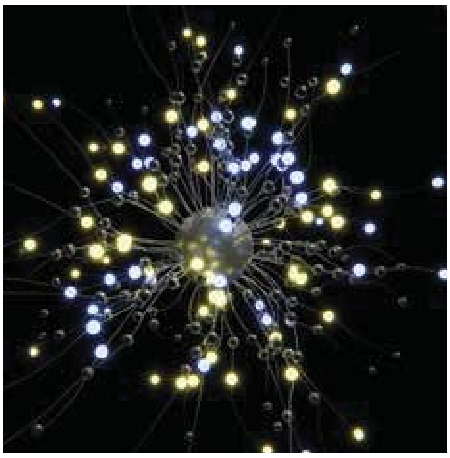
Inside

Deloitte.

EMEA
TECHNOLOGY
EDITION
2017

In this issue

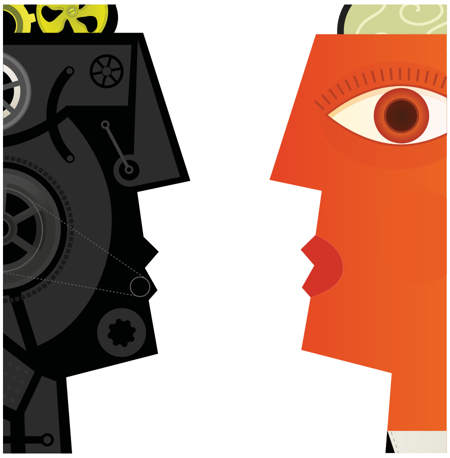


Page 11

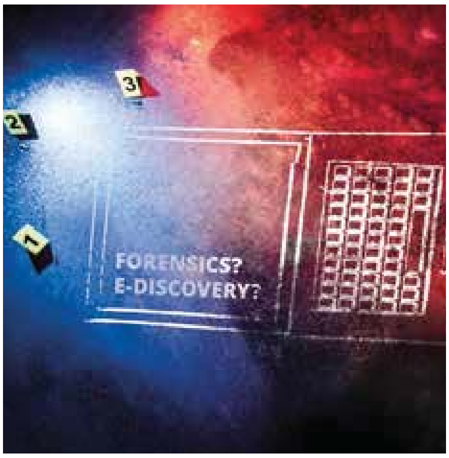
Page 42

Page 58

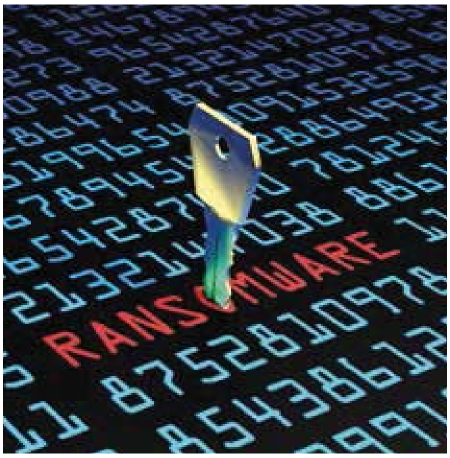
Companies are confronted with a changing environment and need to respond to challenges...



Page 68



Page 84



Page 93

Foreword

Dear readers,

It is with great pleasure that we present our very first EMEA Technology edition of Inside magazine. This edition addresses the current hot topics capturing the technology market's attention and provides you with technological related views and business practices in the financial industry.

With the underpinnings of IT shifts, it has never been more important for CIOs and Technology Leaders to anticipate and understand current and future disruptive technologies rising in the global and connected world. Over the past few years, an exponential number of new players have entered the financial markets with products ranging from payments, Artificial Intelligence, blockchain and Robot Process Automation to name but a few. These innovations are challenging the current companies' business models. To maintain the leading role in value chain creation, incumbent firms will not only have to adjust radically their processes, but also define new ways to collaborate in an ever-growing global world.

In this fast-paced world involving and connecting global business players, we believe it is important to provide you with an edition gathering diverse views from international contributors. The EMEA Technology edition is a joint effort by technology professionals from across the Deloitte network, sharing their knowledge and perspectives.

At Deloitte, we truly believe that CIOs, having a cross-dimensional view on new technologies, will be the ones better positioned to shape the future of their firm's business. For this reason, this edition showcases innovative thinking and practical analysis from three different perspectives that are all critical for a successful technology transition:

- **Digital Perspective:** How and to what extent digital innovations disrupt the technology landscape and influence your business strategy and model
- **Transformation & Technology Perspective:** How technology changes can reengineer and improve your processes
- **Risk & Cyber Perspective:** How technology reinforces trust and confidence as the cornerstones in companies today

Change is the only true constant. We wish you an insightful read of the contributions that we hope will provide your company with the right tools and mindset to surf on the wave of game-changing technology.

Welcome to this edition!

Michel de la Belliere
Partner
EMEA FS Consulting
co-Leader

RLWiddas

Richard Widdas
Partner
EMEA FS Consulting
co-Leader

Koen Vandaele
Managing Partner
EMEA Consulting
Leader

Editorial

Dear readers,

We are pleased to share with you this EMEA Technology edition of Inside magazine.
In this edition, we react to the increasing number of game-changing technologies that transform your business and the society globally by providing you with an edition that includes the views of contributors from accross our network.

In a world of fierce competition, information and information management are recognized as one of the primary assets of a company. This is why CIOs and Technology Leaders are not only expected to be service providers for the business, but also for more and more partners, innovators and change agents that manage the emergence of new technologies. In this edition, we aim to present the key trends, which might well be your business as usual in the coming years.

New technologies have shaken the client/provider relationship and organizations now need to adapt their business models to face new competitors and business models which will enable them to tackle new opportunities. In this way, digital and related services providing transformations are a key topic we want to emphasize with the development of FinTech hubs and the new ways of consuming retail services.

These digital innovations are only sustained by efficient and agile organizations that have made the necessary investments in their core functions. In section two, we will cover the elements that will enable you to make the most of the benefits of new technologies through the internal delivery chain.

None of these technologies can deliver their benefits without trust. The trust customers have when making a payment or when employees validate an electronic identity is key to securely manage the growing number of players required to deliver a service. The customers' trust in the services you provide should be at least equal to the one employees have in the system they log in to every morning.

We hope this edition will provide you with inspiring thoughts and will bring you even more success in anticipating these coming trends.

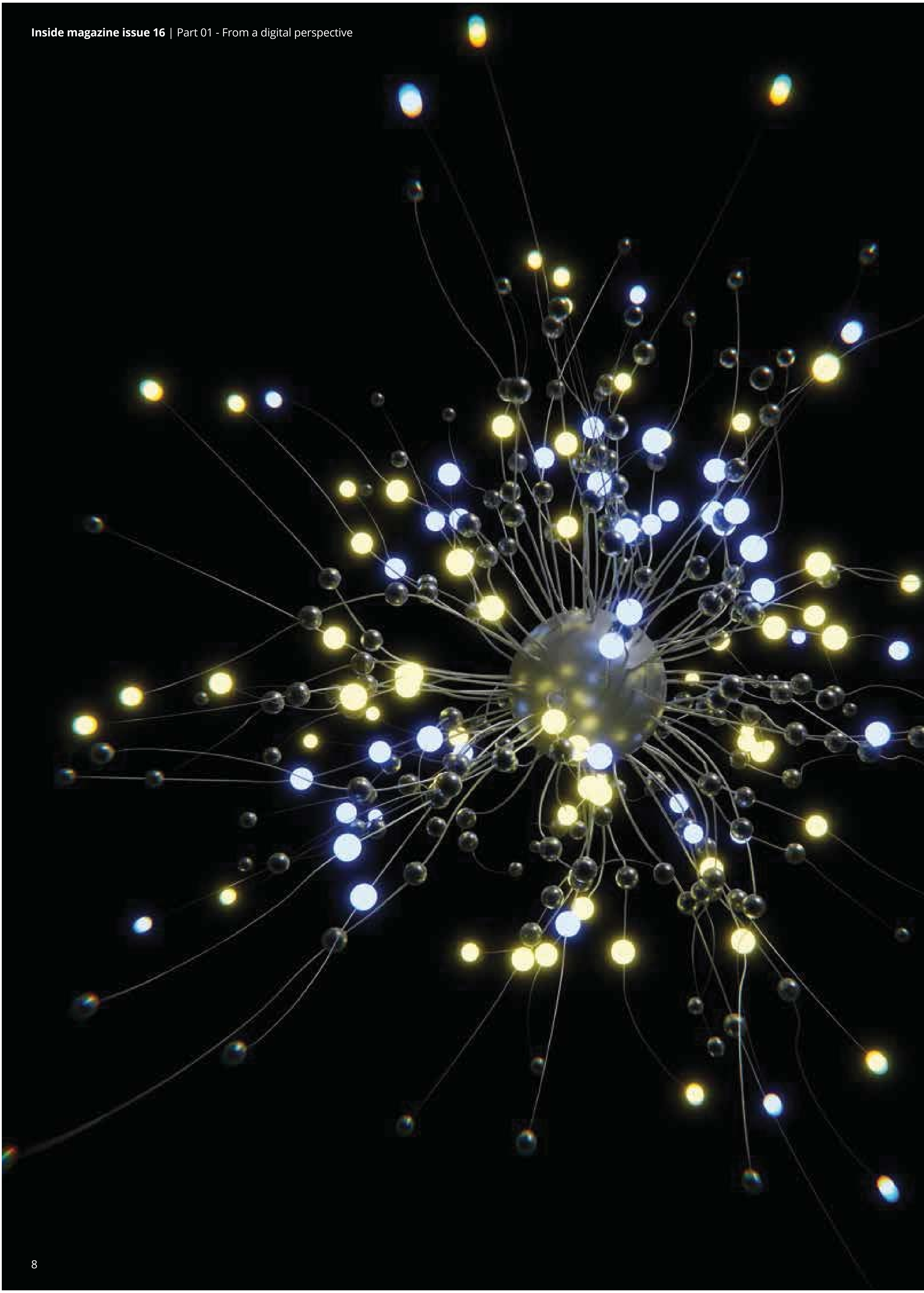
Stephen Marshall
Partner
Global FS Technology
Leader

