

FINANCIAL CRIME RISK AND COMPLIANCE

An Industry on the Cusp of Modernization and
a Market Full of Opportunities



MAY 2022

WHITE PAPER®

THIS WHITE PAPER IS FOR:

Those interested in where the Financial Crime Risk and Compliance market is headed. Specifically, how modernization creates opportunities for financial institutions to improve programs and operations, consultants to offer better services, technology companies to build better products, investors to find better investments, and workers to build more fulfilling careers.



OUR UNIQUE LENS:

Our understanding, perspective, and opinions of Financial Crime Risk and Compliance are sharpened from 25 years of experience as buyers, builders, sellers, and the overlap between these roles. Over two decades we built programs, dealt with audits and examinations, and presented to boards of directors. We know firsthand what motivates compliance executives and institutions to buy consulting services and software. We know what it takes to hire and manage hundreds of Financial Crime Risk and Compliance workers. We know the process for securing budget and the time, effort, and cost to implement software. As builders and sellers of consulting firms and RegTech products, we know how to pitch prospects, close deals, and sometimes, lose deals. We know how to build software and break into a crowded, complex, and reluctant buying environment. We know how to start, fund, and sell RegTech companies. We know how to successfully integrate those companies and how post acquisition integration fails. In sum, we see all sides because we've been on all sides.

INTRODUCTION

Everyone in Financial Crime Risk and Compliance knows better solutions to decades-old problems are needed now - improving programs, developing better technology, and reducing inefficiency. However, for governments, institutions, solutions providers, and investors, the notion of modernization is complex, confusing, and risky. Buying the right products, building the right solution, and investing in the right companies is a guessing game, and wrong guesses are costly.

Decision-makers are overwhelmed. It feels impossible to keep up with new laws and regulations, new technology, cryptocurrency's rapid growth, and fast-moving world events impacting financial crime. So much happening so fast impedes decision-making, further entrenching the status quo.

With so much complexity and confusion, clarity is critical. Without clarity, efforts to modernize will not succeed. With clarity, institutions will make better decisions on needed program changes and new technology purchases. Technology firms will build products buyers need and investors will understand where best to invest.



Needless complexity harms progress. Simplicity engages more people. In the case here, we want more people to understand how they, regardless of their role in the Financial Crime Risk and Compliance industry, will benefit from modernization. "Modernization" is a vague concept that leaves people confused. Let's clear that up and see where the market is headed.



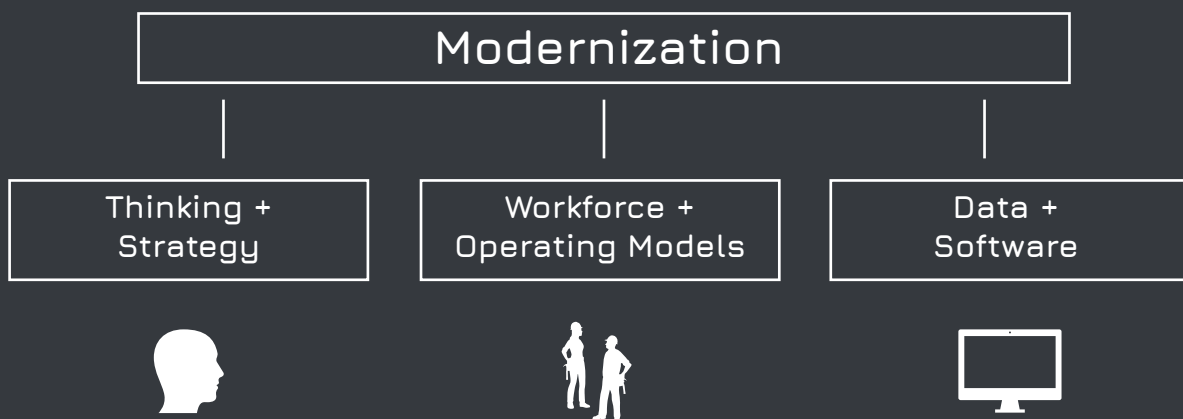
NEXT: How We Think About Modernization

MODERNIZATION

If we only think of modernization as better technology, then modernization will fail. Of course, Financial Crime Risk and Compliance needs better software. Overlooking non-technical opportunities to modernize is a mistake. Today's programs are the result of continually adding more processes, more software applications, and more people without accounting for long-term impacts. Over the years, programs grew into a jumble of inefficiency and complexity.

