives and the consequences of preventive measures. At the same time, the absence of sufficiently reliable outcome information must not be transformed into an unsupported conclusion that the system produces no value. Uncertainty about effectiveness is not evidence of ineffectiveness, just as the importance of the objective pursued is not evidence that every measure adopted in its name is effective.

The findings of the Netherlands Court of Audit should be understood within a broader European context in which the implementation, coordination and effectiveness of anti-money laundering measures have been subjects of continuing institutional examination. The European Court of Auditors' Special Report 13/2021, *EU Efforts to Fight Money Laundering in the Banking Sector Are Fragmented and Implementation Is Insufficient*, identified weaknesses in the implementation and coordination of the European framework. Those findings did not establish a single explanation for the limitations of financial crime prevention, nor did they provide a comprehensive quantitative assessment of the amount of criminal activity prevented by banking controls. They nevertheless demonstrated that the existence of extensive legislation and supervisory arrangements does not automatically ensure consistent implementation or establish that the intended public objectives have been achieved. A framework may contain detailed legal obligations while experiencing difficulties involving institutional coordination, information exchange, operational consistency or the evaluation of outcomes. These challenges become particularly significant when successive legislative reforms introduce additional requirements, more extensive monitoring expectations or new supervisory structures. Such developments may address identified weaknesses, improve harmonisation or strengthen institutional capabilities, but their adoption does not in itself establish that the preventive system has become more effective. A responsible assessment must therefore examine not only whether the legal framework has expanded, but also whether the resulting obligations and institutional arrangements are capable of achieving their intended functions, what evidence exists about their performance and which limitations remain unresolved.

The expansion of Financial Crime Compliance has also been accompanied by increasing reliance on measurable operational indicators. Banks can report how many customer files have been reviewed, how many beneficial ownership structures have been examined, how many monitoring scenarios are operating, how many alerts have been generated and how many investigations have been completed. Supervisory authorities may examine these figures alongside governance arrangements, risk assessments, internal controls, staffing levels and the quality of documented decisions. Such information is indispensable for understanding whether an institution possesses the operational capacity to fulfil its obligations and whether its

procedures are functioning as intended. However, operational indicators must be interpreted in relation to the purposes they are intended to serve. A large number of monitoring alerts may indicate extensive detection coverage, but it may also reflect poorly calibrated thresholds, insufficiently differentiated risk assessments or weaknesses in data quality. A relatively small number of alerts may indicate a more targeted monitoring system, but it could equally reveal inadequate coverage or a failure to identify relevant activity. An increase in reports submitted to a financial intelligence unit may result from improved detection, changing criminal behaviour, altered reporting practices or greater institutional caution. Similarly, a high proportion of investigations closed without reporting may reflect effective clarification of initially uncertain activity, but it may also indicate that the underlying detection scenarios are insufficiently precise. Without further evidence, none of these developments establishes whether financial crime prevention has become more effective. The methodological challenge is therefore not that operational indicators are inherently unhelpful, but that their meaning depends on the questions being asked, the characteristics of the control being assessed and the evidence available to support a conclusion.

A further difficulty arises because Financial Crime Compliance is not a single preventive intervention with one clearly defined legal purpose or measurable outcome. Anti-money laundering obligations address risks associated with the movement, concealment and use of criminal proceeds, while counter-terrorist financing measures concern the provision or collection of funds connected with terrorist purposes, including circumstances in which the funds themselves may originate from lawful sources. Financial sanctions may impose asset-freezing obligations, prohibitions on making funds or economic resources available and other restrictions that must be applied independently of whether a transaction appears suspicious under an anti-money laundering monitoring model. Other financial crime responsibilities may concern fraud, bribery, corruption, market abuse, proliferation financing or particular reporting duties established under separate legal frameworks. Although banks may organise these activities within a common compliance function and employ overlapping technological systems, information sources or investigative resources, the legal purposes and performance criteria applicable to them are not necessarily identical. A sanctions-screening control designed to identify persons or entities subject to restrictive measures cannot be evaluated solely through the same criteria as a customer due diligence process intended to establish identity, ownership and the purpose of a business relationship. Nor can the effectiveness of transaction monitoring be determined simply by comparing the number of alerts it generates with the number of transactions prohibited under a sanctions regime. The legal obligations involved may require different forms of evidence, different responses and different standards for assessing whether the relevant function has been performed. Meaningful evaluation must therefore begin with an understanding of the specific legal objective, institutional responsibility and operational purpose of the measure concerned.

This complexity also affects how the legal mandate of banks should be understood. Financial institutions have been assigned significant preventive responsibilities because their position within the financial system provides access to information and operational capabilities that may be useful in identifying and addressing financial crime risks. They maintain customer relationships, process payments, record transactions and observe patterns of financial behaviour that may not otherwise be

available to public authorities in the ordinary course of their activities. Legislators have therefore required banks to perform functions that contribute to broader systems of prevention, financial intelligence and enforcement. Nevertheless, these responsibilities do not transform financial institutions into general criminal investigative authorities, nor do they provide an unrestricted mandate to examine every aspect of a customer's financial affairs. The powers and obligations of banks must be determined by reference to the legal instruments applicable to the relevant activity. An obligation to conduct ongoing monitoring does not automatically answer every question about the amount of information that may be collected, the intensity of scrutiny that should be applied to different customers or the circumstances in which additional investigations are necessary. A duty to report suspicious activity does not automatically establish a separate power to restrict a customer's access to financial services. A bank's contractual ability to terminate a business relationship is not identical to a statutory obligation to do so. These distinctions matter because the legitimacy of an intervention cannot be established merely by referring to the general importance of financial crime prevention. It must be assessed by identifying the applicable legal requirements, the authority supporting the particular action and the conditions governing its exercise.

The distinction between legal duty and operational implementation is especially important because Financial Crime Compliance has developed through multiple layers of regulation and institutional interpretation. The Financial Action Task Force establishes influential international standards that shape national and regional preventive frameworks, while European legislation creates obligations through regulations and directives with different legal effects. National legislation and competent authorities determine important aspects of implementation, supervision, enforcement and institutional responsibility. Supervisory guidance may influence how financial institutions are expected to interpret requirements, organise controls and demonstrate compliance. Banks subsequently translate these obligations and expectations into internal policies, procedures, information systems and decision-making structures. Each layer contributes to the operation of Financial Crime Compliance, but the existence of a requirement at one level does not automatically establish its legal character at another. A recommendation adopted by an international standard-setting body does not become directly binding on an individual bank merely because it is internationally influential. Supervisory guidance may be highly relevant to the interpretation and implementation of applicable requirements without necessarily having the same legal status as legislation. An internal policy may impose mandatory instructions on employees while reflecting choices made by the institution within the discretion permitted by law. These distinctions are not merely technical. They determine whether a particular measure is legally required, whether alternative forms of implementation may be permissible and which authority is responsible for approving, reviewing or changing the institution's approach.

