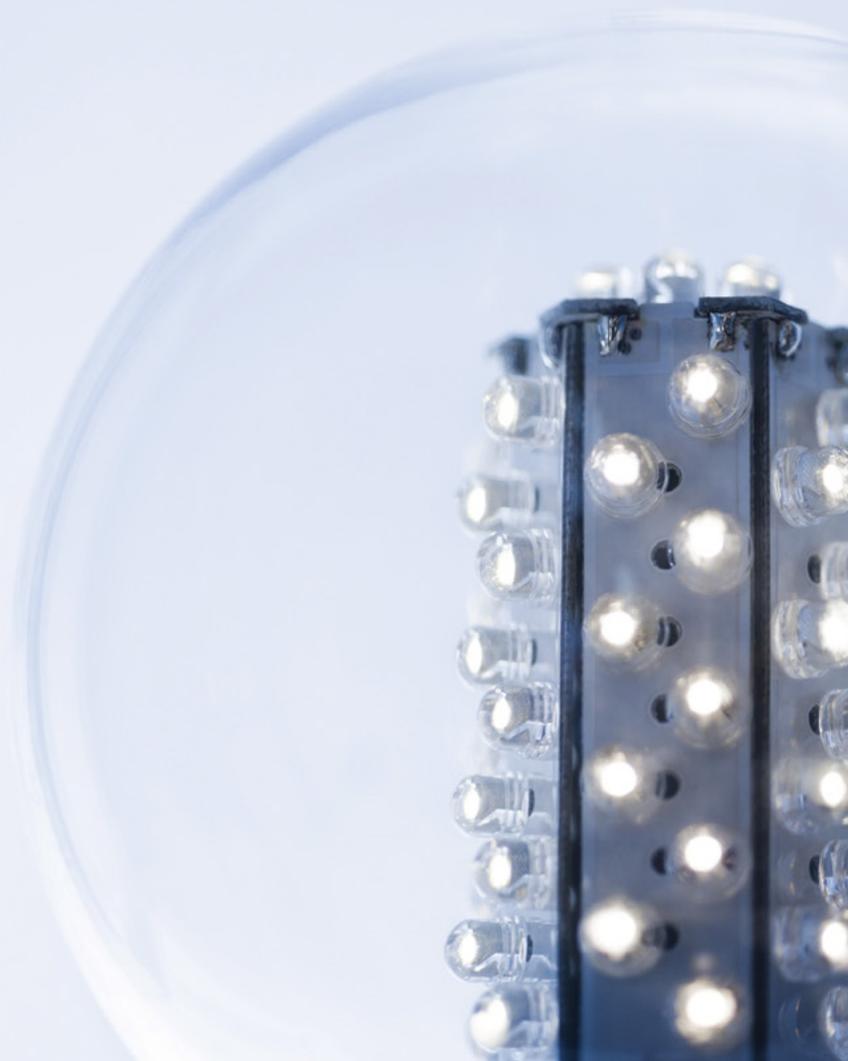




# Intelligent automation in financial crimes

**Forging an innovative compliance  
strategy for the future**

[kpmg.com/us/forensic](https://kpmg.com/us/forensic)





# What we can't have is a failure to innovate

Many may remember the Captain's speech in Cool Hand Luke with that infamous line "What we have here is a failure to communicate." Well today with technology, being leaps and bounds ahead of what you installed yesterday, you can no longer have a "failure to innovate." Financial Institutions face rapid innovations that are evolving practically overnight, and if they are to remain competitive, Financial Institutions cannot afford a similar failure. Innovation, not only in business, but also in compliance, is essential. Institutions must embrace new technologies and find ways to become more agile or risk disruption to their business.

Yet, the compliance mandate has never been more broad, challenging compliance leaders who seek to meet their strategic compliance objectives, further reduce compliance cost, and ensure effective management of regulatory change. Unsurprisingly, compliance leaders increasingly recognize that leveraging new technology capabilities to automate their compliance activities can help them meet these objectives, while simultaneously setting the stage for greater efficiency and cost savings.

As Financial Institutions expand their use of Intelligent Automation - from operational tasks to compliance activities -Financial Crimes compliance programs<sup>1</sup> are ripe with opportunities to automate, and integrate these capabilities into their programs to more efficiently and effectively manage regulatory compliance risks.

