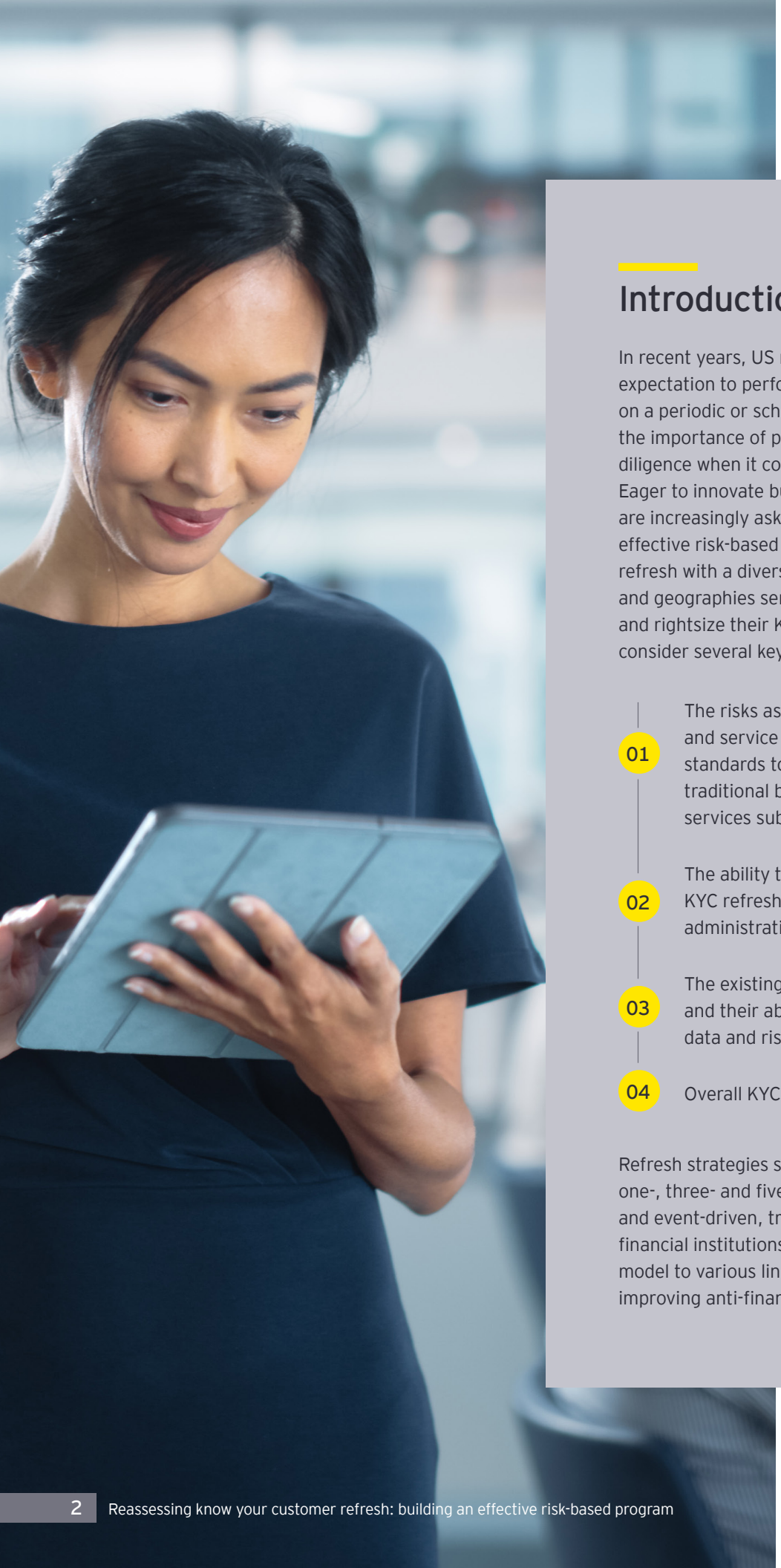
Reassessing know your customer refresh: building an effective risk-based program

EY
Building a better working world



Introduction

In recent years, US regulators have made clear that the expectation to perform a know your customer (KYC) refresh on a periodic or scheduled basis is risk based, emphasizing the importance of program effectiveness over administrative diligence when it comes to financial crime compliance. Eager to innovate but wary of the risks, compliance leaders are increasingly asking the same question: What does an effective risk-based program look like in the context of a KYC refresh with a diverse set of customers, products, services and geographies served? As organizations begin to reassess and rightsize their KYC refresh programs, they need to consider several key components, including:

