BPO | Banking & Financial Services

From risk to resilience: A quick guide to dynamic risk management and monitoring in banking

Recent years have seen transnational financial crime grow exponentially, adversely affecting financial institutions, businesses and individuals worldwide. Globalization and digitization, along with the rapid growth and use of AI, have led to an increase in deception, blackmail, corruption, money laundering and social engineering fraud. It's now easier than ever for criminals to operate globally and commit financial crimes with increasing efficiency and sophistication.

It's estimated by the United Nations Office on Drugs and Crime (UNODC) that money laundered globally exceeds 2% to 5% of the global GDP — €715 billion to €1.87 trillion — each year.[1] All passing through global financial networks.

Industry leaders are looking for more efficient and effective ways to mitigate their exposure to money laundering attempts. Given the risks, banks need a better approach to customer due diligence (CDD). For example, organizations now need more frequent and comprehensive methods of regulatory risk management when checking a customer's information.

One option is dynamic risk management and monitoring, which tracks chains of customer affiliations to help mitigate risk. In a dynamic risk model, you can gather customer information to understand the nature and purpose of each relationship. This applies not only when opening an account but throughout the entire customer relationship, including active and passive transactions. In this guide, you'll learn how to strengthen your CDD process with dynamic risk management and monitoring.

Risk management: The good, the bad and the dynamic

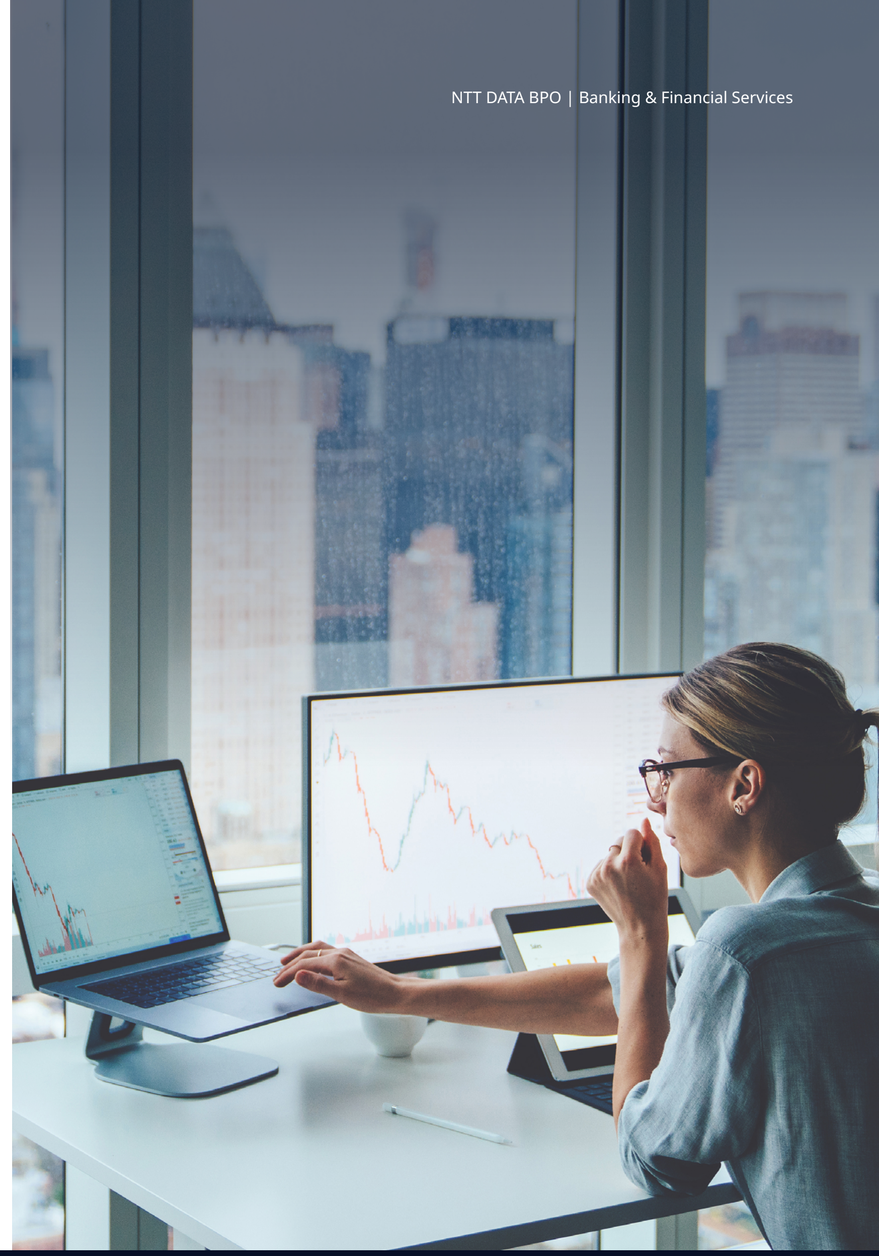
While traditional risk management can certainly help organizations, it tends to focus solely on regulatory compliance. It also involves reactive measures, versus proactively and continuously assessing customer risk. Practices tend to be siloed, with no attempt to reassess as better data becomes available or look at risk holistically.

