Each edition of the magazine will be addressing subjects related to a specific function. Please find below an overview of the spotlight for the upcoming editions of the magazine:
In this issue

Companies are confronted with a changing environment and need to respond to challenges...

**Part 01**
From a digital perspective  08

**Part 02**
From a core transformation/technology perspective  42

**Part 03**
From a risk and cyber perspective  54

10
**Welcome to the ValueWeb**
The value mechanism for the Network Revolution

14
**Innovation monitoring**
A tool for the digitally savvy financial services industry

48
**Blockchain**
From the hype to the concept with POCs

56
**Ransomware**
An exponentially growing cyber threat
20
Cognitive Intelligence
When intelligent machines learn to venture into the business world

28
Is there a best way to set up an efficient “robo advisory” solution within your IT application landscape?

38
Let’s meet Pepper
Banking Services of the Future!

44
Robotic Process Automation for the Finacial Industry
A virtual workforce increasing capacity and improving efficiency

64
How should we tackle new KYC challenges?

70
A big step toward the European Digital Single Market
Regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

78
PSD2
Challenges and Opportunities for the CIO

84
Toward privacy in the digital market
How the General Data Protection Regulation will affect your business
Dear readers,

We are very pleased to present you the 13th edition of Inside magazine. Similar to the past three years, our October edition is dedicated to Chief Information Officers (CIOs) with a focus on the financial services industry.

With the new green and black Deloitte identity, we want to reflect the importance of the digital disruption that the financial industry is facing.

The CIO plays a central role within the organization of a company with your extensive knowledge of technology as well as your broad understanding of the business needs. Your role as CIO includes keeping up to date with technology trends, guiding the company executives through their digital strategy, and helping them in critical technology choices by providing them with a variety of different solutions and depicting their advantages and disadvantages.

Between digitalization and core transformation of the industry offered by technology improvements, the continuous follow-up and the assurance of integrating the current regulation within the new technology is a big challenge. Furthermore, the financial sector is facing the highest number of organized cyber-attacks—an additional hot topic for CIOs. Through these articles, our experts intend to help you and your companies keep up with this fast-changing world and prevent you from being left behind. For that purpose, we hope you will find information or guidance in these lines to remain competitive and build the future of the financial industry.

We look forward to receiving your impressions and comments.

Joël Vanoverschelde
Partner
Technology & Enterprise Application Advisory & Consulting Leader

Pascal Martino
Partner
Strategy & Corporate Finance Deloitte Digital Leader for Luxembourg

Etienne Ranchin
Analyst
Business Operations & Human Capital
Dear readers,

In a world in constant evolution, topics that headline CIOs’ agendas are multiple and heterogeneous. In last year’s CIO edition of the Inside magazine, we drew a path to understand and navigate through those disruptive trends and determine topics on which to spend valuable time and money. Where do you stand now and what are the elements that will drive your future decisions? In this 13th edition of Inside magazine, we focus on three perspectives that will be key topics for tomorrow.

Digital remains one of the most important opportunities for transformation even though it has already been under the spotlight for some time. To highlight this fact, we have selected several articles that focus on new and trending topics in digital. From the internet of value to robo-advisory and cognitive intelligence, digital still has the potential to reshape the future of the financial services industry.

From a core process and technology perspective, we believe that Robotic Process Automation and Blockchain will be further examples of subjects driving the transformation. Robotic Process Automation will bring tools to create a virtual workforce—increasing capacity and improving efficiency. Blockchain and distributed ledger technologies tend to make disintermediation the new standard.

In the third part, we have decided to focus on the risk and cyber perspective. Transformation could arise through multiple channels, and CIOs must quickly adapt to new challenges and embrace opportunities. The Know Your Customer (KYC) process and the exponentially growing cyber threat are two prominent examples. Transformation will also be driven by new regulations such as privacy in the digital market with the General Data Protection Regulation (GDPR), electronic identification and trust services for electronic transactions in the internal market (eIDAS), as well as payment regulation (PSD2).

We wrote this edition of Inside with the objective to provide you with essential and contemporary market topics and points of view. We hope that you will enjoy reading this magazine and that it will offer you fresh insight.

Yours sincerely,

Patrick Laurent
Partner
Technology & Enterprise Application Leader
Industry Leader

Stephen Marshall
Partner
Financial Services Technology Leader
Deloitte UK

Sebastien Genco
Senior Manager
Technology & Enterprise Application Deloitte
Part 01
From a digital perspective
Welcome to the ValueWeb
The value mechanism for the Network Revolution

Chris Skinner
Chairman
The Financial Services Club

We share a belief in banks because governments say they can be trusted. Governments use the banks as a control mechanism, which manages the economy, and yet now we come to bitcoin and the internet age, where some of these fundamentals are being challenged. Considering it took 330 years between the emergence of steam power to the last steam power patent during the Industrial Revolution, that implies there’s a long way to go in our transformation during the “Network Revolution”.

Let’s first consider the Network Age as we see the collapse of time and space. Einstein would have a giggle, but it is the case today that we no longer are separated by time and space as we were before. Distance is collapsing every day through our global connectivity.

We can talk, socialize, communicate, and trade globally, in real-time, at almost no cost. I can make a Skype call to anyone on the planet thanks to the rapidly diminishing costs of technology—there are phones out there today that cost one dollar, and the cheapest smartphone in the world is currently the Freedom 251. It is an Android phone with a 4-inch screen that costs just 251 rupees in India, around US$3.75. In other words, what is happening in our revolution is that we can provide a computer far more powerful than anything before, and put it in the hands of everyone on earth, so that every single person is on the network.

Once on the network, you have the network effect that creates exponential possibilities—everyone can now trade, transact, talk, and target one-to-one, peer-to-peer.

This is why I think of the network as the revolution of man and money, as we went from disparate, nomadic communities in the first age; to one that could settle and farm in the second; to one that could travel across countries and continents in the third; to one that is connected globally, one-to-one. This is indeed a transformation and shows that man is moving from single tribes to communities to connected communities to a single platform: the internet.
The importance of this process is that each of these changes has seen a rethinking of how we do commerce, trade, and finance. Our shared belief system allowed the barter system to work until abundance undermined bartering, and so we created money; our monetary system was based upon coinage, which was unworkable in a rapidly expanding industrial age, and so we created banking to issue paper money. Now, we are in the Network Revolution, and banking is no longer working as it should. Banks are domestic but the network is global; banks are structured around paper but the network is structured around data; banks are distributed through buildings and humans, but the network distributes through software and servers.

So much excitement is hitting the mainstream as we are now at the cusp of the change from money and banking to something else. However, in each previous age, the something else hasn’t replaced what was there before. It’s added to it. Money didn’t replace bartering; it diminished it. Banking didn’t replace money; it diminished it. Something in the Network Age isn’t going to replace banking, but it will diminish it. By diminish, we also need to put that in context. Bartering is still at the highest levels it has ever been—about 15 percent of world trade is in a bartering form—but it is small compared to the monetary flows. Money in its physical form is also trading at the highest levels it has ever seen—cash usage is still rising in most economies—but it is not high compared to the alternative forms of monetary flow digitally and in foreign exchange markets. In other words, the historical systems of value exchange are still massive, but they are becoming a smaller percentage of trade compared to the newest structure we have implemented to allow value to flow.

The first massive change in the network effect of financial inclusion is that the five billion people who previously had zero access to digital services are now on the network.
This is why I’m particularly excited about what the Network Age will do, as we connect one-to-one in real-time, and it will create massive new flows of trade for markets that were previously underserved or overlooked. Look at Africa, for instance: African mobile subscribers take to mobile wallets like ducks to water. A quarter of all Africans who have a mobile phone have a mobile wallet, accounting for nearly every citizen in more economically vibrant communities like Kenya, Uganda, and Nigeria. This is because these citizens never had access to a network before; they had no value exchange mechanism, except a physical one that was open to fraud and crime. Africa is leap-frogging other markets by delivering mobile financial inclusion almost overnight.

The same is true in China, India, Indonesia, the Philippines, Brazil, and many other under-served markets. The first massive change in the network effect of financial inclusion is that the five billion people who previously had zero access to digital services are now on the network.

A second big change is the nature of digital currencies, cryptocurrencies, bitcoin, and shared ledgers. This is the part that is building the new rails and pipes for the fourth generation of finance, and we are yet to see how this rebuilding will work out. Will all the banks be based on an R3 blockchain? Will all clearing and settlement occur through Hyperledger? What role will bitcoin play in the new financial ecosystem? We don’t know the answers to those questions yet, but what we will see is a new ecosystem that diminishes the role of historical banks. The question for historical banks is whether they can rise to the challenge of the new system.

The Network Age is a digital networked value structure that is real-time, global, connected, digital, and near-free. It is based upon everything being connected, from the seven billion humans communicating and trading in real-time globally to their billions of machines and devices, which all have intelligence inside. This new structure obviously cannot work on a system built for paper with buildings and humans, and is most likely to become a new layer on top of that old structure.
This is why I think of the network as the revolution of man and money, as we went from disparate, nomadic communities in the first age; to one that could settle and farm in the second; to one that could travel across countries and continents in the third; to one that is connected globally, one-to-one.
Innovation monitoring
A tool for the digitally savvy financial services industry
Global financial players are beginning to embrace the paradigm shift in digital banking, and have also realized that the traditional financial services sphere is being revolutionized. In order to stay ahead of the “digital disruptors,” banks have realigned their innovation monitoring strategies.

Tech giants like Google and Amazon are proving to be revolutionary challengers. These firms are looking to raise customer expectations by providing a new digital experience. Specifically, they are still running in their current ecosystem, but with improved interoperability and point-of-sale simplicity.

**Do you know the latest digital trends in the financial services industry?**

Electronification, automation, biometrification—these are just a few of the topics that have compelled the financial services sphere to be digitally redefined by capabilities that push a digital driven approach. As banks and financial institutions realign their strategic vision for the future of the financial services industry, most have turned to investing and revamping their technological capabilities. In particular, financial services firms have an impetus to invest in Big Data analytics. The benefit of analytics for this industry lies in understanding clients better in order to deliver tailored and custom products.

**How are new entrants trying to get ahead?**

New entrants to the financial services industry are popping up to bring about a notion that challengers can defy the odds and take down the traditional behemoths of the industry. These rivalries are not just emerging in the FinTech space by startups which hone in on one particular area of the financial services value chain, but also by big players looking to redefine the entire model.

**How can firms capitalize on these trends?**

While investing in these technological capabilities is fundamental to success, an equally crucial part of the digital transformation is the development of a specific mindset and culture of innovation. That requires adopting a visionary approach to innovation that lays out the ground work for a coherent digital vision, which is not simply a watch-and-learn approach but rather a scope-and-adopt methodology.
Financial services innovation, in part brought about by electronification, has reached a new tipping point in its development. In many ways banks, insurers, and firms alike are looking for new ways to improve the delivery of services to clients, implement state-of-the-art technologies, and automate various capabilities. These revolutionary technologies that have aided the mobile and digital revolution are elevating clients’ expectations like never before. In order to stay abreast of this new wave of change, firms are rethinking their approach to manage innovation. Most firms are adapting to the innovation movements in their own way.

To effectively manage these “digital disruptors,” a clearly defined and strategically-oriented vision toward a digitalized service model is required. To achieve this, firms need to expand their scope toward the way in which they monitor the innovation ecosystem.

**Cashless optimization**
- Cryptocurrencies
- Blockchain
- Unified payment interface
- Cloud computing
- E-commerce
- Real-time analytics
- Crowdfunding

**Platform innovations**
- AI & Machine learning
- Robo-advisers and HFT Systems
- Big Data analytics
- Wearable technology
The value in digital innovation monitoring

The innovation landscape is undeniably changing. This in turn has resulted in a highly competitive market, where a means of differentiation is of paramount importance. Interestingly, the shifting digital landscape has created a paradoxical dilemma for banks and financial institutions. On one hand, they are being driven toward digital innovation in a complex manner by providing revolutionary technology to clients. On the other hand, simplicity has become the order of the day, due to customers preferring fast and easy transactions.

Going digital is one way to embrace the paradigm shift in the financial services industry, ensuring higher efficiency in various processes and an improved connectivity and customer experience. For banks in particular, transforming and innovating can also prove to be a rebuffing strategy due to the increased competition of Neo-Banks. For CEOs of banks, the good news is that innovative digital strategies can be applied to the full spectrum of their operations. Despite this, most banks are only in the preliminary stages of adopting a culture of digitally native strategies. The reason boils down to the fact that with the sheer amount of technological innovations in the market, it is often difficult to develop a concise and strategized approach.

Digitalization has been pushed to a revolutionary speed due to “digital disruptors.” Firms like Google, Apple, and Alibaba are all looking at ways to revamp traditional financial models by positioning themselves with the new payment methods that are transforming the market. Commercial players will also need to consider the evolving needs of the millennials. This generation of people born between the 1980s and 2000 are likely to vastly change the way firms serve their clients. In particular, the trend is shifting toward digitalized wealth management, whereby robo-advisers, biometric security, and gamification are all vital to appeal to the millennials.

To capitalize on the latest developments in the market, financial firms will need to understand the innovation ecosystem much deeper than before. This understanding and awareness will need to go beyond the realization that innovation is required to stay competitive in the market.

Payment developments

- Third party API
- P2P Lending
- NFC

Evolving customer preferences

- Augmented & Virtual reality
- Video banking
- Financial education
- Biometric identification
- Virtual identification
The innovation monitoring sphere

1. Market overview and monitoring
A comprehensive analysis of the firm’s operating ecosystem is fundamental to the innovation monitoring process. This includes determining the firm’s strategic innovation goals specific to their operations, business lines, and regional presence.

Across the value chain, trends in technology that affect financial services and consumer behavior are analytically processed, so that all the latest and revolutionary innovations are assessed. If the institution has a global footprint, the innovation monitor covers the full scope both locally and globally to meet the firm’s global objectives. A close analysis of the disruptive innovations in the market will be evaluated so that their value chain disaggregation can align the optimum benefits of scale and scope to the firm.

2. Information advisory structure
With the high volume of innovation in the market, an effective monitor will be able to filter through the vast amounts of developments to provide a customized approach that will address the most pressing innovations in the industry. To confront this digital dilemma, the scope of the innovation monitor will look at how digitalization and FinTech developments are evolving.

Banking, for one, has long been an integrated business with traditional one-stop banking models dominating the market. Now we have begun to see a disintegration of the value chain, whereby innovators are doing business not by recreating the universal banking model, but by developing niche services. To cultivate a robust digitalized strategy, firms will need to monitor and align their key capabilities for their forward-looking strategy to the innovative movements in the market.

As a result, the innovation monitor will address the opportunities from these technologies, which will require planning, investment, and a coordinated approach to developing the digital growth trajectory of the firm.

3. Impact assessment
To fully leverage the developments in the innovation monitor, it is necessary to analyze the impacts that valuable innovations could have on the firm. This phase is invaluable in addressing the firm’s capabilities and how these changes in the industry will affect the company. The added value here lies in addressing each sector in the financial services value chain and looking for a way to translate new technologies to help the firm differentiate themselves from competitors by providing high quality and high value-added digital functionalities for customers.

The impact assessment is the pivotal advisory service in the innovation monitor that will help to successfully drive useful change for the firm. Such a scenario analysis will highlight the unforeseen opportunities that create a strategic differentiator for the business.

4. Delivering value
Once the impact assessment has been conducted, the firm can begin to cherry-pick the most valuable innovations to tactically integrate into their service offerings or backend support.