01 The risks associated with the institution's product and service offerings, which require differentiated standards to meet risk-based expectations (i.e., traditional banking products vs. broker-dealer services subject to suitability requirements)

02 The ability to assess the quality of current KYC refresh outcomes (risk productive vs. administrative) in a quantitative, data-driven way

03 The existing suite of ongoing monitoring controls and their ability to identify changes to customer data and risk considerations

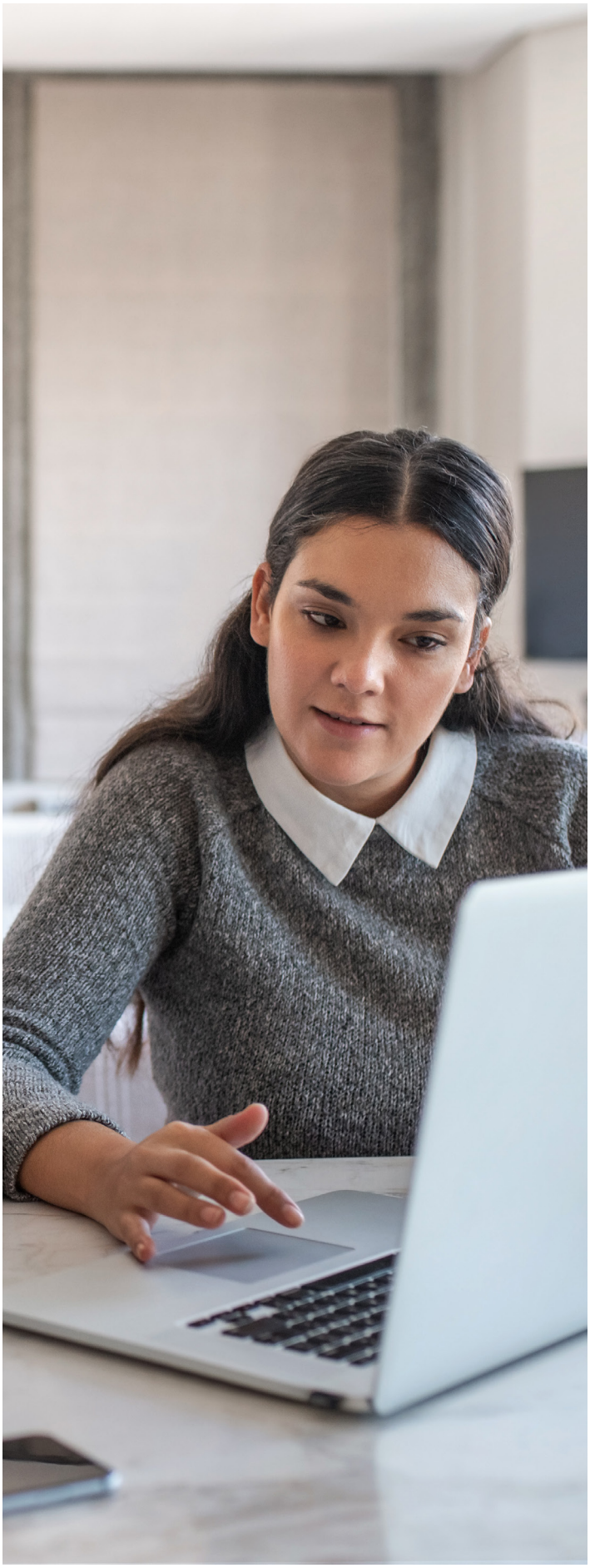
04 Overall KYC control and data quality sustainability

Refresh strategies span the continuum between traditional one-, three- and five-year year periodic review cadences and event-driven, trigger-based models. The challenge for financial institutions is to apply the appropriate refresh model to various lines of business, reducing costs and improving anti-financial crime risk management.