Today's risk landscape is more complex, with digital technologies, AI, social engineering, increased mobile access and global attacks all playing a part. Enter dynamic risk management, which model includes updated risk policies and regulations.

Dynamic risk management helps you establish a crucial framework that allows you to create effective policies, processes and procedures for continuously tracking and reporting any suspicious activities to protect your organization.

Benefits of dynamic risk

Key Features	Dynamic Risk	Traditional Risk
Customers are reviewed regularly based on relative risk score	✓	–
The risk code reflects current estimated risk	✓	–
It can be used to upgrade or downgrade risk regularly	✓	–
It learns from historical patterns of risk changes	✓	–
It leads to a focused view of risk of the customers	✓	–
The cost of review is proportionate to the risk of profiling	✓	–
It is compliance-based approach	–	✓
It is dynamic-based risk approach	✓	–



A dynamic risk management strategy helps you foresee monetary transactions, customer contacts and chains of customer affiliations. You can investigate anything suspicious because you're constantly reassessing the risk individuals and groups pose based on new information. But you need to be able to develop and implement procedures for continuous dynamic risk management.

To do this, you should:

1. Establish risk-based procedures to develop **customer risk profile personas.**
2. Establish data feeds from all relevant data sources to continuously update customer status.
3. Create risk personas for each customer.
4. Ensure risk policies and regulations are updated in the model.
5. Provide **standards** for conducting and documenting analysis associated with the risk management process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Dynamic risk management traces all current customer transactions and predicts any likely future transactions.