The external innovation marketplace can often appear convoluted. Having a strategic approach to the available opportunities will help firms realize which innovations are of strategic value.

Firms need to capitalize on seeing the end-to-end spectrum of the digital innovation market.
Understanding the innovation market is all about fully harnessing the potential of digital movements to revolutionize traditional business models. For financial firms, it is less of a question about whether to innovate, but rather which innovation could empower the firm with the right cutting-edge tools and capabilities to stay competitive.

Finding the added value in a digital market being flooded by vectors of change is challenging for any financial firm. Therefore, the company must expand its capacity to monitor the innovative technologies. To manage the level of information available and the different business models offered, a strategic innovation monitor could be the key to navigating around the new innovation ecosystem.
Conclusion

- The rapid evolution of the digital financial services sphere has put great pressure on firms that have tried to monitor the developments.
- In most cases, firms have not yet deployed a clear and concise strategy toward how they watch, learn, and invest from innovative players in the market.
- The use of a keyword and long-term strategized innovation monitoring tool will offer a unique opportunity for global financial service players to stay ahead of the market.
- The innovation monitoring tool is an invaluable asset toward a proactive and holistic approach in analyzing the modernizing market.
Cognitive Intelligence

When intelligent machines learn to venture into the business world

Jean-Pierre Maissin
Partner
Technology & Enterprise Application
Deloitte

Ronan Van Der Elst
Director
Technology & Enterprise Application
Deloitte

Nicolas Griedlich
Senior Manager
Technology & Enterprise Application
Deloitte

Martin Mouton
Analyst
Technology & Enterprise Application
Deloitte

Michel Van Der Poorten
Cognitive Solutions Strategist
Financial Services Sector, IBM

Cognitive intelligence is a booming technologic trend. This new concept might very well be the next revolution that improves revenue growth, operational efficiency, and risk management.
AI is becoming an increasing part of companies’ investments and fundamental research, which in turn is spurring a significant activity of development.

Introduction
Artificial Intelligence, Cognitive Intelligence, and Machine Learning are areas that tend to make machine processing more akin to human reasoning. Algorithms hidden behind these “smart machines” are rational agents that solve problems, thanks to the sheer amount of computing power available that the human mind has difficulties processing. Unlike classical algorithms, they mimic cognitive human functions in that they understand, reason, and learn. Areas of computer science like Artificial Intelligence, Cognitive Intelligence, and Machine Learning could change our vision on business, the way we operate in it, and how we make decisions.

Nevertheless, Artificial Intelligence is a topic that the majority of actors mature enough to activate cognitive capabilities still need to get familiar with. Indeed, notions like “Intelligence,” “Cognition,” or “Learning” as applied to machines are still in their infancy; intelligent machines are able to reason, plan, and process natural language based on computational, logical, and statistical methods, but all of these abilities are limited to the algorithms’ specific features.

These cognitive abilities can contribute to the autonomous processing of huge amounts of data and the identification of real-time patterns to make predictions. In doing so, they actively decrease the risk of human error. In providing efficient solutions to certain specific tasks, machines can improve workplace operations, giving companies the ability to optimize their operations, reduce their costs, and optimize customer experience. No further explanation is needed as to why this subject is branding itself as the future of business tools.

1. Artificial Intelligence as a top priority in technology investments for the next years¹
Artificial Intelligence is a booming area revealing a growing interest from companies, fueled by the steady and frequent introduction of new use cases. AI is becoming an increasing part of companies’ investments and fundamental research, which in turn is spurring a significant activity of development.

For the mature companies that have a clear view of their business model, and would like to optimize their operations and make decisions with a reduced risk of human errors, leveraging AI algorithms is a smart choice. We see data-driven companies promoting a culture of using analytics for business decisions, investing in predictive software based on machine learning concepts to improve operations and to provide a better insight into how their customer population is evolving. Take for instance Gartner’s example of a food concession provider at sporting events that used an intelligent BPM (Business Process Management) system to monitor oversupply of snacks and waiting times at different stands. This tool helped to redirect customers to where they would be served more quickly, providing a better customer experience. Similar systems can also be used to implement more critical tasks, like assisting strategic corporate decisions through advanced analytics and complex mathematical predictive models. Cognitive intelligence is not only adopted by sectors with a high analytic maturity level; it is also applied by mass retail companies like the aforementioned food supplier as well as Amazon.

This is not the only way in which companies make use of AI. One of the trends in which we have seen a real boom is bots used directly for customer service that are programmed to seem human. In a relatively short time, these have evolved from basic planning assistants to natural language processors, actively helping people out with their web requests. E-commerce is one of the sectors in particular in which this application is successfully deployed, implementing bots to help customers in choosing their products. The customer

describes the aspects of the product they want to buy and the context in which they will use it, and the machine will figure out the best fit (providing for instance a selection of insulating gear in response to the request “I need a jacket for a skiing trip in February”). Moreover, machine learning also provides deeper insights into customer behavior, and can anticipate the next trends in their purchases.

One of the other major areas in which machine learning and other cognitive algorithms can be particularly relevant is cyber security. These algorithms are designed to discern even the smallest of suspicious patterns in enormous amounts of data—an impossible task for the human eye and mind. Monitoring takes place in real time, and uses learning mechanisms to detect every threat or attack as soon as possible to minimize the harm it can do, making customers’ data safer.

These varied business needs have prompted a surge in AI software development. From powerful code libraries (some of which are available in different programming languages like Java, C, and Python, enabling custom developments of predictive algorithms based on fundamental functions of resolution like regression, neural networks, and decision trees) to complete software stacks, an ecosystem with a wide variety of tools has been developed over the past few years in order to implement cognitive functions. And this is only the beginning. Software suites offer the complete stack of cognitive data analysis as well, from data collection and integration to advanced cognitive analysis with data transformation and exploration features. These tools are often integrated into the cloud, allowing the use of open data.

One of the other major areas in which machine learning and other cognitive algorithms can be particularly relevant is cyber security.
IBM Watson is a particular example of how these different tools are applying machine learning concepts; it understands natural language and can be trained to solve problems specific to a given industry. After having trained Watson on what is called a data “training set,” it can then be asked to answer questions related to that field, or even predict new behavior given new input data. A major area of expertise here is oncology, where Watson is used to assist oncologists in making more informed treatment decisions. First, Watson is “trained” by uploading and analyzing structured and unstructured data in clinical notes and reports that assemble key patient information written in plain English. By combining data from patient files with external sources, like scientific articles, Watson is able to identify potential treatments. The doctor can then consider the treatment options provided by Watson when making decisions for individual patients.

2. Artificial Intelligence’s autonomy is limited; these technologies still rely on human action

AI algorithms are bound by the cognitive functions through which they are implemented. As there is currently not one instance of artificial intelligence that can fully imitate every cognitive function of a human being, AI architectures are unable to act without a human touch. The level of human involvement generally depends on what you wish to obtain from the machine. Prediction expression of an output variable given some input variables will differ in that sense, for instance, from correlation between variables, which in turn will require yet another level of involvement compared to other applications etc.

Machine learning illustrates these different levels of human involvement by dividing its algorithms into two groups: supervised and unsupervised learning. Let us illustrate the supervised learning approach with a classification problem: a retailer wants to determine if its clients are going to buy its newly released product, and does so by analyzing their age, behavior, and the products they previously bought from its catalog. The retailer can then use a suitable model for classification problems, like logistic regression, to predict whether its clients are going to buy the new product or not. The model is fed (“trained,” as it were) with data obtained from the first sales of the new product, yielding a predictive function aimed at describing whether or not a client will continue to be part of the future purchasers based on predictor variables like age, behavior, or bought products. Data generated from further sales can then be used to iterate on the resolution model to improve the prediction: this is why the machine is said to “learn”—it improves with experience. In the area of information management, the learning step is generally associated with an increase of the data set volume, enabling a more accurate resolution of the predictive system.

For unsupervised learning, on the other hand, humans only need to provide a set of variables, and the chosen algorithm will work on finding correlations between them, i.e., without being based on an initial “training set.”
A good example is the correlation of pixels in a numeric picture: application of neural network algorithms on the set of pixel intensities can be useful to determine the expression of some pixels as a function of the surrounding ones, which helps compress pictures by reducing the number of stored individual pixels.

Tools embedding natural language processing, like Watson, need to be trained as well. Watson can answer questions about a specific problem or area of interest, if you train it to do so. The first step is to define a training set of documents (HTML, PDFs, etc.) that will be fed into Watson, which must contain the answers to the expected questions specific to the use case. Then a question/answer management tool is needed to train the machine: for each question entered, an ideal answer to that question must be chosen. Each new question can either be matched to the answer of a previously answered question or can be provided with a full new answer. In that way, Watson will be able to answer the questions related to your specific business case in an increasingly better manner.

3. Implementation of cognitive technologies: taking the first steps

Depending on your specific needs as well as your existing infrastructure, AI can be implemented in multiple ways. Before any investments take place, a thorough understanding of your business’s specific needs is crucial to establish what kind of tool is necessary to activate the cognitive functions that can solve your problem. If your problem needs perception skills, your architecture will require a system incorporating image recognition or natural language processing. If you need to perform predictive analyses on large data sets, you might need a complete software suite handling data integration, transformation, and analysis. When you already have a data lake in place, chances are that you only need to integrate a predictive tool or that you can even develop your own machine learning algorithms based on code libraries. Evaluating your own application portfolio is a necessary step in efficiently integrating cognitive functions in your IT landscape. Cognitive intelligence indeed requires a high level of maturity in terms of enterprise data management practices and analytics capabilities. Considering the importance of human actions in the configuration process of cognitive machines, companies with a low level of information management maturity might run the risk of failing to effectively leverage these kinds of advanced analytics technologies. Indeed, insufficient knowledge, poor quality, or lack of proper integration of one’s own data in the target BI system will lead to inaccurate implementations of cognitive functions. Patterns detected through cognitive analysis might be wrongly influenced by unmanaged noise in the data, which could finally produce inappropriate predictions. Therefore, the implementation of Cognitive technologies might need a significant digital transformation of the enterprise to enable artificial functions to effectively and efficiently leverage massive data sets coming from almost fully automated processes (think for instance of robotics, or the Internet of Things). It is essential, then, that large amounts of data are handled through appropriate big data platforms—the hardware and software technologies of which are able to support cognitive computing capabilities.

One of the trends in which we have seen a real boom is bots used directly for customer service that are programmed to seem human.
Deloitte believes that when humans rely on their own experiences and knowledge, augmented by a stream of analytics-driven insights, the impact on value can be exponential. We have seen achievement of this impact as the rule, rather than exception, in insight-driven organizations.

Through the effective use of technology, including leading analytics technologies from IBM, Deloitte helps our clients become insight-driven organizations. Specifically, we help them ask the right questions first, and then apply advanced analytical and machine learning techniques to make their decision-making processes more efficient. Through Deloitte’s strategic alliance with IBM, we can provide capabilities spanning the range of “right questions,” from tactical to operational to strategic—all backed by IBM’s deep stack of analytics technology.

The following are just a few examples of our analytics teaming priorities:

- **Watson Analytics:** This cloud service combines the power of IBM’s Watson cognitive computing technology with Big Blue’s predictive analytics capabilities and puts them in the hands of business users. Watson Analytics provides a unified experience that brings together a complete set of self-service enterprise data and analytics capabilities in the cloud. Leveraging Watson Analytics as a shared common platform with clients, Deloitte can guide them in identifying their most valuable insights, predicting outcomes, visualizing results, and then creating reports or dashboards to share these new insights.

- **Sales Performance Management:** IBM Cognos ICM offers an enterprise application that leading organizations use to streamline compensation processes, reduce errors, meet compliance requirements, and drive improved sales performance. Organizations are able to design and manage highly complex compensation programs, including sales commissions, MBOs, and noncash rewards. Deloitte helps deliver on this solution, providing deep technical capabilities, a long history with Varicent, and the know-how to match technical solutions to the strategic goals of the enterprise.

- **Automated External Reporting (AER) for Finance:** Though companies have made significant investments in technology to improve their accounting and reporting processes, much of this effort has focused on improving the “close” and “consolidate” processes. In conjunction, the processes to prepare and submit financial statements and other external reports (i.e., statutory, tax, regulatory, and other) continue to be operationally inefficient and, in some cases, ineffective. AER is Deloitte’s approach to assisting companies in moving past these challenges, providing an efficient, sustainable and technology-enabled process to optimize external reporting and overcome operational inefficiencies while enabling financial analytics. And, Deloitte’s most significant AER reference is IBM Finance and Tax, who have been very successful in deploying AER, with Deloitte’s help.

Artificial Intelligence is a booming area revealing a growing interest from companies, fueled by the steady and frequent introduction of new use cases.

**Watson**

Deloitte was the only professional services organization selected for the inaugural IBM Watson Ecosystem Board of Advisors, which shapes the direction and strategy of the ecosystem by offering external views on the marketplace and potential opportunities for ecosystem partners. “We chose Deloitte because of its experience at the intersection of business and technology, its knowledge of the Watson product, and the value we’ve realized from our strategic and longstanding relationship,” says Mike Rhodin, SVP, IBM Watson Group. We were also pleased to have IBM Watson featured in Deloitte’s 2015 Global Report, acknowledging the broader impact our two companies can have when we work together.

Cognitive computing is emerging as a very real opportunity, as well as a threat, for many businesses. It is a component of the broader trend around big data, but it is particularly important because cognitive computing focuses on the realm of unstructured data, which is clearly dominant in volume over that of structured data. Given Deloitte and IBM’s already strong client and alliance relationship, our collaboration around Watson is a natural extension, enabled by the emergence of powerful cognitive computing and analytics technologies. Deloitte is proud to have been the first global systems integrator to join IBM in investing time, money, and people toward applying Watson technologies to solve business problems. Deloitte is also a member of the Watson Partner Program, giving us access to many resources, including the Watson Developer Cloud, which provides an expansive sandbox for our professionals to gain hands-on experience.

**Watson Health**

In April of 2014, IBM announced the Watson Health unit, which will provide patients, physicians, researchers, and insurers secure access to individualized insights and a more complete picture of the many factors that affect people’s health. Watson Health draws on IBM’s collaborative relationships with leaders across the healthcare ecosystem, and builds on IBM’s strengths in cognitive computing, analytics, security, and cloud, to improve the ability of doctors, researchers, and insurers to innovate by surfacing new insights from the massive amount of personal health data created daily. As the number one ranked Life Sciences & Healthcare consulting firm globally (based on both revenue and capabilities), Deloitte is embracing cognitive computing, and specifically IBM Watson Health’s offerings, as a potential path forward for our healthcare provider, health plan, and life sciences clients who are challenged with the rapidly shifting landscapes of their business environments.
Conclusion

• Cognitive intelligence refers to software programmed to augment human cognitive functions. These technologies are becoming better through machine learning and a continued human feedback throughout all interactions.

• Cognitive machines can be used to automate predictions and help make decisions or optimize operational processes.

• Certain artificial intelligence programs understand natural language and can provide an enhanced customer experience when responding directly to clients’ needs.

• Cognitive technologies are just beginning to emerge: underlying algorithms need a substantial configuration phase to work efficiently.