Regulatory context

The current regulatory landscape for a KYC refresh is defined by these three key features:

1. **Innovation**: Regulators have signaled a tolerance for innovative approaches to the customer refresh process, so long as solutions are risk based and effective in developing a customer risk profile and identifying potentially suspicious behavior. Notably, this includes alternatives to the traditional periodic refresh model.[1] Industry consortiums like The Wolfsberg Group have called for the reallocation of resources away from ineffective or inefficient controls toward those with more productive outcomes, demonstrating an openness to novel KYC frameworks.[2]
2. **Evolution**: The regulatory focus of the 2010s that scrutinized corporate and commercial banking business lines has expanded into new areas within the enterprise, namely wealth management, as regulatory expectations of non-KYC topics such as suitability impact KYC obligations.[3]
3. **Global consensus**: While there is still no international consensus on minimum requirements for a KYC refresh, US regulators have been deliberately non-prescriptive in their guidance in order to encourage innovation and mitigate the operational burden of outdated or ineffective risk management activities. It is incumbent upon financial institutions to interpret that regulatory guidance in the context of global regulatory feedback in non-US markets and design a fit-for-purpose KYC refresh strategy.



[1] "FinCEN Guidance," *FinCen website,* https://www.fincen.gov/sites/default/files/2020-08/FinCEN_Guidance_CDD_508_FINAL.pdf, accessed September 2024.

[2] "Demonstrating Effectiveness," *Wolfsberg Group website*, https://www.db.wolfsberg-group.org/assets/ce0c1862-f0d6-4068-93e0-10736d6268a8/Wolfsberg%20Group_Demonstrating_%20Effectiveness_JUN21.pdf, accessed September 2024.

[3] Boba, Matthew C., "Doing Business Under FINRA's New Suitability and KYC Rules," *Chapman website*, https://www.chapman.com/media/publication/76_media.1172.pdf, accessed September 2024.

Common industry practices

Across the enterprise landscape, KYC refresh models vary between business lines according to customer, product and transaction risks. Refresh approaches are also shaped by compliance cultures within individual business segments and the corresponding importance placed on KYC activities by operations personnel. In general, standard refresh practices are observed to be the following:

- **Retail banking** refresh is characterized by a heavy focus on digital customer experiences, such as prompts embedded within online banking experiences. Unless a customer is high risk (and, therefore, revisited annually), refresh is typically trigger based and reliant on ongoing monitoring controls to capture changes in customer information, with the use of negative consent more common (i.e., using a customer's declination to change the customer due diligence (CDD) information as consent that the data is current). In addition, retail banking institutions are increasingly exploring third-party data capabilities to supplement or even supplant customer outreach altogether.
- **Wealth and asset management** are governed by Financial Industry Regulatory Authority guidelines, obligating broker-dealers to have scheduled KYC touch points with customers for suitability purposes which are typically cross leveraged for purposes of completing refresh activities. Some firms are moving away from scheduled refresh and employing a hybrid approach to refresh where lower-risk customers are reviewed on a trigger basis while high-risk customers are revisited annually. In addition to periodic client meetings, refresh activities utilize negative consent communications via email or direct mail, with a relatively low degree of digitalization as part of the KYC process. Given the comparatively high level of client interaction and proximity, wealth management oftentimes has a less rigid approach to the KYC refresh, allowing many institutions to rely on periodic attestations from financial advisors in lieu of customer outreach.
- **Commercial and corporate banking** institutions have the most robust KYC refresh regimes. Due to the complexity of legal entities, refresh is frequently performed by dedicated operations teams tasked with manually reviewing large volumes of KYC cases in a resource-intensive, time-consuming process. Standard practices range from traditional periodic refresh (one-, two- and three-year refreshes or one-, three- and five-year refreshes) to selective, trigger-based models for lower-risk customers, with many institutions employing a combination of the two. Digitalization and customer self-service portals are in the early stages, but similar to retail banking, organizations are deploying a greater degree of third-party data verification and enrichment solutions to enhance the cumbersome nature of the refresh journey.

Defining a risk-based KYC refresh strategy

With demonstrated regulatory tolerance for innovation and a broad array of industry approaches, financial institutions should feel empowered to reassess their legacy controls and define a rightsized KYC refresh model. Doing so requires a clear-eyed view into organizational priorities, capabilities, and limitations. Institutions should start by understanding the overlap between their regulatory framework and their products, services, customers and geographies before taking the three-step approach shown below.

01 Determine programmatic outcomes of current KYC refresh model

Organizations should perform a data-driven analysis to evaluate whether KYC refresh reviews are productive (i.e., result in material account updates, increased suspicious activity report filings, changes in customer risk rating) or administrative (i.e., do not result in material account updates or impact downstream anti-money laundering (AML) risk management activities). More often than not, refresh models that take a check-the-box approach will have a greater concentration of immaterial outputs, indicating that the program contains inefficiencies that are failing to accurately capture AML risks. In these cases, migration to a more risk-based KYC refresh regime may be appropriate. This can take many forms: deployment of an event-driven model, extended refresh cycles, a reduced scope of refresh reviews (data elements and documents), or negative consent for certain customer data points to name a few.

