

CELENT

Celent Solution Brief

AGENTIC AI IN ACTION: SYMPHONY RISK INTELLIGENCE

Transformer Technology Series

Ian Watson
Celent Risk

October 5, 2026

CONTENTS

Executive Summary.....3

Context.....4

Agentic and Multi-Agent Systems4

SymphonyAI Company Overview5

SymphonyAI Risk Intelligence platform6

An Operating Model for Compliance6

Embedded Governance..... 10

Benefits and Outcomes..... 11

Celent Perspective.....13

EXECUTIVE SUMMARY

Last year, Celent profiled Sensa Agent Flow as one of the first practical uses of agentic AI in financial-crime investigations. SymphonyAI has since widened the proposition. Symphony Risk Intelligence (SRI) uses AI agents across the complete client lifecycle to help institutions manage compliance on a continuous basis.

Beyond the Agent Parade

GenAI in financial crime is moving beyond copilots and isolated process steps. Vendors are now building agents for onboarding, screening, transaction monitoring, investigations, and reporting. Simply having an AML agent is therefore about to become as distinctive as having a cloud strategy. What matters to financial institutions (FIs) is whether those agents can work together, adapt as a case develops, and operate under controls that the model risk team, internal auditors, and regulators can live with.

From Agents to a Platform

SymphonyAI's answer is Symphony Risk Intelligence (SRI). The platform combines packaged financial-crime agents with manager agents that orchestrate workflows across the AML value chain, including data preparation, detection, investigation, and reporting. Financial institutions can use SymphonyAI agents, configure their own, or incorporate agents from other providers. Governance is embedded across the platform, including access controls, evaluations, guardrails, audit trails, and human approval points. Some capabilities remain on the roadmap, but the direction is clear: move from periodic compliance processes toward controls that update as threats, regulations, and evidence change.

Celent's Take in Brief

The interesting part of SRI is not any single agent. Agents are relatively easy to announce and somewhat less cooperative when exposed to production data. SRI's stronger proposition is the combination of financial-crime expertise, multi-agent orchestration, and a common framework for controlling agents from multiple sources, and managing data quality. Its phased deployment model makes sense: institutions can begin with an AI overlay or agent-led investigation workflow before replacing core detection systems. The test now is whether SymphonyAI can turn that architectural promise into repeatable production deployments.

CONTEXT

GenAI is moving beyond copilots and isolated LLM-enabled process steps. AFC vendors are using agentic AI to automate end-to-end processes like onboarding, transaction monitoring, alert triage, and investigation. Soon every vendor will have an agent for each of these. What will distinguish one from another is not only their ability to provide end-to-end functionality, but also applying agents to surrounding processes like data ingestion, rule optimization, and AI governance.

Agentic and Multi-Agent Systems

Unlike traditional AI models, which typically perform narrowly defined tasks, agentic AI performs multiple tasks in sequence or in parallel, makes independent decisions, and adapts dynamically to situations created by previous decisions.

Agentic systems direct actions of multiple specialist agents, allowing them to share insights, pass output from one step in a process to another, and execute actions in pursuit of a common objective. This capability is particularly useful in automating processes where there isn't a straightforward step-by-step approach but multiple decision points with numerous options stemming from each (such as the investigation of AML alerts).

Don't Believe the Hype

The term *agent* is being applied with considerable enthusiasm. An LLM that summarizes an alert is useful, but it is not an agentic system. Nor is an RPA workflow with a conversational interface. Renaming automation as agentic does not make it autonomous. It does, however, make the presentation look more current.

Celent applies a higher bar. An agentic process must connect multiple tasks, operate with meaningful autonomy, adapt as new information emerges, and proactively determine what should happen next, not follow a fixed sequence. This does not mean removing people from the process. In regulated workflows, that would be a bit too adventurous. It means the system can reason across a process and decide which action, tool, or specialist agent to invoke next, with humans inserted at defined control points.