Modernization creates a moment to assess everything a program is doing, not just the technology it uses. Modernization is the opportunity for management to retire ineffective processes. For institutions and corporations, modernization presents opportunities to update processes, organization structure and find better ways to build a great workforce. For SaaS and DaaS companies, modernization creates opportunities to build software buyers need. For consulting firms, modernization creates opportunities to provide strategic planning and outsourcing services. For investors, there are opportunities to fund, invest in, and acquire firms offering new solutions.

COMPONENTS



NEXT: Understanding the Complexity

COMPLEXITY

Why does the complexity of this market cause confusion?

Here are five contributing factors:

- 01 Confusing Terminology and Acronyms
- 02 Siloed Organizational Structures
- 03 Mixed Signals from the Government
- 04 Buyer and Seller Mindsets
- 05 Marketing Hyperbole



01 Confusing Terminology and Acronyms

As with all industries, Financial Crime Risk and Compliance has its unique language, and it's often so confusing even those in the industry aren't sure what certain words mean. For example, many unfamiliar with the specifics of financial crime compliance may assume things like "fraud," "money laundering," and "corruption" are all the same thing. Those in the field even use different words to convey the same thing. For example, in financial institutions, "sanctions compliance" is what non-bank multinationals may call "trade compliance." Concepts like "third party risk management" entail cross-disciplinary concepts like "know your customer," "enhanced due diligence," and "monitoring." Even a simple word like "case" means something different to different people.

Confusion around terminology is particularly problematic in conversations between vendors and potential customers. As one example, in 2019, there was (and is) a startup whose marketing and sales pitch spoke about being able to reduce "monitoring caseloads" by 90% and complete the remaining "cases" in under two minutes. Upon hearing this, we thought we'd stumbled upon a product that would either save the industry billions of dollars a year or the vendor was using the wrong words in their pitch. After a few questions, we got the answer. The vendor's product analyzed what most call "alerts" (not 'cases') from "sanctions screening" (not "monitoring"). "Cases" are detailed, time-consuming investigations, and "monitoring" is a term for transaction monitoring. So, in this case, the vendor's product was useful but not in the way it was marketed. For vendors, using the wrong words harms their credibility with buyers.

#BANKS #FINANCIALINSTITUTIONS
#FINANCIALSERVICES #FINTECH
#SECURITIES #BROKERDEALER #INSURANCE
#MSB #PAYMENTS #CRYPTOEXCHANGES
#CREDITCARD #CORRESPONDENTBANKING
#RETAIL #WHOLESALE #COMMERCIAL
#CONSUMER #LENDING #DEPOSITS
#MERCHANTSERVICES
#RISK #COMPLIANCE #LEGAL #REGULATORY
#REGULATION #OPERATIONS #AML #BSA
#KYC #CIP #CDD #CRR #EDD #TM #SAR
#CTR #314A #314B #USAPA #AMLA #ABC
#FIU #FINCRIME #FINANCIALCRIME #FRAUD
#CYBERCRIME #CYBER #SANCTIONS
#ECONOMICSANCTIONS #FININT #QC
#QA #TESTING #AUDIT #EXAM #PROGRAM
#POLICY #REGTECH #BLOCKCHAIN
#CRYPTO #MACHINELEARNING #AI
#RPA #ANALYTICS #SCENARIOS
#RULES #MONITORING #SURVEILLANCE
#SCREENING #DETECTION #REPORTING
#RECORDKEEPING #NEGATIVENEWS
#ADVERSEMEDIA #PUBLICRECORDS
#INVESTIGATIONS #RISKASSESSMENT
#RISKRATING #REMEDICATION #LOOKBACK
#ISSUEMANAGEMENT #BOARDREPORTING
#CAMS #CFCS #CFE#FRB #SEC #OCC #FDIC
#FATF #FINCEN #OFAC