02 Assess core controls to test feasibility of risk-based KYC refresh strategy

If and when current KYC refresh programs are found to be unproductive, institutions should consider if their broader existing control suite is equipped to support a more risk-based refresh model. Regardless of the form that it takes, institutions should consider their internal operational and technological capabilities to do so, including the following:

a. Scope and maturity of control suite: Event-driven refresh relies on the ability for institutions to identify, assess, document and incorporate risk events into a holistic customer risk framework. Can adverse media screening results or politically exposed person alerts identified during daily monitoring be investigated and cycled back into the customer risk rating on an ongoing basis? Can out-of-pattern transaction activity or SAR filings feed into KYC refresh routines? Connectivity between traditionally disparate AML processes is a prerequisite to the success of an event-driven refresh model.

b. Comprehensive customer view: Risk-based refresh programs avoid unnecessary customer outreach. Financial institutions need to have a strategy in place to manage the refresh for customers across the lines of business and assess data fields and documentation requirements against procedures. Regulators are increasingly assessing CDD data quality consistency for higher-risk customers shared across lines of business. The refresh strategy should consider how to identify — and control — potential risk attribute misalignment across lines of business by virtue of executing a refresh.

c. Data quality: A refresh program is only as good as the information it captures. Any reliance on an event-driven model requires a robust assessment of available third-party data sources, including origin, reliability and coverage. Overall data quality — including whether systems-level lineage and related controls are mature — should inform the refresh strategy. Crucially, institutions must be able to deduplicate their own customer population across business lines to consolidate refresh efforts.

03 Rightsize KYC refresh models

Depending on the outputs from the programmatic review and control assessment, institutions should rethink their existing refresh model in the context of their customer base and service offering. Where a refresh is found to be more administrative in nature or internal risk management controls prove effective, transition to a more targeted refresh approach may be appropriate. For example, a wealth management business line with dedicated relationship managers and a robust control suite might elect to rely on periodic risk attestations in place of a full refresh routine. A commercial bank with a global refresh team and strong ongoing monitoring processes may decide that customer activity reviews need not be performed on certain customer segments during every refresh as a matter of course. By finding the intersection of the risk and productivity curves, institutions can chart a smarter, leaner KYC refresh strategy.

Common challenges

Although promising, migration to a risk-based refresh strategy can be fraught. Institutions seeking to modernize their refresh model should take care to sidestep familiar pitfalls, such as:

01 **Oversimplification:** Not all risk events can always be captured by ongoing monitoring. Organizations may need to create manual processes or accept limitations for certain low-risk customer types. Indeed, a bespoke refresh model — employing some combination of trigger-based refresh for lower-risk customers and a scheduled refresh for higher-risk customers — can better match the contours of an institution's compliance needs and optimize refresh efficacy.

02 **Competing priorities:** Financial institutions should resist the urge to prioritize operational excellence over risk management. The risk-based refresh should be pragmatic and provide adequate coverage across the enterprise to properly identify and manage AML and counter-terrorist financing risk.

03 **Impatience:** Like any transformation, the maxim "walk, don't run" applies. Organizations defining a risk-based strategy should start with targeted pilot programs, isolated populations, and a thorough understanding of the technological and data requirements before embarking on a migration toward a risk-based refresh model.

Conclusion

Financial institutions have long hesitated to step away from traditional AML controls for fear of regulatory scrutiny and unknown risk management outcomes, accepting the necessary evils of wasted time and money. In reality, technological developments and the regulatory appetite have left the door open for organizations to reconsider their legacy processes and improve their financial crime compliance models, especially in the KYC refresh space. Compliance leaders should feel empowered to do so.

Contacts

Ron Giammarco
Partner
Ernst & Young LLP
renato.giammarco@ey.com

Don Johnson
Partner
Ernst & Young LLP
donald.johnson@ey.com

Daniel C. Longcore
Senior Manager
Ernst & Young LLP
daniel.longcore@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

What makes EY distinctive in financial services

Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus — to build a better financial services industry, one that is stronger, fairer and more sustainable.

© 2024 Ernst & Young LLP.
All Rights Reserved.

SCORE no. XXXXX-XXXUS
2409-51494-CS BDFSO
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com