• Implementation of cognitive technologies depends on your specific needs, existing infrastructure, and IM maturity level. It could also hide future showstoppers to the launch of the offering.
Is there a best way to set up an efficient “robo advisory” solution within your IT application landscape?
The buzzword “robo adviser” is promising disruption in the wealth management industry, especially as the leading eleven pure robo advisers have seen explosive growth since their entry on the market. They further increased their total AUM by 11 percent over the first six months of 2015 to a total of US$21 billion after a ~65 percent growth from the previous eight months at the end of 2014.\(^2\) Even if these new market entrants are still nascent and represent a trivial amount relative to the US$25+ trillion retail investable assets in the United States,\(^3\) the top five robo advisory market actors in the United States already represent US$34 billion AUM in early 2016.\(^4\)

The fastest growing segment of the wealth management industry is now online and referred to as “robo adviser.” It is expected to grow Assets Under Management (AUM) by 2,500 percent until 2020 to reach a potential US$489 billion market.\(^1\)

The CIOs within investment firms (i.e., banks, asset managers, family offices, etc.) are in front of various dilemmas to implement innovative solutions for their internal clients while ensuring risk mitigation and a satisfying level of service.

The wealth management industry has been subject to increasing pressure over the past years, with an uncertain economic outlook, low-rate environment, and increased regulations. While compliance costs are raising the bar for new entrants, technological breakthroughs are lowering that bar and enabling market disruption.

In order to better understand the span of possibilities offered to CIOs for implementing a robo adviser, they first need to understand the current span of functions that robo advisers can cover across the wealth management value chain. Depending then on the current maturity level of the investment firm and its strategic objectives, several options will be offered to its CIO in order to set up a robo advisory solution. Obviously every option will have various impacts and bring new opportunities, as well as constraints in terms of integration with the existing applications landscape. Working with a simplified decision tree could help the CIO evaluate the relevance of every scenario based on several decision criteria, alongside the IT perspectives this trend is posing to incumbent actors in the wealth management industry.

---

**Pascal Martino**  
Partner  
Strategy, Regulatory & Corporate Finance  
Deloitte

**Patrick Laurent**  
Partner  
Technology & Enterprise Application Leader  
Deloitte

**Julien Schaffner**  
Director  
Operations Excellence & Human Capital  
Deloitte

**Mathieu Genty**  
Manager  
Technology & Enterprise Application  
Deloitte

---

---

**Figure 1. AUM Growth of eleven leading robo advisers (USD Billion)**\(^3\)
Robo advisers are offering automated management services at low or zero cost.

Robo advisers target the independent replication of many of the activities performed by wealth managers through online access, (supposedly) at lower cost. Technology made this possible through fast-growing online multi-channel tools accessible 24/7, and robo advisers take advantage of this situation to settle among the financial world and investment professionals.

They are providing access to financial information on demand and delivering added-value services anytime and anywhere. Robo advisers are offering automated management services at low or zero cost. Fees on AUM are reduced (but the spread remains significant, mostly between 0 percent and 0.85 percent) and Exchange-Traded Funds (ETFs) are widely used in order to reduce fees.

Robo advisory covers a wide range of financial FinTechs
The core model of the “robo adviser galaxy” can be attributed to the use of algorithms based on the traditional Modern Portfolio Theory (MPT), financial analysis, and analytics to develop automated portfolio allocation and investment recommendations tailored to the individual client.

Another fast-growing B2C robo adviser segment is the “hybrid adviser,” combining robot and human advice. The recipe for asset allocation remains the same: extensive use of ETFs to benefit from low fees and diversification.

The scope of robo advisers tends to also encompass social trading platforms, algorithmic trading solutions, and data analytics players, with a variety of brand new solutions following the hype for automated forms of investment advice.

B2B platform solution providers represent the third main segment of this new galaxy of FinTechs. Further developing their model, some actors have extended their B2C solution of automated investment advice and discretionary asset management with B2B platform solutions for professional actors, whether they are banking institutions or independent financial advisers. Other providers only offer white-labelled automated advice and investment management solutions as a service for financial institutions. These toolkits enable professional players to launch a digital wealth platform for their own end-user investors.

B2B platforms are providing integrated online wealth management plug-and-play solutions enabling the offer of standard robo advisory features with automated digital workflows (e.g., four-eyes principle), investment recommendations, as well as an electronic signature. Patterns configuration according to the philosophy of the financial adviser may also be provided, or a module selection for the D2C interface.
Robo advisory services are continuously evolving

Process of Robo Advisory

- Knowing customer needs
- Processing customer information
- Customized solution in matter of seconds
Setting up a robo advisory solution within the landscape applications of the IT department should theoretically reduce the existing cost base for providing discretionary services to mass affluent customer segments. The challenge is important for IT departments as many different technical options are available to do this, but all of them will offer various levels of agility and involve some benefits and disadvantages that CIOs need to take into consideration.

Selecting the right business model according to the enterprise and digital strategy is the first step in any technical implementation. Indeed the business must decide which model they want to implement and for which client segment. The difference may be large between a technology assisted adviser and fully automated investment services from the client onboarding.

Technology-assisted advisers use technology to facilitate the acquisition and onboarding of new clients, but all investment management decisions are performed manually, and a human adviser remains the primary owner of the process. Examples of such services can be found at Personal Capital and Vanguard Personal Adviser Services, which usually invoice those services below one percent of the AUM depending on the invested amount. These services are usually targeted at Baby Boomers whose preference is to keep a human adviser.

Automated investment services acquire and manage clients’ portfolios entirely through software. Examples include Wealthfront and Betterment. Each automated investment service has a different fee model, but they are usually less expensive than technology assisted advisers due to the avoidance of any manual work. Their investment management services also tend to improve at a much faster rate than the alternatives because unlike manual services, software constantly improves. These services are usually targeted at Millennials and younger generations, looking for simple solutions, available 24/7 and at lower costs.

As soon as the CIO has a better idea on the key strategic objectives, the current capability and maturity, as well as the type of solution needed, he or she can envisage three main scenarios.

**Scenario 1: The IT department can build its own robo adviser internally**

by developing an in-house robo advisory solution to leverage internal expertise, architecture, and resources. Most of the algorithms used by robo advisory are publicly known functions and rules that are possible for anyone to leverage. Moreover this will enable the organization to remain the owner of main data (E.g., client data, strategic asset allocation, and model portfolios of the bank); the robo advisory solution will thus be easier to integrate within the IT landscape of the bank using the data flows that are already in place. It will be easier as well in terms of regulatory and compliance aspects, as everything is internally managed. This will also challenge the IT department, since the implementation of robo advisory solutions requires specific skills that could be scarce within the IT organization. It could therefore represent additional costs; external support or specific recruitment could be required to provide ad hoc expertise such as:

- Big Data and predictive analytics to collect and analyze all the relevant information concerning clients to advise, market movements, and all the information coming from different channels to be automatically integrated
- Cybersecurity to setup and monitor all the flows of data and the access rights, and protect the robo adviser from cyber threats

- User experience and user interface to design the look, feel, and functionalities of the homemade robo adviser, in line with most disruptive FinTechs
- Mathematics to enable modelization of the advice model based on clients’ age, tolerance for volatility, investment goals (e.g., capital appreciation vs. recurring income), investment time horizon, etc.
Creating your own robo adviser will also add complexities to the maintenance of the IT landscape. The robots should support clients in multiple time zones, which means no service disruption at all. This will involve large and complex deployments and a new culture of release management because of the significant dependencies that the robo adviser will have with all the other applications. The robo adviser is the front end proposed to the client but it is highly depending on the quality of the information provided, and managed in a correct way, to feed it.

Scenario 2: Partner with a robo advisory FinTech by acquiring a B2B white-labelled solution, at a fair price and offering growth potential in relation with the firm strategy and IT/digital roadmap. Going this way would be the fastest and easiest solution in order to set up an advisory solution, no matter the current level of maturity of the IT application landscape. It could also enable the service of a new fringe of customers at a lower cost and meet a strategic objective of revenue growth through client segment diversification. This would reduce the need for the IT department to acquire the majorities of the skills needed to develop a best-of-breed solution, which will definitely improve the time to market and minimize the hiring costs.

In terms of attention points, we can identify four main areas:

1. The integration part with internal IT systems and the dependency it creates toward an external provider. FinTechs’ main advantage should remain their agility to adapt to new trends and meet new requirements in a timely manner, ensuring constant innovation and improved customer experience. The CIO will therefore have to consider the SLA and level of insourcing he would like to ensure in order to remain agile and independent. A preference could be given to open source solutions or APIs that will enable the acquisition of sufficient internal knowledge. The CIO also needs to be careful with a partnership with a robo advisory FinTech as there are points to take into consideration like unclear contractual issues, changing requirements or unforeseen charges, and a dependency on the external provider, which could reduce flexibility.

2. There will also be some difficulties in terms of consistency of data and which referential to use. The FinTech solutions will likely come with a limited scope of investment products that could not be aligned to the internal financial instrument referential. Those discrepancies could lead to difficulties in case the client may perceive data discrepancies using two distinct services from the investment firm. Aligning all data across the systems could represent a high effort. A solution could be to limit the robo advisory offer as a unique offer to clients (e.g., mass affluent).

3. From a regulatory perspective, depending on the FinTech origin and market deployment, some of the processes and functionalities required to cope with local regulations could be weak or missing. It will be important to consider:
   - The global and local regulation compliance
   - The existing implementation in countries that are within your scope
   - Compatibility with the firm’s internal processes
   - The responsibility and ownership against the regulation obligations (provision of financial advice, portfolio reporting)

4. Lastly, the security aspect cannot be neglected, especially regarding confidentiality of data, but also on malware that could affect client portfolio management. For private banks, and depending on their countries, it might always be an issue to send client data to a third party that will use them to automate advisory processes, but also host them on a server physically located outside of the bank or abroad. The same applies to the protection of the firm’s IP.

Selecting the right business model according to the enterprise and digital strategy is the first step in any technical implementation.
Investment firms often ignore the fact that they already have the capability to propose a robo advisory service by leveraging existing systems and assembling disparate processes into a consistent end-to-end process.

Scenario 3: Leveraging on current applications
Investment firms often ignore the fact that they already have the capability to propose a robo advisory service by leveraging existing systems and assembling disparate processes into a consistent end-to-end process. Robo advisory is nothing more than a marketing name to describe the objective every CIO/COO has had in mind for several decades: a fully automated and paperless STP (straight-through processing) process.

As an existing investment manager, it is likely that a portfolio management system is already in place in the current architecture of the bank and that KYC and investment profiles are being digitized. Moreover, a lot of data is available in the various data marts and at your market data providers to better understand the next moves on the market and the most appealing products to your clients. Robo advisory is about assembling together all those capabilities to support a new offering in a fully automated and digitized way.

The advantages are numerous:

- The required skills will mostly be available within the organization
- The products and processes are already mature
- It should not lead to additional expensive investments in new technology and licenses

Of course it will bring some constraints as well:

- The time to market and agility will not be as good as a pure player solution
- The offering could not be that distinctive to clients in terms of user experience
- The running costs will remain high since the solution will rely on existing architecture
- The software vendors might invoice some “new” functionality of existing systems because they will be robo-branded
Key opportunities and challenges for IT

Every scenario is bringing a set of advantages as well as constraints

<table>
<thead>
<tr>
<th>Scenario</th>
<th>NEW</th>
<th>FINTECH</th>
<th>LEVERAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human resources</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
<tr>
<td>Time to market</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
<tr>
<td>Regulatory risk</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
<tr>
<td>Effort</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
<tr>
<td>TCO</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
<tr>
<td>Integration complexity</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
<tr>
<td>Security/privacy constraints</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
<td>⭐⭐⭐⭐</td>
</tr>
</tbody>
</table>

- The type of costs and level of required investment could be from 1 to 100, depending on the selected solution. Buying a FinTech white-labelled application will create annual license and maintenance costs per user, but with reduced implementation costs compared to creating your own home made solution, which will imply a lot of investments for implementation (project and integration costs, consultancy fees, talent acquisition effort, loss of opportunities to work on other initiatives aiming at cost reduction/efficiency gain) but also for its maintenance (skills, 24/7 online infrastructure).
- The location of the infrastructure for BPO (business process outsourcing) or ITO (information technology outsourcing), needs to be thoroughly analyzed. Indeed the target setup of the infrastructure dedicated to the new robo adviser solution, i.e., whether it would be hosted internally or externally, will have huge impacts on the costs, security, flexibility, and the future developments of the robo adviser. If the robo adviser is hosted externally, it will need to access specific data (client information, portfolio models, asset allocation models, investment politics, etc.). The same type of issues should be considered when implementing a solution internally, but with an objective to make it available in several locations.
- Cybersecurity/privacy concern regarding data, especially client-related, for BPO/ITO, is one of the key challenges of the robo advisers. The applications need to be fed with a lot of information on client profiles in order to wisely advise the customers. For external solutions, this means sending some very private client information outside of the bank with the associated risks. This must be carefully managed and designed, also considering the respective local regulations of the investment firm and the hosting infrastructure.
- Using providers as brokers or third parties is an important point to analyze when using a robo adviser on the market. Using a solution on the market involves a dependency on third parties. What if the bank wants to trade with a specific broker not yet available with the solution? This constraint will become less prominent, given the enforcement of regulation rules regarding inducements.
- Flows (data or transactional) between the external robo adviser and the bank could become a nightmare in terms of volume of data. In order to manage this, the bank will have to create/modify a data warehouse that stores the information needed by the external FinTech, but with the constraint of high availability and near-to real-time accuracy.

Given all of those challenges and opportunities, the CIO will have to opt for the most relevant solution in his or her context.
Illustrative decision tree based on two single strategic drivers

<table>
<thead>
<tr>
<th>KEY STRATEGIC DRIVER</th>
<th>Maturity of existing advisory processes</th>
<th>Level of automation</th>
<th>Availability of knowledge and skills</th>
<th>DECISION CRITERIA (SAMPLE)</th>
<th>RELEVANCE OF SCENARIO</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Option 1</td>
<td>Option 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>New</td>
<td>Fintech</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>TIME TO MARKET</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>OR</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>EFFICIENCY GAINS</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Sources:
3. Deloitte analysis
4. Deloitte analysis
5. Deloitte analysis
6. Deloitte analysis
7. The Economist Intelligence Unit, report Retail Banking: “In Tech We Trust”, 2016
Conclusion

• Robo adviser solutions offer various levels of functionality, enabling the digitalization and automation of client onboarding, investor risk profiling, and investment allocation through an algorithm-based assessment, providing online investors with proactive and on-demand access to financial advice.

• Incumbent actors may take advantage of the ongoing market consolidation to integrate robo advisory services into their offering and technologies, but it also brings some risks related to the variable pricing model and moving regulations.

• Big data analytics providers may further disrupt the offering through ad hoc automated advice that answers specific investment needs or questioning. Major players from both finance and Big Data are funding such B2B solutions designed for global banks and hedge funds.

Considering the low maturity of the market and those threats and opportunities, the CIO will be facing a difficult choice when asked to propose a technology solution that enables the marketing of a robo advisory offering.

The first prerequisite will be to validate the key strategic objectives of the firm, which the new offer must reach since it will highly influence the scoring of the various options available. There will be a low chance that implementing a brand new solution internally will be a satisfying option in the case that the investment firm’s primary objective is to rapidly propose a new service on the market.

The CIO will then have to assess the current maturity of the related processes and the availability of required knowledge. More importantly, the CIO will have to avoid a common pitfall to go for the fastest (in appearance) solution, such as plugging an existing white-labelled solution on the information system architecture. It could also hide future showstoppers to the launch of the offering.

The successful CIOs will therefore be the ones who are:
1. Clear about their objectives
2. Realistic about their capabilities
3. Aware of technical complexities and regulation constraints
Let’s meet Pepper
Banking Services of the Future!