The evolution of the European anti-money laundering framework makes this legal differentiation particularly significant. The directive-based system has developed through successive legislative measures and national implementation, while the European Union has adopted a new framework intended to strengthen harmonisation, institutional coordination and supervision. Regulation (EU) 2024/1624 establishes an important component of the future substantive anti-money laundering and counter-terrorist financing regime, alongside related legislation and

the establishment of the Anti-Money Laundering Authority. However, the adoption of this framework does not mean that all of its substantive requirements apply immediately or that existing national arrangements cease to be relevant before the applicable transition dates. The principal provisions of Regulation (EU) 2024/1624 generally become applicable from 10 July 2027, subject to the regulation's specific provisions and exceptions. For the purposes of this book, the principal legal reference date is 1 October 2026. The distinction between the framework applicable on that date and requirements that will become applicable subsequently must therefore be maintained throughout the legal analysis. This temporal precision is essential because institutions may need to prepare for future obligations while continuing to comply with the legal framework governing their present activities. Regulatory preparation, institutional anticipation and the existence of a binding obligation are related but distinct matters. The changing European framework consequently illustrates why Financial Crime Compliance cannot be understood as a static collection of rules detached from their sources, legal effects and dates of application.

The relationship between binding obligations and institutional discretion becomes particularly relevant when banks determine how their controls should operate. Legislation may require institutions to identify and verify customers, assess financial crime risks, monitor business relationships and report specified information, but it does not necessarily prescribe every operational detail of the systems used to perform these functions. Within the applicable legal framework, institutions may need to determine how monitoring scenarios are configured, how customer risk classifications are applied, which information sources are used, how investigative responsibilities are allocated and how the performance of controls is evaluated. Such decisions may be influenced by the institution's activities, products, customer population, geographical exposure, technological capabilities and risk assessment. They may also reflect historical arrangements, previous supervisory findings or decisions concerning institutional risk appetite. The existence of operational discretion does not mean that every alternative is legally acceptable, nor does it allow banks to weaken mandatory controls merely because doing so would reduce costs or administrative effort. It does, however, create a responsibility to distinguish between measures necessary to fulfil binding obligations and choices whose continued justification should be assessed through appropriate evidence and governance. A control may have been introduced in response to a genuine weakness, but its continued necessity cannot always be established solely by referring to the circumstances that originally justified it. Risks may change, technology may improve and alternative arrangements may become available. Without periodic examination, institutions risk treating established practices as legally inevitable even where the applicable framework permits different methods of achieving the required objectives.

The consequences of these choices are not confined to the internal operation of banks. Financial Crime Compliance can significantly affect customers, businesses and other participants in the financial system because preventive controls frequently require the collection and examination of personal or commercially sensitive information. Customers may be asked to explain the purpose of transactions, provide documents concerning their income or business activities, identify beneficial owners or demonstrate the origin of funds or wealth. Some requests may be necessary to fulfil specific legal obligations, while others may arise from the bank's assessment of particular risks or from its chosen approach to implementing broader requirements. Investigations may delay transactions, and unresolved concerns may lead to

restrictions on services or decisions concerning the continuation of a business relationship. For individuals, such consequences may affect the ability to receive income, pay essential expenses or conduct ordinary financial transactions. For businesses, they may interfere with payments, commercial relationships, access to financial services and continued operations. These consequences may be justified where they are required by applicable law or supported by sufficiently established legal and factual considerations, but their potential significance makes it important to examine the authority under which they occur. The fact that an institution pursues a legitimate public objective does not eliminate the need to determine whether a particular intervention remains within the applicable legal framework, whether the information requested is relevant to its stated purpose and whether appropriate safeguards are maintained. Nor does the existence of a risk automatically establish that every possible preventive response is legally available or justified.

The protection of privacy, personal data, equal treatment and other fundamental rights therefore forms an essential part of the legal context within which Financial Crime Compliance must operate. The General Data Protection Regulation establishes requirements concerning lawful processing, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability, subject to the specific legal provisions governing the processing concerned. The Charter of Fundamental Rights of the European Union provides a wider framework of rights that may be relevant when EU law is implemented or applied within its scope. These requirements do not mean that banks are prohibited from collecting information necessary to fulfil statutory obligations, nor do they establish that individual preferences can override mandatory preventive measures. They do, however, require attention to the legal basis, purpose, scope and safeguards applicable to the processing and use of information. A control involving extensive personal data should be connected to an identifiable lawful purpose, and the information processed should be assessed against the requirements governing that purpose. Where an institution possesses discretion over the design of a monitoring arrangement, the consequences of alternative configurations may be relevant to determining whether its choices are appropriately justified. Conversely, a proposed reduction in information processing must preserve the institution's ability to fulfil binding legal obligations. The relationship between financial crime prevention and fundamental rights is therefore not a simple opposition between security and privacy. It concerns the application of multiple legal requirements within a coherent framework in which preventive duties, institutional authority and individual safeguards must each be understood according to their legal significance.

These questions become more complex as financial institutions increasingly rely on automated systems, risk classifications, transaction analytics and artificial intelligence. Technological arrangements may assist institutions in processing large volumes of information, identifying patterns that warrant attention and applying defined detection criteria consistently. They may also create or reinforce risks associated with inaccurate data, discriminatory outcomes, excessive profiling, insufficient transparency or inadequate human oversight. A customer risk classification may influence the intensity of monitoring applied to a business relationship. An automated alert may initiate an investigation that leads to additional information requests or restrictions. A model may assign significance to characteristics or patterns whose relevance is not readily apparent to the person affected, particularly where the underlying analytical process is complex. The

existence of an automated result does not establish that the underlying assessment is correct, that the identified activity is unlawful or that a particular intervention is legally justified. Nor does the use of technology relieve the institution of responsibility for the systems it adopts and the decisions made through them. The legal requirements applicable to such arrangements depend on the nature of the processing, the decision involved and the relevant legislative framework. Questions concerning data protection, equal treatment, automated decision-making, transparency and accountability must therefore be examined in their proper context. The potential efficiency of technology is an important consideration, but it cannot replace the need to establish legal authority, evaluate relevant evidence and maintain appropriate responsibility for consequential decisions.

Proportionality occupies an important position within this assessment, although its precise legal operation depends on the applicable provisions and circumstances. A preventive measure may be effective in performing its immediate function while imposing burdens or intrusions that require separate justification. Another measure may appear less intrusive but fail to provide the capability necessary to fulfil a binding obligation or address a material risk. An institution that expands monitoring without identifying the relevant legal objective, risk and expected contribution may increase operational activity and customer intrusion without establishing that the additional processing is necessary or appropriately targeted. Conversely, an institution that reduces monitoring solely to decrease costs, alerts or administrative burdens may create gaps in its ability to identify relevant activity or comply with statutory duties. A responsible assessment must therefore begin by determining what the applicable law requires, identifying the risks and objectives relevant to the control, examining how the existing arrangement performs and considering whether proposed alternatives preserve legally sufficient capability. This does not require proof that one particular monitoring architecture is the only conceivable lawful design, nor does it imply that every aspect of effectiveness can be measured precisely. It requires a defensible process through which the institution can explain the relationship between its legal responsibilities, the measures selected, the evidence available about their operation and the consequences of the choices made. JUST FCC therefore does not begin from the assumption that more monitoring is necessarily better or that less monitoring is necessarily preferable. Its concern is whether the selected arrangements can be justified within the legal and factual circumstances in which they operate.