In planning for 2018, now is the perfect time for Financial Crimes Officers to assess how, and to what degree, they can integrate Intelligent Automation to support their compliance efforts and goals, including into their Know Your Customer (KYC) activities, transaction monitoring and screening, and compliance testing, amongst others.

---

<sup>1</sup> Financial Crimes Compliance Programs typically include Anti-Money Laundering (AML), Office of Foreign Asset Controls (OFAC)/Sanctions, Anti-bribery and Corruption (ABC), Insider Trading, Human Trafficking and other surveillance compliance area.

# Levels of intelligent automation

Innovation today means considering new approaches, supported by technology, to help alleviate compliance problems and costs. Many terms, such as Intelligent Automation, have been floated to describe the increasing role that technology is playing in organizations, ranging from robotics to machine learning to cognitive, or artificial intelligence (AI). For our purposes, we use the term Intelligent Automation to span the spectrum of innovation that can be brought to bear on Financial Crimes Programs today.

The characteristics of each of these levels along the automation continuum is reflected below:

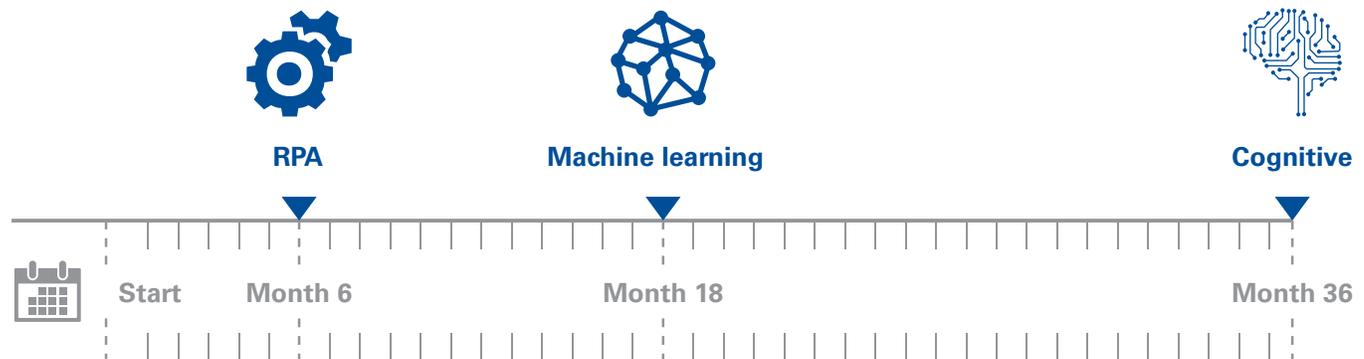
**Robotics Process Automation (RPA)** is the entry point to automation and is directed towards having software programmed to perform highly repeatable rote tasks between existing disparate systems and applications. Robots (virtual workers or “bots”) can be used to drive higher consistency and accuracy and allow for humans to focus on higher value tasks, thereby dedicating more of their time on areas of potentially higher risk.

**Machine learning** refers to software algorithms which are not explicitly programmed that can predict outcomes or draw inferences based on input data. The algorithms can learn automatically from experience as new outcomes are made available and can greatly enhance the effectiveness of bots when analysis tasks are required in a process. Machine learning is one of one of the main components that drive predictive capabilities and is a core foundation for cognitive systems.

**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. Cognitive systems utilize deep learning techniques on both structured and unstructured data which can extract meaning from documents using Natural Language Processing (NLP) and uncover hidden patterns in large complex datasets.