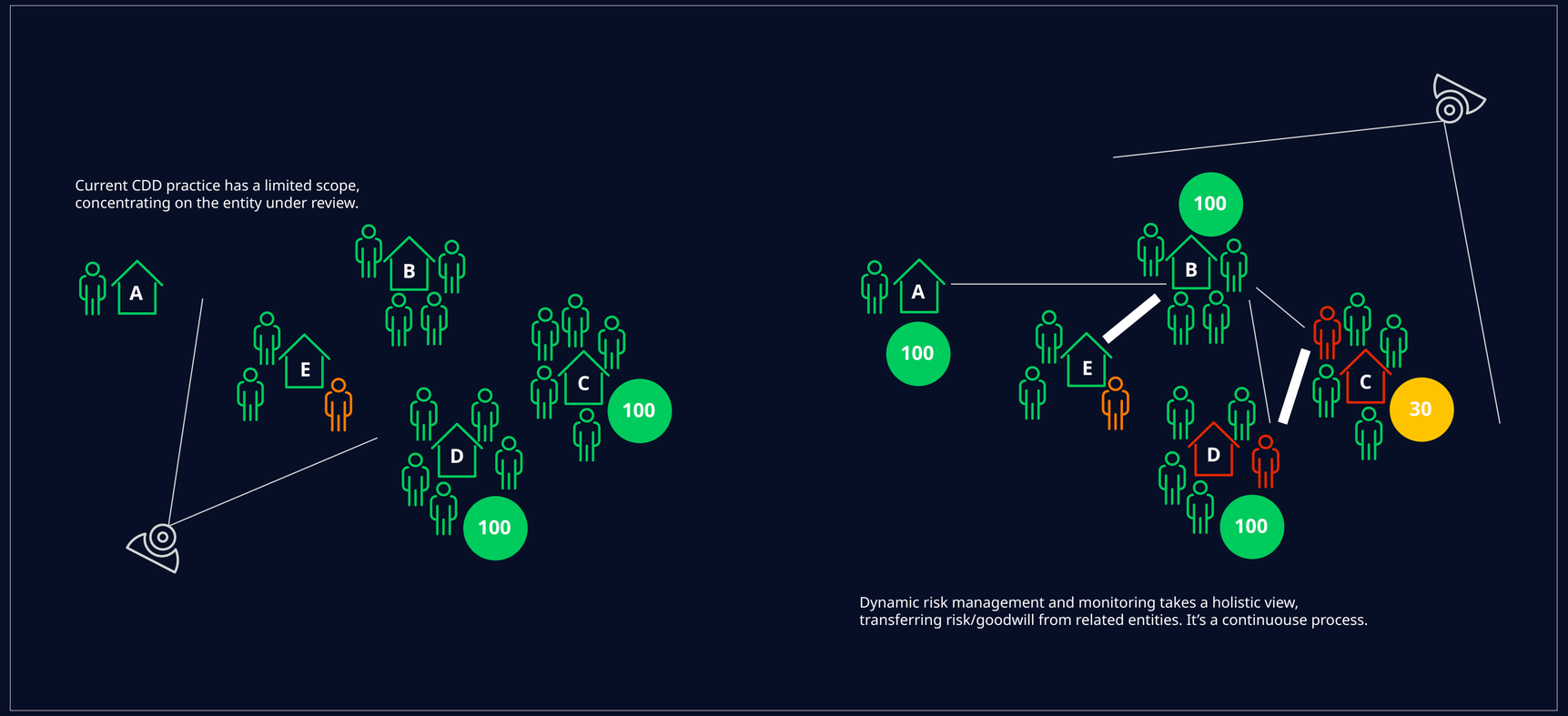
Changes in risk management practices

Dynamic risk management and monitoring is a radical shift in risk management practices. This approach helps you identify hidden patterns and links between customers and then evaluate risks from connected parties. This approach constantly reassesses the risk individuals and groups pose based on new information.

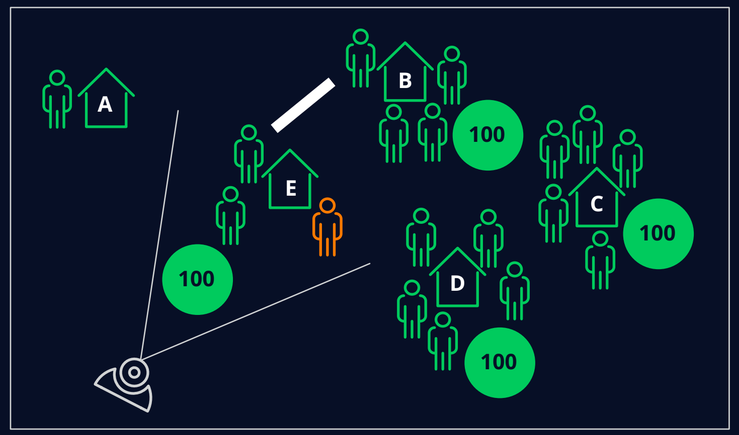
Data sources for network modeling include:

- Key personnel changes
- Suspicious activity reports and politically exposed person reports
- Sanction alerts
- Networked entities or suppliers
- Related individuals' employment
- All transactions

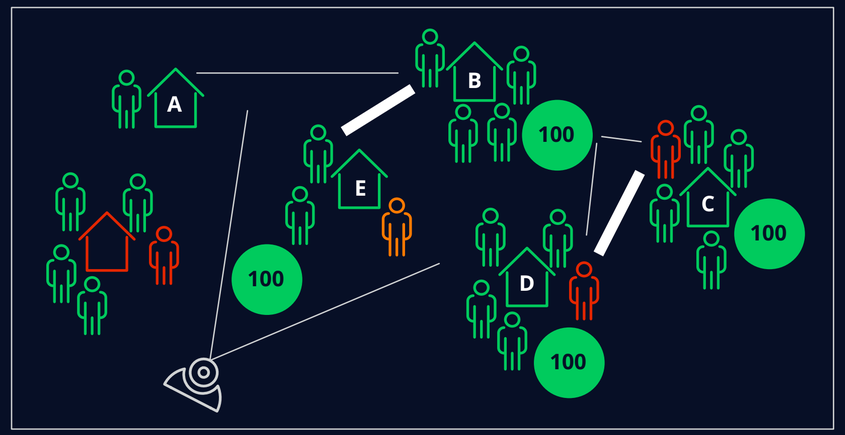
Data from all structured and unstructured sources is used to develop a deep-learning-based network risk propagation model. It also helps build a unique risk scoring methodology. Using both processes will result in increased operational efficiency, decreased environmental risks and increased agility.