The exercise of preventive responsibilities also raises questions of institutional accountability that extend beyond the technical performance of individual controls. A bank may refuse to establish a relationship, request extensive information, delay a transaction or terminate access to services. A monitoring system may generate an incorrect result, a risk classification may rely on inaccurate information or an internal procedure may produce consequences that were not adequately anticipated when it was designed. These circumstances raise questions about explanation, review, correction and, where applicable, legal remedies. Whether and to what extent a bank must explain a Financial Crime Compliance decision depends on the relevant legal and contractual framework, including any applicable confidentiality restrictions. In some circumstances, obligations concerning suspicious activity reporting or other legally protected information may limit what can be disclosed to a customer. In others, applicable rules may require the institution to provide information, consider a complaint or make a decision capable of appropriate review. Accountability cannot

therefore be reduced to a general expectation that every decision must be explained in the same way. It requires identifying the applicable duties, the rights and interests affected, the authority responsible for the decision and the mechanisms through which errors or unjustified consequences may be addressed. The fact that an employee followed an approved procedure may be relevant to the assessment, but it does not necessarily resolve questions concerning the legality of the underlying procedure, the adequacy of the information used or the institution's responsibility for the resulting consequences.

Responsibilities also differ between the individual professional applying a control and the institution responsible for designing and governing the framework within which that professional operates. An employee reviewing a transaction-monitoring alert must work within approved procedures, assess the information available and determine whether closure, further investigation or escalation is justified. That employee does not ordinarily possess the authority to redesign the monitoring architecture, change the institution's risk appetite or disregard mandatory legal requirements. Those responsible for designing, approving and overseeing the framework must address broader questions concerning legal coverage, risk differentiation, information processing, operational performance, control effectiveness and the continued justification of particular measures. Management bodies and relevant control functions must ensure that responsibilities are appropriately allocated, that material weaknesses are identified and that decisions concerning significant changes are subject to suitable governance. Compliance, legal, privacy, risk management, technology and internal audit functions may each contribute to these assessments within their respective mandates. This division of responsibility is important because sound professional judgement cannot compensate for a fundamentally inadequate monitoring architecture, while a well-designed architecture cannot eliminate the need for careful assessment of individual circumstances. Accountability must therefore operate at both levels. It concerns the quality of decisions made within established arrangements and the institutional responsibility for determining whether those arrangements remain legally sufficient, operationally appropriate and adequately justified.

The practical importance of these distinctions can be illustrated through an ordinary transaction-monitoring decision. Consider a customer whose financial activity differs from the behaviour anticipated when the business relationship was established. An automated monitoring system may generate an alert because the transactions exceed a threshold or exhibit a pattern identified as potentially relevant to money laundering risk. The existence of the alert establishes that the monitoring system has identified activity meeting its configured conditions, but it does not establish that the customer has engaged in unlawful conduct. The professional responsible for reviewing the alert must examine the relevant circumstances, assess the information already available, determine whether additional information is necessary and consider what action is required under the applicable legal framework and the institution's approved procedures. The quality of that assessment depends on understanding the purpose of the monitoring control, the relevance of the identified activity and the evidential limits of the available information. An investigation that produces additional documentation without improving the assessment may increase administrative activity without necessarily strengthening the decision. Conversely, an investigation that fails to obtain information necessary to resolve a material concern may leave the institution unable to fulfil its responsibilities. The appropriate outcome cannot be

determined merely by counting investigative steps or measuring the time spent reviewing the alert. It depends on the legal requirements, the relevant facts, the evidence obtained and the authority of the person responsible for deciding or escalating the matter. The example illustrates why operational judgement becomes more defensible when the professional understands not only the procedure being followed, but also the legal purpose and evidential reasoning underlying it.

A similar distinction applies at the institutional level when a bank evaluates the design of a monitoring scenario. A control may generate a substantial number of alerts, many of which are closed after investigation because the underlying activity is adequately explained or does not warrant further action. The institution may conclude that the scenario requires examination, but the high number of closures does not automatically establish that the control is unnecessary. Some alerts may concern relevant activity that must be assessed, and a control may contribute to legally required detection capability even when only a limited proportion of alerts leads to reporting. At the same time, a large volume of investigations cannot by itself justify the continued operation of a scenario if evidence indicates that its design is poorly targeted, unnecessarily intrusive or operationally inefficient. A meaningful review would examine the legal objective, the relevant risks, the quality and coverage of detection, the information processed, the consequences of false positives, the availability of alternative configurations and the uncertainty associated with proposed changes. It would also consider the risk that a revised scenario might fail to identify activity that the existing arrangement detects. Decisions about modifying or retiring material controls should therefore remain subject to appropriate testing, validation, legal assessment and governance. The objective is not to achieve a predetermined reduction in alerts or an automatic expansion of monitoring coverage, but to maintain arrangements capable of fulfilling applicable obligations through measures that remain justified in light of their purposes, performance and consequences.

These examples also demonstrate why claims about the effectiveness of Financial Crime Compliance must be expressed with care. A statement that a control prevents a particular amount of criminal activity requires evidence capable of supporting that conclusion, including an appropriate understanding of what would otherwise have occurred. In many circumstances, such evidence may not be available. A claim that compliance measures are ineffective merely because their ultimate impact cannot be quantified is subject to the opposite problem: uncertainty about causation does not establish the absence of a preventive contribution. A more defensible approach is to identify the level at which a conclusion can be supported. An institution may be able to demonstrate that a control satisfies an applicable requirement, operates reliably, identifies defined patterns of activity or produces information meeting established quality criteria. It may also be able to identify weaknesses, unnecessary processing, discriminatory effects or opportunities to improve detection. Such findings can support meaningful decisions even when the contribution of the control to broader criminal justice outcomes remains uncertain. This approach does not eliminate the need for public evaluation of the wider system. It recognises that institutional control assessment and system-wide effectiveness evaluation are related but different exercises, each requiring evidence appropriate to the conclusions being drawn. The objective should be to improve the quality of available evidence and the precision of institutional claims rather than to demand impossible certainty or accept assumptions that have not been adequately examined.

The emphasis on evidence must not obscure the independent importance of legal compliance. Banks do not have discretion to disregard binding obligations because the broader effectiveness of the regulatory framework is disputed or insufficiently understood. A statutory requirement remains applicable according to its legal terms even where evidence concerning its contribution to public outcomes is incomplete. The responsibility of an institution is to fulfil that requirement while exercising any permitted discretion over implementation in a legally appropriate manner. Questions about whether a legislative obligation should be amended, expanded or repealed belong primarily to the relevant lawmaking and public policy processes, although financial institutions, professional organisations, researchers and other stakeholders may contribute evidence and analysis to those discussions. Questions about how an existing obligation should be implemented may fall within the institution's responsibilities, subject to applicable supervisory requirements and internal governance. Questions about how an individual case should be handled ordinarily depend on the authority delegated to the relevant employee and the procedures governing that decision. Distinguishing these levels of responsibility prevents criticism of the wider regulatory system from being confused with permission to disregard the law. It also prevents the existence of binding duties from being used to shield every institutional implementation choice from scrutiny. Legal compliance and critical evaluation are therefore not competing objectives. They concern different dimensions of responsible institutional conduct.