Figure 1 sets out Celent’s four-part test for an agentic system.

Figure 1: Criteria for an Agentic System

Multi-step	Proactive	Adaptive	Autonomous
Chain together complex tasks, deploying different AI models as tools for each interim goal	Develop strategies independently to reach a target outcome, rather than merely responding to prompts	Alter tactics in real time as new information arises or as conditions change	Operate without requiring human intervention, delivering compliance processes and decisions end-to-end

Source: Celent 2026 Risk Previsory Report

The 2025 Celent brief focused on Sensa Agent Flow, a multi-agent system that automated parts of an AML investigation. Now with the advent of SRI, Agent Flow goes from a standalone product to being one component inside a broader platform.

SymphonyAI Company Overview

SymphonyAI is a private company established in 2017 to provides AI and SaaS enabled business solutions for a variety of industries, including retail, media, industrial, and financial services.

Table 1: Company Snapshot: SymphonyAI

Year Founded	2017
Headquarters	Palo Alto, California USA
Number of Employees	2,000
Financial Structure	Private
Industries Served	Retail Banking, Corporate Banking, Insurance, Money Services Business, Gaming, and Payment Service Providers
Geographic Presence	North America, Europe, Middle East, Asia, Africa

Source: SymphonyAI

SymphonyAI Financial Services is the financial crime division of SymphonyAI. In 2022, SymphonyAI acquired NetReveal, the financial crime solutions business of BAE Systems to sit alongside their Sensa product. In 2023, SymphonyAI joined their NetReveal and Sensa businesses to create a unified AI-powered product offering.

SymphonyAI's next-generation financial crime solution today includes generative AI, including a copilot-supported case management system, SRI Investigation and an agentic AI module, SRI Agent Management. SymphonyAI has now unveiled an end-to-end, agent-native risk and compliance platform. It provides clients with a continuous operating model that embeds automation, agents, and governance across the compliance lifecycle. This integrated solution is called the Symphony Risk Intelligence platform (SRI).

SYMPHONYAI RISK INTELLIGENCE PLATFORM

For now, simply having an AFC agent may feel differentiated. This won't last. Soon, every serious AFC technology provider will have agents to perform any and every step in the AML or fraud prevention operating chain. We are writing this brief on SymphonyAI's SRI because it is not just a set of agents, it is an end-to-end platform for financial-crime compliance built around the architecture, governance, domain knowledge, and production performance behind the agents.

An Operating Model for Compliance

SRI has an intelligence layer that lays across the financial crime stack. It connects data, external intelligence, models, policies, and controls, then uses agents to act on that information across existing compliance systems.

Compliance operates as an end-to-end process, even if the technology that runs it doesn't. AML vendors have spent several decades ignoring this fact. Agents collect data, generate alerts, investigate and adjudicate cases, and file reports for regulators: agentic AI makes it possible to run a single technology process across all those steps.

These are not simply LLM calls dressed up as agents. While existing rules and machine-learning models do much of the underlying work, SRI agents use these tools to execute multi-step tasks, decide what to do next, pull up data, and hand work to other agents or investigators.

None of these agents run in isolation. There is a System of Intelligence that enables context created at one stage to be available to every other stage. The system doesn't need to rebuild a resolved entity, a new typology, or an investigator's adjudication each time.

How Agents Change the Operating Model

With SRI, SymphonyAI has created a System of Intelligence for financial crime. By connecting institutional data, external intelligence, risk models, policies, controls, and outcomes, agents continuously understand risk and orchestrate action to ensure compliance. Individual SRI Agents are how that intelligence is turned into governed action.

An SRI Agent is not a single model call answering a single question. It is a component built to pursue a defined task across multiple steps — deciding what to do next based on what it finds, calling on data and tools autonomously, and handing off to another agent or to a human when the situation calls for it. Rather than embedding generative-AI features inside existing applications, SymphonyAI has built financial-crime expertise into these agents: resolving customer data, curating threat and regulatory intelligence, triaging alerts, investigating cases, and drafting disclosures.