COMPLEXITY

02 Siloed Organizational Structures

Those not entrenched in the daily operations of Financial Crime Risk and Compliance may wonder why organizations have separate departments for things called “AML,” “Fraud,” and “Anti-Corruption.” They all seem financial crime related; why aren’t they one department? When each operation started, institutions did not foresee how much and how quickly each group would grow. As these groups evolved over the past 20 years, they added more layers of management, investments in technology, and created their own processes and cultures. Each department likely reports to a different executive position. AML and Sanctions may be part of a compliance department. Fraud may be part of an operations department. Anti-Corruption may be part of a legal department, and Cybercrime may be part of an information security department. This is confusing to the C-Suite, boards of directors, employees, customers, vendors, and investors, but changing entrenched operating structures is hard.

03 Mixed Signals from the Government

As much as the government states it wants “innovation” and promotes modernization, regulators get nervous when Financial Crime Risk and Compliance programs purchase new software, change processes, or realign organizational structure. When the status quo is compliance, regulators fear change increases their risk. And it does. When programs fail, lawmakers and the media harshly criticize regulators. The desire to avoid these public scoldings makes regulators nervous about change.

Changing processes or software that currently works, no matter the cost or inefficiency, makes regulators wary. Executives see this wariness and then the risk it poses to them. A mutual risk aversion sets in, which slows and, in many cases, halts innovation.

“ Well defined terminology, truly integrated organizational structures, and a more supportive regulatory environment would not only bring clarity to the financial crime space, but would also create a more effective combating regime. ”

Vic Maculaitis, Founder and Managing Partner

COMPLEXITY

04 Buyer and Seller Mindsets

Financial Crime Risk and Compliance sellers and buyers see the market differently, and these differences cause confusion. By nature, buyers are risk-averse. Before AML programs report suspicious activity, sanctions programs block transactions, and fraud investigators stem losses, management must first ensure compliance with a long list of technical requirements, or else their jobs are at risk. Such an environment creates a risk-averse market where adhering to the status quo is safe.

Colliding with this risk-averse mindset is the startup ethos of “let’s try new things and disrupt.” While this mindset makes many young companies successful, a Financial Crime Risk and Compliance buyer views it as risky. This disconnect makes for awkward and confusing sales pitches where buyers tend to be “window shopping,” and sellers think they have a prospect making a buying decision. Being what it is, human nature means both sides assume the other is thinking similarly (projection), and both leave the sales meeting or product demo believing they got what they wanted. However, they don’t want the same thing. For product companies, this is particularly problematic. They mistakenly believe they validated product-market fit when in fact, they only met a potential buyer mainly interested in seeing “what is out there” and leaving it at that.

05 Marketing Hyperbole

You read earlier about the vendor that touted investigating “cases” in two minutes and reducing false positives by 90%. Their aggressive marketing pitch drew our attention, so you could say it worked in that regard. However, the problem with this pitch, and many like it, is that the claims are hyperbolic and likely unverifiable. Claims that products “reduce work time by 43%” or “save 29% in investigation costs,” or “reduce false positives by 80%” are not believable because, unfortunately, buyers have heard so many exaggerated claims in the past few years, their level of skepticism is quite high. As a result, marketing claims are now background noise. Buyers perceive most claims as hyperbole and lose interest in learning about new products or services. They are cynical, and in many cases, rightly so.



NEXT: Our View of the Marketplace

MARKET OVERVIEW

THE DRIVERS

Transnational Issues

Nation-State Responses

Laws and Regulations

Transnational issues like drug and human trafficking, terrorism, proliferation, corruption, cybercrime, and fraud require nation-states and global alliances to act.

Laws and regulations drive industry (especially financial services) to follow suit.



THE INDUSTRY RESPONSE

Anti-Money Laundering

Fraud

Corruption

Cybercrime

Sanctions

5 core disciplines of Financial Crime Risk and Compliance. Each discipline entails programmatic and operational components that are developed by industry to mitigate risk and fulfill legal and regulatory obligations.