What is Pepper? Entirely mobile banking, without branches and 100 percent free - no checking account fees. Pepper aims to challenge the status quo of banking and create a different and progressive experience. Based on innovative technology capabilities, it provides smart banking using valuable insights that keep customers informed and helps them to better control and manage their financials.
Bank Leumi Le’Israel is a leading universal bank. The goal of the bank is to be a leader in banking technology innovation in order to deal with the major challenge that financial institutions are facing today – **How to respond to changing customer expectations in the digital age?**

One of the main initiatives toward the digital landscape was the decision to establish Pepper as part of Leumi Group in order to lead the banking services of the future. Since Leumi core systems are old and complex MF systems that don’t fit the agile approach of digital banking, Leumi has decided to implement T24 platform by Temenos. Project partners, in addition to Leumi and Temenos, are Deloitte (with participants from Deloitte Israel, Luxembourg, and Poland) and Matrix.

**Why establish Pepper?**

**Changing customer expectations** in the digital age are forcing banks to respond. Customers are expecting a more intimate relationship with their bank and require a unique and compelling experience. They are expecting more flexibility and interactivity through digital platforms. Expectations are shifting to instant, 24/7 contact through digital channels, which includes more personalized products and services as well as real-time insights (such as unusual account activity). Customers are expecting that their needs will be anticipated—quickly.

**New entrants, new threats** - New business models that leverage technology to meet evolving client needs are emerging. Venture capitalists, large internet companies, and others are backing a rapidly growing set of startups that can compete with corporate banks. It is predicted that finance will be the most disrupted industry in the next 10 years!

In a world of increasing competition, banks are forced to be more creative in ways to recruit digital clients and prevent client abandonment. Using digital tools will enhance relationship management by offering insights that will build trust in recommendations. Currently, without significant adoption of digitalization, banks will lose customers.

Banks must **become more agile** in order to achieve the required flexibility and capability to put in place new products and services in a timely manner. Banks need to accelerate time-to-market using pre-built financial services knowledge and the reuse of existing content.

Finally, in order to increase **productivity and profits**, banks should significantly reduce operational costs. Digital tools, combined with innovative technology, brings not only customer service advancements but also empowerment—which in turn means lower operational support requirements for banks, such as reduction in call volume and reduction in chat sessions. Rather than providing generic, one-size-fits-all answers, insights based on the customer’s personal situation are presenting customers with self-service advice that is most accurate and relevant in the context of their banking relationships.

It shouldn’t surprise us to notice a correlation between project objectives and the 2015 Global CIO Survey. For example:

- In the survey, the top three business objectives were performance (driving operational performance), customers (attracting and retaining customers), and cost (reducing operational or product costs)
- Focusing only on the financial services industry, innovation was identified as a top business priority
- When asked which technologies will have a significant impact on the business within two years, CIOs unsurprisingly named analytics, business intelligence, and digital

**What were the main concerns and challenges?**

A major challenge was becoming **more agile** in order to support a quick reaction to market opportunities as well as quick deployment. Since the legacy core system lacks the ability to integrate changes within a short time frame and at reasonable cost, it was decided not to use Leumi bank MF but to implement Temenos’ T24 solution.

**Regulation was one of the project main concerns.** The complex and increasing Israeli regulation requirements have defined a major gap between T24 off-the-shelf capabilities and the required solution for Pepper services and architecture. Since our goal was to maintain as minimum developments as possible, this challenge was even more complex.

“Now more than ever, customers—especially the millennials—aren’t willing to accept the age-old banking experience. They expect a radically different kind of banking.”

Lilach Bar David, Pepper CEO
What were Deloitte’s Responsibilities?
Based upon Deloitte’s deep understanding of the local financial market, complex regulation requirements, digital worldwide trends, global knowledge, as well as benchmark capabilities, Deloitte provided substantial added value to the project by supporting and allowing a detailed and comprehensive analysis process to meet project goals in the best possible way.

Initiation & Pre-Analysis
- Identify relevant regulations that affect the scope
- Identify high-level gaps between regulation requirements and vanilla processes in scope
- Prepare a work plan to cover relevant aspects of business requirements

Analysis
- Identify and document list of gaps and prioritization
- Design To-Be processes
- Define business requirements document
- Lead scope control board

Design
- Define Functional Specification document (FSD)
- Provide guidance in aspects related to business requirement and regulation

Build Support
- Support build of the solution and interfaces
- Provide guidance in aspects related to business requirements and regulation for Temenos team responsible for building the solution and interfaces

Sources:
1. http://www.pepper.co.il/
It is predicted that finance will be the most disrupted industry in the next 10 years.

Tests
• Support test scenarios based on the use cases that were defined in the BRDs, and the test cases defined in the FSDs

Deployment
• Supporting following implementation steps in regulatory and business requirement aspects

Ongoing Project Management
• Provide Insights to project management from Deloitte experience with aspects such as governance, scope management, change management, etc.

Conclusion
• Only through core system transformation can banks achieve the necessary breakthrough to operate efficiently and compete effectively.
• The benefits of digital solutions for corporates are enormous, offering convenience, control, improved liquidity management, cost savings, and ultimately profit. These benefits stimulate transaction growth, directly feeding the bank’s bottom line.
• Banks are facing a challenging time ahead—customer’s needs are moving to a digital landscape while new technology companies offer “traditional” banking solutions to end customers without being a bank.
• Banks have to look at technology, product, and customer behavior changes through a prism of being more mobile, more social, more analytical, and taking a more diversified view on what customers are expecting the bank to deliver.
• Banks need to embrace new innovative technologies, while mitigating the gap between the technology companies’ technical language and banks’ business needs.
• It is predicted that:
  – By 2020 at least 66 percent of the global population will be online; that means an additional 3 billion global consumers!
  – In 2025 the biggest banks in the world will be technology companies.
• Innovation and Digital Capabilities are with no doubt building blocks for success, Digital services are more than differentiators, they are essential to service delivery.
Part 02

From a core transformation/technology perspective
PROCESS AUTOMATION FOR THE FINANCIAL INDUSTRY

A virtual workforce increasing capacity and improving efficiency

We have seen it in movies, we have read fantastical futuristic fiction about it, and now it is upon us: Robots performing human tasks.

The future posed by film creators and novelists is still a bit further away, but the technological advancements that could make it possible are coming. We have already seen robots in factories for years, mimicking human arms and legs, but now we are on the verge of seeing robots that replicate the human brain. Just like their physical cousins transformed manufacturing, these “virtual” robots are likely to change the way we run our business processes. Robot-led automation has the potential to change today’s workplace as dramatically as the machines of the Industrial Revolution changed the factory floor.
Why Automate?
Organizations—financial industry players in particular—are facing significant internal challenges and external industry and consumer changes. To survive, they must focus their efforts on creating value for their customer; focusing very often means investing. They have no choice but to optimize their cost side and hunt for any efficiency waste. Financial institutions must take at least three dimensions into account that have an impact on their business:

- **The economic dimension**: Client expectations are more demanding while the competition is stronger. That leads institutions to face cost challenges.

- **The strategic dimension**: Institutions have ambitions to grow, but usually face difficulties to take regulatory changes, consumer trends, and technology trends into account.

- **The operation dimension**: Institutions want a fully scalable, nimble, low-cost operating model.

Several business processes are not as intelligent as they could be. Some of them cut across many IT systems that do not always talk to each other; others are just too time consuming. Running them smarter is nonetheless an expensive proposition—it either involves a massive IT transformation such as a core system transformation (CST) or extensive business process improvement efforts.

Other organizations decide to rely on third parties to improve process execution through business process outsourcing (BPO) and offshoring. All of these initiatives are usually complex, require time and substantial investments, and have a fair amount of risk.

Most industries, including the financial industry, are now realizing that another alternative based on robot-led automation could be the solution. Tools classified as “Robotics Process Automation” (RPA) have been maturing quietly over the last decade to the point where they are now used for enterprise-scale deployments, very quickly and at very low cost. They can address the issues of many financial institutions, recognizing that some of their processes are inefficient—most of them relying on manual workarounds, poor operating controls, high operating cost, and complex business and IT states.

**What is RPA?**
Robotics Process Automation is a way to automate repetitive and often rules-based processes. These transactional processes are typically located within a shared services center or another part of the back office.

We are not talking about mechanical droids; RPA is purely software-based. Such software, commonly known as a “robot,” is used to capture and interpret existing IT applications to enable transaction processing, data manipulation, and communication across multiple IT systems. Multiple robots can be seen as a virtual workforce—a back-office processing center—but without the human resources. The robots undertake processes just like their human counterparts, and can work on multiple processes, just like a shared services staff member can learn to work on an accounts payable process and a travel and expenses process. The robots use a virtual machine and dedicated logins to interact with different applications and systems in the same way as human teams.

Robotics Process Automation is a way to automate repetitive and often rules-based processes.
What are the benefits?
The business benefits of RPA are undeniable—robotics help to eliminate, simplify, standardize, and automate. Implementing robotics provides an opportunity to improve profit by reducing errors, avoiding costly offshoring, and obtaining quick results within weeks. In most financial institutions today, there are many routine processes performed manually that lack automation through IT transformation, and for which macros and other automation tools are too limited to effectively address. Robotics can address this gap by helping companies to automate business processes quickly and cost effectively without the need to create, replace, or further the development of expensive platforms.

Finance and accounting is a back-office function that is a perfect fit for RPA, as many of the processes are rules-based and can be easily optimized by a robotic workforce.

RPA solutions also support companies to achieve operational excellence by improving processes, and to better respond to changing business practices on the long term. It will allow financial institutions to re-define the way they think about administering business processes, IT support processes, workflow processes, remote infrastructure, and back-office work. In doing so, RPA provides dramatic improvements in accuracy and cycle time and increased productivity in transaction processing, while elevating the nature of work by removing people from repetitive tasks.

Here is a sample of benefits experienced by organizations using RPA solutions:

**OPERATIONAL EFFICIENCY**
Software robots are designed to perform tasks faster than a person can.

**COST EFFECTIVE**
The cost of a robot software represents one ninth of a full-time employee in an onshore location such as Luxembourg. Overhead and fixed costs associated with housing and employing a person are reduced when replaced by robots.

**ACCURACY**
Robots are programmed to follow rules, so their productivity is higher while error rates are minimal, reducing risk and increasing customer satisfaction.

**RISK MITIGATION**
Because RPA technology tracks and monitors all the tasks that it automates, it also helps companies to become more audit and regulatory compliant.

**FLEXIBILITY AND SCALABILITY**
Robots are scalable and easy to switch on and off. They can work through the night, weekends, and holidays, offering maximum flexibility to cover peak periods such as month-end.
Hype or reality?
Despite the hype that has been built on the marketing aspects of RPA tools, there is a strong market need for them. Many global financial institutions, global business services (GBS), and offshore service providers are focusing their attention on automation, fueling this fast-paced industry. The innovations put forward aim at matching the strategic needs for efficiency and fast change.

In Deloitte’s 2015 Global Shared Services Survey, robotic automation was the most prioritized technology for shared services and GBS leaders, ranking higher than implementing analytical software and cloud computing. For them, both continuous improvement and increasing the level of automation are key strategic priorities, and they will remain highly desirable for the next ten years.

It is interesting to note that despite the attention on the topic, the current industry adoption level of robotics is low. As the new RPA model starts to progressively yield good results, the need for automatization will become more evident.

The next step in the evolution of automation is to offer end-to-end integration for supporting businesses with different tools and services. It could combine speech recognition, optical recognition, and other cognitive tools with rule-based steps to provide customers a way to save effort and expenses of integrating different tools. The added value potential of RPA as we see it today is already quite substantial, and offers leaders a new way to achieve excellence with a quick return on investment.

Robotic Process Automation is a catalyst for business process transformation and innovation. Although RPA technologies are still evolving, they are already quite mature. They offer companies a good alternative to core transformation and outsourcing and provide an effective way to lower operating costs and decrease cycle times while increasing employee productivity and accuracy.

Automatization is an upward trend from which a steady growth is expected, both in terms of functionality development and in market implementation over the next years. The evolution of the technology combined with new business examples create high expectations for many more financial industry players to quickly implement these tools.

The next step in the evolution of automation is to offer end-to-end integration for supporting businesses with different tools and services.
From the hype to the concept with PoCs
Introduction
Blockchain and Distributed Ledger Technologies (DLT) are bringing disintermediation to nearly all industries. A survey from Greenwich Associates highlights that financial and technology firms are expected to invest more than US$1 billion to bring blockchain technology to capital markets in 2016. According to the World Economic Forum, financial services will be transformed by this technology, with the expectation that at least 10 percent of the global GDP will be stored on blockchain platforms by 2025.

DLT can be defined as a database that can be shared across the network. Underlying this technology is blockchain that consists in a decentralized ledger that operates in a transparent environment.

With the increase of investments around blockchain and DLT, the hype continues to grow as several initiatives, startups, and technological platforms continue to blossom. However, it is still a nascent technology with limited feedback and lessons learned, making it difficult to know how to develop and take full advantage of this technology.

In this context, in order to explore the capabilities of DLT and demonstrate the economic viability of concrete use cases, Deloitte has launched various initiatives worldwide ranging from forming alliances with startups to the setup of development labs.

The aim is also to acquire internal competencies so that Deloitte can support clients in building and integrating custom solutions based on different technological platforms and partners. Several platforms, technologies, protocols, and methods are available for blockchain development and the choice of a particular solution is highly dependent on the business objective.

Three of them are presented in the following sections:

- **Cross-currencies payment rail using Temenos and Ripple.**
- **ArtTracktive** to track art pieces on Ethereum.
- **AirMes** to enable transaction regulatory reporting on Ethereum in the context of EMIR, MiFIR, and SFTC regulations.

**Temenos-Ripple integration**
In the context of cross-currency settlements, there is a need to reduce the time of international transfers usually performed through SWIFT protocols. The Temenos-Ripple PoC, co-developed by Deloitte and Bluzelle, consists of the integration of Ripple into Temenos’s Core Banking Systems with the objective to enable financial institutions to send payments, either in local or foreign currency, in real time without relying on intermediary banking relationships.

To conduct this PoC, a Hybrid Agile methodology structured around quick runs has been followed. The developed solution enables cross-currency payments to be routed to Ripple and allow the execution of an international payment in six seconds. This immediacy ensures that the best possible exchange rate is used for the transaction. The benefits for banks are to obtain higher exchange rate margins and considerably reduce the costs for using the SWIFT network. The solution also improves the user experience, since international payments are executed almost instantaneously.

By developing this PoC in only 8 weeks, it has been proven that blockchain integration can be quickly implemented from design to production.
A survey from Greenwich Associates highlights that financial and technology firms are expected to invest more than US$1 billion to bring blockchain technology to capital markets in 2016.

ArtTracktive: solving the traceability issues in art

The ArtTracktive PoC shows how the key challenges faced by the art industry—namely the traceability of information, the trust of counterparties, and the transparency of transactions—can be addressed by using a distributed ledger for tracking the origin and the journey of works of art. Today the traceability of work of art is inefficient, inconsistent, time-costly and mostly paper-based.

ArtTracktive proposes a platform to solve traceability issues in art by recording interactions between all parties involved on a blockchain in processes such as lending and selling.
Parties interact with the blockchain through a web application in order to record their actions from the introduction of the piece of art, its certification, and the notification of sell/lend, all the way to the shipping and customs clearing.