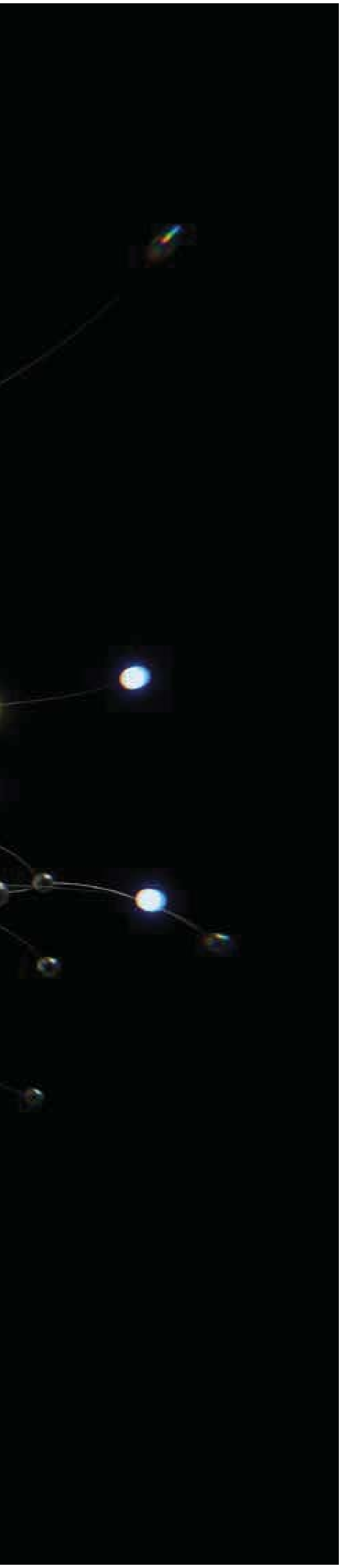
Patrick Laurent
Partner
EMEA FS Technology
Leader

Harry Goddard
Partner
EMEA Technology
Leader

Part 01

From a digital perspective





What makes a successful FinTech hub in the global FinTech race?

Louise Brett
Partner
Fintech Leader
Deloitte

Financial technology, or FinTech, refers to the application of disruptive technologies in the financial services industry. Although FinTech is not new, it has been under the spotlight in recent years as advances in exponential technologies and new business models have challenged existing products, services and processes, and enabled faster, cheaper or more engaging solutions to be created. FinTech innovations can come from both start-ups and incumbent financial institutions.

A FinTech hub is the focal point for FinTech activity within a region or a network. It is the ecosystem encompassing the entire infrastructure, organizations and people within the hub, as well as how those elements are organized and engage with each other. Hubs are often defined as cities, as is the case with this article, but can also be wider regions (e.g. Silicon Valley), countries, or narrower locations (e.g. Level39 in London).

Just as organizations have distinctive traits that differentiate them from competitors and peers, FinTech hubs possess inherent attributes that make them unique based on their history and local intricacies. However, as with organizations, there is a common set of identifiable and interrelating factors that contribute to the overall success of the hub.

In this article, we look at the key factors contributing to the success of FinTech hubs across the globe and draw a connection to the key factors that CIOs and management need to consider when creating an innovative environment in their organizations.

Four key factors contributing to the success of FinTech hubs

In partnership with the Global FinTech Hubs Federation, Deloitte released the Connecting Global FinTech report in April 2017[1] that analyzed 44 hubs from around the world according to a number of qualitative and quantitative factors. These factors comprise the fundamental building blocks for a hub to thrive, and include:

Talent **Capital** **Demand** **Policy and Regulation**

Overall, we found that the strength of a FinTech hub is directly related to the ability of FinTech organizations to access talent, capital, and demand, as well as the effectiveness of progressive policies and regulations designed to enable FinTech growth.

01. Talent

The ability to attract, develop and retain talent in three key domains is crucial to a FinTech hub's success on a global scale. These domains are:

- Finance

  Domain expertise within financial services: an understanding of not only the products and services but also the pain-points and opportunities within existing processes.

- Technology

  Technical expertise: the ability to develop the software and hardware required to turn ideas into solutions.

- Entrepreneurship

  Less tangible than the other two domains, entrepreneurial talent is the ability to identify commercial opportunities and bring together resources required to materialize ideas. This is a key factor that distinguishes successful hubs from less successful ones.

Peripheral talent pools are key as well; legal, marketing and business development skillsets all serve to bolster the talent mix within a hub. This mix, in turn, nurtures a culture of innovation that is an extremely powerful pull factor and serves to attract and retain talent on a global stage.

Although our report found that most European hubs agreed there is good access to talent within their hubs, access to talent was less consistent across other areas of the globe. In particular, a number of emerging hubs across Asia cited a technology skills shortage (specifically software developers and engineers) as a specific challenge in their hub.

With the recognition of the importance of developing and sustaining the talent pipeline, some hubs have implemented specific policies and programs to improve access to FinTech talent. Examples include the UK's Tech Nation Visa, which enables tech talent from across the world to work in the UK's digital technology sector, and Hong Kong's FinTech Career Accelerator Scheme, a government-led program that co-ordinates the placement of highly educated students in financial services organizations, FinTech start-ups and regulatory authorities.

Once hubs have established themselves globally, they have the natural advantage of becoming a magnet for talent and creating a virtuous cycle of attracting and retaining talent. Creating this 'culture of innovation' is an organic and unpredictable attribute for a hub to attain; and leads to different niches and strengths across hubs. For example, talent from army-trained technicians in Israel have enabled the hub to lead in cyber security FinTech innovations.

[1] http://Deloitte.co.uk/fintechhubs

02. Capital

Start-ups need access to seed and scale capital to develop and grow their ideas, and will move to where they can raise investment. Therefore, access to capital, whether it comes from private investors (e.g. angel investors, venture capital, and private equity communities), governments or corporates, is a key driver of FinTech activity across hubs. As Venture Capital (VC) investment deals are the best documented of these sources of capital, they are viewed by the industry as a credible barometer for the state of FinTech activity across hubs. Higher values and volumes of VC investment activity is therefore a proxy for higher levels of FinTech activity.

In addition to start- and scale- up funding for FinTech companies, investment is also required to fund initiatives such as not-for-profit accelerators, sandboxes and incubator programs that foster collaboration within the FinTech ecosystem.

In some areas, entrepreneurial patriarchs who have actively built and exited companies also serve as a strong source of capital, re-investing further into the hub. Peter Thiel and Elon Musk in Silicon Valley are examples of this trend.

Globally, US$17.4 billion of VC investment was put in to FinTech across 1,436 deals in 2016. China and the United States accounted for the majority of these investments, with US$7.7 billion and US$6.2 billion being invested respectively.

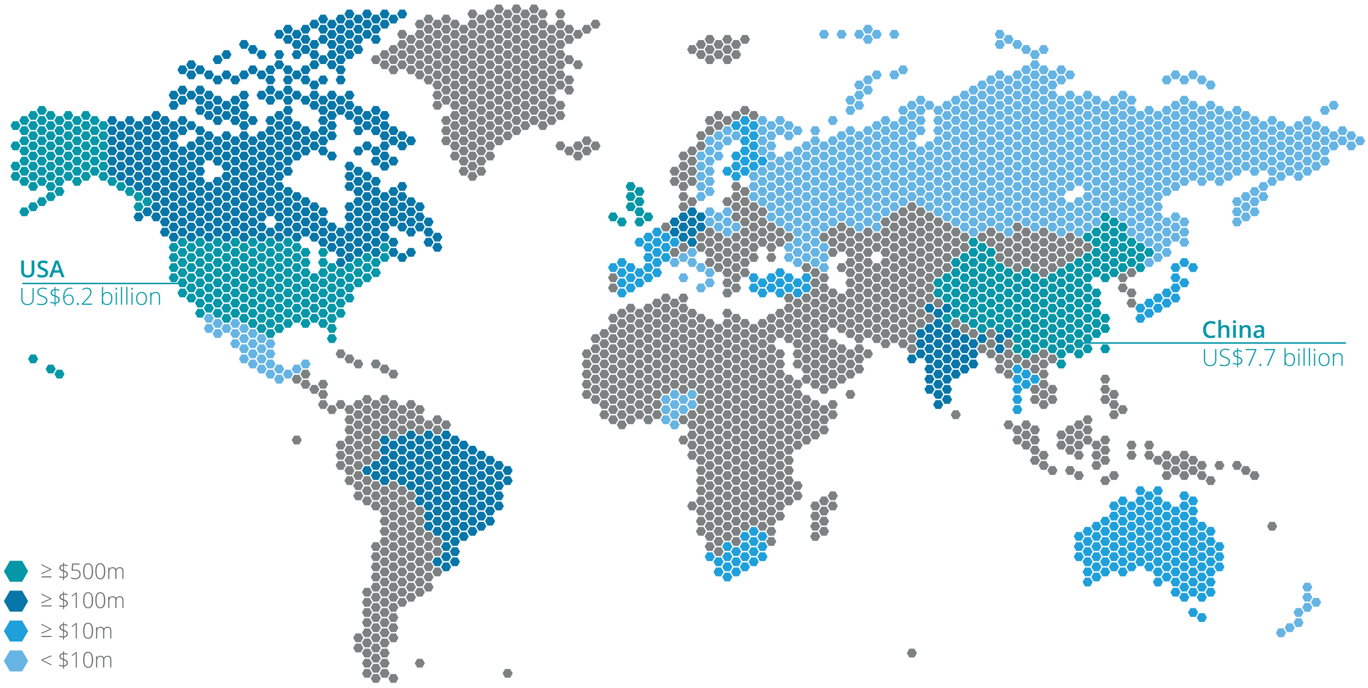
Since a large value of VC investments come from a small number of hubs, it's unsurprising that our report found 32 percent of hubs surveyed identified low access to capital as a primary challenge in their hub, while 25 percent cited low exit opportunities as a major challenge.