# Intelligent automation continuum

 <b>RPA</b>	 <b>Machine learning</b>	 <b>Cognitive</b>
<ul style="list-style-type: none"> <li>— Automate highly repetitive manual alert resolution tasks.</li> <li>— Complete tasks autonomously using virtual robots.</li> <li>— Interface directly with existing systems.</li> <li>— Design, test, implement quickly with relatively low investment or expenditure.</li> <li>— Reduce human factor significantly.</li> </ul>	<ul style="list-style-type: none"> <li>— Use machine learning models to enhance current transaction monitoring rules post processing with the most predictive risk factors.</li> <li>— Use models to provide the likelihood of whether the alert is a false or true positive, speeding up human analysis, allowing for more efficient alert review and escalation.</li> <li>— Streamline model risk management and simplify regulatory requirements with the use of accepted, proven models.</li> <li>— Incorporate more advanced models to enable the use of structured and unstructured data to support elements of self-learning.</li> </ul>	<ul style="list-style-type: none"> <li>— Automate transaction monitoring through decision support and advanced algorithms that incorporate advanced self-learning capabilities and NLP to interpret unstructured content.</li> <li>— Ingest, consider, and interpret massive amounts of data on which to formulate hypotheses, well beyond the capabilities of human review.</li> <li>— Increase coverage and uncover emerging risks by considering patterns, events, and factors; reduce false negatives.</li> <li>— Establish base domain knowledge prior to solution deployment, establish feedback mechanism to train machine over time.</li> </ul>



**When cognitive is integrated with RPA, this represents the mature state of IA on the spectrum.**

It is also valuable to remember that as an Institution moves along the Intelligent Automation continuum from RPA to cognitive, the rates of return increase, but so too does the costs involved, the timeframe to implement, and the number of risks associated with using more sophisticated technology.

For most Institutions, RPA offers the most immediate impact on efficiency, and RPA is cheaper and faster to implement than machine learning and cognitive. In contrast to RPA, machine learning and cognitive is more complex and takes longer to achieve, however greater benefits are possible.



**Eighty-five percent of CEOs recognize the importance of integrating automated [business] processes with artificial intelligence and cognitive processes.**

*(Source: KPMG International's 2016 Global CEO Outlook Study)*



## Levels of automation examples



### Robotics process automation

RPA bots can assist with gathering information needed for anti-money laundering (AML) alert investigations. The bots can retrieve customer and counterparty data from internal systems, external sites, and Internet search results based upon prescribed procedures that can be coded. Once the data is retrieved, the RPA bot can be programmed to automatically upload the data into the Institution's case management system. This provides analysts with requisite information needed up front. By automating these simple and repeatable processes, the Institution can realize greater efficiency and streamline their investigative process.

Similarly, Institutions can code RPA bots to scan public databases and sources for pending regulations, laws, and rules applicable to the Institution and its compliance efforts. Using formulas and parameters, the results can be rated in terms of potential relevancy and the bots can alert the compliance function in accordance with prescribed parameters.



### Machine learning

Using the historical outcomes of previous alerts and other data and information available within and outside an Institution (through KYC data or public source external information for example), machine learning models can be trained to identify risks by using a pool of available existing data as a baseline and then learning from feedback provided over time, which refine the machine's understanding of the risks to be identified.



### Cognitive

Cognitive can be the key driver in uncovering emerging risk as the Institution matures from deterministic rules-based scenarios to systems that functionally can be programmed to interpret an extremely broad set of data types and sources such as transaction activity, customer onboarding, enhanced due diligence, previous alert/case resolution, external sources such as negative media, as well as research sites like Factiva and WorldCheck.

Armed with this repository of information and the power to mimic the aspects of human judgment and decision making, machines can decision tier 1 alert level reviews for either immediate closure or escalation. When alerts cannot be confidently classified, then they would be provided to human resolvers.

## Drivers of change

Three primary drivers in particular are encouraging Institutions to integrate Intelligent Automation—regulatory scrutiny, cost pressure, and innovative competition .

**Regulatory scrutiny** – While in the past, Institutions have largely been able to address increasing regulatory scrutiny and the resulting fines and enforcement actions by adding head count, this is not a sustainable approach, particularly in a cost-cutting environment. With no signal that regulatory scrutiny will abate, Institutions are pivoting their compliance approaches to incorporate greater automation.

**Cost pressure** is also driving Institutions to figure out how they can innovatively incorporate Intelligent Automation into their Financial Crimes compliance risk management activities. The drive for shareholder value that executive management and the Board of Directors require is uniquely felt by those trying to deliver under the high intensity scrutiny of the regulators. The question Financial Crimes Officers constantly face from internal stakeholders is “can you do more with less?” As a result, Financial Crimes Officers are increasingly seeking innovative ways to meet their compliance obligations and those of their Institutions.