The main lessons learned from this PoC are around the development of Smart Contracts. For example, the specialization of Smart Contracts with minimum data (fit-for-purpose) is important, due to the cost associated with the storing of fields—which can become very expensive on Ethereum. It has also been required to implement a specific trace-back chaining mechanism to ensure an effective technical tracking of transactions that is not native in Ethereum, as opposed to Bitcoin.

**Transaction Regulatory Reporting with AirMes**

The AirMes PoC provides an answer to recent regulations that enforce the need for a timely reporting on post-trade transactions. EMIR, MiFIR, FSTC, and others involve challenges in terms of data quality, data reconciliation, timing, and cost that a blockchain can address thanks to its immutable shared ledger of pre-reconciled transaction reports.

In this concept, the first counterparty loads reporting information to the application, where the smart contract performs data quality checks and automatically validates transactions. Occasionally, a data quality operator may propose adjustments to correct irregular input data before the validation.

Once transaction reports are validated and signed by the first counterparty, the second counterparty receives the reporting information for confirmation and sign-off. At this point, the Unique Trade Identifier (UTI) required by the regulator is generated and stored onto the blockchain. Reporting information is finally sent to the trade repository, which can approve or reject it based on a predefined set of criteria such as the appropriate format. One of the main strengths of the process is that it can be supervised in real time by the regulator, enabling real-time analytics to detect fraudulent activities, exceptions, and more.
Transaction Regulatory Reporting process based on blockchain will be faster and more efficient
This PoC has been developed following an agile methodology with three sprints of two weeks. In order to enable the modification of reporting data, two smart contracts are activated within this PoC: the proof-of-process, which contains the hash of the reporting data and can be modified; and the actual reporting smart contract, which contains the hash of the reporting data only when A and B agree on common data (final hash) as well as the UTI.

One of the main challenges faced during the development is related to the implementation of asynchronous business validation of the data. The design of the state machine is a critical activity that must be performed by a cross-functional team with subject matter experts, software developers, and end-user interface (UX) designers.

Another lesson learned is that, even if it has not been demonstrated in this PoC, the trade repository could also be disintermediated, if the law allows it, as the solution itself provides data quality control and immutable transaction reports storage.

It has also been learned that data interface and API specification standards is key to enable industrialized deployment of this solution, especially if the insertion of the data on the DLT is made online by different participants. This is not only a question of type of data (dates, integer, decimal, etc.), but also a question of format and cross-field business rule controls.

Without it, it will be very difficult to enable streamlined system-to-system integration and asynchronous business validation of data or transactions.

Conclusion

Deloitte has learned a lot about various aspects of blockchain technology by developing these proofs-of-concept in a startup spirit:

- Technological: deep understanding and technical expertise on the use of blockchain platforms, their pitfalls and strengths
- Methodological: setup of agile organization and processes that can deliver Minimum Viable Products (MVPs) within a few sprints of two to three weeks
- Organizational: the added value of cross-functional teams involving business experts, software developers, and UX designers, who explore together how to leverage the technology to enable disruptive business and operating models in a digital world
- Marketing and communication: the importance of timely and targeted marketing and communication in a context and an environment where lot of players are struggling to gain a strong position on a promising technology; more than pieces of eminence like white papers, various practical PoCs prove one’s hands-on expertise on the topic, and generates a lot of attention and interest from existing market players and new entrants such as Fintechs, RegTechs and other startups

Deloitte Luxembourg has the ambition to continue developing those proofs-of-concept—not only on its own and by contributing to the recently launched Deloitte EMEA Grid Blockchain Lab, but also, and preferably, by working with market players and ad-hoc communities. Objectives are manifold: demonstrate use cases and their potential for disruption and disintermediation; test DLT platforms; assess startups and how they can work with incumbents; grow functional, technological, and technical expertise; and generate new exciting opportunities and projects.
Part 03

From a risk and cyber perspective
An exponentially growing cyber threat

Nowadays, organizations are in a race to improve the state of their cyber risk programs and the maturity of their security capabilities. Meanwhile, cybercriminals are continuously advancing their methods of generating revenue. One such threat that is growing exponentially is ransomware.

Stéphane Hurtaud
Partner
Governance, Risk & Compliance
Deloitte

Maxime Verac
Senior Manager
Governance, Risk & Compliance
Deloitte

Yasser Aboukir
Senior Consultant
Governance, Risk & Compliance
Deloitte
Ransom-what?
Many companies have already heard about Locky, TeslaCrypt, CTB-Locker, and other ransomware that have been in the headlines during the last months. Ransomware is a type of malicious software that restricts or limits users of a targeted organization from accessing their IT systems (servers, workstations, mobile devices, etc.) or their data, until a ransom is paid. There are two types of ransomware:

- **Crypto Ransomware**: Targets the data and file systems on the device itself, so the computer is functional except the ability to access the encrypted files
- **Locker Ransomware**: Prevents the victim from using the system by locking components or all of the system

A typical method of infection is an email containing a malicious attachment that will download the ransomware. Users may encounter this threat through a variety of means, but ransomware is often distributed as attachments to a series of phishing campaigns. Ransomware can also be downloaded by unwitting users who visit malicious or compromised websites, or it can arrive as a payload, dropped or downloaded by other malware. The most prevalent versions of the malware are TeslaCrypt and Locky, which encrypt files on a computer’s hard drive and any external/shared drives, then direct to a payment page that requests a ransom amount.

Ransomware can harm an organization’s reputation, especially if intellectual property or other relevant information is compromised. It can also affect an organization financially, especially if the business activities are disrupted and the ransom amount is paid.

**Source**: Symantec 2014-2015 Ransomware Detection

**Crypto Ransomware**
64%

**Locker Ransomware**
36%
Who are the victims?
The threat agents behind ransomware are continuously evolving, and have become more focused and selective when launching their ransomware attack campaigns. Initially, ransomware attacks have been non-targeted, i.e., they mostly spread through large email phishing campaigns and demanded small payments (~1-5 Bitcoins) from individual users. However, threat actors have evolved to target specific organizations instead, hoping to land a bigger payday. Consumers are still the most likely victims of ransomware (accounting for 57 percent of all infections between January 2015 and April 2016), but realizing the potential for higher profits, cybercriminals are increasingly targeting the business space with organizations.

New ransomware knows where you live: Threat agents are now taking geographical location into account when targeting victims, especially to focus on wealthier countries, likely because victims in those countries are more able or willing to pay (as illustrated in Figure 2, the vast majority of infections occur in the USA and Europe). Another objective with those geo-targeted ransomware is to develop elaborate attacks integrating local specificities (local language, local currency, etc.) and to spoof local institutions like the regional postal service or law enforcement agency, luring the targeted organization to open the attachment and download the ransomware.

In Luxembourg, the Computer Incident Response Center Luxembourg (CIRCL) receives four to five reports of ransomware infections per week. CIRCL has stated, based on its operating Malware Information Sharing Platform (MISP), that Locky and TeslaCrypt ransomware are the evolving ransomware varieties targeting the Grand Duchy right now.

1 Symantec - Ransomware and Businesses 2016
2 In May 2016, the developers of TeslaCrypt released the master decryption key and shut down the ransomware, thus ending the ransomware
A very attractive business model

Ransomware is considered to be a major and exponentially growing threat in 2016, based increasingly on anonymizing payment methods (e.g., Bitcoin digital currency) and anonymous networks (e.g., Tor anonymity network).³ The Cyber Threat Alliance estimates that the group behind the CryptoWall ransomware attacks caused US$325 million in damages, after infecting hundreds of thousands of computers across the world.⁴

The popularity of ransomware attack is growing continuously. The FBI has reported a 33 percent increase in the number of complaints filed involving ransomware.⁵

- In 2014, over 1,800 complaints were filed
- In 2015, more than 2,400 complaints were filed, with a reported loss of more than US$24 million
- In the first quarter of 2016, US$209 million was paid to ransomware criminals

The popularity of ransomware among cybercriminals can be attributed to three main advantages:

- It is a low-maintenance operation for threat actors, and tools have become more advanced and much cheaper.
- It provides the opportunity to target on a wide scale, allowing a higher return on investment.
- It offers a quick path to monetization, since the users pay adversaries directly in cryptocurrencies. Furthermore, the relatively low initial ransom cost (if compared to the high value of victim's data) complemented by the gradual increase scheme (the sooner you pay, the cheaper it is), is a strong incentive for victims to pay the ransom.

In other words, the return on investment is faster than with most types of malware because there is no middleman involved, and there is no need to resell anything such as personal data; it's a cash deal only. The simplicity of the business model is a compelling attraction for the criminal elements.

---

As illustrated in Figure 2 above, the initial step in a ransomware attack is to deliver the ransomware—or in other words, infecting the victim. The most common delivery methods are:

- **Phishing:** Nearly all phishing emails now contain ransomware. Phishing consists of a fraudulent email that appears to be from an official source, such as a supervisor, bank, or partner organization. The email includes an attachment that, once downloaded, infects the target computer. Once embedded in the computer, the malware typically spreads itself across the network. A recent wave of ransomware phishing emails targeted HR teams since they often receive unsolicited email from job applicants.

- **Drive-by Download:** A drive-by download occurs when compromised software or a website "pushes" a download to a target computer without the user’s consent. This kind of attack has become less common over the years as more web browsers use proactive security to prevent unauthorized downloads and alert users. That said, it remains important to maintain up-to-date versions of your web browsers and other critical software. Organizations should have patch management in place to quickly apply security fixes.

- **Corrupted Software:** Software should only be downloaded directly from the home page of known software vendors. Although some legitimate free software sites do exist, even these tend to include unwanted commercial "bloatware" that may serve ads or change your browser settings without consent. Those changes in turn can make it more likely that you will be exposed to compromised websites. Free software on unknown sites is often a "Trojan", disguising malware or other viruses.

**Anatomy of a ransomware attack and delivery models**

A ransomware attack is a multi-step process. If the proper defenses are in place at the various steps of the attack, the impact can be greatly reduced.

**Figure 2 - Anatomy of a ransomware attack**
Malvertising: Malvertising is any form of advertising intended to spread malware through the internet. This often happens when legitimate advertising is compromised by a malware. Illegitimate ads created by hackers can spread malware directly using malicious scripts, causing “drive-by downloads”. They might entice users to click the fake ad and potentially download ransomware. Most malvertising can be prevented through common ad blocking software.

Social Engineering and Self-Propagation: Social engineering can take place in two ways. Some ransomware passes itself off as a “fine” from a government agency, which can confuse the end user and make them take actions that spread the infection. Once a computer is infected, the other form of social engineering takes place: The infected user’s email contacts and other data are used to spread the infection to other users. The new group of targets unthinkingly accesses the message, believing it to be from their colleague—a prime example of self-propagation.

Demand ransom

Users attempt to access files and are alerted that the data has been encrypted.

Decrypt

Decryption keys will eventually be provided upon payment of a ransom.
The new trends of ransomware
The first versions of ransomware were basic, and often used poor encryption, making it relatively simple to recover encrypted files. However, the threat agents behind ransomware are continuously learning from their mistakes, and have become more sophisticated in their latest variants. According to the latest cyber threat reports, the ransomware threat landscape is evolving in the following ways:

- Ransomware has primarily plagued Windows platforms. Recent platform-agnostic capabilities have been developed and targets have expanded to other operating systems (such as Linux, Android, OS X, etc.)
- More data extortion techniques. At the end of 2015, a Chimera crypto-ransomware was discovered with three disturbing capabilities: (i) encrypting files, (ii) doxing, and (iii) extortion. After encrypting files, if the ransom is not paid, attackers claim to make those files public over the internet. This trick, in most cases, pressures the victim into paying the ransom, despite having a data backup.
- Increased adoption of IP address anonymizing services for ransomware delivery (e.g., Tor anonymity network). These services can complicate the profiling of the threat actor behind a ransomware campaign.
- Increased adoption of cryptographic key provisioning. This process ensures unbreakable cryptographic communication between hosts. When cryptography is implemented correctly, the encrypted files are impossible to recover without a key.
- Wide variety of technical sophistication. Some types of ransomware depend on links to third party libraries, making them easy to detect. However, other types of ransomware use different techniques (e.g., thread injection, process replacement, etc.) to avoid detection. For instance, CTB-Locker uses more advanced techniques (e.g., position-independent code wrapper) that make it almost impossible to detect using traditional signature-based methods.
- “Ransomware as a Service” or RaaS. This is an evolution discovered in mid-2015, in which the creation of ransomware has been commoditized, allowing attackers to develop and distribute customized ransomware. This also gives uninstructed cybercriminals a foothold in ransomware business.
- Ransomware uses every possible attack vector to get into victims’ machines. In some ransomware versions, complex obfuscation and covert launch techniques are used. These allow them to evade detection in the early stages of infection. In addition, cybercriminals are seeding legitimate websites with malicious code to distribute ransomware.
- Exponential deletion. Increased use of time-based motivation techniques, in an effort to maximize criminal actors’ revenues (e.g., encrypted files are gradually deleted permanently).
Protect your business and your intellectual property from ransomware

Ransomware is not new to the world of crime-ware. However, newer more sophisticated methods of delivery, detection, and monetarization, means ransomware continues to be a highly profitable business for cybercriminals. Ransomware promises to be more threatening, and organizations should be proactive in developing and maintaining their readiness and resilience against it. Although the initial cost may be perceived as high, investing in cybersecurity can pay huge dividends in the long term.

The following preventive and detective controls can help your organization be prepared for ransomware threats:

- Implement an effective backup and recovery strategy (offline backups, storage in a secure/separate location, retain backups at multiple points in time, etc.)
- Develop awareness programs for your users
- Implement robust vulnerability and patch management processes
- Manage the use of privileged accounts and configure access controls correctly
- Consider recourse to whitelist filtering to prevent execution of unknown programs
- Implement content filtering to filter out emails and web content
- Harden the security configuration of your devices (including mobile devices)
- Assess the readiness of your IT infrastructure and incident response processes by performing ransomware attack simulations
How should we tackle the new KYC challenges?

Maxime Heckel
Director
Operations Excellence & Human Capital
Deloitte

Bastien Collette
Senior Manager
Operations Excellence & Human Capital
Deloitte

In the aftermath of the financial crisis and several recent cases of fraud, money laundering, and tax evasion, today’s worldwide attention is mostly focused on financial institutions’ anti money laundering/counter terrorism financing (hereafter AML/CTF) duties and obligations. The focus is especially on the way the institutions apply underlying controls on their counterparties. Legal frameworks and related professional standards have changed and are still evolving drastically, increasing compliance requirements toward market actors¹, which therefore increases pressure on regulators to enforce the rules.

¹ FATF recommendations, 4th European AML Directive, national AML/CTF legislations, tax transparency regulations like FATCA or AEOI/CBS, etc.
increased operational efficiency

Compliance cost increase

Onboarding time

Reaching sustainable compliance is currently an objective for the industry

Increased risk management

Regulatory pressure

Variety of requirements

Technology evolution

Compliance cost increase

Onboarding time

Reaching sustainable compliance is currently an objective for the industry

Increased risk management

Regulatory pressure

Variety of requirements

Technology evolution
As a result, financial institutions are struggling to comply with this ever-evolving AML/CTF and tax transparency framework. The entire Know Your Customer (hereafter KYC) process chain needs to be enhanced to ensure that all counterparties' information is collected, qualified, stored, monitored, and screened, including related parties and the shareholding structure. The resulting risk assessment must be reviewed on a recurrent basis, including the risk of reputation, which until recently was often underestimated. On that basis, reaching sustainable compliance in a cost-effective way is an objective for the industry, now more than ever. This must coincide with an increased volume of KYC documents/data to be collected and processed, with strong requirements to decrease onboarding time, especially in the fund industry or in digital banking structures.