Table 2 shows how SRI's agents automate every step of the AML value chain.

Table 2: SRI Agentic Activity across Value Chain

Step in AML Value Chain	What Agents do there	What they replace
Data & KYC	Resolve entities, cleanse records, and maintain a golden customer record across systems	Manual data matching and reconciliation across siloed source systems
Detection & coverage	Monitor threat and regulatory intelligence and map it against existing controls to find gaps	Periodic, manual rule-tuning cycles measured in months
Alert generation	Score and prioritize alerts against institutional risk appetite before a human sees the queue	Undifferentiated alert queues triaged in the order they arrive
Investigation	Assemble evidence, research counterparties, and draft a policy-aligned case narrative	Investigators manually gathering and compiling case information for every alert
Reporting	Pre-populate disclosures with full lineage back to the source evidence	Manual compilation of SARs/STRs after the investigation is complete
Model tuning	Learn from adjudication outcomes to refine detection accuracy continuously	Model improvement tied to scheduled release cycles

Source: SymphonyAI, Celent

Agents Managing Agents

What makes SRI truly agentic are the manager agents that oversee and direct the worker agents. A manager agent decides which specialist agent to invoke next, in what sequence, and when to pause for human review. It makes that decision based on what earlier steps found, not a fixed script. An agent that simply sends work through a predefined route is RPA with an LLM on top. SRI manager agents move a process from task to task, constantly evaluating progress and changing tactics based on what the previous step concluded or accomplished.

For example, if a coverage assessment finds a gap, the manager agent can trigger a model-update recommendation. If a cross-reference check during watchlist enrichment finds conflicting designation status, the manager agent can escalate for analyst review.

This adaptive sequencing is what turns task automation into process automation, and it holds across every workflow the platform supports. It's also what makes the platform extensible: because the manager agent layer decides which specialist agents to invoke next, it can coordinate an FI's own custom agents or third-party agents the same way it coordinates its own.

Three examples show how a manager agent directs specialist agents to accomplish the overall objectives.

Threat and Regulatory Intelligence Agents

Most financial-crime intelligence, (e.g. regulatory guidance, new typologies, enforcement actions) exists as unstructured text, entirely separate from the detection system it affects. Turning a single piece of that intelligence into deployed detection logic can require 150-to-350-hour and take two-to-six-months. During that time, risk exists while the control does not.

SRI’s Threat and Regulatory Intelligence Agents continuously monitor trusted sources, including regulators, FIUs, FATF, and law enforcement. They turn unstructured publications into structured findings, capturing emerging threats, associated red flags, and changes in regulatory requirements and expectations.

The agents map these findings against the institution’s existing controls to identify where coverage is strong, partial, or missing, and recommend changes to rules, models, and controls. Full lineage connects each recommendation to its original source, giving teams a clear view of what needs to change and why.

Where a detection gap is confirmed, a Model Building Agent can use the recommendation to develop or update the underlying model. Data scientists and compliance specialists can then review proposed changes, simulate their impact, and progress them through an AI-assisted governance workflow, preparing updates for deployment in a matter of days.

This reduces the manual effort required to translate threat and regulatory intelligence into action while strengthening governance. Compliance teams can assess coverage as threats and requirements evolve and show regulators how source intelligence informs the institution’s controls.