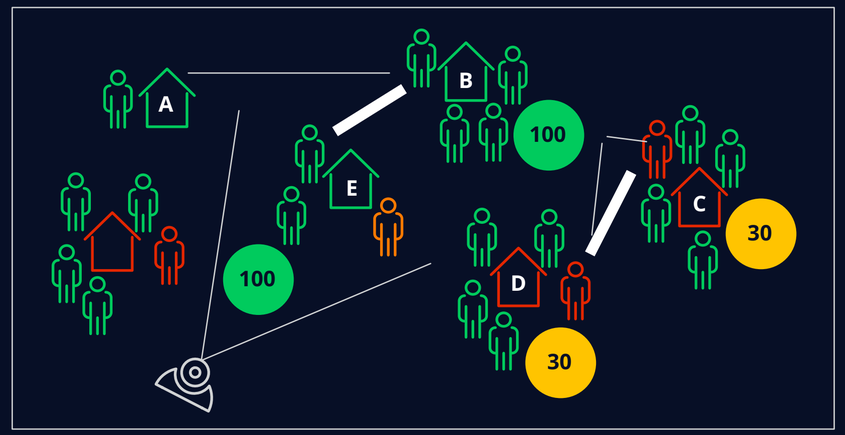
Deep learning-based network risk propagation model



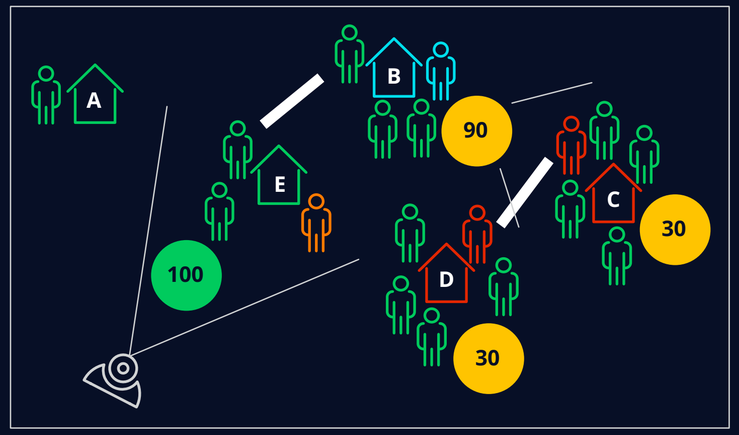
The model starts with a score of 100 (perfect score) for all individuals entities. The connections between entities/individuals are established. The strength of the relationship is identified.



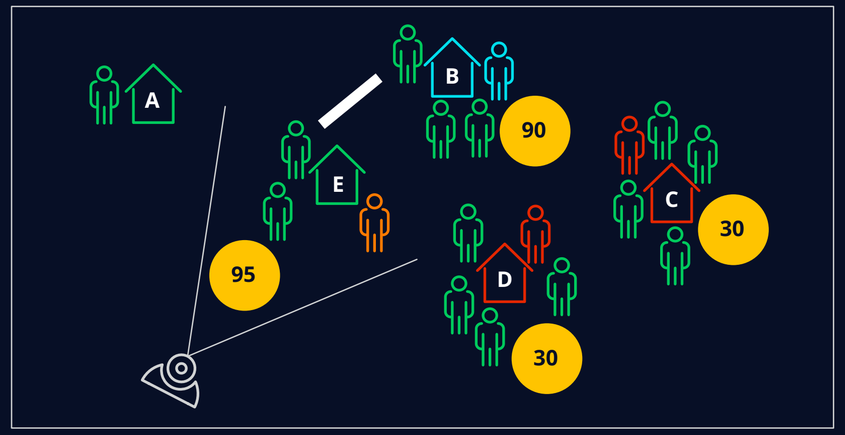
The model identifies an individual as high risk



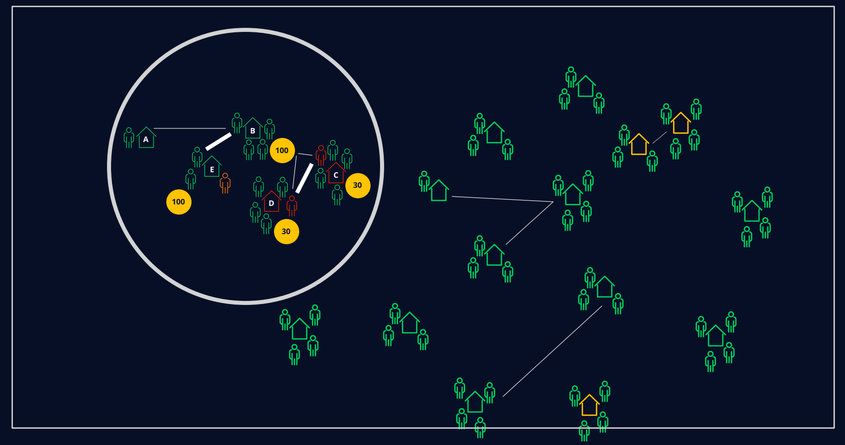
The model identifies an individual as high risk



