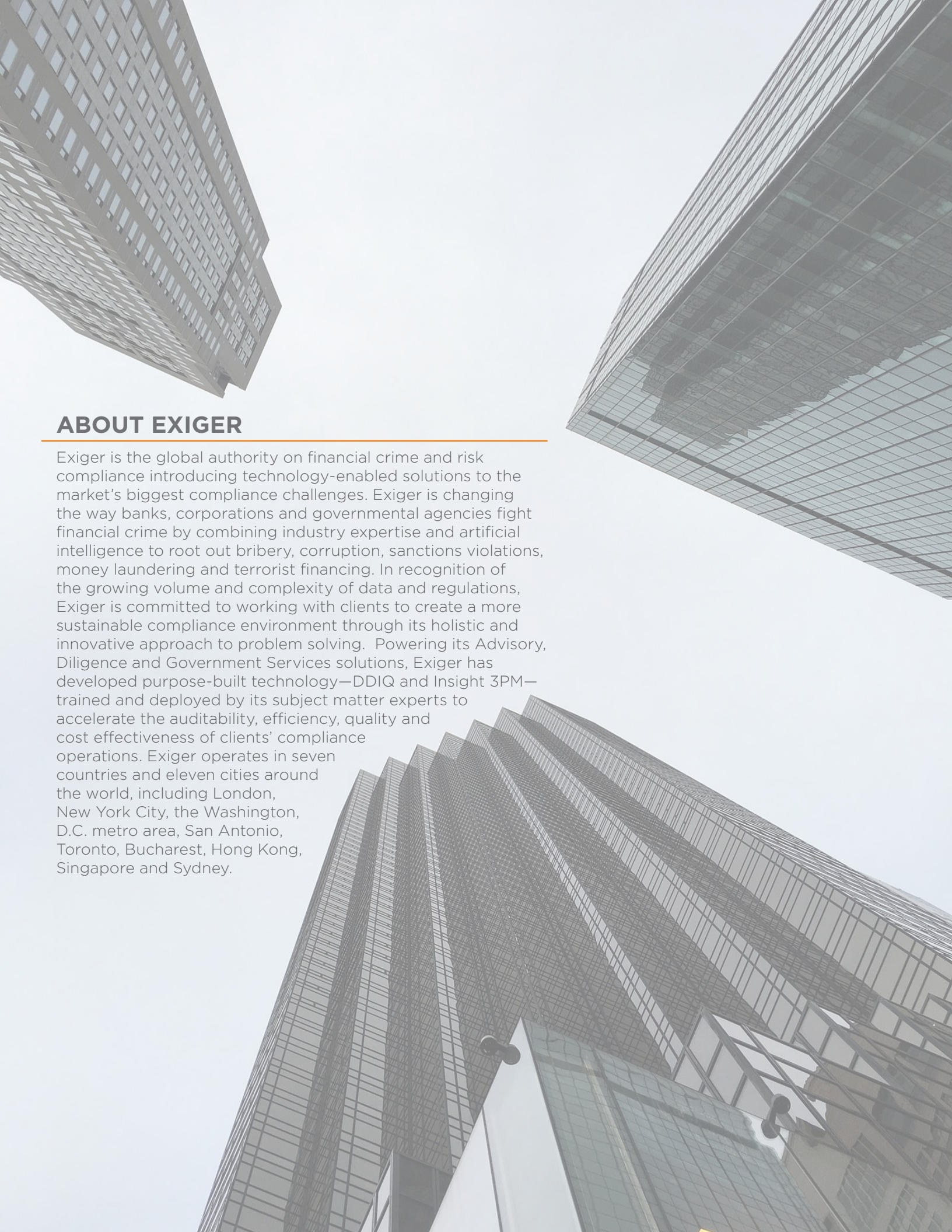
Client Alert

Complementary, Not Contradictory:

Why SR21-8 Builds on SR11-7 to Integrate Effective Risk Management in your BSA/ AML Compliance Program

EXIGER

Governance. Risk. Compliance.



ABOUT EXIGER

Exiger is the global authority on financial crime and risk compliance introducing technology-enabled solutions to the market's biggest compliance challenges. Exiger is changing the way banks, corporations and governmental agencies fight financial crime by combining industry expertise and artificial intelligence to root out bribery, corruption, sanctions violations, money laundering and terrorist financing. In recognition of the growing volume and complexity of data and regulations, Exiger is committed to working with clients to create a more sustainable compliance environment through its holistic and innovative approach to problem solving. Powering its Advisory, Diligence and Government Services solutions, Exiger has developed purpose-built technology—DDIQ and Insight 3PM—trained and deployed by its subject matter experts to accelerate the auditability, efficiency, quality and cost effectiveness of clients' compliance operations. Exiger operates in seven countries and eleven cities around the world, including London, New York City, the Washington, D.C. metro area, San Antonio, Toronto, Bucharest, Hong Kong, Singapore and Sydney.