The new KYC challenges
Up until this point, it is clear that current AML/CTF practices are redundant within financial institutions and therefore inefficient, requiring every counterparty to exchange information with every financial institution in their operating network. The market is becoming increasingly ready to cope with next curve, which is why we observe rapidly emerging KYC utilities on the market.

Knowing that toggling between KYC utilities is neither efficient nor cost effective, we anticipate those utilities to be expanded over time to not only propose a KYC document repository but value-added services on top.

The utilities are central repositories that offer to collect, qualify, and store KYC documents and related signaletic data of institutions’ counterparties. As a consequence, a synergy effect is created at both the information contribution and consumption sides, since mutualization of documents, data, and some KYC steps occur. Obviously, this is only happening if such a platform is able to show a high market adoption rate (i.e., critical mass of up-to-date documents/data).

This mutualization approach makes sense in a market where actors are progressively looking to reduce in-house involvement in non-core activities by outsourcing them to external providers. Nevertheless, a few blurry points remain. What is the point in having multiple utilities to cover the same feature? Can financial institutions satisfy their needs by subscribing to one utility only? Are those utilities able to cover local specificities, requirements, and several market segments? Those three questions symbolize the main issues with KYC utilities: they are only able to cover a limited scope of the KYC burden felt in the market, mainly because they address one or two main functions each (e.g., KYC documentary platform only, counterparty screening and risk scoring only, etc.) or cover a limited market segment (e.g., correspondent banking only, fund industry only, etc.). It is unlikely that a single player will capture the whole market and the entire set of business/technical requirements in AML/CTF. In the near future, multiple players will have to co-exist and specialize among specific areas (e.g., geography, line of business, etc.) and in the best case, provide “interoperability” among themselves. Knowing that toggling between KYC utilities is not efficient or cost effective, we anticipate those utilities to be expanded over time to not only propose a KYC document repository but value-added services on top.

Value-added services may include new generation onboarding and ongoing monitoring chains such as screening/adverse media search/background check, risk scoring, AML/CTF country risk assessment, on-site due diligence (when required), or FATCA/CRS accounts pre-classification and reporting.
Such end-to-end KYC managed services must also cover several jurisdictions, types of counterparties (financial institution, legal entity and arrangement, retail, etc.) and market segments (banking, fund industry, life insurance, corporates, etc.), allowing market actors to reduce their unit costs (savings through mutualization of technology, resources, and expertise), as well as the organizational/operational impact of seasonal peaks of activities (for instance QI/FATCA/CRS reporting). It must be understood that even if an outsourced approach toward AML/CTF activities will help to reduce related costs while increasing risk management, it will not withdraw the ultimate AML responsibility from financial institutions. The compliance function is thus not coming to an end, and would instead be more focused on the risk-based approach maintenance, operations oversight, and diligence on the most risky cases, switching from an administrative (applying a “tick the box” process) to a real risk-based approach function.

**Technology and data sources evolution**

From a purely technological standpoint, we observe that most financial institutions are still using “generation 1.0” solutions, e.g., out of the box name screening (fuzzy matching), rules-based customer profiling, etc., whereas “generation 2.0” tools are offering new ways to perform counterparty due diligence (adverse media search rather than watchlist screening) or customer profiling (machine learning rather than rule-based engines). Such technologies are quite costly, mainly for small/mid-size businesses and especially knowing that Return on Investment (ROI) cannot be part of the equation.

This is also valid for market data sources where alternatives could be found to the usual and expensive consolidated “watchlists”. Indeed, more and more counterparty screening solutions are relying on open source data and offer to identify corporate shareholding structures and related/linked parties as well.

This is certainly not an exact science (false positives will still be generated), nor fully ready yet, but underlying cost-effectiveness is promising. At the same time, it is important to keep an eye on other emerging innovative technologies such as blockchain, digital passport, or video/online client onboarding. These could play a significant role in automating the future of finance, assuming market actors can overcome the challenges related to these processes.

**What’s in it for a CIO**

In order to keep the pace in this changing environment, CIOs should be focused on a few key priorities:

- Be conscious of upcoming KYC regulations, assessing the impact related to the additional information to be collected and stored in systems, data privacy, and new needs for business features that will be triggered.
Conclusion

Answers to the above KYC challenges have to go through both increased risk management and operational efficiency. This implies that one must think and act differently:

• Financial institutions need to be more efficient while not making any compromise on service quality or compliance with regulations.
• Mandatory and high risk activities such as AML/CTF and KYC do not represent a differentiator across the competition.
• It is still possible to tweak the KYC chain, but not in a sufficient scale, since “gen 1” technology still used today shows a limited internal optimization potential.
• Duplication of AML/CTF tasks and redundancy of related controls within the financial institutions create significant inefficiencies at the industry level.

The entire model needs to be upgraded, and we think that externalization (and therefore mutualization of fixed costs) is the only way to generate substantial savings while increasing compliance level.

With regards to practical implementation, financial institutions should also ensure that service providers are ready to integrate near future technological evolutions. For instance, the use of blockchain technology enables cost savings and removes effort duplication across entities carrying out AML/CTF activities. Validated results would be recorded into the Blockchain in order to share encrypted and up-to-date KYC data to all the stakeholders.

• Review both AML/CTF and AEoI (Automatic Exchange of Information) application value chains to identify weaknesses and opportunities to create synergies; especially knowing recent multiplication of both data sources and regulatory needs (including recurrent electronic reporting).
• Monitor the evolution of KYC utilities, especially the interoperability dimension.
• Assess the cost-effectiveness benefit for replacing existing AML/CTF technology framework in favor of the most recent ones, for instance, drastically reducing the number of false positives (from counterparty screening or transaction filtering/monitoring).
• Assess the business case to mutualize related operations through externalization (i.e., managed services approach), and therefore accessing new technologies, enhanced KYC data, documentation framework, and dedicated expertise.
Inside magazine issue 13 | Part 03 - From a risk and cyber perspective

A big step toward the European Digital Single Market

Regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)

On 23 July 2014, the European Parliament and the Council of the European Union have adopted the regulation EU 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the “eIDAS” regulation).¹ Repealing the 15-year-old European directive on a community framework for electronic signatures (Directive 1999/93/EC),² this new regulation aims at providing a common transnational foundation for secure electronic interaction between European citizens, businesses, and public authorities. Thus, by providing the building blocks for ensuring trust, convenience, and security in the online environment, the eIDAS regulation represents a major contribution to the European Digital Single Market.

Roland Bastin
Partner
Governance, Risk & Compliance
Deloitte

Irina Hedeå
Director
Governance, Risk & Compliance
Deloitte

Ismaël Cisse
Manager
Governance, Risk & Compliance
Deloitte

“Given its inherently transformative nature, eIDAS is clearly an enabler to building a genuine digital single market.”

Andrea Servida, Head of the eIDAS Task Force in Directorate General “Communication networks, content and technology” (DG CONNECT) of the European Commission.³

Toward the digital market and the paperless world, eIDAS opens the door for end-to-end electronic transactions and processes that replace the traditional activities and manual processes, while keeping the same legal value. The opportunities for organizations implementing eIDAS trust services are evident: increase the efficiency of the business processes, reduce their operational costs, grow their business, and build a competitive advantage, among others.
The rise and rapid evolution of information and communication technology over the past 20 years have completely transformed the nature of the interactions between citizens, businesses, and public administrations. New digital services and uses have emerged that leverage on these new technologies while responding to customers’ needs for mobility, convenience, rapidity in service response time, and multi-channel access to the services. In the banking industry for example, this evolution was reflected by the development of services such as online and mobile banking, along with the rapid adoption of these services by customers.

This trend is well illustrated in the analysis of the Digital Agenda Scoreboard key indicators published by the European Commission, which reveals that the percentage of individuals aged between 16 and 74 years old who use online banking in the European Union rose from 19 percent in 2005 to more than 45 percent in 2015. However, as these new electronic services grow in magnitude, the risks related to cybercrime, identity fraud, and leakage of personal data have never been higher than they are today and are still increasing. It leaves many organizations with several questions:

• How can I ensure the identity of a counterpart (natural or legal person) during an electronic transaction?
• How can I ensure the authenticity of an online service (e.g., online public service, electronic commerce)?
• How can I perform digital business or administrative transactions in a convenient, secure, and seamless manner while maintaining the legal value of these transactions?
• And how can I do all this in a cross-border manner within the EU?

The ambition of the eIDAS regulation is to address these questions, and thereby to build trust for electronic transactions, which is the absolute precondition for ensuring that the different actors (i.e., citizens, businesses, and public authorities) adhere to the opportunities raised by the digital economy. In order to attain this goal, the eIDAS regulation addresses two building blocks of the digital economy: electronic identification and trust services.
Electronic Identification
Identification of a person without his or her physical presence will be possible through “electronic identification (eID)” as defined by eIDAS. As of today, several eID means are deployed in the EU, either by the member states (e.g., electronic identity cards or eID cards) or by private actors (e.g., private smart cards, authentication tokens, and mobile applications). Currently, there is no mutual recognition of these eID means between EU member states, nor alignment on the level of assurance offered by these eID means. For example, a Luxembourgish citizen's eID card is not automatically recognized by other EU member states for authentication for online services and electronic transactions.

By 29 September 2018, a EU citizen with an eID card (notified according to eIDAS) will be able to access any online public service from any EU member state, and perform his/her administrative procedures online with the same trust as if the person was physically present.

Mutual recognition
In practice, eIDAS gives EU member states the opportunity to notify the European Commission of their eID means (articles 7 and 9) and makes it mandatory for other member states to recognize the eID means for authentication on their online public services. As a concrete application of this provision, a European citizen with an eID card (among the list of notified eID means) will be able to access any online public service from any member state and perform his or her administrative procedures online as if he was physically present in the concerned administration. This will allow the development of cross-border digital administration services such as tax filing, online registration to university programs, online access to medical records across the EU, and more.

eIDAS brings an important change to the current European digital market, as the regulation defines a framework for cooperation and interoperability between member states to ensure a cross-border mutual recognition of the eID means.
Nevertheless, the trust placed in the eID means (e.g., authentication tokens, private smart cards, eID cards) will depend on the level of assurance that they provide regarding the identity of the physical or legal person behind them.

The regulation defines three assurance levels: Low, Substantial, and High, which depend on several aspects—such as the identity proofing and verification processes for the eID means, the management activities of the entities involved in the issuance of the eID means, and the technical and security specifications of the eID means. Each public sector body offering an online public service in a member state will define the minimal assurance levels required for the eID means used to access their online service, depending on how critical the information is, the sensitivity, and the expected level of security of the online public service and the administrative procedures performed therein.

The recognition of the notified eID means by all EU member states is mandatory as of 29 September 2018. However, as of 29 September 2015, the member states have already had the option, on a voluntary basis, to notify their eID means to the European Commission, and to recognize the eID means defined by other member states.

**Liability and obligations in case of security breach**
Mutual recognition of eID means will help break down the barriers related to electronic administration. However, like for all electronic processes, the benefits come with new risks and security issues. To address them, the regulation enforces member states’ accountability for the eID means under their responsibility.

Member states will be held liable for damages caused intentionally or negligently in a cross-border transaction due to a failure to comply with the regulation. In addition, in the case of a security breach affecting the reliability of the notified eID means, member states will have to suspend or revoke the cross-border authentication or the compromised parts and notify other member states as well as the European Commission.5

**Implementing acts**
As previously mentioned, with eIDAS, every EU member state can allow their citizens to benefit from a secure, convenient, and cross-border digital administration across the entire EU. However, in order to achieve this goal, they need to respect and implement a common set of rules, which were defined in the Commission’s implementing acts adopted in 2015:

- Implementing act 2015/296 establishing the procedural agreements for cooperation between member states on electronic identification6
- Implementing act 2015/1501 describing the requirements of the interoperability framework between national eID means7
- Implementing act 2015/1502 describing the requirements of the assurance levels for the eID means8
- Implementing act 2015/1984 describing the circumstances, formats and procedures of notification of eID means o the European Commission9

The recognition of the eID means (notified according to eIDAS) will be mandatory as of 29 September 2018 for all EU Member States.
“A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.”

**Article 25(2) of the eIDAS regulation.**

**Trust services**
Previous to eIDAS, when the European Union adopted the Directive 1999/93/EC on electronic signatures, the objective was the promotion of electronic signature, the development of international electronic commerce, and cross-border activities. However, the main shortcoming of the previous framework was that, as a directive, it was transposed differently in the national laws, thus leading to a lack of harmonization between member states regarding the technical standards as well as the cross-border recognition of the legal value of the electronic signatures. In practice, under the previous directive, electronic signatures carrying a legal value within one member state (i.e., in accordance with the member state’s national law) were not recognized as such in other EU member states. These limitations hindered the development of the electronic signature in Europe and its adoption by businesses and citizens.

eIDAS addresses the cross-border harmonization of the electronic signatures’ legal value within the EU. In addition, leveraging the new technologies and the development opportunities identified for the European Digital Single Market, the eIDAS regulation goes further by defining new trust services in addition to the electronic signatures:

- **Electronic seals**: Trust service intended for legal persons to ensure the origin and integrity of data and documents
- **Electronic time stamps**: Trust service aiming at ensuring the correctness of the time linked to data and documents
- **Electronic registered delivery service**: Trust service aiming at transmitting data and documents between third parties and providing evidence relating to this transmission.

Since 1 July 2016, eIDAS created opportunities for banks to remotely open clients’ accounts, sign electronically contractual documents, validate electronic transactions, and deploy other electronic services while ensuring a cross-border legal value of these documents and processes within the EU. Other financial businesses are able to implement online signatures of documents between several counterparties in the EU, in a matter of minutes, instead of days or even weeks with the traditional paper-based processes, for the same legal value.
• **Website authentication**: Trust service aimed at ensuring visitors of a website of the identity of the legal person owning the website

• **Validation service** for qualified electronic signatures, qualified electronic seals, certificates related to those services, and certificates for website authentication

• **Preservation service** for qualified electronic signatures, qualified electronic seals, and certificates related to those services

For addressing the risks related to the provision of these trust services and for ensuring an adequate level of security, the regulation defines security requirements for trust service providers in terms of risk management and security incident management, such as the definition of measures for prevention, mitigation, and notification of incidents.

Moreover, for each of the trust services, the regulation defines statuses of qualified trust service providers and qualified trust services (i.e., trust services provided by qualified trust service providers and meeting specific security requirements).

In addition to the requirements applicable to all trust service providers, qualified trust service providers are subject to even stricter requirements related to their qualified status:

• Requirements regarding their systems and activities related to the trust services they offer (management and operational processes, usage of trustworthy systems and products, etc.)

• Requirements for audits of their systems and activities by a conformity assessment body at least every 24 months against specific standards referred to in the Commission's implementing acts

**Legal effect of trust services and electronic documents**

All trust services (qualified and non-qualified) and electronic documents benefit from the principle of non-discrimination as evidence in legal proceedings, meaning that no judge can deny the legal effect and admissibility of a trust service or an electronic document in any court of the EU member states.