Table 3: Threat & Regulatory Intelligence Agents

Traditional Process	With SRI Threat Curation Agent
<div>1. SMEs read new intelligence and assess relevance</div> <div>2. Teams review existing controls for coverage gaps</div> <div>3. Specialists define red flags and detection requirements</div> <div>4. Data scientists build or update rules and models</div> <div>5. Teams test, tune, and approve changes</div> <div>6. Updates are deployed, monitored, and refined</div> <div>Result</div>	<div>1. Agents continuously monitor sources and structure relevant intelligence</div> <div>2. Threats are mapped to controls to identify and prioritize gaps</div> <div>3. Agents recommend rule and model updates for testing and human approval</div> <div>4. Approved updates are deployed through governed workflows, with full traceability</div> <div>Result</div>
<div>2–6 months from publication to production</div> <div>150–350 hours of expert effort per new typology</div> <div>Multiple manual handoffs</div>	<div>From publication to production in days</div> <div>SME capacity is significantly increased</div> <div>Coordinated, agent-led workflows</div>

Source: SymphonyAI

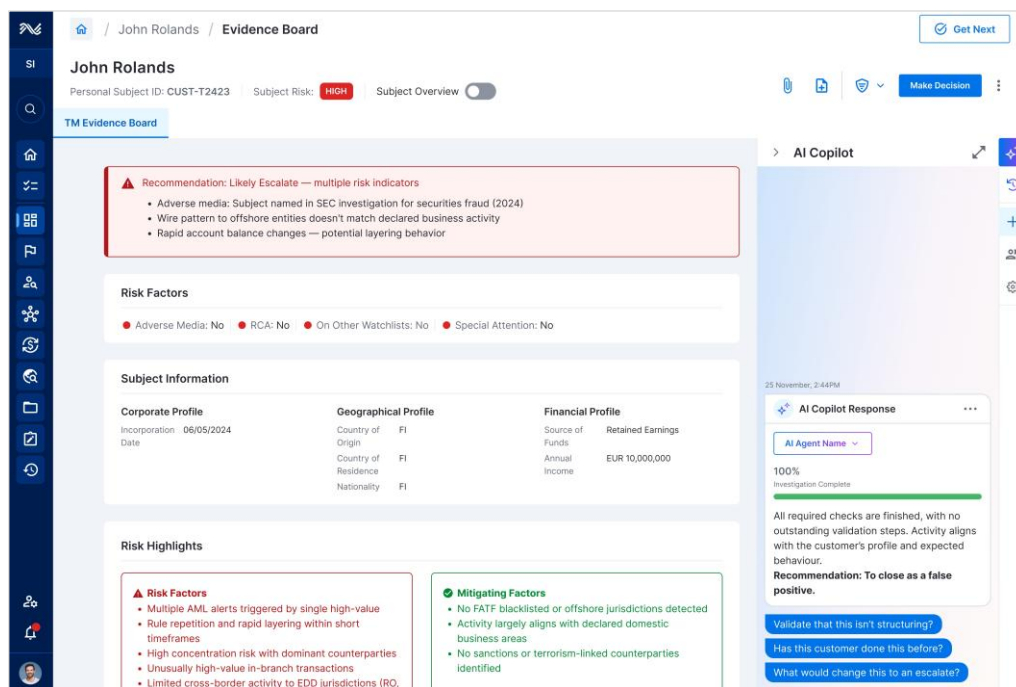
Investigation Manager Agent

Today, an investigator typically starts from a raw alert and has to gather customer context, transaction history, and external research before they can even begin assessing whether something is suspicious — work that has to happen before the actual judgment call, on every single case, regardless of how experienced the investigator is.

SRI's Investigation Manager Agent coordinates specialist agents for summarization, transaction intelligence, web and adverse-media research, requests for information, and narrative generation. Together, these agents generate an Evidence Board containing the evidence, analysis, and a proposed conclusion in a format suited to the case, instead of following a fixed template. The investigator's starting point changes from an empty queue to a set of assembled, evidence-backed cases, which the analyst can then adjudicate. The decision stays with the human with actions and findings traceable back to their source.

SymphonyAI's experience is that this cuts case resolution time by approximately 70% and lifts investigator productivity sixfold.

Figure 2: Dynamically Generated Evidence Board in SRI Investigation



Source: SymphonyAI

Watchlist Enrichment Agent

Watchlist records are often sparse: a name, date of birth, designation type, and little else. Analysts must research the subject's background, corroborate the identity, and judge the credibility and freshness of each source before deciding whether a match is genuine and how much risk it represents.