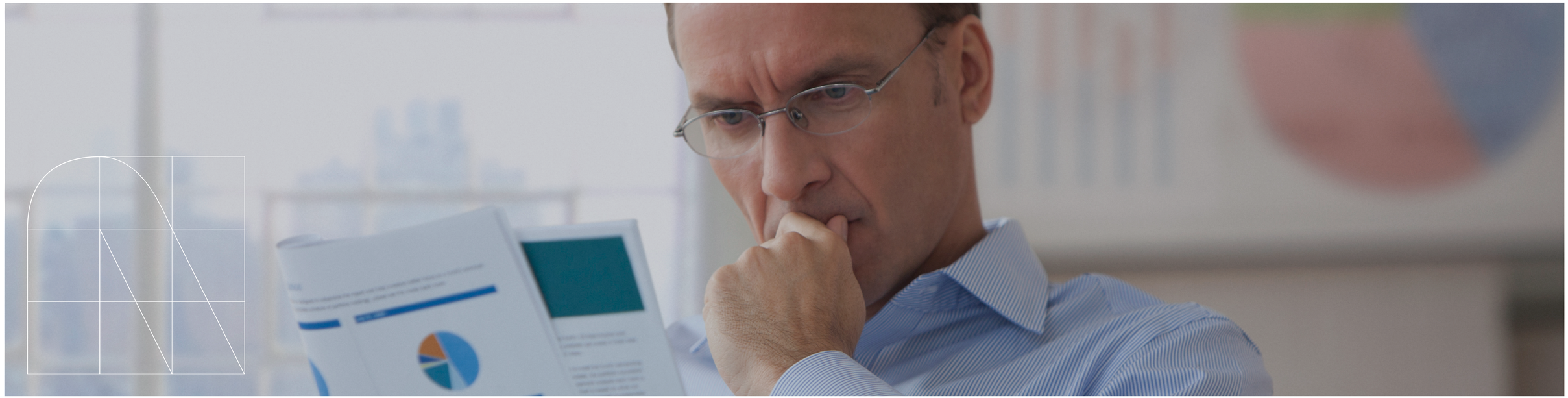
The network dpp learning model identifies an individual related to the “high risk idividual”. Depending on the sgrength of the relationship, the new entity (B) has its score lowered to reflect the risk.



The risk further propagates to company (E) considering the strong relationship between entities (B) and (E). Parties will be flagged for enhanced review if the threshold for high risk is breached.



Deep learning-based network risk propagation model



Leveraging a deep-learning-based network risk propagation model presets thresholds and flags an event when those thresholds are breached. Thresholds for review trigger set responses using AI-based predictive analytics for evaluating risks.

This is important because when dynamic risk isn't part of the risk management program, the risk of exposure to unscrupulous entities/customers increases. The potential for damage to your bank's reputation will outweigh the costs of establishing a comprehensive risk management practice.

Introducing deep learning techniques into your CDD program can help you safeguards all channels and circumvent internal and external fraud intrusions into customer accounts and institutional assets. Take a proactive approach to risk management today so you'll be prepared for what lies ahead.

Ready to get started?

From anti-money laundering solutions to big data analysis and business intelligence, NTT DATA can help resolve all your risk and compliance challenges. Contact us at bpo@nttdata.com or visit our BPO page to learn how to redefine your CDD program with dynamic risk management.

About the authors

Shabi Christopher,
Business Consulting Director, Analytics and FinTech Programs, NTT DATA

Shabi is a management professional with over 25 years of experience in corporate planning, technology implementation, solution design and analytics. He's demonstrated value additions in global project implementations and bottom-line impact valued at over $80 million. A key contributor to financial strategy, Shabi has played a critical role in architecting more than $100 million in deals. He directs know your customer, customer due diligence, enhanced due diligence and banking operations for global financial services clients. This includes service design, delivery, partner management and coordination with global teams.

Dr. Clifford Paul,
Financial Analysis Manager, NTT DATA

Dr. Paul is a financial strategist in the compliance arena with more than 24 years of experience. He's responsible for tracking the company's financial performance against the budget, analyzing business performance and market conditions to create forecasts, and helping senior management make tactical and strategic decisions by providing periodic reports. Dr. Paul has authored research articles in many peer-reviewed journals, as well as presented papers at both national and international conferences.

Sources

[1] Europol. "Money Laundering."
https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime/money-laundering

Visit us.nttdata.com to learn more.

NTT DATA is a $30 billion trusted global innovator of IT and business services. We help clients transform through business and technology consulting, industry and digital solutions, applications development and management, managed edge-to-cloud infrastructure services, BPO, systems integration and global data centers. We are committed to our clients' long-term success and combine global reach with local client service in over 80 countries.