Also, **innovative competition** is a growing challenge for many Institutions. Every Financial Crimes Officer dreads calls from business line leaders complaining that “You’re standing in the way of my doing business. Don’t you know that none of our competitors have all these onerous requirements?” In reality, that business line leader may have a point. Innovative competition is finding new ways to meet regulatory requirements without having such direct, sometimes intrusive impact on an Institution’s customers. It includes finding ways to enhance the customer experience all while meeting regulatory obligations. The Financial Crimes Officer must be an integral player in the innovation landscape at the Institution so as to meet the regulatory requirements in a way that differentiates the Institution from its competitors.



# Developing a strategy for your journey

To make a reasoned decision as to what class, or mix of classes, of Intelligent Automation to implement, financial crimes stakeholders first need to design an Intelligent Automation strategy for their financial crimes activities. This strategy should foundationally be built upon what investment the Institution is willing to make and the benefits sought, including a weighing of the risks potentially involved, and the level of efficiency and agility desired. It is important that the Intelligent Automation strategy be aligned with the size and scope of the Institution and its risk tolerance. For certain Institutions, cognitive may not be warranted, at least not today or in the immediate future.

The strategy should also take into account any lessons the Institution has learned from their previous "technology waves" and knowledge of their existing current state, particularly of their data capabilities. Financial Crimes Officers need to work with their business and Information Technology partners to develop a strategy and then continually evaluate that strategy through its implementation.





# Integrate intelligent automation into financial crimes compliance

Three areas in particular within a Financial Crimes compliance program where Financial Crimes Officers may find that the various types of Intelligent Automation can help reduce costs and increase efficiencies and effectiveness are:

1. Transaction monitoring
2. Know Your Customer (KYC)
3. Compliance testing

## **Dependencies to automating Financial Crimes compliance activities**

Financial Crimes compliance officers may find certain dependencies exist to automating financial crimes processes and activities, which ultimately dictate what can be achieved in the short term. For example, an Institution may find that data needed for a KRI or to help code which transactional alerts can be more easily cleared as false positives does not exist or the data does not have integrity. This data may need to first be remediated as a foundation. In addition, the ability of the Institution's existing technology infrastructure to support varying levels of automation, and aggregate data, should also be evaluated to understand what automation is operationally possible without further investment in the infrastructure.

## 1. Transaction monitoring (TM)

Transaction monitoring is a prime example of where financial crimes compliance can benefit from enhanced technology. Typical AML transaction monitoring platforms are designed to consider rules-based typologies and scenarios, which not only require constant tuning and updates, but, since they are typically more simplistic and rule-based, can fail to take into account a multitude of risk factors. This often results in a large number of false positives for humans to resolve.



**RPA** – Institutions can employ bots to scan the internet and specified public due diligence sites and to collect relevant data from internal sources and acceptable sources (as identified by the Institution). They can also compile the due diligence results into an electronic case file for an analyst's review. Deploying the bot to complete these research and record-keeping tasks, saves the analyst valuable time.



**Machine learning** – Machine learning augments human decision making, building upon RPA. At this stage, machine learning is brought to bear on the investigative process through review of triggered activity and can be used to operationally automate aspects of the review process. In reviewing and assessing historical outcomes of investigations, the machine can be deployed to build statistical models that incorporate gathered data and calculate a likelihood for disposition, either closure or escalation. Those transactions that have a high likelihood for escalation would be subject to further review by humans who apply judgment to the resolution. That judgment is then assessed in terms of how the models could or should be updated. Since false positives tend to be pervasive in transaction monitoring systems, machine learning models can provide Institutions with significant gains by quickly identifying alerts for closure along with the rationale for that conclusion.



**Cognitive** – Unlike RPA or machine learning, cognitive does not rely on an Institution's underlying, rules-based, transaction monitoring systems currently in place. To effectively transition to cognitive, Institutions need to build upon the foundation of alerts and cases previously dispositioned and any of the machine learning models to the extent already in place. This can provide a domain knowledge base from which the cognitive platform will rely.

A domain knowledge base is generally specialized to the Institution. It consists of all of the underlying structured and unstructured models which have been learning and adapting to the Institution's risks, outcomes, processes, and procedures. Because of this foundation, the machine does not need to limit its monitoring to the risks the Institution already knows and has identified and captured in a rule or set of rules. Rather, with cognitive, the machine looks at patterns that exist in the data and the machine can identify if those patterns have been seen previously. If the pattern is new, the machine would flag the transactions for human review.