The structure of **JUST FCC — IN THEORY** reflects these distinctions. The first part, **Origins and Purpose**, examines why Financial Crime Compliance exists, how banks acquired preventive responsibilities and how international standards and European legislation developed. It considers the historical development of anti-money laundering measures, the incorporation of terrorist financing, the emergence of financial sanctions and the broader reasons banks became participants in systems of financial crime prevention. It also examines what the framework is intended to achieve and what can reasonably be established about its effectiveness. The second part, **The Legal Framework**, moves from the historical and institutional context to the principal sources of law governing EU banks. It distinguishes international standards, European legislation, national requirements and supervisory guidance and examines the core obligations concerning financial crime risk management, customer due diligence, ongoing monitoring, investigations, reporting, financial sanctions, governance and record-keeping. Together, these parts establish why preventive responsibilities were assigned to banks and what those responsibilities require within the applicable legal framework. Their purpose is not to reproduce every legislative provision or replace detailed legal analysis in a particular jurisdiction, but to provide a coherent understanding of the mandate within which financial institutions operate.

The third part, **The Limits of the Mandate**, examines the boundaries of those responsibilities and the distinctions necessary to determine when particular interventions are required or permitted. It considers the relationship between binding legislation, supervisory expectations, contractual arrangements and institutional policies, together with the legal conditions governing decisions that may affect access to banking services. These questions are important because a bank may possess discretion to adopt measures that are not prescribed in their precise form by legislation, but that discretion does not remove the need for an appropriate legal basis or justification. The fourth part, **Effectiveness, Accountability and Fundamental Rights**, extends the analysis to the standards governing the design,

justification and consequences of preventive measures. It examines proportionality, excessive monitoring, data protection, equal treatment, profiling, automated decision-making, transparency, customer complaints, legal remedies, responsibility for errors and the relationship between extensive financial surveillance and fundamental rights. This part also considers how effectiveness and proportionality should be understood when evaluating compliance arrangements. The four parts are intended to form a continuous argument rather than separate collections of legal topics. The origins of Financial Crime Compliance explain why banks acquired preventive responsibilities; the legal framework establishes the obligations governing those responsibilities; the limits of the mandate clarify the authority within which banks must operate; and the examination of effectiveness, accountability and fundamental rights provides the basis for assessing whether the resulting arrangements and decisions are justified.

The relationship between these four parts is essential because no single perspective provides a complete account of responsible Financial Crime Compliance. A legal analysis that ignores operational consequences may fail to identify important questions about the implementation of preventive duties. An assessment of effectiveness that disregards binding obligations may confuse criticism of public policy with permission to depart from the law. An emphasis on customer rights that overlooks mandatory preventive responsibilities may misstate the applicable legal position. Conversely, an operational approach that treats internal procedures as sufficient justification may fail to distinguish institutional preferences from legal requirements or to recognise the consequences of measures imposed on customers. The JUST FCC approach seeks to connect these perspectives without treating them as interchangeable. It recognises that some questions can be answered by identifying a clear legal requirement, while others demand distinctions between overlapping legal regimes, careful interpretation of applicable provisions or an assessment of evidence that remains incomplete. Where the law leaves room for institutional judgement, the objective is to identify the considerations relevant to a defensible decision rather than suggest that one answer will necessarily be appropriate in every circumstance. This approach requires attention to both the authority under which a measure is adopted and the quality of the reasoning supporting its implementation.

The purpose of this book is therefore not to provide a complete operational manual. Its task is to establish the legal, conceptual and analytical foundations necessary to understand what Financial Crime Compliance requires, why those requirements exist, where their limits lie and how the exercise of preventive authority should be assessed. The companion book, **JUST FCC — IN PRACTICE**, develops the operational implications of that understanding. It examines customer due diligence, risk assessment, transaction monitoring, investigations, reporting, financial sanctions, governance and the evaluation of controls. It also develops the JUST FCC method for examining monitoring objectives, identifying applicable legal requirements, assessing relevant risks, evaluating available evidence, considering alternative control designs and documenting decisions about legal sufficiency, effectiveness and proportionality. The distinction between the two books is not a division between abstract principles and practical responsibilities. The legal foundations examined in *IN THEORY* directly affect everyday compliance decisions, while the operational arrangements examined in *IN PRACTICE* must remain connected to those foundations. The first book addresses what the law requires, why preventive responsibilities exist, where their boundaries lie and what can reasonably

justify their exercise. The second examines how institutions can fulfil those responsibilities through appropriately designed controls, sound professional judgement and defensible institutional decisions. Their relationship reflects the proposition that implementation cannot be assessed adequately without understanding the mandate on which it rests.

The significance of this approach extends beyond the technical performance of individual compliance controls. Financial Crime Compliance forms part of the relationship between private financial institutions and public authority because banks perform preventive functions established by law while continuing to operate as providers of financial services. Their activities may contribute to important public objectives, but their decisions can also affect access to banking, the processing of personal information and the ability of individuals and businesses to participate in economic life. Failures in preventive arrangements may expose the financial system to criminal misuse, while unjustified or poorly targeted measures may impose significant burdens without a sufficiently established contribution to the risks they are intended to address. The legitimacy of the framework therefore depends not only on the seriousness of the threats it seeks to prevent, but also on the clarity of its legal foundations, the adequacy of its implementation, the accountability of the institutions involved and the capacity to examine its performance and consequences. A system that cannot adequately explain the purpose of its measures, distinguish legal requirements from institutional preferences or separate evidence of activity from evidence of results risks weakening confidence in its operation, even where many of its obligations remain necessary and valuable. Conversely, a system that recognises these distinctions is better positioned to support informed oversight, responsible professional judgement and evidence-based improvement.

JUST FCC does not proceed from the assumption that contemporary Financial Crime Compliance is either fundamentally successful or fundamentally flawed. It does not suggest that existing controls should be retained merely because they are established, nor that they should be reduced merely because their wider impact is difficult to quantify. Financial crime risks evolve, legal requirements differ and evidence is frequently incomplete. Some obligations are mandatory even where their broader contribution to public outcomes cannot be measured precisely. Some risks may justify extensive preventive measures because less intrusive alternatives cannot provide the capability required by law. Other measures may warrant reconsideration because their contribution is insufficiently established, their operational design is poorly targeted or their consequences are not adequately justified. The challenge is to distinguish these circumstances through legal analysis, risk assessment, appropriate evidence and accountable governance. That task begins by recognising that historical development explains why banks acquired preventive responsibilities but does not establish that every subsequent operational expansion was necessary; that legislation imposes binding obligations but does not always determine every aspect of implementation; that operational activity can often be measured but does not automatically demonstrate broader preventive outcomes; and that measures adopted for legitimate purposes remain subject to the limits and safeguards of the legal order. Recognising these distinctions does not weaken the responsibility to combat financial crime. It provides a more precise foundation for understanding what that responsibility entails and how it can be exercised lawfully and responsibly.

Financial Crime Compliance must first be understood in terms of its origins, legal obligations, effectiveness, institutional authority, accountability and fundamental rights. Only then can its practices be evaluated and improved without compromising the duties they are intended to fulfil.