However, on a positive note, a more recent report issued by Innovate Finance in July 2017[2], shows that in the first half of 2017, VC investment from countries other than China increased significantly. Excluding exceptional "mega-rounds" of Chinese investments in 2016, global VC investment in FinTech in the first half of 2017 increased by over 28 percent year on year.

FinTech investment globally is expected to continue increasing in the near-term and access to capital is expected to improve as investors become more familiar with FinTech innovations.

FinTech investment globally is expected to continue increasing in the near-term and access to capital is expected to improve as investors become more familiar with FinTech innovations.

Global Fintech VC deal value 2016[3]



[2] http://new.innovatefinance.com/reports/h1-2017-vc-fintech-investment-landscape/

[3] Deloitte "Connecting Global FinTech" report

03. Demand

As with any other industry, demand drives supply in the FinTech space. Demand for FinTech products can come directly from consumers (business-to-consumer or B2C) or other businesses (business-to-business or B2B).

The more established a financial services industry is within a hub, the more likely it is for the hub to have a stronger FinTech market. This is because consumers within those markets are likely to be more educated about financial products and are therefore less averse to trying new financial products and services. Secondly, established financial institutions looking to expand or improve their own offerings can provide a source of investment for B2B FinTech companies. This is why, for example, Barclays has invested in setting up its RISE program in key financial services centers such as New York and London.

Although this generalization is true for the major financial hubs noted in our report such as London, New York, Chicago, San Francisco, Hong Kong and others, a strong financial services industry does not always equate to a strong FinTech hub. For example, although Tokyo has a strong financial services industry, regulation and other factors have meant that FinTech has been slow to take off, compared to some of the other financial hubs.

Our report also found that most hubs surveyed from across the world believed they have good access to FinTech demand. However, around a third of hubs identified that much of the demand comes from outside of their local markets, thus highlighting the global nature of FinTech. This was particularly in the case of smaller hubs, such as Lisbon, or more geographically remote hubs, such as Auckland.

04. Policy and Regulation

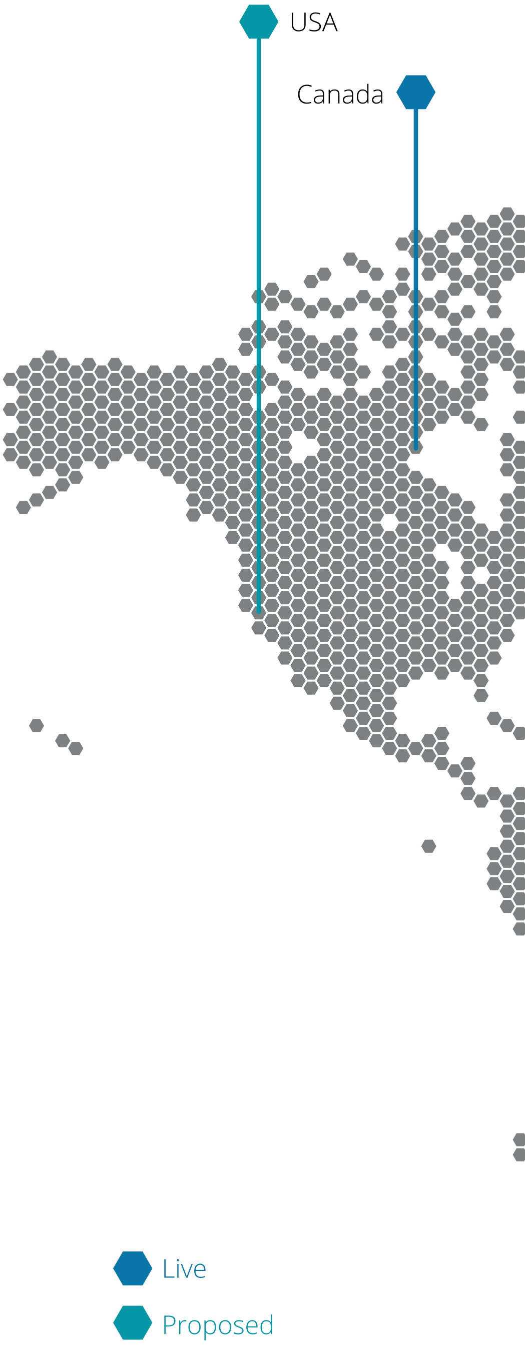
Policy and regulation are key factors that contribute to the success of a FinTech hub. Governments and regulators need to strike a balance between promoting innovation and effective competition, while protecting investors and consumers. These bodies provide the framework, policies[4] and procedures that both encourage and safeguard FinTech within the hub.

Testament to how important supportive regulations are to FinTech growth, are two of the world's leading FinTech hubs, London and Singapore, also known for their progressive regulatory bodies: the Financial Conduct Authority and the Monetary Authority of Singapore, respectively. These regulators have put in place initiatives that foster FinTech collaboration within their hubs such as FinTech offices, accelerator programs, international agreements and sandbox environments where FinTech and financial institutions can 'test' innovations in a safe production environment with less onerous regulations.

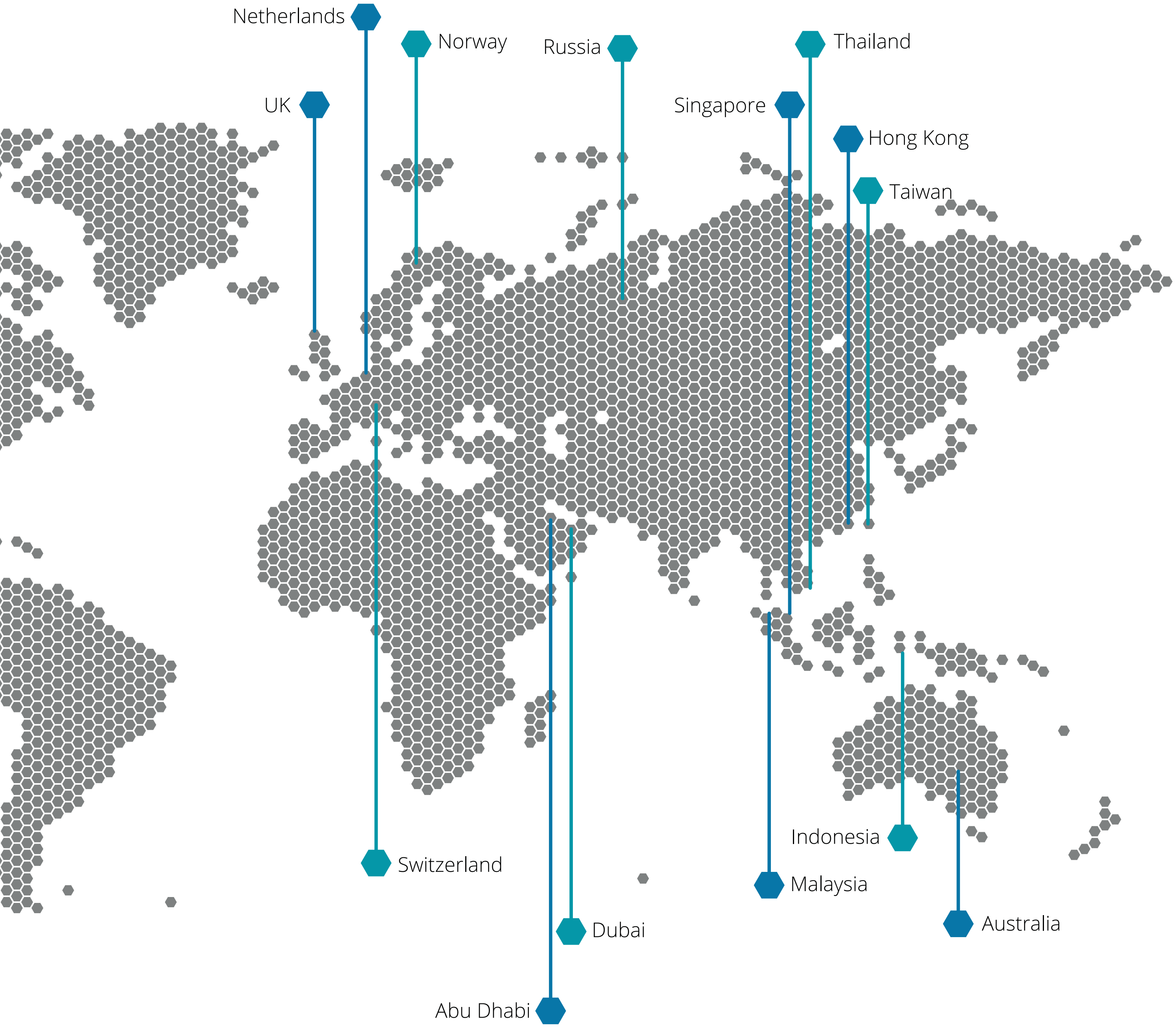
The FCA and MAS are regarded as pioneers, leading the new wave of FinTech growth. The UK in particular has benefited from first-mover advantage in setting up a regulatory sandbox to support FinTechs. However, with their model being adopted across the globe and as regulatory sandboxes and inter-regulator co-operation agreements become more commonplace, progressive regulators will need to continue regulatory reforms in order to maintain an edge in supporting FinTech growth.