Nevertheless, only qualified trust services benefit from the presumption of reliability in legal proceedings (i.e., presumption of integrity, correctness of the origin, and accuracy) and cross-border recognition of qualified status in the EU member states. In the specific case of the qualified electronic signatures, the regulation goes even further in Article 25 by bestowing a qualified electronic signature the equivalent legal effect of a handwritten signature.
Supervisory body
The trust in these digital services would have no value without a proper governance framework, including adequate supervision. Thus, the regulation introduces the role of supervisory bodies designated by the member states and responsible for:
• supervising of the trust service providers’ activities
• granting qualified statuses to trust service providers and trust services
In addition to their supervision tasks, supervisory bodies are urged by the regulation to cooperate, mutually and with other authorities such as member states’ data protection authorities and the European Union Agency for Network and Information Security (ENISA).

Trusted lists and EU trust mark for qualified trust services
To enable European citizens and organizations to use the qualified trust services in a confident and convenient manner, the regulation defines two concepts:
• The trusted lists (Article 22), which are established, maintained, and published by each member state and include information related to qualified trust service providers and qualified trust services under the member state’s scope of responsibility
• The EU trust mark (Article 23) for qualified trust services, which is a logo that can be used by qualified trust service providers to indicate the qualified trust services they provide

International aspects
In the increasingly globalized world, development of the digital economy at the international level is key for business development. The regulator truly understands that and opens the door to conditional mutual agreements between the EU and third countries with the objective of mutual recognition between qualified trust services in both markets.

Since 1 July 2016, the provisions pertaining to trust services and electronic documents under the eIDAS regulation are applicable in the EU member states, which means that European citizens, businesses, and public authorities can already benefit from these innovative services and their cross-border legal value in the course of electronic transactions. In practice, since 1 July 2016, eIDAS created opportunities for banks to remotely open clients’ accounts, sign electronically contractual documents, validate electronic transactions, and deploy other electronic services while ensuring a cross-border legal value of these documents and processes within the EU.

Other financial businesses are able to implement online signatures of documents between several counterparties in the EU, in a matter of minutes, instead of days or even weeks with the traditional paper-based processes, for the same legal value.

The legal tools introduced by the eIDAS regulation give private sector and public authorities a tremendous opportunity to set themselves apart by offering innovative cross-border digital services to their customers. If before this regulation, the legal value of the digital signatures and transactions was limited inside the borders of a member states, eIDAS brings the enablers for developing an EU digital market where the confidence in electronic identities and electronic transactions has no border. In a business development perspective, boulevards of opportunities are opening for the organizations in the private sector and a large palette of process optimization comes out for the public sector.

Organizations choosing to implement eIDAS trust services will now start a journey to:
• define their business digital strategy and the processes to be digitally transformed
• identify which eIDAS trust services are relevant for their digital strategy
• design the target business solutions leveraging the eIDAS trust services, while taking into account governance, risk, compliance, and information security considerations
• integrate the eIDAS trust services and solutions within their existing IT infrastructure
• assess the organizational changes for their employees, clients, and partners

In their digital transformation project, they should also consider key aspects such as regulatory, legal, technical, and operational factors.

The European Union has provided the fertile ground for a trustworthy, secure, and convenient digital single market. It is up now to European actors of the digital economy (citizens, businesses, and public authorities) to unlock the full potential of electronic identification and trust services for their activities.
In addition, organizations in the Grand Duchy of Luxembourg can combine the eIDAS opportunities with the law on electronic archiving of 25 July 2015\(^1\) in order to take their digital transformation to a new level, namely by:

- digitizing their original paper documents and archiving them while keeping their legal value
- transforming the traditional business processes into electronic processes while keeping the same legal value

Exploiting all these opportunities is not a complex exercise, but should be done by involving all the concerned actors of the organizations, including the business, IT, and Information Security, and should consider eIDAS requirements before launching a digital transformation.

The European Union has provided the fertile ground for a trustworthy, secure, and convenient digital single market. It is up now to European actors of the digital economy (citizens, businesses, and public authorities) to unlock the full potential of electronic identification and trust services for their activities.

Sources:
PSD2

Challenges and Opportunities for the CIO

Patrick Laurent
Partner
Technology & Enterprise Application Leader
Deloitte

Pascal Eber
Partner
Operations Excellence & Human Capital
Deloitte

Steve Hauman
Director
Technology & Enterprise Application
Deloitte
Introduction to PSD2

The revised Payments Services Directive (PSD2) follows in the footsteps of PSD—adopted in 2007—and is a fundamental step in implementing the SEPA (Single Euro Payments Area) directive. The original PSD aimed to regulate payment services provided by banks as well as payment and e-money institutions, which are formally called Payment Service Providers (PSPs). Following the vote to adopt the new revised directive, the European Commission highlighted that the new legislation focuses on making payments throughout Europe safer and more secure, and enables innovation by allowing new payment services to enter the market.

The drivers behind the regulation are clear: innovation, competition, and consumer protection. These are recurring themes that are being consistently pushed by regulatory authorities throughout Europe, both centrally and within its member states. The changes proposed by PSD2 are far-reaching. Set against a backdrop of increasing Fintech investment, PSD2 now enables many new third parties to participate in a market that has previously not been open to them, whereas traditional players might lose control and influence within these markets if they are not careful to address these new challenges.

New stakeholders, new rules, and new processes

Two new types of third-party PSPs have been identified by PSD2: Payment Initiation Service Providers (PISPs) and Account Information Services Providers (AISPs). Together, under PSD2, they are called Third Party Service Providers (TPSPs).

Previously, Payment Service Users (PSUs) with multiple accounts were only able to create a holistic view on their financial portfolio by sequentially accessing their individual accounts through separate interfaces. AISPs now enable PSUs to access and aggregate account information from all accounts that could be of any use to them.

Additionally, a payer had to initiate a payment directly through his bank, while today PISPs are able, on behalf of a PSU, to directly access and initiate payments through the bank’s payment infrastructure.

In order for TPSPs to directly connect to the financial institutions’ infrastructure, a new set of technical standards and connection requirements have been in development. These requirements are referenced as XS2A or “Access to Account.”
Challenges and opportunities for the CIO
CIO environments all over Europe will be heavily affected by these new regulations. CIOs who can and want to move quickly could use these regulatory changes as an opportunity to accelerate open banking and digitization. PSD2 embeds a strategic component for banks; they could use PSD2 to reposition themselves, or be disrupted in terms of customer experience. Another Fintech may take over the services of its customers, and use the bank only as a booking or processing entity. The use of external Fintech platforms will contribute to the creation of new ecosystems that could enable new business and operating models more efficiently.

The legacy problem
Until recent years, building IT systems was seen as an important way to differentiate from the competition. Financial institutions believed that there was value in building their own proprietary, and therefore closed systems were seen as “the” way to deliver the best service to the end client. For most banks, the successive waves of investments in the IT landscape resulted in cumbersome legacy platforms linked with enormous maintenance budgets just to keep them running.

In order for banks to survive in the banking market of tomorrow, financial institutions need to embrace aggressive standardization approaches and commoditization of their IT. This will not only make IT operations more cost effective, but will also encourage innovation.

Financial institutions need to step away from closed legacy systems to more open standards and software. They should accept that off-the-shelf solutions exist and are more cost-efficient than building them by themselves. With an open mind, financial institutions should look at how new fintech players could complement their application landscape more than trying to compete with them.

Mandatory use of APIs
PSD2 will force significant challenges upon the infrastructure of financial institutions, who will need to answer to these new regulations with an open, pluggable, and flexible IT architecture. Not only will TPSPs need to be able to access the IT architecture by apps that are developed outside the bank, but exposed services need to be shareable and reusable and allow agility in a rapidly changing environment.

XS2A proscribes that financial institutions expose enterprise assets for regulated third parties through open application programming interfaces (APIs). In computer programming, an API is a set of subroutine definitions, protocols, and tools for building software and applications. A good API makes it easier to develop a program by providing all the building blocks, which are then put together by the programmer.

APIs are not new: In the past decade, APIs have become the de facto paradigm for sharing data, and have enabled organizations that hold large amounts of data to become platforms for third party innovation. Large platforms such as Google, Twitter, and Facebook offer APIs to third parties, e.g., for login or for initiating messages. In the payment space, PayPal has pioneered external APIs since 2010, on the basis of which an entire new ecosystem flourished.

A few examples of the banking services that might be exposed through APIs include account initiation, account fund availability, account balance, payment guarantees, real-time payments, payment refunding, conditional payments, crypto-payments, e-mandate management, authentication, online contracting, personal data verification, and bank statement status reports.

Banks need to therefore invest in application service governance and API management. Financial institutions will need to build or buy an API management gateway and create new APIs to provide access to financial institution assets.

The security aspect in the overall API Architecture will need to be taken up carefully. The European Banking Authority (EBA) recently published a Consultation Paper on draft technical standards of strong customer authentication as well as common and secure communication under PSD2. These technical standards will ensure appropriate levels of security, while at the same time maintaining fair competition between all payment service providers and allowing for the development of user-friendly, accessible, and innovative means of payment.
A strong API strategy can create additional business value

Although the use of APIs within banks could initially be strongly driven by regulations, they can also create significant business value and address the strategic priorities of top management.

Some examples of how APIs could contribute to create business value within the financial services industry:

- The use of APIs could simplify time-to-market in making products and services available to the market. Accessibility of services toward new market players could increase, resulting in an increase of market share and revenues.

- Traditional ways of transforming business ideas into IT solutions can be quite time-consuming and cost inefficient. Using APIs, both for internal and external use, could enable CIOs to reduce costs through lower time-to-market, reduce the overall development lifecycle costs, as well as integrate partner solutions or services in a more efficient way.

- APIs could improve the internal or external user experience by developing dedicated or specialized mobile applications to give access to developers to APIs. CIOs would have new ways to keep pace with disruptive innovation as seen in non-banking environments or Fintechs.

- More and more financial institutions could start experimenting with internal or external Hackathons, in order to identify best practices and lessons learned as well as engage with new a digital ecosystem of developers and partners. This engagement will be further facilitated if an efficient API strategy is in place.

- APIs also enable banks to explore new business models. For example, Fidor, an innovative German online bank, created a standard API layer on top of their core banking system, which allows developer communities to build their own applications and banking services, integrate solutions into the Fidor platform, and monetize their technology platform on top of traditional banking services.
API-based P2P payment or lending solutions

Peer-to-Peer or Person-to-Person (P2P) payments are a fast and simple way for people to directly send money to others using a mobile phone number or email address through online banking, a smartphone, or a tablet. With a growing number of people expecting to access reliable P2P functionality, financial institutions gain a competitive edge by offering an API-centric solution that safeguards users’ sensitive information while securely delivering money faster.

One example in this sphere is Lending Club, the world’s largest online credit marketplace, facilitating personal loans, business loans, and financing for elective medical procedures. Borrowers access lower interest rate loans through a fast and easy online or mobile interface. Investors provide the capital to enable many of the loans in exchange for earning interest. They operate fully online with no branch infrastructure, and use technology to lower costs. They pass the cost savings to borrowers in the form of lower rates and investors in the form of attractive returns. They are transforming the banking system into a frictionless, transparent, and highly efficient online marketplace.

Personal Financial Management solutions

Recent years have seen the emergence of a multitude of PFM tools, each of which purports to be the best way to keep track of your finances. PSD2 forcing mandatory financial institutions to expose data will likely accelerate the commercialization of these kind of tools.

For example, German based Treefin is using APIs to offer customers a single and aggregated view of their investment portfolio, insurance policies, and bank accounts. While creating a holistic view of the client’s financial assets, the PFM solution proposes suggestions in order to further optimize the client’s portfolio and optimize financial returns. The introduction of PSD2 will enable local players, like Treefin, to expand their services across Europe more easily.

The Open Bank Project

The Open Bank Project provides an open source developer friendly “API for banks” that developers and companies can use to build innovative applications and services based on the account holder’s transaction data. It uses a secure, enterprise-ready technology stack and supports secure internet protocols such as OAuth.

 Deploying the OBP API can encourage a community of developers to grow around the bank and enable them to build innovative products and services for customers based on the “bank as a platform” principle. Services may be offered through an app store, and the best ideas can be cherry-picked for use in branded interfaces. Customers can benefit from freer innovation cycles, greater choice, and quality; and the bank, as the gatekeeper to the OBP API, may charge customers for this added value.

The Open Bank Project also delivers a PSD2 sandbox that demonstrates a PSD2 API solution. The API provides a secure avenue that allows bank account holders to access their banking data and services through approved third party applications, following the consent of both the bank and customer.
Conclusion

Overall we can conclude the following:

- CIO environments all over Europe will be heavily affected by new regulations. CIOs that can and want to move quickly could use these regulatory changes as an opportunity to accelerate open banking and digitization. The Revised Payments Services Directive (PSD2) will force a more open banking model as it requires banks to open access to data and transactions to new market entrants.
- Mandatory use of open APIs will force significant challenges upon the financial institutions infrastructure that need to answer to these new regulations with an open, pluggable, and flexible IT architecture.

However, creating a strong API strategy can create additional business value.
- PSD2 will accelerate the adoption of open banking, reinforce the creation of new business models, redistribute responsibilities in the overall value chain, and therefore have a significant impact on the overall banking landscape.

Banking app stores

Banking app stores are comparable with public app stores in other industries, but are created, branded, and hosted by banks. They mostly provide API-based access to bank functions and development platforms in order for third party developers to create custom apps. Examples include Crédit Agricole (CA Store) and Deutsche Bank (Autobahn App Market).

Open source banking systems

Open source banking systems are banking-specific applications or components that are made available to an open source licensing process. Cyclos developed an open source online payment, Hyperledger is a peer-to-peer distributed ledger technology for a new generation of transactional applications, and OpenChain and MultiChain are examples of open source blockchain.

Sources:

Internal Deloitte Publications
1. Deloitte – Inside Magazine issue 12 – The early bird catches the worm: anticipating the challenges and opportunities of PSD2
2. Deloitte – Waiting for PSD2 – Will the EU Digital Single Market deliver both payment security and access to information?
3. Deloitte – PSD2 opens the door to new market entrants – Agility to be kept to keeping market position

External Publications
5. PWC – 2016 – Catalyst or threat – the strategic implications of PSD2 for Europe’s banks
6. Forrester – 2016 – APIs Turn Disruption into Business Opportunities
8. Gartner – 12 January 2015 – The business value of banking APIs
9. Gartner – 19 February 2016 – Use PSD2 to accelerate Open Banking
11. FinExtra – March 2016 – Preparing for PSD2: Exploring the business and Technology implications of the new payment service directive

Internet References
17. https://www.lendingclub.com/
18. https://www.fidorbank.uk/
22. https://www.hyperledger.org/
Toward privacy in the digital market:
How the General Data Protection Regulation will affect your business

Introduction and context
Published in the Official Journal of 4 May 2016, the General Data Protection Regulation (GDPR) entered into force on 24 May 2016, and will be applicable across the European Union from 25 May 2018 onward. Indeed, unlike a directive, a regulation does not have to be transposed into national law to become applicable.

The GDPR is the result of a lengthy revision of the European directive 95 / 46 / CE from 1995. The objective behind this new text is to provide a unified data protection framework applying directly to all EU member states as well as to all EU citizens to guarantee a high level of protection for citizens while playing the role of enabler of the digital single market.

With this new regulation, the EU intends not only to strengthen citizens’ control over the use of their personal data, but also to simplify the regulatory landscape for businesses.

The GDPR will impose high standards and uniform rules that strengthen consumer rights, boost European competition, and kick-start innovation.

Consequently, the GDPR will have an impact on all layers of the operating model of organizations where personal data could be used—both personal data of its customers and of its employees. The GDPR will require to assess the “as is” in order to identify the gaps with a compliant “to be” as a target, taking into account that both existing activities as well as new personal data processing activities will fall under the GDPR.