The Federal Reserve's recent interagency guidance on Model Risk Management for Bank Systems Supporting BSA/AML Compliance, encourages a prudent, risk-based, and tailored approach to managing the risk associated with the transaction monitoring ("TM") systems used as part of an effective BSA/AML compliance program. To suggest otherwise, misreads the SR21-8 guidance. This is not the time to take the foot off the gas and risk undoing the recent gains on TM data quality and scenario alignment made by applying sound risk management and compliance principles.

Regulators expect financial institutions ("FI") to test all aspects of a BSA/AML system, model or tool for functional performance, appropriateness of data, outcomes and conceptual soundness. The risk associated with the tool, system or model is what drives the rigor and scope of the testing. Regardless, a key component of that testing is an effective check and challenge process, conducted by an independent, competent authority with the appropriate experience, and skillset to successfully design and execute a testing protocol. This competent authority, whether it sits in the second line of defense or a trusted outside advisor working on behalf of the second line, must understand the BSA/AML risks, assess the limitations of the chosen system, model, or tool, and then challenge the assumptions to assess the impact of accepting those limitations.

FIs that rely on tools or systems rather than defining it as a model, must still adhere to the principals espoused by the guidance. While a tool, as explained in SR21-8* may not require the testing rigor of a model or system, under SR11-7 and SR21-8, both models and systems likely still have the following:

1. An information input component, which delivers assumptions and data to the model.
2. A processing component, which transforms inputs into estimates (output).
3. A reporting component, which translates the estimates into useful business information.

Regardless of model or system definition, component testing should take a consistent approach across the FI whether it be for BSA/AML or, for example, liquidity risk management. FIs should test the fitness for purpose of the data input, they should test the processing component by challenging the algorithms/calculations and assessing the conceptual soundness (i.e., alignment of the BSA/AML risk assessment with the

* SR21-8 specifies that tools that lack one or more of the components likely would not be considered models such as stand-alone, simple tools that flag transactions based on a singular factor, such as reports that identify cash, wire transfer, or other transaction activity over certain value thresholds or systems used to aggregate cash transactions occurring at the bank's branches for the purposes of filing Currency Transaction Reports.

selected TM scenarios, rules and reports), and they should test the reporting component by assessing the outcomes and evaluating the governance around the implementation and operation.

Who Can Do the Testing?

Of course, the check and challenge process should not be duplicative of other functions. The regulators don't care who does the testing as long as they are capable and objective. SR21-8 has not changed this view. As has been the case, there remain three main options:

1. Internal model validation team
2. Independent compliance control testing team (Compliance Assurance)
3. Trusted external consultant

One way to avoid confusion is for the risk group at the FI to have second line oversight of compliance's risk management requirements (i.e. model validation expertise), and for compliance to have second line oversight of risk's compliance requirements (i.e. subject matter expertise in the BSA/AML domain). Compliance often maintains an assurance testing function that is independent within the compliance department that is responsible for independently testing controls, whether first line or second line. For sure, an appropriately qualified assurance team could conduct the testing necessary for effective check and challenge to ensure operation in accordance with the regulatory guidance. Although they may not have formal validation protocols defined by a model risk management program, it is likely they would still be expected to apply the same testing coverage principals similar to those defined in SR11-7. The assurance function may therefore still require a partner such as the model risk management team or a trusted advisor to adequately and effectively validate the model. Together, these functions can leverage their respective domain expertise to create the necessary coverage and provide appropriate check and challenge.

> "It all comes down to objectivity and subject matter expertise."
>
> **JONATHAN BALL**
> *Managing Director & Global Head, Analytics, Exiger*

While smaller FIs may not have separate risk and compliance departments and larger FIs may include compliance as part of their risk department, the important point is independence and expertise. If an FI must go outside their firm for that expertise or independence, they should consider the principles discussed in the agencies' third-party risk management issuances when selecting a partner. They should also consult these issuances, as well as the MRMG when choosing to use a third-party model.

At the end of the day, SR21-8 has clarified, but not changed the regulatory expectations on TM system testing. FI's continue to be expected to use qualified personnel who can objectively test all aspects of their TM system, regardless of whether it is considered a model or a system. Qualified means capable of assessing the system or model, and designing a test plan that will provide effective check and challenge. Objective means independent of the model or system selection, design, implementation or operation. All aspects include the data feed to the system/model, alignment of system/model to the intended risks, algorithm or calculation component, outcomes testing, and overarching governance.

For more information, contact:

Jonathan Ball

Managing Director | Global Head, Analytics

jball@exiger.com

EXIGER

New York City | McLean | Silver Spring (DC Metro) | San Antonio | Toronto
Vancouver | London | Bucharest | Hong Kong | Singapore | Sydney

www.exiger.com