Our report indicated that by March 2017, six regulators had replicated the FCA's and MAS' regulatory sandbox regimes in their jurisdictions while eight other regulators had proposed similar initiatives. By August 2017, a number of additional regulators had also announced sandbox regimes, e.g., Bahrain and Lithuania. The trend is likely to continue, especially given that the European Union Commission is presently reviewing the possibilities of a Europe-wide regulatory sandbox.

Regulatory sandboxes[5]



[4] For example, two substantial pieces of regulation that will come into effect across the EU in 2018 are the revised Payments Services Directive (PSD2) and General Data Protection Regulation (GDPR), which aim to put customers in control of their own data and keeping that data safe. More information on the impact of these regulations on FinTechs can be found here: http://blogs.deloitte.co.uk/financialservices/2017/08/psd2-and-gdpr-friends-or-foes.html



Regulator aside, governments also play an important role in supporting FinTech growth. The government in India, for example, has established policies and programs and provided investment to support the development of FinTech and start-ups in the country. The Start-up India program, which provides simplified regulatory processes, tax exemptions, patent reforms, mentorship opportunities and increased government funding for start-ups is one such example. Other initiatives led by the central government in India include the introduction of a nationwide Unified Payments Interface, a central digital identity base that enables e-KYC to be completed economically and the demonetization of bank notes in 2016 — all of which are expected to benefit FinTech growth.

[5] The European Union Commission are expected to publish their FinTech action plan in the fourth quarter of 2017. Source: http://europa.eu/rapid/press-release_MEMO-17-1528_en.htm

As a CIO, what does this mean for me?

As can be seen above, the success of FinTech hubs depend on a variety of interdependent factors. While there is no magic formula, we discussed four key factors that need to be taken into consideration when creating a successful FinTech ecosystem. These factors are equally important for management looking to create a supportive environment for FinTech innovations within their organizations.

The more established a financial services industry is within a hub, the more likely it is for the hub to have a stronger FinTech market.

Talent

Just as successful hubs need to secure a pipeline of FinTech talent, innovative organizations need to develop FinTech competencies through a combination of attracting new blood, training existing talent pools and creating an environment that retains high-caliber innovators and technologists and begins to adopt the DNA & start-ups.

Key considerations for CIOs and management:

- What are the talent gaps in your organisation? How are you going to address those?
- How do you develop a culture and set of performance metrics and frameworks that attracts and retains, rather than drains, talent?

6. http://annualreport2013.volkswagenag.com/group-management-report/sustainable-value-enhancement/research-and-development/key-r-d-figures.html
7. https://www.statista.com/statistics/314863/research-and-development-expenses-of-tesla/

Capital

In the same way that access to capital investment can make or break a start-up's success, the ability for innovative teams to access internal funding and resources is crucial to an organization's ability to innovate. On the flip side, simply throwing money at 'innovations' does not guarantee success and organizations with the largest innovation funds are not always the most successful. For example, although Tesla is widely regarded as a forward-thinking innovative company, Tesla reportedly only spent US$232 million on R&D in 2013[6], in contrast to automotive competitor Volkswagen's reported 2013 R&D spending to be US$13 billion[7].

Key considerations for CIOs and management:

- What funding is available for innovative initiatives?
- How are investments structured?

Demand

If there is no demand, there is no viable product or service. Successful innovative organizations pay attention to their customer's needs and know where and how they fit in their customers' lives. More than that, successful organizations know where other companies' products and services fit in their customers' lives and know when to partner with other parts of the ecosystem to provide a seamless experience for their customers.

Key considerations for CIOs and management:

- How well do you know your customers? And the wider ecosystem?
- What networking or partnering opportunities are there? What is the process for establishing collaboration opportunities?

Policies and Regulations

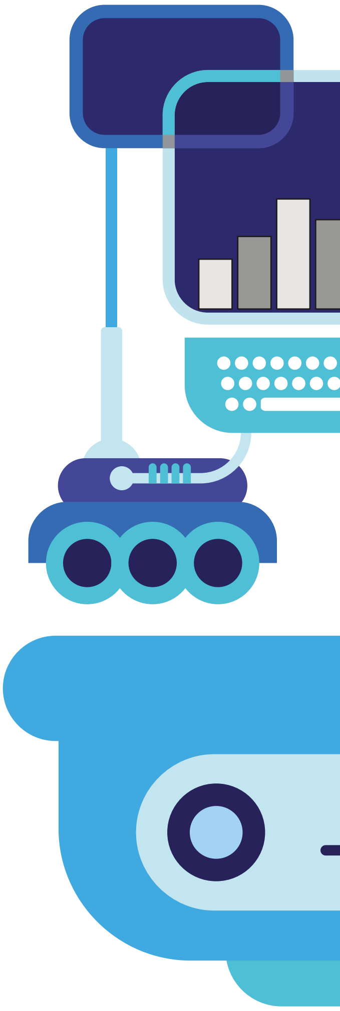
As we saw previously, policies and regulations can both enable or constrain FinTech developments within hubs. Governance structures, policies, and procedures all serve to support or restrict an organization's ability to innovate. Successful organizations need to balance, on the one hand, robust governance and controls to manage risk and compliance with regulations, and on the other hand, flexible procedures and policies that support rather than stifle innovations.

Key considerations for CIOs and management:

- What are the risks and governance processes in place to make decisions?
- What are the reporting lines for innovation arms or acquisitions? Are there conflicting governance models and policies between innovation practices and the main organization?

Compliance and Competitiveness

Why open banking may be the solution for banks



Pascal Eber
Partner
Operations Excellence &
Human Capital
Deloitte

Ronan Vander Elst
Partner
Deloitte Digital
Deloitte

Alexandre Havard
Senior Manager
Operations Excellence
& Human Capital
Deloitte

Esther Bauer
Manager
Strategy, Regulatory &
Corporate Finance
Deloitte

Andy Fossion
Consultant
Deloitte Digital
Deloitte

As the European Union tries to respond to an ever-evolving payment landscape in Europe through the Revised Payment Services Directive (PSD2), banks are facing important challenges while trying to be compliant. The legislation created a panoply of opportunities, but also challenges, from a strategic, organizational, and technological perspective. As banks try to navigate this maze, they will need to reconsider their operating models and how open banking may be the next logical step.

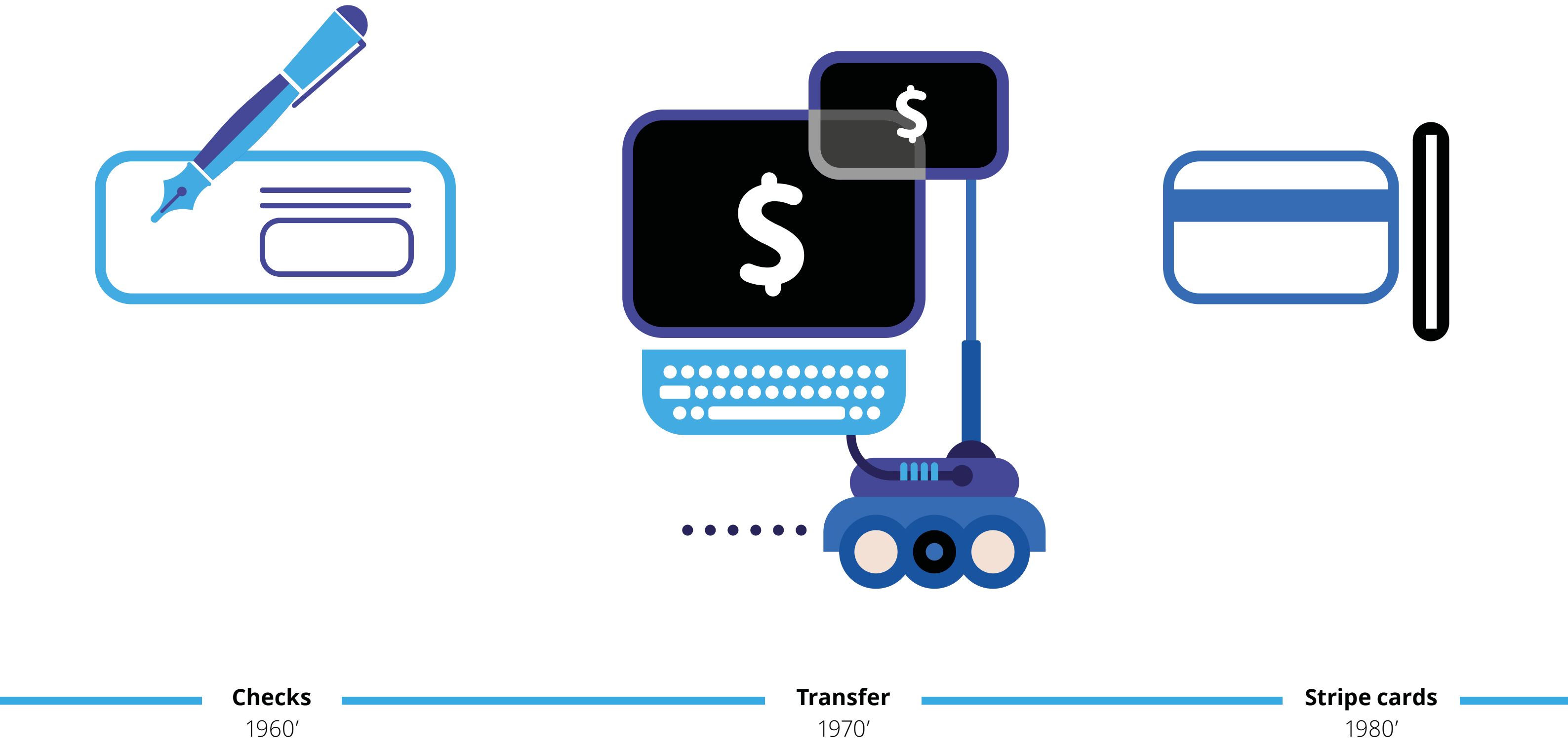
Payment initiation service providers (PISP) intiate payments between the payee’s and payer’s accounts and account information service providers (AISPs) aggregate information between customers’ payment accounts.