Beyond compliance, the GDPR should also be thought in the light of the digital market, as its implementation will enable organizations to gain a competitive edge by enhancing consumers’ experience and trust.
How will the GDPR affect your business’s operating model?

**Governance and Organization**

The entire GDPR is built on the principle of accountability, and clearly defines and expands the roles and responsibilities of controllers and processors. Controllers, as well as the potential processors, will have direct obligations to implement organizational and technical measures such as privacy policies, appropriate security measures, maintenance of records of personal data processing, and performance of privacy impact assessments. They will also be requested to notify data protection authorities of personal data breaches, and, in specific cases, to appoint a DPO.

In complement, the role of controller will not be limited to implement measures, such as data protection policies, to comply with the GDPR; he will also have the responsibility to demonstrate compliance if requested to do so by its national data protection authority (DPA).

Maintaining documentation on the processing of personal data and on measures implemented to safeguard personal data will be key to demonstrate compliance. To ease accountability, organizations should thus identify owners in charge of maintaining the necessary documentation.

Accountability will make top management leadership essential in the setup of a data protection governance and organizations should make sure that decision makers and key people are aware not only that the law has changed to the GDPR but also of the potential impacts brought by this change.

Although not new, with the GDPR, the role of Data Protection Officer is further developed. Appointing a Data Protection Officer may even become, in specific cases, mandatory. The DPO, who is in charge of monitoring compliance with the GDPR, advising its organization, and cooperating with data protection authorities, will have to define clear communication channels with internal stakeholders (authorized management sponsors, business owners of the processing of personal data, employees, etc.) as well as with external stakeholders (clients, third party service providers, data protection authorities, etc.). The DPO will also have to sustain subsequent communication, supported by authorized management sponsors. This will affect the organigram of organizations, which will have to consider whether to appoint a DPO and where to position him in the organigram.
The GDPR will have an impact on all layers of the operating model of organizations.

The GDPR broadens the territorial scope of the EU legislation to cover both (i) the processing of personal data by controllers/processors established in the EU even if the processing in itself takes place outside of the EU; and (ii) natural persons who are in the EU even when their personal data are processed by a controller/processor not established in the EU. In this regard, when various entities of a cross-border organization exchange personal data, a clear organization with identified roles and responsibilities should be set up to comprehensively tackle data protection and monitor the legitimacy of transfers to third countries.

Data protection authorities will be provided with reinforced powers to enforce the GDPR, among which is the possibility to fine non-compliant organizations up to four percent of their worldwide turnover. Organizations will need to define clear consultation channels with the DPAs with the appropriate level of sponsorship to foster communication and tackle the risk of non-compliance at the earliest stage.

**Business Processes**

Organizations should review, for each of their business processes, the legitimate ground(s) for processing personal data to confirm and document that they legitimately process personal data. Among the grounds legitimating processing of personal data, organizations should take special care of consent since the GDPR will make the conditions for consent more stringent. Indeed, the burden of proof will be on the controller, who is required to demonstrate that the data subject has freely consented to the processing of his or her personal data. Therefore, organizations should take into consideration that consent will be more difficult to obtain and not always ensure a strong level of certainty, since the data subject may withdraw his or her consent at any time.

The GDPR formally gives its place to the risk-based approach. Data Protection Impact Assessments (DPIAs) should be performed to identify risks to the data protection rights of individuals of specific processing, for example when
the purpose of the processing aims at systematically evaluating personal aspects or when it involves the processing of special categories of data (e.g., health data) on a large scale. Whenever risks are identified, it is expected that organizations formulate measures to address them. This assessment should be performed prior to the start of the processing.

The GDPR makes explicit reference to direct marketing, to which data subjects have the right to object. It also strictly frames profiling activities by setting limits. In certain cases, organizations may be allowed to design processes using profiling to make decisions but should implement appropriate measures to safeguard the rights of data subjects. Organizations should review their business processes to ensure that suitable measures safeguarding that the rights of data subjects are embodied. In the context of the profiling, this means foreseeing the possibility, for data subjects, to obtain human intervention to express his or her point of view and to contest the decision.

**Personal data**

The GDPR expands the rights of data subjects by introducing, among other things, the right to be forgotten\(^1\) and the right to data portability requiring both organizational and technical measures to be implemented. For example, data portability implies that data subjects may request to receive their personal data in a structured, commonly used, and machine-readable format. They will also be able to request that the personal data be transmitted directly from one organization to another.

As a result, organizations should be ready to handle requests requiring the implementation of data management processes. In this context, they should know what personal data they hold, from where it came, and whether the personal data are transferred. Information audits may be performed across the organization, or within particular business areas to map this information.

Beyond compliance, the GDPR should also be thought in the light of the digital market, as its implementation will enable organizations to gain a competitive edge by enhancing consumers’ experience and trust.

The regulation contains a personal data breach notification obligation that should be taken into consideration by organizations in the frame of their data management processes, notably due to prescriptions in terms of timing (i.e., without undue delay, but in principle, no later than 72h after having identified the breach) and of communications means (e.g., when the personal data breach is likely to result in a high risk for data subjects, controllers will have to communicate the personal data breach to them). Communication is required to be in clear and plain language, and should describe the nature of the personal data breach.

Therefore, organizations will have to review their information security management procedures and operational processes to ensure that personal data breach can be detected, reported, and investigated, and that notification requirements will be assessed and, where necessary, satisfied.

---

1. Art. 56.2 of the GDPR
2. Already established in 2014 by the “Google v. Spain” ruling of the EUCJ
The GDPR requires organizations to ensure a level of security appropriate to the risk presented by the processing.

Supporting systems
As described above, the GDPR requires organizations to have clearly identified their information assets and the systems hosting them to be in a position to meet the requirements of structured communication to data subjects or of handling erasure requests. Organizations should review their information asset classification and management and should assess whether their system configuration allows them to meet the forthcoming requirements or whether additional technical or organizational measures should be implemented.

The GDPR as a way to gain a competitive edge in the digital market
Data privacy in the digital area: “Smarter, faster, better”
In today’s digital era, data privacy is becoming increasingly critical for businesses, pushed forward not only by the EU legislator but by EU customers as well, who are even more aware of data protection matters. With legal texts such as the GDPR, it is now necessary that data privacy issues are included in the digital initiatives of organizations. Indeed, organizations should adopt a proactive stand on privacy matters, which, on top of enabling compliance, creates and reinforce consumers’ trust and fidelity.
By complying today with the GDPR, organizations will be able to gain a competitive edge tomorrow. They should not hesitate to advertise to their customers on why, how, and what personal data they process. Transparency toward customers demonstrates the benefit of the service, fostering customers’ willingness to see their personal data processed since they do know which data are actually processed and why. On top of this, it will consequently allow organizations to perform direct marketing and profiling activities efficiently.

**Regulatory synergies and limitations**

Data privacy is not a novelty and was in existence before the GDPR. Therefore, organizations are likely already subject to existing laws and regulations governing this matter and requiring controls similar to GDPR. Such a legacy may be built on to reach compliance with the GDPR faster and at a lower cost.

Implementations of other regulations should take the requirements of respecting the GDPR into account, especially if these regulations imply the monitoring or profiling of the activities of the company’s employees or clients.

**How to move forward?**

The GDPR will call for actions by organizations. This may be complex, as it will require the assessment of the existing framework against the new requirements, in order to identify possible gaps, set up an action plans with measures to be implemented in order to support the affected layers (governance, business processes, personal data, and supporting systems), and accordingly define a roadmap of implementation with May 2018 as a deadline.

---

**Conclusion**

This regulation will affect organizations at various levels. Rather than seeing it as a constraint, organizations can make the best of it by using the GDPR as leverage to gain a competitive edge. Besides that, existing laws and regulations should also not be put aside, since on one hand, they can provide synergies and ease future implementations, and on the other hand, some requirements will need to be considered in the light of the GDPR obligations. The regulatory agenda may have other developments on this topic, such as expected delegated acts to be produced by the EU Commission to further detail the GDPR requirements or the topic of the “privacy shield framework,” enabling organizations to transfer personal data to the US.

On 12 July 2016, the European Commission has adopted the EU-US Privacy Shield framework with an adequacy decision. By notifying the member states, the new framework for EU-US personal data transfers enters into force immediately. The adoption of the Privacy Shield signals a return to normality for transatlantic data transfers, after the previous Safe Harbor framework became invalidated by the European Court of Justice on October 2015. As of 1 August 2016, US companies will be able to self-certify with the US Department of Commerce operating the Privacy Shield.
Contacts

**Editorial committee**

**Joël Vanoverschelde**
Partner - Advisory & Consulting Leader
EU Institutions & Supranationals Leader
+352 451 452 850
jvano@deloitte.lu

**Pascal Martino**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 119
pamartino@deloitte.lu

**CIO services**

**Patrick Laurent**
Partner - Technology & Enterprise Application Leader
+352 451 454 170
palaurent@deloitte.lu

**Marc Halmes**
Partner - Technology & Enterprise Application
+352 451 453 710
mhal@deloitte.lu

**Jean-Pierre Maissin**
Partner - Technology & Enterprise Application
+352 451 452 834
jpmaissin@deloitte.lu

**Advisory & Consulting Leader**

**Joël Vanoverschelde**
Partner - Technology & Enterprise Application
EU Institutions & Supranationals Leader
+352 451 452 850
jvano@deloitte.lu

**CEO & CFO services**

**Benjamin Collette**
Partner - Strategy, Regulatory & Corporate Finance Leader
+352 451 452 809
bcollette@deloitte.lu

**Laurent Collet**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 112
lacollet@deloitte.lu

**Annick Elias**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 454 386
aelias@deloitte.lu

**Petra Hazenberg**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 689
phazenber@deloitte.lu

**Joachim Heukmes**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 037
jheukmes@deloitte.lu

**Pascal Martino**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 119
pamartino@deloitte.lu

**Pierre Masset**
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 756
pmasset@deloitte.lu

Please do not hesitate to contact your relevant experts in the magazine
CCO/CISO/CRO/CIA/BOD services

Laurent Berliner
Partner - Governance, Risk & Compliance Leader
+352 451 452 328
lberliner@deloitte.lu

Roland Bastin
Partner - Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu

Eric Collard
Partner - Forensic, AML & Restructuring
+352 451 454 885
ecollard@deloitte.lu

Thierry Flamand
Partner - Insurance & Benefits Actuarial Advisory
+352 451 454 920
tflamand@deloitte.lu

Stéphane Hurtaud
Partner - Information & Technology Risk
+352 451 454 434
shurtaud@deloitte.lu

Michael JJ Martin
Partner - Forensic, AML & Restructuring
+352 451 452 449
mmichamartin@deloitte.lu

Jean-Philippe Peters
Partner - Business Risk/Risk & Capital Management
+352 451 452 276
jpeters@deloitte.lu

COO & CHRO services

Pascal Eber
Partner - Operations Excellence & Human Capital
+352 451 452 649
peber@deloitte.lu

Simon Ramos
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 702
sramos@deloitte.lu

Basil Sommerfeld
Partner - Operations Excellence & Human Capital Leader
+352 451 452 646
bsommerfeld@deloitte.lu

Deloitte Solutions

Vincent Gouverneur
Partner - Outsourced Solutions Leader
+352 451 452 451
vgouverneur@deloitte.lu

Lou Kiesch
Partner - Outsourced Solutions
+352 451 452 456
lkiesch@deloitte.lu

François-Kim Huge
Partner - Outsourced Solutions
+352 451 452 483
fkhuge@deloitte.lu

Xavier Zaegel
Partner - Outsourced Solutions
+352 451 452 748
xzaegel@deloitte.lu

Healthcare

Luc Brucher
Partner - Healthcare Leader
+352 451 454 704
lbrucher@deloitte.lu

Insurance

Thierry Flamand
Partner - Insurance Leader
+352 451 454 920
tflamand@deloitte.lu

Investment Funds and Hedge Funds

Johnny Yip
Partner - Investment Funds & Hedge Funds Leader
+352 451 452 489
jyiplanyan@deloitte.lu

Technology, media and Telecommunications - Public Sector

Georges Kioes
Partner - Technology, Media & Telecommunications & Public Sector Leader
+352 451 452 249
gkioes@deloitte.lu

PSF

Stéphane Césari
Partner - PSF Leader
+352 451 452 487
scesari@deloitte.lu

Private Equity - Real Estate

Benjamin Lam
Partner - PE/RE Leader
+352 451 452 429
blam@deloitte.lu

Bank & Credit Institutions

Martin Flaunet
Partner - Bank & Credit Institutions Leader
+352 451 452 334
mflaunet@deloitte.lu

CCO/CISO/CRO/CIA/BOD services

Laurent Berliner
Partner - Governance, Risk & Compliance Leader
+352 451 452 328
lberliner@deloitte.lu

Roland Bastin
Partner - Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu

Eric Collard
Partner - Forensic, AML & Restructuring
+352 451 454 885
ecollard@deloitte.lu

Thierry Flamand
Partner - Insurance & Benefits Actuarial Advisory
+352 451 454 920
tflamand@deloitte.lu

Stéphane Hurtaud
Partner - Information & Technology Risk
+352 451 454 434
shurtaud@deloitte.lu

Michael JJ Martin
Partner - Forensic, AML & Restructuring
+352 451 452 449
mmichamartin@deloitte.lu

Jean-Philippe Peters
Partner - Business Risk/Risk & Capital Management
+352 451 452 276
jpeters@deloitte.lu

COO & CHRO services

Pascal Eber
Partner - Operations Excellence & Human Capital
+352 451 452 649
peber@deloitte.lu

Simon Ramos
Partner - Strategy, Regulatory & Corporate Finance
+352 451 452 702
sramos@deloitte.lu

Basil Sommerfeld
Partner - Operations Excellence & Human Capital Leader
+352 451 452 646
bsommerfeld@deloitte.lu

Deloitte Solutions

Vincent Gouverneur
Partner - Outsourced Solutions Leader
+352 451 452 451
vgouverneur@deloitte.lu

Lou Kiesch
Partner - Outsourced Solutions
+352 451 452 456
lkiesch@deloitte.lu

François-Kim Huge
Partner - Outsourced Solutions
+352 451 452 483
fkhuge@deloitte.lu

Xavier Zaegel
Partner - Outsourced Solutions
+352 451 452 748
xzaegel@deloitte.lu

Healthcare

Luc Brucher
Partner - Healthcare Leader
+352 451 454 704
lbrucher@deloitte.lu

Insurance

Thierry Flamand
Partner - Insurance Leader
+352 451 454 920
tflamand@deloitte.lu

Investment Funds and Hedge Funds

Johnny Yip
Partner - Investment Funds & Hedge Funds Leader
+352 451 452 489
jyiplanyan@deloitte.lu

Technology, media and Telecommunications - Public Sector

Georges Kioes
Partner - Technology, Media & Telecommunications & Public Sector Leader
+352 451 452 249
gkioes@deloitte.lu

PSF

Stéphane Césari
Partner - PSF Leader
+352 451 452 487
scesari@deloitte.lu

Private Equity - Real Estate

Benjamin Lam
Partner - PE/RE Leader
+352 451 452 429
blam@deloitte.lu

Bank & Credit Institutions

Martin Flaunet
Partner - Bank & Credit Institutions Leader
+352 451 452 334
mflaunet@deloitte.lu
Our expert authors, who are brimming with excitement about these disruptive topics, have written articles to help decision-makers to apprehend the new paradigms—if not to understand them all.