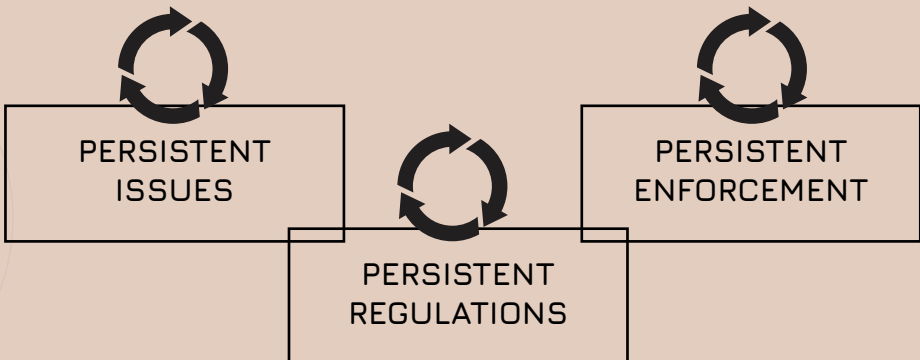


THE MARKET IS CREATED

As programmatic and operational components are developed – needs for people, processes, and technologies follow.



PERPETUATION



MARKET OVERVIEW

THE BUYERS

Financial
Institutions

FinTech/
Crypto

Multi-National
Corporates

Whether the organization is a regulated entity within the financial services sector, or simply a business that operates across borders, complying with rules and managing financial crime risk is an obligation that requires people, processes, and technology.



THE SELLERS

Professional
Services Firms

Technology
Companies

Membership
Organizations

Deliver consulting (advisory) and managed services (staff augmentation/outsourcing).
Services are focused on resources or people.

Deliver data and software products (tools, platforms, and systems). Products are focused
on processes or operations.

Deliver training, seminars, conferences, and certifications. Services and products are
focused on people development.



THE INVESTORS

Venture Capital
Firms

Corporate
Venture Capital

Private Equity
Firms

Investors seed tech companies to develop solutions for buyers. As both tech companies and services firms gain traction, further growth investment ensues. End goals for private growth companies is often a strategic acquisition by larger (often) publicly traded companies or PE firms with synergistic portfolio companies.



NEXT: Where We Are Headed



MARKET OUTLOOK

The market is self-perpetuating and will undoubtedly continue to grow. The interdependence among the hundreds of thousands of workers, consultants, software firms, regulators, and law enforcement, creates a permanent existence of a Financial Crime Risk and Compliance “industrial complex.”

As a result we see the following six trends:

- 01 Better Strategy and Operating Models
- 02 New Laws, Regulations, Enforcement, and Risk
- 03 Demand for Trained and Skilled Workers
- 04 Growth of Outsourcing and Managed Services
- 05 Technology That Accelerates Routine and Repetitive Work
- 06 Better Technology to Detect Suspicious Activity



01 Better Strategy and Operating Models

As we mentioned earlier, focusing modernization efforts only on better technology will fail to sufficiently improve Financial Crime Risk and Compliance. As mandated by the AMLA 2020, the requirement to modernize gives the industry the impetus it needs to genuinely think through and plan how to move from where it is today to where it needs to be five and ten years from now. This means undertaking many non-technical projects to improve how financial crime is detected, investigated, and reported. It is time to determine the strategy needed to get from today to this future. As part of this assessment, management needs to determine if decade-old operating models and department organizational structure still make sense. Management needs to find ways to address ossified thinking about which group reports where and internal politicking that keeps defunct operating processes in place year after year. Contemplating and making changes that may involve combining departments, replacing old systems, and bringing in new talent threatens the status quo. These changes are complicated and take time, but the mandate to modernize provides the opportunity to start now.

MARKET OUTLOOK

02 New Laws, Regulations, Enforcement, and Risk

Crime is a never-ending part of the human condition. This won't change. Unfortunately, a modern world creates more opportunities for criminals. As the methods to commit crime increase and the world is increasingly unstable, governments react with new laws and regulations. For businesses, this means more rules and requirements.