Using only sparse records, the Watchlist Enrichment Agent enriches entity details, assesses source credibility and currency, and cross-references other records for conflicts. The result is a risk-tiered score, a narrative summary, source citations with credibility scores, and clear screening guidance attached directly to the record. Previously this was left for the analyst to assemble. SymphonyAI reports that each enrichment can cost less than \$0.50 per record and includes a full audit trail.

Embedded Governance

SRI has an embedded governance layer that treats governance as part of the agentic operating model, not simply a control layer added after deployment. Governance defines what each agent can access, which actions it can take, when it must escalate, and where human approval is required. To act autonomously, agents need clear operating boundaries that prevent unauthorized actions and keep decision-making within institutional policy. Autonomy without the governors listed below is an audit finding waiting to happen.

Human in the Loop

SRI allows institutions to set the level of human oversight for each agent or workflow. Institutions can insert human review at any stage in the process. Firms can increase autonomy gradually as confidence in an agent's performance grows. Governance scales at the same pace as automation, not behind it.

Table 4: Embedded Governance

Scope & access control	Policy, rules & human oversight
<ul style="list-style-type: none">Clearly bounded tasksLeast-privilege access to data & systemsRole-based access and strong authentication	<ul style="list-style-type: none">Embedded policies & red-line rules in decision logicClear confidence thresholdsClear escalation paths & ability to pause/stop agent
Data, privacy & compliance	Monitoring, audits & fail-safes
<ul style="list-style-type: none">PII minimizationControls to prevent data exfiltrationAligned to regulation and internal policies	<ul style="list-style-type: none">Full audit trails of prompts, actions, data accessed, and outcomesReal-time anomaly detectionSafe rollback for changes

Source: SymphonyAI

Evaluation, testing, and drift monitoring

Because agent performance degrades and changes as models and workflows evolve, SRI continuously tests agent outputs for factual integrity, completeness, and policy compliance. Performance is tracked across versions to catch regressions, drift, and recurring failure patterns before they reach production volume. Guardrails enforce policy and factual accuracy requirements before results reach investigators.

Auditability and lineage

SRI creates a complete record of the data, tools, model interactions, decisions, and human approvals associated with every agent run. For a regulated institution, this record makes agentic processes defensible. One that stands up to internal audit and regulatory examination.

Model choice and control

SRI is designed to support multiple commercial and open models. Sending every task to a single foundation model is technically simple but commercially expensive. SRI enables institutions to choose models based on reasoning performance, cost, latency, data residency, and internal procurement requirements. Steps that do not require LLM reasoning run deterministically, reducing token consumption and giving institutions tighter control over operating cost.

Bring-your-own-agents

Because agentic architectures are well suited to combining specialized agents from multiple providers, institutions can govern internally developed or third-party agents through the same orchestration, access controls, evaluation, and oversight framework as SymphonyAI agents. This will become increasingly important as institutions adopt more third-party agents.

Benefits and Outcomes

The value of agentic automation is not simply that it makes individual investigators more productive. Its bigger impact is on the economics of the compliance operating model. Increasing capacity no longer means increasing cost, and updating the compliance process doesn't increase the risk of remediation. Instead, institutions can scale capacity while reducing costs and accelerate the pace of compliance change while reducing risk.

Scaling Capacity

Agents can take on much of the investigative and screening work that consumes analyst time today, allowing institutions to release capacity while working at the same rate. At a major US financial institution, agent-led sanctions investigations reduced manual investigative effort by 90%, cut average review time roughly tenfold, and, with 50 agents running in parallel, processed more than 300 alerts per hour. Agent and investigator decisions agreed more than 98% of the time.

The benefit is not simply faster processing. Institutions can absorb transaction growth, new customers, and expanding screening requirements without a proportional increase in compliance headcount.