This is why cognitive is a key to finding new and emerging financial crimes risks. It is through cognitive that one truly addresses risk.

## 2. Know your customer (KYC)

Financial institutions devote substantial time and resources to performing KYC during onboarding and periodic review intervals. Depending upon the size of an Institution and its volume of new customers annually, Institutions may dedicate hundreds of hours per month to KYC tasks, often supplemented by contractors and consultants. Time investments for each customer typically range from a few hours for a low risk customer to upward of 24 hours for high risk customers.

KYC typically includes process steps for conducting external due diligence; screening customers and often related parties such as controllers and ultimate beneficial owners; clearing of identified negative news (which can be hundreds of pages of documentation requiring review); and reaching out to the front office or intermediary team, often multiple times, to obtain requisite information that adheres to internal protocols to meet regulatory requirements. The same is true for each periodic review to be performed.



**RPA** – KYC processes tend to be comprised of highly repetitive tasks, which are ripe for Intelligent Automation to augment and help expedite. As a result, many Institutions have already identified elements of their KYC process where RPA can assist. This would include such tasks as document retrieval from public news sources, negative news screening requests and retention of the results using pre-defined search criteria, and import of the data into a KYC system from documentation.

If properly setup, RPA can save significant time—enabling KYC analysts to devote more time to areas of onboarding that require deeper analysis, such as clearing of a more finite list of negative news results or assessing residual gaps in information or documentation needed. Since bots 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.

When implementing Intelligent Automation to supplement KYC work, financial crimes compliance personnel would continue to perform targeted testing of results achieved using automation to understand the precision with which the machines perform or to refine the parameters that are being used in order to achieve greater accuracy. Over time, it may be possible to scale back the testing or quality assurance (QA) reviews as the accuracy and consistency increase to an acceptable level.



**Machine learning** – For Financial Crimes Officers seeking greater automation of KYC processes, machine learning can be implemented to automate the reading and extraction of data from unstructured documents. This, coupled with RPA, can result in a more reliable and more efficient customer risk rating process. If the KYC customer file and risk rating can be updated in a more rapid manner, Institutions can then migrate to more of a real-time risk assessment, enabling a more accurate analysis of the customer's actual risk at a point in time.



**Cognitive** – With the RPA and machine learning solutions in place and functioning well the machine can apply judgment based on the domain knowledge base. For example, using semantic language processing to evaluate negative news articles allows for a very diverse set of sources to be used to gather articles, while cognitive can help identify the most relevant articles. Over time, with feedback from financial crimes QA staff, the technology can be refined to further improve accuracy and reliability. Cognitive technology can also be used to identify KYC outliers that could be risk indicators (e.g., a customer that is stated to be regulated in a jurisdiction like Cayman Islands without a record available via the Cayman Monetary Authority). Through greater automation and technology's ability to learn and re-calibrate, Financial Crimes Officers can better prioritize their KYC efforts and the information they obtain to be more reflective of actual risks, with a robust audit trail of analysis to justify any changes.

### 3. Compliance testing

Financial Institutions also invest significant time and resources in their Compliance testing of AML and sanctions controls. This can range from the testing of data feeds and systems validations to third-party vendor or outsourced processes and other internal processes. Since some of the tasks associated with testing are repetitive, Intelligent Automation can be a valuable tool here as well. Further, given that a machine is performing the tests, sampling becomes obsolete. The entire population can be tested, which eliminates the sampling errors.



**RPA** – RPA can help quickly identify issues from initial data sets (including documentation) that humans must review as part of their testing scope work. Depending on how structured the data is at a given Institution, RPA could further be used to conduct basic testing procedures to identify data completeness. For example, when testing an Institution's KYC compliance, RPA could easily examine whether KYC files include required data points like address, date of birth, citizenship, source of wealth, etc. in accordance with the Institution's protocols on 100 percent of the files, identifying outliers for further root cause analysis.



**Machine learning** – This can be used to ingest structured and unstructured data and rely upon a library of test steps to automatically assess the data. The data collected could be read by the machine and then reviewed by humans, if exceptions were identified. If the first line monitoring uses automation, then it may be more effective for the second line (the compliance function) to review and evaluate the effectiveness of the first line's QA reviews rather than the outcomes produced.



