Managing Regulatory Change for **Financial Crime**

Given the sophistication of financial criminals it is hard to believe that many large financial institutions still manage enterprise-wide regulatory change management processes manually, in a non-uniform way.

Yet, motivation to combat fraudsters and money launderers is higher than ever before. Monetary losses to financial crime are estimated at approximately $1.6 trillion globally, equivalent to the 12th largest country in the world by GDP[1]. And according to specialist financial crime advisory firm Lysis[2], seizure rates are as low as 1%, meaning that the vast majority of financial crime goes undetected.

Financial institutions are rarely out of the spotlight for anti-money laundering (AML) control failures. More than $26bn in fines has been levied in the last ten years, with 2019 hitting record heights. Many are turning to Regulatory Technology (RegTech) to transform horizon scanning and regulatory change management processes, to ensure that policies and controls adequately safeguard the business.

What do financial institutions need to know, for financial crime peace of mind?

- Do we have the correct governance model and controls framework in place for mitigating money laundering (ML) and terrorist financing (TF) risks associated with our customers?
- Have we implemented a methodology for calculating the AML risk associated with our customers, which encapsulates the risk-based approach and the business risks of the firm?
- Have we captured all of the regulations that apply to our business?
- Do we understand our obligations in different jurisdictions, and have we applied them to our policies and controls?

- Are we clearly applying the regulations, not just undertaking a checklist exercise?
- Have we interpreted the regulations in a risk-based manner that fits the risk appetite of our firm?
- Are regulatory changes and updates reflected in our policies and controls, and linked together?
- Once evidenced, how do we connect relevant regulations to policy then apply them to our remediation work?
- Do we have a full and transparent audit trail to evidence our decision rationale?
- Do we have the correct level and depth of management information to instill transparency?
- Do we have the correct systems in place to monitor and combat risk, on-going?

[1] World Population Review 2019

[2] www.lysisgroup.com

Master regulatory intelligence and change to combat financial crime

To effectively monitor and implement regulatory change financial services firms need to:

- Have **complete visibility** of all regulation relevant to financial crime, enterprise-wide
- Ensure that senior management and the board have **full awareness of regulatory obligations** they must comply with, and the consequences of non-compliance
- Quickly align regulatory intelligence with business taxonomies to ensure that **compliant policies and controls** are in place, and applied quickly and consistently across the enterprise
- Ensure that every client's risk appetite is classified accurately, in accordance with regulation, and maintain a **defensible audit trail** that fully evidences compliance actions and decision rationale
- Instill the correct level of **understanding of individual responsibilities** in combating financial crime, and **top-down implementation** of a compliance culture

Automate regulatory intelligence and change, with CUBE DRP

CUBE Digital Regulation Platform (DRP) supports your second line of defense. We work with Compliance, IT, Information Security, Cybersecurity and Controls teams wanting to take the heavy-lifting out of the regulatory change management process.

With CUBE DRP you know which regulations are relevant to your business, you gain rapid insights into your compliance status, you have time to create and apply effective policies and controls, and you are able to monitor your compliance status in near-real-time.

Underpinned by Artificial Intelligence (AI), Natural Language Processing (NLP) and Robotic Process Automation (RPA), CUBE DRP delivers exceptional automation of the entire regulatory change lifecycle for financial crime compliance.

Key features

- **The world's richest single source of global financial services regulatory intelligence**
- A robust Digital Regulation Platform (DRP) that addresses **regulatory change across the enterprise,** including financial crime, AML, cybersecurity, technology risk, information assets and more
- **Continuous horizon scanning** to quickly identify new, updated and upcoming regulation
- **Intelligent, automated mapping of all relevant regulation** onto a CUBE-developed best practice AML taxonomy, or your own financial crime taxonomy
- **Automated regulatory gap analysis,** pinpointing the impact of regulatory change on your policies and controls, in near-real time
- **Fully-integrated with pre-existing internal and third-party systems,** including GRC platforms
- **deep insight into your compliance status** of all financial crime policies and controls, enterprise-wide
- **Consistent application of the right compliant action, at the right time**

Why choose CUBE?

- **Vast time and cost savings** through automation and the elimination of repetitive manual processes
- **Continuous monitoring** of your compliance status, 365/24/7
- **Scalable compliance** accommodating exponential growth in information, regulations, business operations and jurisdictions
- **Avoidance of enforcement fines** resulting from breaches of financial crime and technology-related regulation and law
- **Reputational risk mitigation** which fosters trust and safeguards revenues
- **Defensible audit trail** enabling you to prove that you are managing technology risk in line with all current regulatory obligations
- **Lightweight, versatile infrastructure (SaaS)** that deploys quickly, scales easily and requires no internal IT overheads or maintenance
- **Seamless integration with pre-existing systems and processes,** via CUBE's Open API connectors

For a deeper dive
visit www.cube.global
or email connect@cube.global