In addition to fast-changing world events and government's responses to them, the multi-year effort to expand regulation to include professions such as lawyers, accountants, investment advisors, and real estate brokers is gaining steam. Media reports reveal the ease of establishing anonymous companies, examples of how ruling elites and oligarchs hide money, and how that money mysteriously purchases homes, yachts, and other lavish assets are driving formerly reluctant governments closer to enacting strict anti-financial crime laws on previously protected classes.

03 Demand for Trained and Skilled Workers

Since 2016 we've heard how modernization will shrink the Financial Crime Risk and Compliance workforce. This is just not true. More people work in the field today than did in 2016, and this growth will continue for many years for three reasons:

- Challenger banks, FinTech, crypto, software, consulting firms, and data start-ups need skilled workers. Every organization needs these people: policy writers, analysts, investigators, auditors, developers, salespeople, product managers, and trainers
- New worldwide AML laws and increasing sanctions require more people to operate programs and implement new policies.
- Once new technology reduces inefficient work, better software will detect more complex and risky activity. This demands the attention of more experienced investigators and managers. Work is shifting from routine and repetitive to complex and high stakes.

Today there is a current shortage of ready, trained Financial Crime Risk and Compliance workers and no easy solution to this problem. Financial institutions, corporations, consulting firms, and software firms cannot find enough qualified workers. When they do, competitors often poach them away for better pay. Remote work poses another retention challenge, making it easier for workers to switch jobs.

MARKET OUTLOOK

04 Growth of Outsourcing and Managed Services

Because of the difficulty of recruiting and retaining talent, many institutions, corporations, and FinTechs outsource some or all of their transaction monitoring, third-party risk management, case investigation, and due diligence work. Outsourcing does not eliminate the problem of understaffing for the Financial Crime Risk and Compliance industry; it transfers the problem to the services providers, many of whom work in lower-cost parts of the US, Eastern Europe, Latin America, and Asia. But through size and scale, outsourcing, or managed services firms, can better “industrialize” recruiting, training, and retaining staff. In addition, outsourcing firms are incentivized to fine-tune analysis, investigation, and reporting processes, reduce inefficiency, and use technology to automate many manual tasks. Outsourcing operations also reduces needed technology investments financial institutions and multinationals face if they are to keep operations in-house.



DIFFERENTIATING THE LIKE SERVICES

“Outsourcing” and “Managed Services” are terms used both independently and interchangeably. For our purposes, they are separate business functions. For Managed Services, we apply the definition of a service managing complete end-to-end processes. Using suspicious activity reporting as an example, the managed service vendor provides the system (software) to detect alerts and the business processes to investigate and resolve alerts through the capability to file a SAR. In other words, managed services encapsulate the entirety of people, processes, and technology. Applying this definition, there are very few actual Financial Crime Risk and Compliance managed service offerings in the market today. There are, however, many outsourcing providers in the market.

Outsourcing, for purposes here, is defined as one or more specific processes that are part of an end-to-end process. Using suspicious activity reporting again as an example, an outsource vendor would be given alerts from a client’s transaction monitoring system and then analyze those alerts. Some alerts are escalated to case investigators back at the financial institution, who may then complete a more detailed review and, if necessary, file a SAR.

MARKET OUTLOOK

05 Technology That Accelerates Routine and Repetitive Work

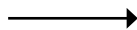
The Financial Crime Risk and Compliance industry wants applications that reduce time spent on low-value work. As a result, RegTech software is building tools that accelerate the manual, routine steps required to assess and dispose of alerts, conduct due diligence, or verify identification. These applications automate data gathering needed by analysts and investigators who spend most of their time hunting and gathering information. Documenting this work often requires many manual steps to copy, paste, screenshot, and create PDFs. Applications that automate the gathering and saving of data, import transaction records into case management systems, and provide simple improvements like “single sign-on” access speed up work and reduce mundane tasks.