Reducing Costs

The cost benefit comes from both automating work and changing how that automation is delivered. Through the model choice described above, SRI uses deterministic processing for routine tasks, smaller domain-specific language models (DSLMS) for tightly defined tasks, and larger language models only where more complex reasoning is required. This avoids the economics of an architecture that sends every step through an expensive large model and helps keep the cost of agentic processing under control as volumes increase.

There is also a less visible cost: the cost of changing the compliance process itself. SymphonyAI estimates that continuous threat and regulatory monitoring can compress the process of turning new intelligence into deployed detection logic from 150–350 hours of effort over two to six months to a matter of days, while removing numerous cross-functional dependencies.

Reducing the Risk of Remediation

Compliance risk exists in the gap between when a new threat emerges and when controls to detect it are put in place. That undetected activity accumulates and later surfaces. Shortening that gap, not only improves detection sooner, it reduces the likelihood that missed activity later becomes a costly look-back or remediation exercise.

At a Tier 1 African bank, augmenting existing rules-based monitoring with SymphonyAI models reduced false positives by 77% while retaining the suspicious activity detected by the existing system. Review of the 200 highest-scoring cases also surfaced 21 additional risks that the rules-based approach had not identified.

Agentic workflows can also make decisions more consistent and easier to defend. Agents apply the same policies and thresholds across cases, while SRI records the evidence used, agent actions, model interactions, and human approvals behind each decision. This does not remove model risk or the need for human oversight, but it gives institutions a more controlled way to increase automation while retaining the evidence needed for compliance review, internal audit, and regulatory examination.

CELENT PERSPECTIVE

The most interesting thing about SymphonyAI's SRI is not any single agent. It is the combination of a suite of agents capable of handling several steps in the AML process with a platform designed to govern, control, and orchestrate agents from multiple sources.

When Celent reviewed the product, we were impressed by how far SRI had progressed from a set of promising concepts a year ago to now a productized platform. SRI demonstrated agents gathering evidence, analyzing transactions, conducting external research, and recommending actions. Functionality we have seen from multiple vendors. It was more interesting to see what was happening behind the curtain. To see how agents are built, configured, tested, deployed, and traced. This showed how SRI is not a collection of agents, but an operating platform.

The agentic market has split into two camps. On one side are generic agent platforms that give institutions the tools to build almost anything, but leave much of the financial-crime domain logic, integration, governance, and workflow design to the FI. At the other, are financial-crime vendors offering packaged agents that work inside their own applications, but are much less enthusiastic when it comes to extending them, governing them, or incorporating agents built elsewhere.

SymphonyAI is bridging those two models. SRI provides packaged agents for transaction monitoring, screening, KYC, and investigations, but also provides the orchestration, governance, evaluation, and control framework within which agents operate. Those might be SymphonyAI agents, agents supplied by another vendor, or agents an FI has built itself.

This combination stood out during our review. Celent has seen generic platforms with strong agent-building and governance capabilities. We have also seen financial-crime applications with useful packaged agents. We have seen fewer providers combine the two in a single AFC platform with this degree of productization.

Simply having a catalog of agents will quickly cease to differentiate vendors. FIs do not want to build every financial-crime agent themselves. But neither do larger institutions want to be locked into a single vendor's agent catalog. As institutions develop more proprietary agents, they will need to govern them consistently, control what data and tools they can access, monitor how they behave, and insert human oversight where required.

Thus, the backend capabilities of SRI are a compelling part of the SRI product. SymphonyAI exposed how agents were assembled, which models and tools they used, what data they could access, how individual runs performed, and where human approval was required. Users could create deterministic and model-based evaluations, inspect complete execution traces, and test how an agent performed when the underlying model, prompt, or dataset

changed. These are the capabilities that will determine whether FIs trust agents with regulated work.

