



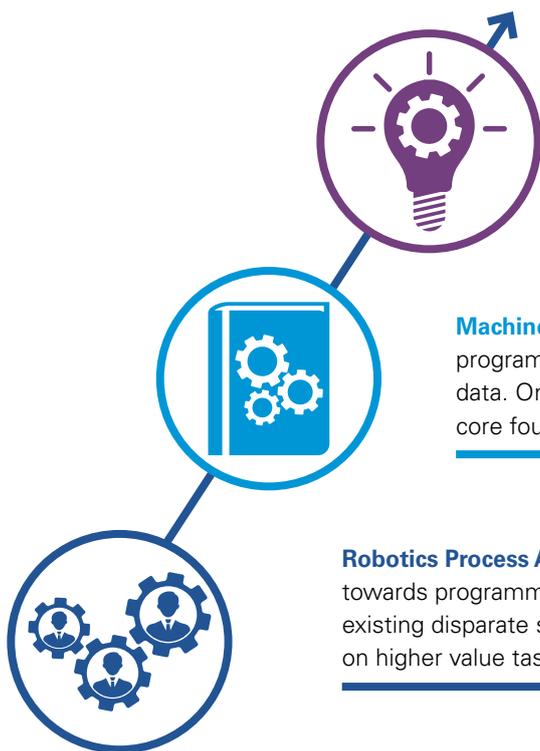
# The role of Artificial Intelligence in combating financial crime

Authors: Pascal Sprenger, Franziska Balsiger

Innovation is essential not only in business, but also in compliance. The automation of Financial Crimes Compliance Programs can help compliance leaders meet their strategic compliance objectives, further reduce compliance cost, and ensure effective management of regulatory change. Simultaneously, it sets the stage for a more efficient and effective management of regulatory compliance risks and cost savings.

### Different levels of intelligent automation

The innovation spectrum for Financial Crime Programs today ranges from robotics to machine learning to cognitive, or artificial intelligence (AI):



**Cognitive** represents a self-learning platform that mimics the attributes of human reasoning and decision-making while interpreting massive amounts of data, beyond what is humanly possible.

**Machine learning** refers to software algorithms which are not explicitly programmed that can predict outcomes or draw inferences based on input data. One of the main components that drive predictive capabilities, it is a core foundation for cognitive systems.

**Robotics Process Automation (RPA)**, is the entry point to automation and is directed towards programming software to perform highly repeatable rote tasks between existing disparate systems and applications. The use of robots allows humans to focus on higher value tasks and dedicate more of their time on areas of potentially higher risk.

The above-mentioned types of intelligent automation can be adopted individually or combined. To make a reasoned decision as to what type, or mix of types of intelligent automation a company should implement, financial crime stakeholders first need to design an intelligent automation strategy. This strategy depends on what investment the institution is willing to make and the benefits sought, including a weighting of the risk potentially involved, and the level of efficiency and agility desired. Therefore, the intelligent automation strategy should be aligned with the size and scope of the institution and its risk tolerance.

## Areas in financial crime compliance where intelligence automation can help reduce costs and increase efficiencies and effectiveness:

### Transaction monitoring:



As it does not rely on an institution's underlying, rules-based transaction monitoring systems currently in place, institutions need to build upon the alerts and cases previously occurred and any of the machine-learning models to the extent that they are already in place, thus providing a domain knowledge base on which the cognitive platform will rely. It is the key to finding new and emerging financial crimes risks because the machine is not limited to monitoring the risks the institution already knows and identified. Instead, it looks at patterns that exist in the data to identify if those patterns have been seen previously.



Machines can be used to automate aspects of the review process and deployed to build statistical models that incorporate gathered data and calculate a likelihood of occurrence (closure or escalation). Machine learning models can provide institutions with significant gains by quickly identifying alerts for closure, along with the rationale for that conclusion.



By employing bots to scan the internet and previously defined public due diligence sites to collect relevant data from internal and other acceptable sources (as identified by the institution), analysts save valuable time.

### Know your Customer (KYC)



With RPA and machine learning solutions in place, cognitive machines can apply judgement based on the domain knowledge base (for example identify the most relevant articles) and can also be used to identify KYC outliers that could be risk indicators. Cognitive allows Financial Crimes Officer to better prioritize their KYC efforts and the information they obtain to better reflect actual risks, with a robust audit trail of analysis to justify any changes.



Machine learning can automate the reading and extraction of data from unstructured documents. Coupled with RPA it can result in a more reliable and more efficient customer-risk rating process and can thus enable institutions to adopt to a more of a real-time risk assessment, enabling a more accurate analysis of the customer's actual risk at a certain point in time.



As KYC processes tend to consist of highly repetitive tasks, many institutions have already identified elements of their KYC processes where RPA can assist and save significant time. Since robots may eventually achieve greater accuracy in the collection of due diligence information, RPA could also reduce or eliminate the need to contact customers repeatedly, resulting in a better customer experience.

## Compliance Testing



Using prior outcomes from compliance monitoring and testing, internal audit activities, regulatory audits, enforcement orders, and other public information, as well as information gathered in the course of an institution's regulatory change management, a domain base knowledge of financial crime compliance can be built and applied to search for patterns and comparing these to the domain base knowledge. This allows the identification of issues that were not simply items that failed a particular test but rather outliers that need to be assessed by a human to evaluate potential risk.



Machine learning can be used to take in structured and unstructured data and rely upon a library of test steps to automatically assess the data, which could be read by the machine, humans will then only review the exceptions identified.



RPA can help to quickly identify issues from initial data sets that humans must review as part of their testing scope work and – depending on how structured the data is at a given institution – RPA could also be used to conduct basic testing procedures to identify data completeness, for example, by examining whether KYC files include required data like address, date of birth, citizenship, source of wealth, etc. by applying the institution's protocols to 100% of the files.

---

### Contact

#### **KPMG AG**

Räffelstrasse 28  
PO Box  
8045 Zurich

**kpmg.ch**

#### **Pascal Sprenger**

Partner,  
Financial Services,  
Regulatory & Compliance  
+41 58 249 42 23  
psprenger@kpmg.com

---

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence.

© 2018 KPMG AG is a subsidiary of KPMG Holding AG, which is a member of the KPMG network of independent firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss legal entity. All rights reserved.