PSD2 – Regulating innovation and change

Throughout history, humans have had payment systems that allowed them to trade goods. These have been subject to evolution over time, moving from simple bartering, grains, or shells to gold-backed currencies. Over the past few years, this evolution has accelerated rapidly.

These new payment systems imply a number of new challenges. In an effort to respond to these changes and encourage competition and innovation, the European Union put into place the Revised Payment Services Directive (PSD2).

PSD2 will open the market to new payment players and extend the scope of services, increasing competition with the aim to encourage innovation, rapidity, efficiency, and safety in payments. Specifically, two new types of third parties will be able to participate in the market: Payment Initiation Service Providers (PISPs), to initiate payments between the payee’s and payer’s accounts, and Account Information Service Providers (AISPs), to aggregate information between customers’ payment accounts. The provisions of PSD2 imply a number of challenges for banks that need to be addressed sooner rather than later.

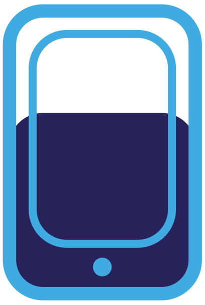


New types of competition will nibble on banks' margins and banks' customer basis

Agile and flexible non-bank players have already entered the payment services market, such as Amazon, eBay, and Facebook, without the need to maintain heavy banking infrastructure nor comply with complex legislations. They will now have access to parts of banks' infrastructures and data, which banks will be required to share through APIs (Application Program Interfaces). They will position themselves in attractive niche markets benefiting from excellence in customer experience and lower cost bases than banks. Non-bank players (especially merchants) will be able to cherry-pick and focus on the most profitable services.
As new players will be able to provide information and payments services, customers will have broader access to formerly traditional banking services, like advice on their financial situation, debt, credit, and other general questions.[1]
Indeed, requesting a loan or benefiting from financial advisory would make more sense with an aggregated view on all of the customer's assets.

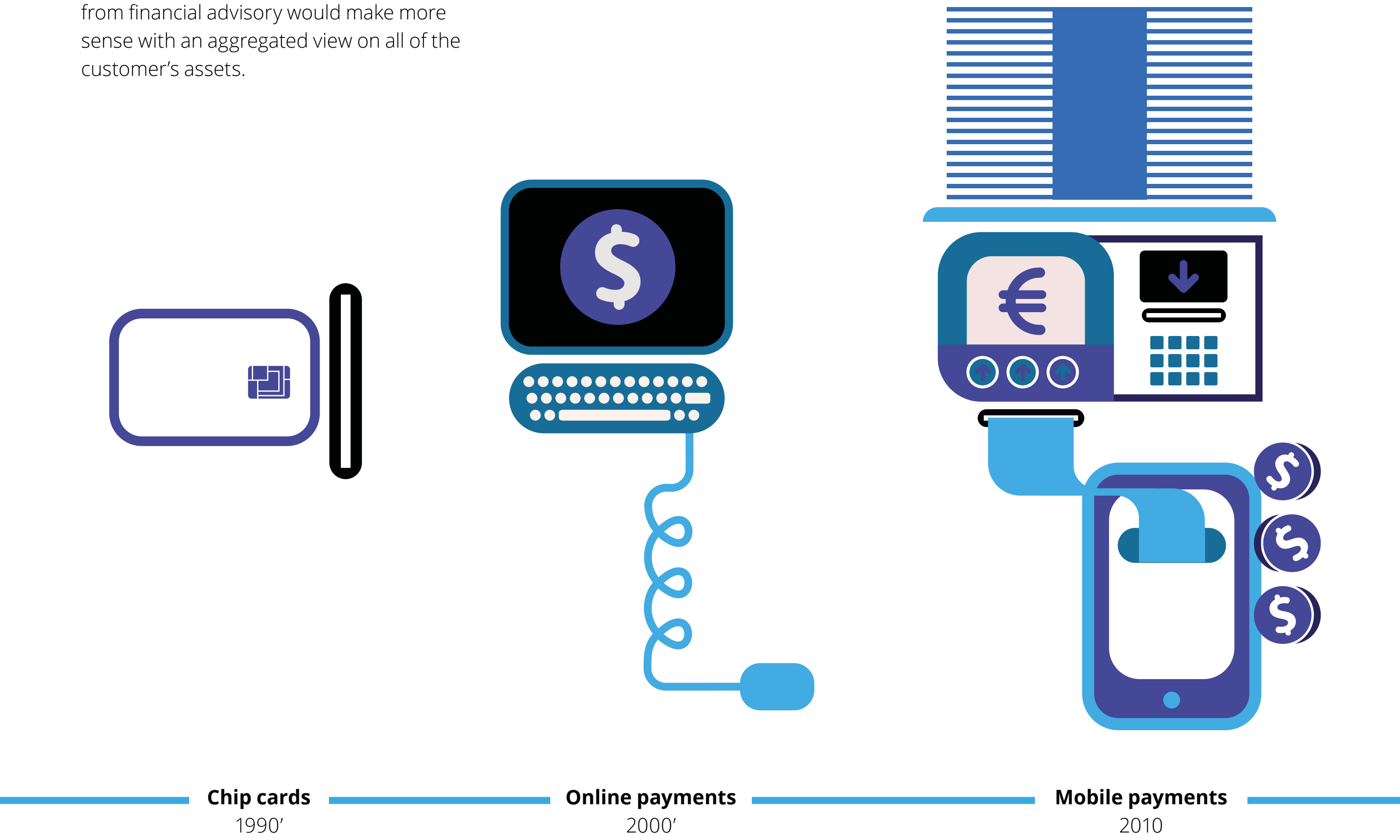
This is a real danger to banks margins, but also banks' customer bases. A recent survey that was carried out by Deloitte in a European country shows that 58 percent of consumers with mobile banking applications would be willing to change to a mobile-only bank to have the ability to perform a greater number of banking-related services. Additionally, 49 percent stated they would trust digital payment services providers, and respectively 43 percent retailers, to access banking services.[2]

Consumer willingness to switch



58%
of consumers with mobile banking applications would be willing to switch to a mobile-only bank

Source: Deloitte



[1] Open banking – A consumer perspective, Faith Reynolds, January 2017

[2] Deloitte – How to flourish in an uncertain future – Open banking

Bank business models will need to evolve and collaboration will foster competitiveness

Banks will be able to react to PSD2 by either complying or competing. In this context, banks need to decide their future business model. They will need to define whether they want to position themselves as one-stop-shop advisers competing with innovative new players in the banking world or become specialists focusing on being balance sheet providers, innovators, or infrastructure providers.[3] One-stop-shop providers face risks and challenges through new competition as well as the opportunity to take advantages of the possibilities available through teaming up with FinTechs and other innovative companies. These banks will essentially need to find ways to drive revenue by enhancing service offerings at minimal costs, and building on capabilities that are available to them through new technological advances. One-stop-shop banks will be able to benefit from aggregating services to enhance customer value and customer experience, being able to compete with FinTechs and challenger banks. For example, they will be able to leverage the precious amount of information that will be accessible through APIs upon customers' request, giving customers a global view on all transactions or monetizing this information to merchants for their own marketing and targeting strategies.

The current state of regulation and the market are still frightening for banks, especially considering the blur around savings and securities accounts. The framework defined by PSD2 is only partial, resulting in only payment accounts being included or not clearly defined standards for APIs. The numerous questions that remain, make grasping the existing opportunities complex and some banks may lose courage when faced with this situation.

Let us look at the example of unknown API standards for example. Today this is already generating worry and leading to thoughts on how they can be standardized in the future (e.g., Berlin group, Open banking working group). At the same time, FinTechs such as Yodlee and Budget Insight have created extremely flexible solutions that allow the aggregation of accounts beyond payment accounts. By working together with companies that have embraced this uncertainty and complexity in their DNA, banks can take advantage of the opportunities of today's environment.

This example provides just a quick glance at the enormous scope of opportunities that may arise once banks venture into open banking. By changing their business models from closed models that consider data as proprietary structures toward open models that embrace collaboration with other players, open banks will be able to deliver new value to customers and be more competitive compared to traditional closed banks.