Part One

—

Origins and Purpose

Question 1 — What Is Financial Crime Compliance?

Financial Crime Compliance, commonly abbreviated to FCC, is a collective term used within the banking sector to describe the activities, organisational arrangements and internal controls through which financial institutions seek to fulfil their legal and regulatory responsibilities relating to financial crime. In everyday banking practice, these responsibilities may involve establishing the identity of customers, understanding the nature and intended purpose of business relationships, assessing exposure to financial crime risks, monitoring financial transactions, investigating activity that requires further examination, reporting relevant information to competent public authorities and implementing restrictions arising from applicable financial sanctions. The term may also refer to the department, control function or wider organisational structure responsible for advising on, implementing, monitoring or overseeing these activities. In some institutions, Financial Crime Compliance is primarily understood as a specialist compliance function, while in others it encompasses a broader combination of operational teams, investigative units, risk management responsibilities and supporting technological systems. Although these organisational arrangements may differ considerably, they share a common purpose: enabling financial institutions to fulfil the responsibilities imposed upon them by the legal frameworks applicable to their activities. Understanding Financial Crime Compliance therefore requires more than identifying the tasks performed by employees or the systems used by banks. It requires an examination of the legal obligations from which those tasks arise, the institutional choices through which those obligations are implemented and the objectives that the resulting controls are intended to serve.

Despite its widespread use within the financial sector, Financial Crime Compliance is not a single, clearly defined or legally unified body of European Union law. The expression functions primarily as an organisational and professional umbrella term that brings together obligations arising under different legal instruments, each with its own scope, objectives, requirements and legal consequences. Anti-money laundering and counter-terrorist financing legislation establishes duties concerning the assessment of relevant risks, the identification and verification of customers, the understanding of business relationships, ongoing monitoring and the reporting of information in circumstances specified by applicable law. Under the European framework in force at the legal reference date used in this volume, Directive (EU) 2015/849, as amended and implemented through national legislation, provides a central foundation for these responsibilities.[1] Financial sanctions arise through a

[1] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, as amended, particularly Articles 8 and 11–13, concerning risk assessment and customer due diligence obligations. The directive operates through national implementation and must be read together with the applicable national legislation. Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 establishes the future directly applicable EU anti-money laundering and counter-terrorist financing framework, generally applicable from 10 July 2027, subject to its specified provisions and exceptions. The legal reference date for this volume is 1 October 2026.

different legal framework and may impose prohibitions on particular transactions, obligations to freeze funds or economic resources, or restrictions on making funds or economic resources available to designated persons or entities. Other areas of law concerning fraud, bribery and corruption, market abuse or certain tax-related obligations may also be included within an institution's Financial Crime Compliance organisation, depending on the nature of its business and the allocation of responsibilities established through its internal governance. The fact that these responsibilities may be administered by the same department or supported by similar technological systems does not mean that they constitute a single legal obligation or that the legal requirements governing one area can automatically be applied to another.

The distinction between Financial Crime Compliance as an organisational concept and the legal regimes that it encompasses is fundamental because the expression *financial crime* may create the impression that banks possess a general responsibility to identify, investigate or prevent every form of criminal activity involving money. Such an interpretation would misunderstand the nature of the responsibilities assigned to financial institutions. Banks are subject to specific duties arising under identifiable legal instruments, and the scope of those duties must be determined by reference to the applicable legislation and the circumstances in which it operates. Although those responsibilities may be extensive and may require substantial examination of customer information and financial activity, they are not unlimited. Nor do they transform banks into police authorities, public prosecutors or courts. Financial institutions participate in a wider preventive and enforcement framework in which different public and private actors perform legally distinct functions. A bank may be required to identify a customer, examine a transaction, investigate relevant circumstances or report information to a financial intelligence unit without being authorised or expected to determine whether a criminal offence has actually been committed. The distinction matters because preventive obligations frequently operate on the basis of risks, indicators, reasonable grounds for suspicion or other legal thresholds that are different from the evidential standards applicable to establishing criminal liability. A compliance decision may therefore be legally necessary even where the available information does not establish wrongdoing, while the existence of a concern or an unusual transaction does not itself justify treating a customer as having engaged in criminal conduct.

Transaction monitoring provides a useful illustration of this distinction because it demonstrates how the responsibilities of a bank differ from those of the authorities responsible for criminal investigation and prosecution. A monitoring system may identify transactions that differ from the activity anticipated for a customer, exceed an established threshold or exhibit characteristics associated with a particular financial crime risk. The resulting alert indicates that the activity meets the conditions defined by the monitoring arrangement, but it does not necessarily establish that the transaction is unlawful or that the customer has engaged in money laundering. Depending on the relevant circumstances, the bank may be required to examine the available information, consider the nature and purpose of the transactions, obtain additional information where necessary and determine whether the applicable legal conditions for reporting have been met. The institution must assess the matter within the boundaries of its own obligations and procedures, rather

than attempt to reach conclusions reserved for criminal justice authorities. This distinction is important both for the quality of the investigation and for the treatment of the customer. An unusual transaction may have a legitimate explanation, while apparently ordinary activity may nevertheless warrant further attention when considered in the context of relevant risk information. The purpose of the bank's examination is to establish whether its preventive responsibilities require further action, not to pronounce upon the customer's criminal guilt or innocence.

Financial sanctions demonstrate why it is equally important not to treat all Financial Crime Compliance activities as variations of the same investigative process. Unlike an anti-money laundering monitoring assessment, which may require the evaluation of transaction patterns and surrounding circumstances, the application of a financial sanctions prohibition may depend on whether a person, entity, transaction or activity falls within the scope of a specific restrictive measure. For example, Article 2 of Council Regulation (EU) No 269/2014 establishes asset-freezing obligations and restrictions on making funds or economic resources available to designated persons and entities.[2] Where such a prohibition applies, the bank must comply with its legal requirements irrespective of whether the transaction would otherwise appear unusual under an anti-money laundering monitoring model. A transaction may be entirely consistent with a customer's established financial behaviour and nevertheless be prohibited because of the involvement of a designated person or another legally relevant circumstance. Conversely, an unusual transaction does not automatically constitute a sanctions violation merely because it requires examination under an anti-money laundering framework. Although sanctions screening and transaction monitoring may both involve automated systems, the examination of financial information and the escalation of potentially relevant cases, the legal questions they address are different. Understanding those differences is necessary to determine the appropriate response, the evidence required and the authority under which the bank acts.