SymphonyAI is not going to supply every agent in an institution's financial-crime environment. Nor should it try. The bigger value to FIs, and the bigger opportunity for SymphonyAI, is to provide the operating and control layer in which those agents can work together safely. A bank could deploy a SymphonyAI transaction-monitoring agent, add a home-built KYC agent, and potentially incorporate specialist third-party agents while applying common orchestration, evaluation, audit, and governance controls across all of them.

This changes the vendor evaluation criteria. Financial institutions evaluating their next generation of AFC technology should be asking more than which vendor has the cleverest transaction-monitoring or screening agent this quarter. The more useful question is which provider can combine useful packaged financial-crime functionality with enough openness and control to govern an increasingly mixed population of vendor and home-built agents.

Few financial-crime providers currently sit in both camps. We think this is the most durable part of the SRI value proposition.

About Solution Briefs

A Solution Brief is a type of Celent Insight that provides research clients with timely updates on vendor/ fintech solutions and strategies. Celent does not charge any fees to write a Solution Brief, and vendors do not have to be Celent research clients to be eligible for one. However, Celent analysts are selective and publish a limited number of notes throughout a year about briefings they found particularly interesting; the decision whether to write a note is at the Celent analyst's discretion. Vendors have the opportunity to check the draft before it's published to ensure we accurately represent the facts and don't disclose anything confidential, but otherwise do not have editorial control. Celent has not undertaken any additional due diligence beyond the briefing itself.

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for financial institutions

Typical projects we support related to AML-KYC software include:

Vendor short listing and selection. We perform discovery specific to you and your business to understand your unique needs better. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes, particularly in risk management and compliance. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front-line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

Support for vendors

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

RELATED CELENT RESEARCH

[Trends in Fraud and AML Convergence at US Mid-Market Banks](#)

April 28th, 2025

[Uncertain Time, Certain Investment](#)

April 14th, 2025

[Shedding Light on Agentic AI in Banking](#)

April 10th, 2025

[Dimensions: Risk IT Pressures & Priorities](#)

April 1st, 2025

[So You Want to Buy an AML System: A Buyer's Guide](#)

Nov 25th, 2024

[Resourceful Resilience: How Operational Resilience Regulation is Leading GRC Transformation](#)

Nov 18th, 2024

[Top Tech Trends Previsory: Risk & Compliance, 2025 Edition](#)

Nov 6th, 2024

[Dimensions: Financial Crime IT Pressures and Priorities 2024](#)

Aug 20th, 2024

For more information please contact info@celent.com or iwatson@celent.com

Copyright Notice

Copyright 2026 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner. This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third-party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations, and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

Americas

USA

99 High Street, 32nd Floor
Boston, MA 02110-2320

[+1.617.262.3120](tel:+1.617.262.3120)

USA

1166 Avenue of the Americas
New York, NY 10036

[+1.212.345.3960](tel:+1.212.345.3960)

USA

Four Embarcadero Center
Suite 1100
San Francisco, CA 94111

[+1.415.743.7960](tel:+1.415.743.7960)

Brazil

Av. Dr. Chucri Zaidan, 920
Market Place Tower I - 4^o Andar
Sao Paulo SP 04583-905

[+55 11 5501 1100](tel:+55.11.5501.1100)

EMEA

Switzerland

Tessinerplatz 5
Zurich 8027

[+41.44.5533.333](tel:+41.44.5533.333)

France

1 Rue Euler
Paris 75008

[+33 1 45 02 30 00](tel:+33.1.45.02.30.00)

Italy

Galleria San Babila 4B
Milan 20122

[+39.02.305.771](tel:+39.02.305.771)

United Kingdom

55 Baker Street
London W1U 8EW

[+44.20.7333.8333](tel:+44.20.7333.8333)

Asia-Pacific

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

[+81.3.3500.3023](tel:+81.3.3500.3023)

Hong Kong

Unit 04, 9th Floor
Central Plaza
18 Harbour Road
Wanchai

[+852 2301 7500](tel:+852.2301.7500)