Organizational impacts will be significant and will pose challenges to banks

PSD2 requires banks to implement significant changes. These changes include compliance requirements, such as the opening of APIs and new security requirements linked to SCA (Secure Customer Authentication) requirements. Furthermore, if banks decide to compete rather than just comply, further countless new activities will result, including integrating partnerships with innovative companies that may have completely different ways of functioning and governance; the need to treat and exploit new data (e.g., obtained from other banks or other companies) requiring big data capabilities, or developing new in-house solutions for automation. In order to be able to address these choices and pursue the strategy chosen by banks, decision makers will need to reevaluate and adapt HR and IT strategies to these new demands.

From a compliance perspective, specific regulatory and technical expertise within organizations as well as adapted IT-infrastructures and financial resources will be required. At the same time a myriad of other regulations, including GDPR[4] and MiFID II,[5] have similar demands in terms of resources, and banks face Sophie's choice in terms of prioritization of projects, generating a need for trained resources that can be complicated to address.

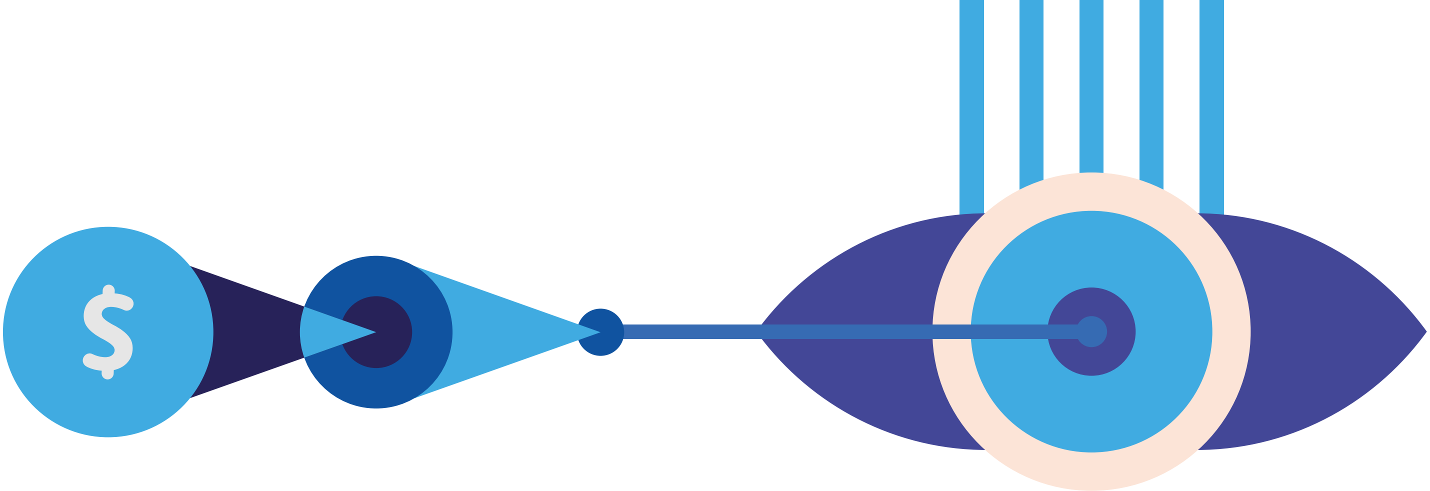
When going beyond pure compliance, these requirements become even more pointed. To compete with innovative players, banks will need to further develop existing capacities including change management, digital IT, and architecture, and also acquire new capabilities such as customer experience and user experience to be able to ensure that their digital (and non-digital) experience is on par with innovative players.

The current state of regulation and the market are still frightening for banks, especially considering the blur around savings and securities accounts.

[3] Please refer to Inside Magazine Issue 15 – The future models of banking in Europe, available at https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu-the-future-models-banking-in-europe-062017.pdf for more details

[4] General Data Protection Regulation

[5] Markets in Financial Instruments Directive II



Open banking – shifting from closed to open banking models

Open banking will represent a paradigm shift in today's world. While today, products, services, functions, and data are treated as proprietary, the world of tomorrow will see bank products, services, functions and data shared for use with third parties that will aim to create benefit for customers and new business values.[6] Incumbent banks that embrace open banking in order to be able to compete, may be able to create new sources of revenue and may benefit from significant advantages given their strong expertise, brands, and trust, as well as access to an existing client base.

Deutsche Bank and Nordea are just two examples that highlight how compliance and competiveness with third parties are not mutually exclusive and have opened websites for developers to experiment and test with ideas and APIs.

- Deutsche Bank's dbAPI interface provides access to the bank's proprietary environment to allow developers to test their ideas and innovations using anonymized banking data. The creation of this portal goes hand-in-hand with another initiative—the hackathon—which is a three-day event allowing developers to test their APIs for three days and allowing the winning team to collaborate with Deutsche Bank's Digital Factory.[7]
- Nordea has launched an API platform that aims to meet PSD2 requirements, but also seeks to capitalize on PSD2 to advance open banking. The bank provides a first iteration of a portal and community hub for developers with access to a sandbox environment and APIs in order to encourage collaboration with third parties and innovators.[8] Initial APIs available include the account information service and the payment initiation service API

Fidor goes even further, putting open banking at the heart of their business model. Fidor (bought last year by BPCE) was founded with the idea to propose a dedicated operating system (fidorOS) with APIs to manage all features that a customer requires in his daily banking life. The idea behind Fidor is to promote open and transparent banking and therefore to leave the possibility for customers to manage their data through any other application that could propose value-added services and improve the banking services.

Deutsche Bank, Nordea, and Fidor are only some examples of banks that are experimenting with open banking to deliver benefits to end customers. Today a number of banks and other players are already daring to make a first shift toward open banking and it is likely that in the future other banks will follow—sooner or later. The three banks show how differently organizations can take advantage of the opportunities of PSD2 and open banking to collaborate in order to remain competitive.

> Incumbent banks that embrace open banking in order to be able to compete, may be able to create new sources of revenue

[6] Open Banking: What Does the Future hold? Deloitte Digital, April 2017

[7] Deutsche Bank

[8] Nordea Bank

Cognitive Intelligence to boost Digital Transformations in FSI

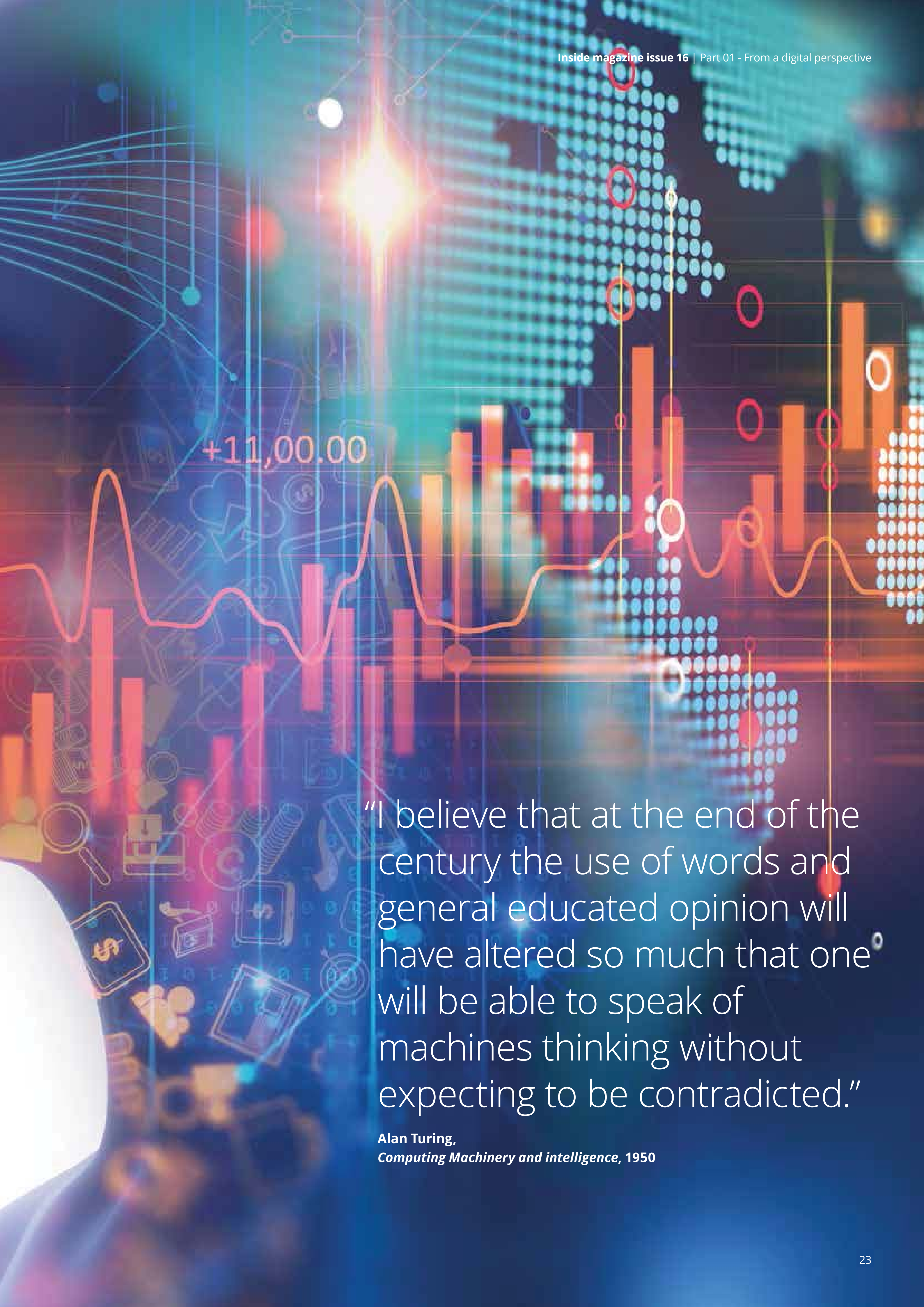
Ronan Vander Elst
Partner
Deloitte Digital
Deloitte

Paolo Gianturco
Partner
FSI Technology
Deloitte

Maxime Gaborieau
Consultant
Technology & Enterprise Application
Deloitte

Still considered science fiction a few years ago, Artificial Intelligence (AI) is now becoming a part of our business environment, just as Alan Turing had predicted. AI is reinventing the entire ecosystem of the Financial Services Industry (FSI) with new business models designed to be more effective, accurate, and self-adaptive. By increasing the level of automation and using dynamic systems, AI supports decision management, enhances customer experience, and increases operational efficiency.