The organisational breadth of Financial Crime Compliance also means that a substantial proportion of the work undertaken by banks concerns the design, maintenance and operation of internal arrangements intended to support compliance with applicable obligations. Financial institutions must establish appropriate governance structures, allocate responsibilities, maintain policies and procedures, train relevant personnel, retain required information and operate controls capable of identifying circumstances that require attention. In practice, these arrangements may include customer risk-classification models, transaction-monitoring scenarios, sanctions-screening tools, investigative workflows, case-management systems, quality assurance processes and management information frameworks. Some elements of these arrangements are required by legislation or other applicable legal provisions, while their precise operational configuration may be determined by the institution within the limits established by law. This distinction is particularly important because the existence of a legal obligation does not necessarily mean that every technological feature, numerical threshold, information request or investigative step employed by a bank has been expressly prescribed by the legislature. For

[2] Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, Article 2, concerning the freezing of funds and economic resources and restrictions on making funds or economic resources available to designated natural or legal persons, entities or bodies. This regulation is used as an illustration of the legal structure of an EU asset-freezing regime. Other restrictive measures may establish different prohibitions, conditions and exceptions.

example, European anti-money laundering legislation requires ongoing monitoring of business relationships, including scrutiny of transactions undertaken throughout the course of those relationships, but it does not establish a single universal collection of transaction-monitoring scenarios or numerical alert thresholds that every bank must apply.[3] Institutions must therefore distinguish the legal requirement to maintain appropriate monitoring from the particular design choices through which they seek to fulfil that requirement.

This distinction does not imply that banks possess unrestricted discretion over their compliance arrangements or that internal procedures can be modified solely according to operational convenience. The design of a control must remain consistent with the applicable legal framework, the institution's risk assessment, relevant supervisory requirements and the governance arrangements through which compliance responsibilities are exercised. A monitoring system that fails to identify activity relevant to the risks it is intended to address may be inadequate even if its configuration is not expressly prohibited by legislation. Similarly, a customer due diligence procedure that omits information necessary to fulfil a statutory obligation cannot be justified merely because it is simpler or less costly to operate. Conversely, the fact that a bank has historically collected extensive information or maintained a particular investigative procedure does not, by itself, establish that every element of that practice is legally necessary. The appropriate question is whether the chosen arrangement enables the institution to fulfil the applicable requirements and address the relevant risks in a manner that can be explained and supported. Where the law permits different approaches, institutional choices should be subject to reasoned assessment rather than treated as inevitable consequences of the underlying obligation. The purpose of identifying discretion is therefore not to weaken compliance, but to clarify where the institution bears responsibility for selecting and justifying the means through which compliance is achieved.

A useful way of understanding Financial Crime Compliance is to distinguish between the legal obligation, the operational control and the result that the control is intended to achieve. The legal obligation establishes what the institution is required to do under the applicable framework. The operational control is the procedure, system or organisational arrangement selected to fulfil that requirement. The result concerns what the control actually accomplishes, whether in terms of satisfying a defined procedural requirement, identifying relevant activity, producing information of value or contributing to a broader preventive objective. These three dimensions are connected, but they should not be treated as interchangeable. A bank may be legally required to conduct ongoing monitoring and may fulfil that responsibility through a combination of automated transaction analysis, customer information reviews and investigative procedures. The fact that these arrangements have been established and are operating may provide evidence of implementation, but it does not automatically establish that they are appropriately targeted, sufficiently reliable or effective in achieving their intended purposes. Equally, evidence that a particular control produces relatively few alerts does not, without further analysis, demonstrate that it is unnecessary or ineffective. Meaningful evaluation requires consideration of the

[3] Directive (EU) 2015/849, as amended, Article 13(1)(d), concerning ongoing monitoring of business relationships, including scrutiny of transactions undertaken throughout the course of those relationships to ensure consistency with the institution's knowledge of the customer, the customer's business and risk profile, including, where necessary, the source of funds. The provision establishes an ongoing monitoring obligation but does not prescribe a universal set of transaction-monitoring scenarios, numerical alert thresholds or technical system configurations applicable to every financial institution.

legal duty, the purpose of the control, the risks it addresses, the quality of its operation and the evidence available about its results.

The distinction between obligations, controls and results becomes particularly significant when considering how banks measure and explain the performance of their Financial Crime Compliance functions. Institutions may be able to demonstrate that customer reviews have been completed within required periods, that transaction-monitoring alerts have been investigated in accordance with established procedures or that sanctions-screening systems have processed relevant information. Such measurements can provide important evidence about operational performance and the implementation of controls. However, they do not necessarily establish the extent to which the institution has prevented financial crime or contributed to broader enforcement outcomes. A high volume of investigations may indicate substantial monitoring activity, but it may also reflect the generation of alerts that ultimately provide little relevant information. A lower volume of alerts may indicate more precise targeting, but it could also result from inadequate detection capability. Similarly, the submission of information to a competent authority may fulfil a legal obligation without enabling the bank to determine how that information was subsequently used. The distinction between activity and outcome is therefore not an argument against maintaining mandatory controls. It is a reason to avoid presenting operational statistics as proof of wider effectiveness where the available evidence does not support that conclusion. This analytical separation provides one of the foundations for the later examination of effectiveness and accountability within the JUST FCC series.

For employees, understanding the different legal and operational dimensions of Financial Crime Compliance has direct consequences for professional judgement. A customer due diligence analyst may need to establish whether the institution possesses sufficient information to identify a customer, understand the purpose of a business relationship and assess relevant risks. A transaction-monitoring investigator may need to determine whether an alert can be adequately explained, whether additional information is necessary or whether circumstances warrant further escalation. A sanctions specialist may need to establish whether a potential screening match concerns a person or entity subject to an applicable restrictive measure and whether the relevant legal instrument requires a particular action. Although these professionals may work within the same Financial Crime Compliance department, they are not necessarily applying the same legal tests, evaluating the same risks or making decisions with the same consequences. Their work requires an understanding of the specific purpose of the relevant control and the legal framework within which it operates. The ability to identify the applicable obligation, distinguish relevant evidence from assumptions and recognise the limits of delegated authority is therefore as important as familiarity with the institution's operational procedures.

The organisational boundaries of Financial Crime Compliance may also differ considerably between financial institutions without changing the underlying legal responsibilities that apply to their activities. One bank may include fraud prevention, financial sanctions, anti-bribery and corruption controls, and anti-money laundering monitoring within a single Financial Crime Compliance function, while another may allocate these responsibilities across separate compliance, operational risk, legal or specialist investigative departments. Such differences may reflect the institution's size, business model, risk exposure, governance arrangements or historical

development. The terminology used to describe an internal function does not determine the legal obligations imposed on the institution, and the placement of a particular responsibility within an organisational structure does not alter the substantive requirements of the applicable legislation. What matters is whether the institution has correctly identified its obligations, allocated responsibilities appropriately and established arrangements capable of fulfilling those obligations. A broad organisational definition of Financial Crime Compliance may be useful for coordination and oversight, but it should not obscure the distinct legal mandates governing the activities performed within it. The same principle applies when institutions adopt internal policies that go beyond the minimum measures expressly described in legislation. Such policies may be binding on employees through the institution's governance arrangements, but their legal basis, purpose and relationship to the bank's contractual responsibilities towards customers must be distinguished from obligations imposed directly by law.

This final distinction is particularly important because Financial Crime Compliance does not operate exclusively within the relationship between banks and supervisory authorities. Its implementation may also affect the contractual relationship between a bank and its customers, including the information that customers are asked to provide, the circumstances in which services may be restricted and the conditions under which a business relationship may be terminated. A bank's internal Financial Crime Compliance policy may establish requirements concerning risk acceptance, customer information or the handling of particular circumstances, while its general terms and conditions may contain contractual provisions concerning the provision or termination of services. These arrangements interact with applicable statutory duties but do not necessarily possess the same legal character. The existence of an internal policy does not automatically establish that a particular action is legally required, just as a contractual provision does not remove the need to examine the statutory and other legal limits applicable to its exercise. These questions are considered in greater detail later in this volume because they illustrate the practical importance of distinguishing legal obligations, institutional decisions and the rights and responsibilities arising within the banking relationship. For the purpose of defining Financial Crime Compliance, the essential point is that a bank's preventive responsibilities must be understood within the broader legal framework governing its conduct rather than treated as an unrestricted authority arising from the general objective of combating financial crime.