**Cognitive** – Using prior outcomes from compliance monitoring and testing, internal audit activities, regulatory exams, enforcement orders, and other public information, as well as information gathered through an Institution's regulatory change management, the domain base knowledge of financial crimes compliance can be built. This can then be applied to an Institution's customers, business lines, products, services, delivery channels, and transactions to search for patterns and compare those to the domain base knowledge. Issues can be identified 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. These issues would be fed back into the domain knowledge.



# Beware of automation compliance pitfalls

A transparent and easily explainable Intelligent Automation framework, regardless of the level of complexity, is imperative when automating financial crimes compliance activities. It provides a foundation of information to educate senior management, as well as regulatory agencies, about how the Institution is integrating automation into the program activities, and to ensure automation efforts align with the Institution's risk tolerance. This transparency should extend not only to the models and algorithms that will predict outcomes, but also to the risk factors that provide the data to make those predictions as well.

In addition, Financial Crimes Officers ought to be wary of "black box" solutions that are offered by many technology vendors. These solutions can have pre-defined risk factors that may not align to the Institution's risk profile, as well as needlessly complex or proprietary algorithms that can hinder the ability to effectively document and explain to stakeholders.

Fundamentally, every decision and action that an Institution undertakes to automate financial crimes compliance activities must be completely auditable and rationalized in "human-readable" language so that all outcomes are fully understood and can be justified against any scrutiny. Using the example of transaction monitoring, every time an alert is flagged as a likely false positive, a Financial Crimes Officer must be able to easily uncover the reason why the model made that determination. The inability to do so will not only potentially expose the Institution to additional risk, but will make it harder to support the conclusions made by the models and subsequent actions taken.

# The technology is available... So, what's next?

Financial Institutions cannot afford a failure to innovate. Whether stemming from regulatory scrutiny, prohibitive labor costs, or innovation competition, Financial Institutions need to take a step back from their historical approach to managing their financial crimes compliance and evaluate how and to what level they will invest in Intelligent Automation to achieve the greatest impact.

As Intelligent Automation quickly becomes a more significant enabler and accelerator in financial crimes compliance, Financial Crimes Officers can integrate Intelligent Automation in a way that is right-sized for their Institution and business goals, with benefits such as greater efficiencies and effectiveness, expanded risk coverage and, as an important added bonus, an improved customer experience.

If you are just beginning to think about how to make these changes and the type of financial crimes compliance activities to which it can be applied, the evaluation can understandably seem daunting. For example, while the Financial Crimes Officer must take the lead in the communication and collaborative efforts that are to occur, driving the implementation process across the enterprise, it is critical that the Institution identify and engage individuals internally and/or externally who will collaborate with this individual throughout the Intelligent Automation journey. These individuals should have a hand in the design and implementation of the ultimate Financial Crimes Intelligent Automation strategy and help coordinate with stakeholders in the Institution's overall Intelligent Automation strategy to ensure greater consistency and risk awareness from the changes. This may include internal resources from Information Technology and the business lines, risk officers, Internal Audit, and others whose roles are strategy development and execution.

In taking that lead, it is wise for the Financial Crimes Officer, to the extent possible, to leverage any existing organizational infrastructure around governance, data quality, model risk management, change management and information security.

So not only must a Financial Crimes Officer make sure there is no failure to communicate but also make sure there is not failure to innovate.

# Contact us



**Teresa Pesce**  
**Global AML and Financial Crimes  
and Enforcement Leader**  
**T:** +212-872-6272  
**E:** tpesce@kpmg.com



**Stephen Marshall**  
**Principal, Advisory, Forensic**  
**T:** +212-954-3025  
**E:** sdmarshall@kpmg.com



**Tom Keegan**  
**Principal, Advisory, Forensic**  
**T:** +212-954-7880  
**E:** tkeegan@kpmg.com

Special thanks to contributing authors: Stephen DeParis, Nicole Stryker, Michelle Harman, and Andrew Epstein, in KPMG's Forensic practice.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

[kpmg.com/socialmedia](https://kpmg.com/socialmedia)



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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 721191