This article deals with the potential implications and applications of AI in the FSI. First, a general presentation will demystify AI. Then, a second part will describe some applications in FSI and more specifically an AI-powered chatbot dealing with MiFID. Finally, we will focus on the outputs and actionable insights for CIOs.



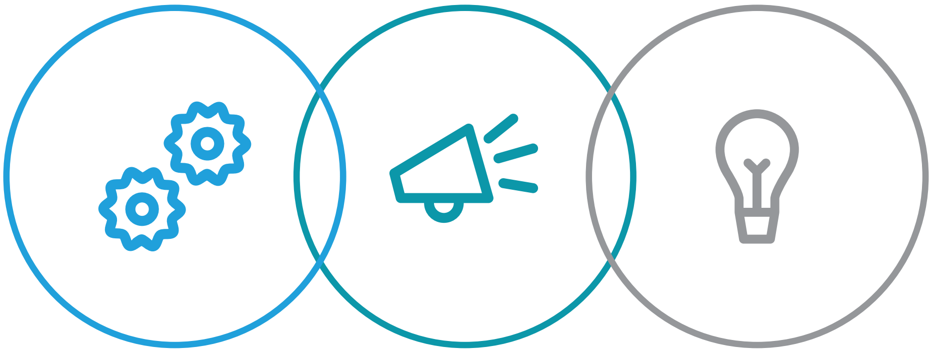
“I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted.”

Alan Turing,
***Computing Machinery and intelligence*, 1950**

> "Artificial Intelligence is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."
>
> **John McCarthy, Stanford University**

Demystifying Artificial Intelligence

AI encompasses, among other things, cognitive automation, cognitive engagement, and cognitive insights:



Cognitive automation
Enable machines to replicate human actions and judgment with robotics and cognitive technologies[1]

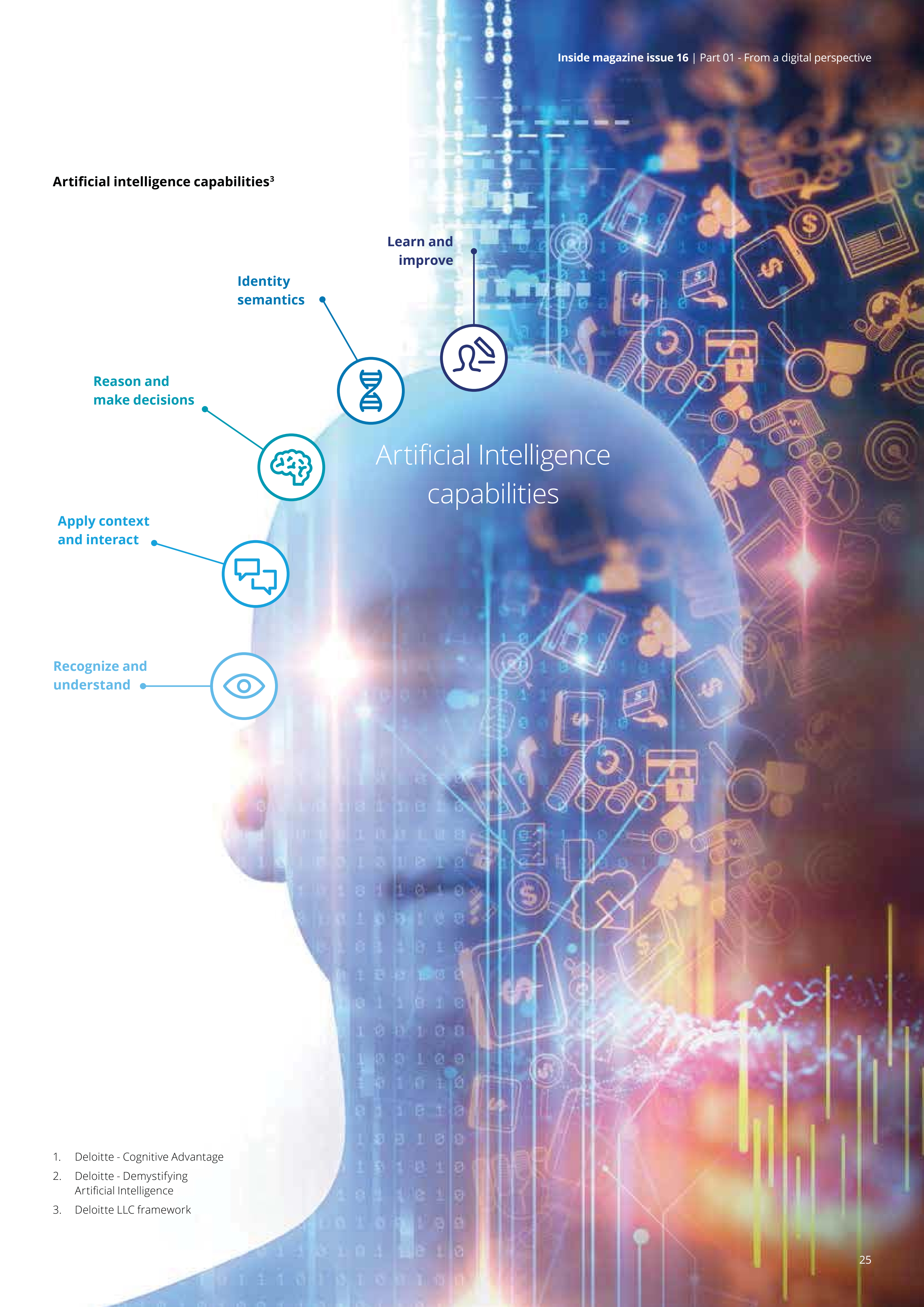
Cognitive engagement
Use intelligent agents and avatars to deliver mass consumer personalization at scale and smarter, more relevant insights to amplify end user experience[1]

Cognitive insights
Employ data science and machine learning to detect critical patterns, make high-quality predictions, and support business performance[2]

Thanks to cognitive intelligence, AI-powered systems are able to mimic some aspects of human intellect by:

- **Recognizing and understanding elements** for which they are programed. This is the first step of cognitive AI. For example, syntax of a text, shapes in handwritten text, figures or faces on an image or a video, syntax of voice, and much more.
- **Applying context and interactions** The capacity to represent links between different pieces of information. For example: "Bob is a dog. Dogs are animals. Dogs hate cats."
- **Reasoning and making decisions** Consists of interpreting the information recognized, possibly by making links with context. Then, decisions are made based on AI insights.
- **Identify semantics** Reasoning and making decisions also works as an enabler to identify the meaning of information recognized. For example, the sentence "I am going to the bank" can have two meanings (the establishment or the riverbank), it is necessary to know the context and to make a link to better understand the meaning of this sentence.
- **Learning and improving** The last and most crucial step of cognitive AI is the function of learning from the data provided, but also from mistakes in order to self-improve. This capacity is referred to as machine learning.

Artificial intelligence capabilities[3]


Learn and improve
Identity semantics
Reason and make decisions
Apply context and interact
Recognize and understand
Artificial Intelligence capabilities

1. Deloitte - Cognitive Advantage
2. Deloitte - Demystifying Artificial Intelligence
3. Deloitte LLC framework

Major trends that are profoundly affecting FSI

Before focusing on specific AI use cases in FSI, this section will present the major trends that currently affect the financial services industry. The year 2017 seems to mark a turning point in FSI. Major trends are profoundly affecting this industry with digital transformation, which is revolutionizing business organizations.

Machine intelligence is one of the main technological trends[4] for 2017, helping companies to make better decisions thanks to AI capabilities.