Financial Crime Compliance should therefore be understood as a collection of legally grounded preventive responsibilities implemented through institutional structures, professional activities and operational controls whose purposes and legal consequences must be examined individually. Its organisational unity does not eliminate the differences between anti-money laundering obligations, counter-terrorist financing requirements, financial sanctions and other financial crime regimes. Its preventive objectives do not transform banks into criminal justice authorities or authorise unlimited scrutiny of financial behaviour. Its operational complexity does not mean that every procedure has been expressly prescribed by law, while the existence of institutional discretion does not permit banks to disregard binding requirements. Equally, the implementation of extensive controls does not automatically demonstrate their effectiveness, and uncertainty about wider outcomes does not establish that the controls lack value. These distinctions provide the foundation for a more precise understanding of the responsibilities assigned to banks

and the decisions made in fulfilling them. Before asking whether Financial Crime Compliance works, whether particular controls are necessary or whether existing practices should be improved, it is essential to establish which legal obligation is involved, which operational arrangement has been selected to fulfil it and what can reasonably be concluded about the results. That is the starting point for the analysis developed throughout this volume and for the wider JUST FCC approach to legally grounded, evidence-informed, proportionate and accountable compliance.

Question 2 — Why Were Banks Given Responsibilities in the Fight Against Financial Crime?

Banks were assigned responsibilities in the fight against financial crime because of the particular position they occupy within the financial system and the information that becomes available to them through the provision of financial services. Banks maintain accounts, execute payments, provide credit, facilitate the movement of funds and establish continuing relationships with individuals, businesses and other organisations. In performing these activities, they collect and retain information concerning their customers, the nature of their financial relationships and the transactions conducted through the institution. Governments and international standard-setting bodies recognised that this position could provide financial institutions with access to information that public authorities might not otherwise possess, or might obtain only after a criminal investigation had already begun. Criminal activity frequently generates financial proceeds that must be transferred, concealed, converted or integrated into the legitimate economy if those responsible are to benefit from them. Where such activity involves regulated financial institutions, records of accounts, payments and customer relationships may provide information relevant to understanding the movement of funds. By imposing obligations concerning customer identification, record-keeping, the examination of certain financial activity and reporting to competent authorities, lawmakers sought to make the regulated financial system less suitable for concealing criminal proceeds and to improve the availability of information that could support prevention, detection and subsequent investigation. The decision to involve banks therefore arose not from an assumption that they possessed the powers or responsibilities of criminal justice authorities, but from the recognition that their ordinary commercial activities placed them at points within the financial system where relevant information could be obtained and preventive measures could be applied.

The historical origins of this approach are closely connected to the international response to drug trafficking and the laundering of criminal proceeds during the 1980s. As governments sought to address the financial structures supporting organised criminal activity, attention increasingly turned towards the methods through which illicit proceeds entered and moved through the legitimate financial system. Criminal enforcement directed exclusively at the underlying offences could leave significant financial resources available to those involved, particularly where funds were transferred across borders, concealed through complex arrangements or integrated into apparently legitimate economic activity. The development of anti-money laundering policy reflected the view that the financial dimension of criminal conduct required preventive measures alongside traditional investigation and prosecution. The establishment of the Financial Action Task Force in 1989

represented an important stage in the international coordination of that response. In 1990, the FATF issued its original Forty Recommendations, which included measures concerning customer identification, the retention of relevant records, attention to unusual financial activity and the reporting of information to competent authorities.[4] These recommendations reflected a developing international consensus that financial institutions should contribute to preventing the misuse of the financial system, not because they were expected to determine criminal liability, but because their existing functions enabled them to identify customers, preserve transaction information and bring potentially relevant circumstances to the attention of public authorities.

The introduction of these responsibilities represented a significant development in the relationship between private financial institutions and public enforcement objectives. Traditionally, banks maintained customer information primarily to administer accounts, execute transactions, manage commercial risks and fulfil the legal obligations associated with providing financial services. The emerging anti-money laundering framework introduced an additional public purpose into the collection, retention and examination of that information. Banks were increasingly expected to consider not only whether a transaction could be processed correctly and consistently with the contractual relationship, but also whether the circumstances surrounding the transaction gave rise to responsibilities under preventive legislation. This did not eliminate the commercial nature of banking or transform every customer interaction into a criminal investigation. It did, however, require financial institutions to incorporate public regulatory objectives into their ordinary operations. Customer identification acquired significance beyond the administration of an account, transaction records became relevant to potential inquiries by competent authorities, and certain information concerning financial activity could become subject to statutory reporting obligations. The resulting framework depended on cooperation between private institutions and public authorities while preserving, at least in legal principle, the distinction between the preventive responsibilities of banks and the investigative and enforcement powers exercised by the state.

The European Community's first anti-money laundering directive, adopted in 1991, made the reasoning behind this division of responsibilities particularly explicit. Council Directive 91/308/EEC of 10 June 1991 recognised in its preamble that preventing the financial system from being used for money laundering could not be achieved by public authorities without the cooperation of credit institutions, financial institutions and their supervisory authorities. The directive consequently required Member States to introduce preventive measures concerning customer identification, the retention of relevant documents, the examination of certain transactions and the communication of information to competent authorities.[5] This legislative approach reflected the understanding that public authorities could not effectively observe every financial relationship or transaction independently, particularly in a financial system characterised by large transaction volumes, continuing customer relationships and increasing international interconnectedness. Banks were therefore assigned

[4] Financial Action Task Force (FATF), *The Forty Recommendations* (1990), particularly Recommendations 12–16 concerning customer identification, record-keeping, attention to unusual transactions and reporting. See also FATF, *History of the FATF*, concerning the establishment of the FATF in 1989 and the publication of its original Forty Recommendations in 1990. The original Recommendations are cited here as historical standards rather than as legislation directly binding on individual banks.

[5] Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, preamble and Articles 3–6. The preamble expressly identifies cooperation between public authorities, credit institutions, financial institutions and supervisory authorities as necessary to prevent the financial system from being used for money laundering. The directive was subsequently repealed and replaced by later European anti-money laundering legislation and is cited here solely as a historical legal source.

responsibilities that made use of their existing position within the financial infrastructure. The directive did not establish a general mandate for financial institutions to investigate every possible criminal offence or to determine whether their customers had committed crimes. Instead, it required the creation of specific preventive obligations intended to support the identification of relevant financial activity and facilitate cooperation with the authorities responsible for the wider enforcement framework. Although the 1991 directive has subsequently been repealed and replaced by later legislation, it remains an important historical source because it demonstrates the original rationale for involving financial institutions in anti-money laundering prevention.