06 Better Technology to Detect Suspicious Activity

Financial Crime Risk and Compliance efforts worldwide, costing billions of dollars a year to operate, detect very little financial crime. Everyone knows this, including lawmakers and regulators. Professionals say so much time, effort, and money is wasted on false positives and manual work it leaves little time for detecting actual crime. This is true in part, but the primary reason more financial crime is not detected is because we do not yet have software good at detecting it. It is not as simple as once clearing away the clutter of false positives, and then all that remains is actual suspicious activity.

Financial crime and laundering go undetected because those who are good at committing crimes and hiding the proceeds know how to make the activity appear legitimate. The best way to do that is to mask activity as plain-looking, everyday, normal business activity. Today, systems operate on the notion that suspicious transactions are outlier activity, meaning they look different and are therefore detectable. This is not true.

This means there is a significant need for better software, data analysis, and machine learning. When systems can reduce inefficiency, regulators and lawmakers will not consider compliance complete. As crime grows every year, there will be a demand that the industry does something to slow its growth. That something requires much better, much more advanced technology.



NEXT: Market Opportunities

MARKET OPPORTUNITIES



“ Modernization creates an undeniable change for Financial Crime Risk and Compliance. There is a lot at stake for institutions, service providers, technology companies, workers, and investors. Those that modernize will stand apart from those that continue to only improve around the edges. The winners will connect new technology, clearer data, efficient operations, and a properly equipped workforce. It won't be easy or fast, but the next decade will be exciting and full of opportunities for everyone in our industry. “

David Caruso, Managing Partner

MARKET OPPORTUNITIES

THE OUTLOOK	Financial Institutions	Professional Services	Technology Companies	Workers
Better Strategy and Operating Models	Adopt	Advise, Design, and Deliver	Enable	Career Development
New Laws, Regulations, Enforcement, and Risk	Foresee Impact, Plan, and Adapt	Interpret and Advise	Agility to Modify	Acquire Knowledge and Expertise
Demand for Trained and Skilled Workers	Recruit, Train, and Invest in Career Development	Recruit, Train, and Invest in Career Development	Recruit, Train, and Invest in Career Development	Differentiate and Compete to Rise
Growth of Outsourcing and Managed Services	Incorporate into a Modern Operating Model	Delivery = Cost Effectiveness and Efficiency for Clients	Partner, Enable, Support Intelligent Operations	Multiple Paths Inside Industry or as an Industry Provider
Technology That Accelerates Routine and Repetitive Work	Adopt	Leverage	Build and Refine	Acquire and Master End User Skills
Better Technology to Detect Suspicious Activity	Adopt	Leverage	Build and Refine	Acquire and Master End User Skills

FOR INVESTORS



Reiterating the Perpetual Growth

Worldwide government mandates to modernize and an unstable world equates to continued laws and regulations. A decade+ of continued growth aligned to the global costs of Financial Crime Risk and Compliance. Constant new market entrants into multiple market segments (software, data, services). Shifts towards customer stability and real recurring revenue models.

Seed, Grow, and Acquire

Three areas for investment: (1) software; (2) data; and (3) services. Many startups and early stage companies are entering with proven management teams and operators. Speed to product market fit provides opportunities to scale with sales teams, product developers, new market locations. Services firms with increasing top line revenues crossing \$100MM present prime acquisition opportunities for large strategics and/or private equity.

ABOUT US

Boutique Strategy Management Consultant

We were founded in 2015 on the core tenets of intelligence, innovation, and integration. Our firm is led by successful founders, operators, and industry executives from the Financial Crime Risk and Compliance space.

We bring unparalleled perspective to a multi-billion dollar market where clarity and expertise matter more than ever.

Our clients include some of the world's largest financial services firms; global management consultants; private equity/venture capital/investment firms; and other publicly traded and private companies.

Let's Talk

contact@i3strategies.us

480-253-9360

i3strategies.us

Vic Maculaitis
Founder & Managing Partner

vicmaculaitis@i3strategies.us

David Caruso
Managing Partner

david@i3strategies.us