The practical attraction of this arrangement lay partly in the fact that banks already possessed information and operational capabilities that could be relevant to the identification of financial activity associated with criminal conduct. A bank administering an account ordinarily records transactions, maintains information about the account holder and processes payments according to established procedures. Where a continuing business relationship exists, the institution may also develop an understanding of the customer's expected financial activities, business model and transactional behaviour. Lawmakers considered that such information could assist in identifying circumstances warranting further examination, particularly where activity differed materially from what was known about the customer or exhibited characteristics associated with the movement or concealment of criminal proceeds. Requiring financial institutions to maintain appropriate records and communicate certain information to competent authorities could therefore support investigations that might otherwise be hindered by insufficient documentation or a lack of visibility over the movement of funds. This approach also offered the possibility of identifying relevant circumstances before the completion of a criminal investigation, thereby introducing a preventive dimension into a system that had previously depended more heavily on the detection and prosecution of underlying offences. The value attributed to banks was consequently associated with their position as intermediaries and record-holders rather than with any presumed ability to establish criminal wrongdoing independently.

Nevertheless, the assumption that financial institutions possess useful information must be distinguished from the much stronger proposition that they can reliably determine which transactions are connected with criminal activity. Access to financial information does not automatically provide an understanding of the circumstances in which that information arises. A payment may appear unusual because it differs from a customer's previous behaviour, because the institution possesses incomplete information about the customer's activities or because the transaction reflects a legitimate development that has not yet been adequately documented. Complex ownership structures, international payments or substantial transfers may arise from lawful commercial arrangements, while transactions associated with criminal conduct may be structured to resemble ordinary financial activity. The interpretation of transaction data therefore depends on context, the quality of available information and the limitations of the analytical methods employed. Bank employees generally do not possess the investigative powers, access to criminal intelligence or broader evidential material available to competent public authorities. Their assessments are consequently made within a narrower informational and legal environment. This limitation does not make their contribution irrelevant, but it explains why preventive obligations are commonly structured around identification, risk assessment,

monitoring, examination and reporting rather than a requirement to establish criminal guilt. The bank's task is to fulfil the duties assigned to it under the applicable framework, even where the available information cannot establish the ultimate nature of the activity being examined.

The distinction between indicators of concern and proof of criminal conduct is essential to understanding the role assigned to banks. Customer identification measures seek to establish who is using financial services and, where required, who ultimately owns or controls a customer. Record-keeping obligations preserve information that may later be relevant to competent authorities. Ongoing monitoring enables institutions to examine financial activity in relation to their knowledge of customers and relevant risks. Investigative procedures provide a means of evaluating circumstances that require attention, while reporting obligations establish conditions under which information must be communicated to the relevant public authority. These activities can contribute to the prevention and detection of financial crime without requiring the bank to reach conclusions that belong to criminal investigators, prosecutors or courts. An unusual transaction is not necessarily a criminal transaction, and a report submitted to a financial intelligence unit does not itself establish that the reported person has committed an offence. Equally, the absence of a definitive conclusion about criminal conduct does not necessarily remove the bank's obligation to act where the relevant statutory conditions are satisfied. The preventive framework therefore operates through legal duties and evidential thresholds appropriate to the responsibilities assigned to financial institutions, rather than through the standards governing the final determination of criminal liability.

The development of this framework also introduced a significant allocation of responsibilities between financial institutions and public authorities. Legislators establish the obligations that determine when banks must identify customers, retain information, monitor relationships and communicate relevant matters to competent authorities. Supervisory bodies assess whether institutions have established and maintained arrangements capable of fulfilling those duties. Financial intelligence units receive and analyse information within their respective mandates, while law enforcement authorities and prosecutors conduct investigations and pursue criminal proceedings under the applicable legal framework. Banks occupy an intermediate position within this structure because they perform preventive functions that support public objectives while remaining private institutions engaged in the provision of financial services. Their role involves identifying and assessing information available through their activities, making decisions within the scope of their obligations and cooperating with competent authorities where required. The effectiveness of the wider system therefore depends on more than the conduct of banks alone. It also depends on the clarity of legal requirements, the functioning of supervisory arrangements, the capacity of public authorities to receive and use information and the interaction between the different institutions participating in financial crime prevention.

Over time, the responsibilities assigned to financial institutions expanded considerably beyond the original emphasis on the laundering of proceeds associated with drug trafficking and other serious criminal offences. The international framework developed through successive revisions of the FATF standards, the incorporation of terrorist financing into the FATF's mandate in 2001 and the subsequent strengthening of requirements concerning beneficial ownership, risk

assessment, customer due diligence and ongoing monitoring.[6] These developments reflected changing perceptions of financial crime risk, evolving international policy priorities and the recognition that financial systems could be misused in different ways. Terrorist financing introduced considerations that were not identical to the concealment of criminal proceeds, including the possibility that funds originating from lawful activities could be directed towards prohibited purposes. Greater attention to beneficial ownership sought to address difficulties associated with identifying the natural persons ultimately owning or controlling legal entities and arrangements. The development of risk-based approaches reflected an effort to differentiate preventive measures according to relevant risks rather than apply identical levels of scrutiny in every circumstance. As these developments were incorporated into European and national legal frameworks, the responsibilities of banks became broader, more detailed and more closely integrated into their everyday operations. What began as a collection of measures intended to support the identification and investigation of money laundering developed into a more extensive preventive architecture encompassing multiple objectives and increasingly sophisticated institutional controls.

This expansion had important consequences for the relationship between banks and their customers. Financial institutions no longer collect and examine customer information solely for the purpose of providing an agreed financial service or managing their own commercial exposure. They must also obtain, assess, retain and, in certain circumstances, communicate information for purposes established by public law. A customer seeking to open an account, receive a payment or maintain an existing relationship may therefore encounter information requests or investigative procedures that arise from the bank's preventive obligations rather than from the immediate requirements of the financial service itself. In some circumstances, legal restrictions on disclosure may limit the explanations that the bank can provide about particular reporting decisions or investigative activities. These features distinguish Financial Crime Compliance from ordinary customer administration and may create tension between the customer's expectation of transparency and the institution's responsibility to comply with applicable confidentiality and reporting requirements. The existence of these obligations does not remove the need for banks to act within the legal boundaries governing information processing, customer treatment and the exercise of contractual rights. Rather, it demonstrates that the preventive responsibilities assigned to financial institutions operate within a broader legal relationship in which public objectives, institutional duties and customer interests must be considered according to their respective legal significance.

The increasing integration of Financial Crime Compliance into ordinary banking operations also changed the scale and character of the institutional arrangements required to fulfil preventive obligations. Banks developed specialist departments, customer due diligence procedures, monitoring systems, sanctions-screening arrangements, investigative teams, internal reporting processes and governance structures intended to support compliance with applicable requirements. Technological developments made it possible to examine large volumes of transactions and customer information, while the increasing complexity of legal

[6] Financial Action Task Force (FATF), *History of the FATF*, documenting the extension of the FATF's mandate to terrorist financing in 2001 and the subsequent development of its standards. See also FATF, *Review of the FATF Standards and Historical Versions*, concerning successive revisions of the Recommendations and the development of requirements relating to customer due diligence, beneficial ownership, risk assessment and other preventive measures.