[4] Deloitte University Press – Tech Trends 2017

Major trends in FSI

Digital Transformation in FSI

Exponential growth of data volume:
First, the increasing use of social networks and connected devices due to the Internet of Things (IoT) has led to an exponential growth of data volume

New players on the marketplace:
New players such as FinTechs and startups are entering the marketplace with innovative solutions

Increasing customer expectations:
Customers' needs are constantly evolving with increasing levels of expectations

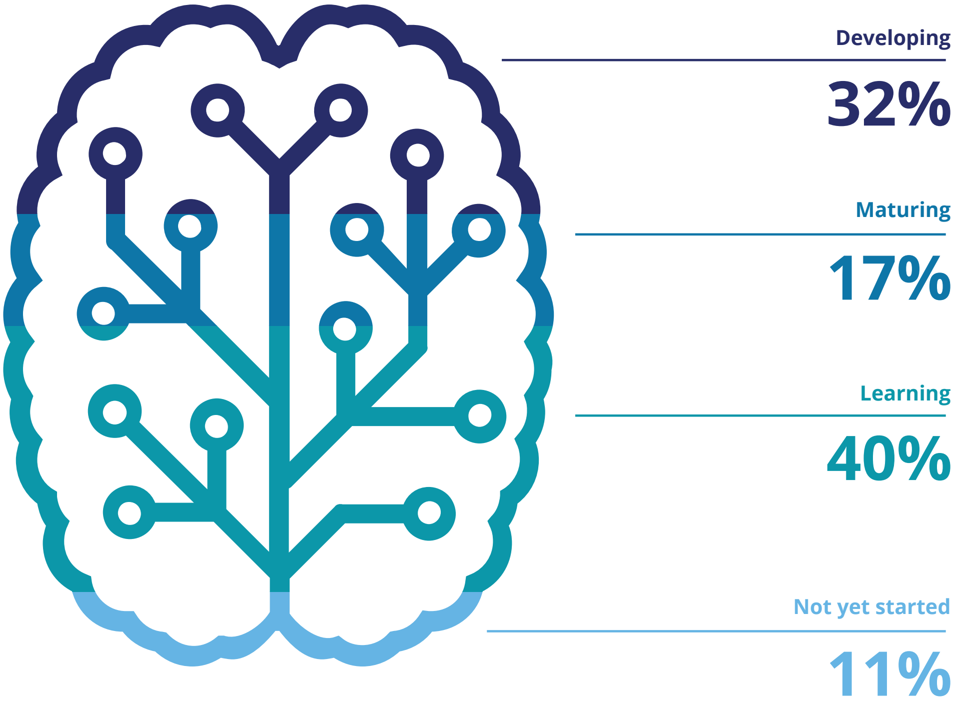
New risks: Innovative technologies simultaneously lead to new problems such as privacy and new risks such as fraud and cybercrime

New regulations: New regulations aim to limit the usage of personal data (e.g. General Data Protection Regulation) or to increase investor protection (e.g. MiFID II)

New technologies: Finally, new technologies deal with Big Data problems to help process large amounts of structured and unstructured data

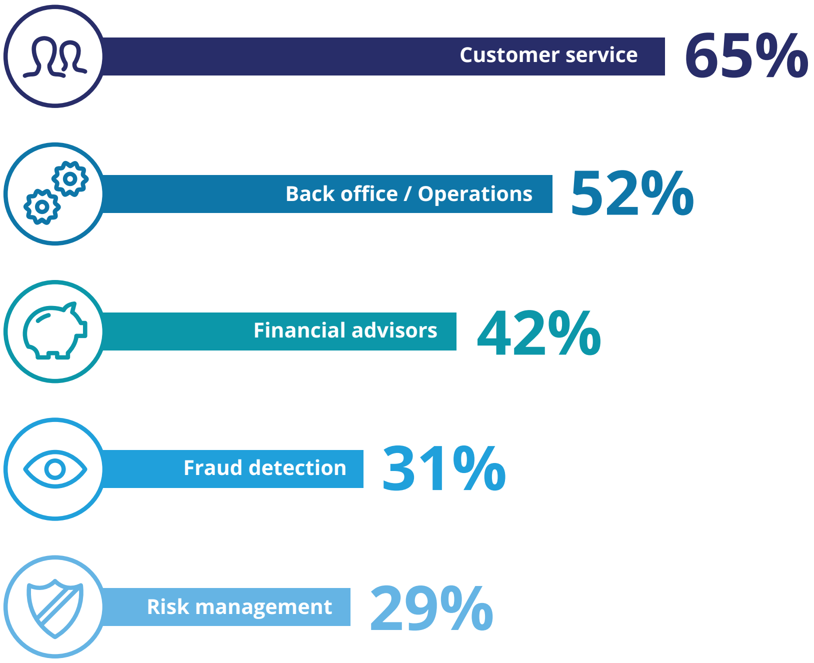
Most companies in the financial sector have already initiated their AI journey
Around nine companies out of ten have already started working with AI.[5] In 2017, 32 percent of companies in the banking industry are in the developing phase of their AI journey.

The AI journey in the banking industry (2017)[5]



Financial companies adopt AI with specific applications in mind, such as customer service, back office, operations, financial advisers, fraud detection, and risk management. In 2017, 65 percent of companies in the banking industry believed that AI would have a significant impact on customer service[5].

Top 5 impacts of AI on the banking industry[5]



[5] Deloitte – AI and you: Perceptions of Artificial Intelligence from the EMEA financial services industry

FSI case study: a chatbot for MiFID

This section will focus on one of the current hot topics in FSI that has a profound effect on customer service. The regulation Markets in Financial Instruments Directive II reshapes the FSI, and we investigate how AI can help financial players to deliver a superior customer experience while still being compliant.

MiFID II, reshaping FSI

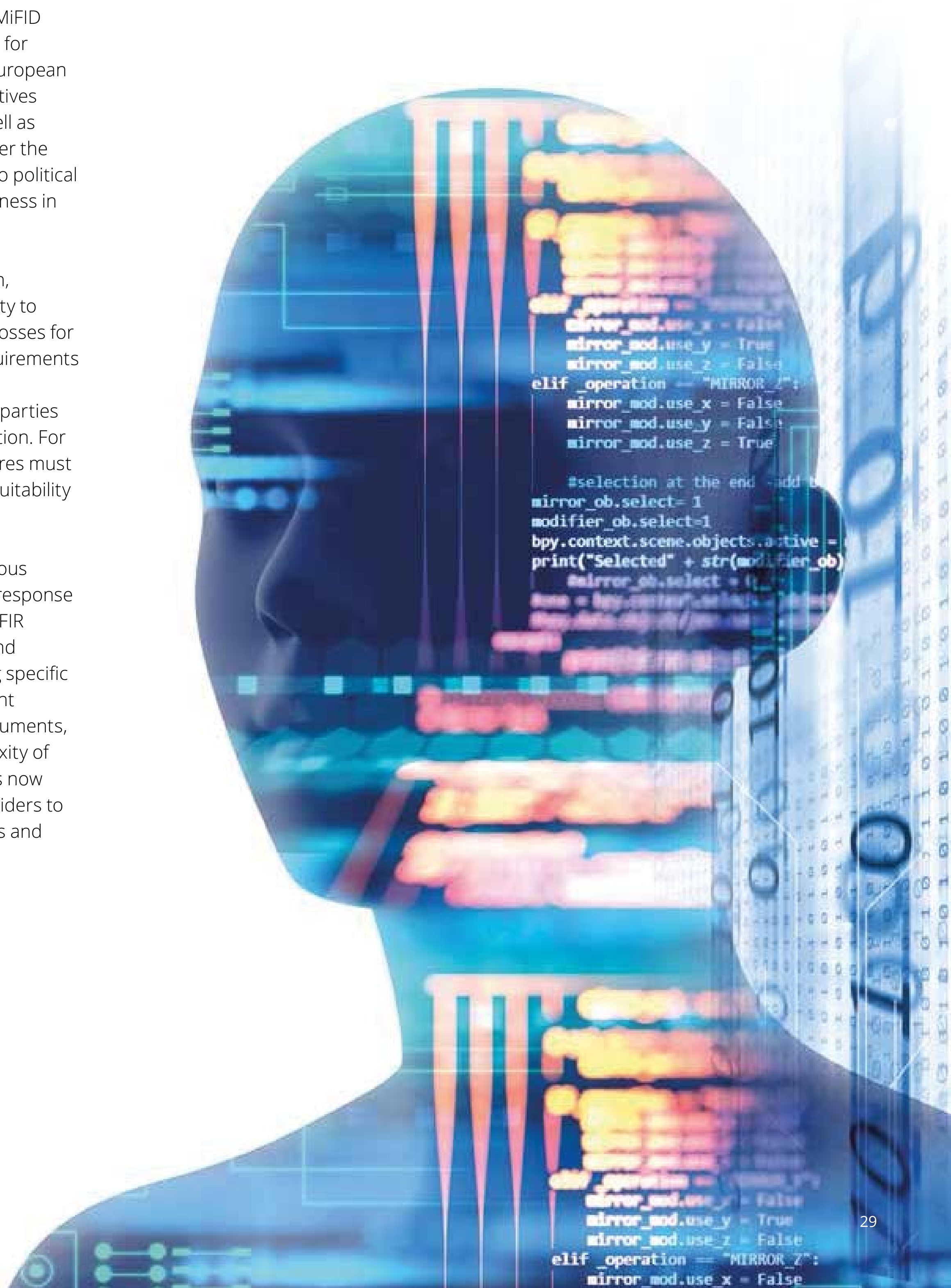
MiFID II is a reform of MiFID I that will enter into force in January 2018. MiFID I provides harmonized regulation for investment services across the European Economic Area. Its primary objectives are to increase competition as well as consumer protection, notably after the subprime crisis of 2008 that led to political change around safety and soundness in the financial system.

Focusing on consumer protection, MiFID II emphasizes the propensity to take risks and the ability to bear losses for consumers. One of the main requirements is to categorize clients as retail, professional, and eligible counterparties with an increasing level of protection. For each kind of client, clear procedures must be implemented to assess their suitability for a given investment product.

MiFID II is one of the most ambitious reforms introduced by the EU in response to the 2008 crisis. MiFID II and MiFIR reinforce consumer protection and securities markets by introducing specific rules such as best execution, client reporting, complex financial instruments, and more. Therefore, the complexity of these new laws and regulations is now prompting financial services providers to initiate comprehensive IT projects and operational changes.

Today, financial services providers implement MiFID procedures with questionnaires to gather the required information from their clients. A MiFID questionnaire is composed of three different sections:

1. Investment objectives of the client
2. Knowledge and experience of investors
3. Financial situation



A chatbot is a computer program that mimics conversations with users applying AI.

Why financial services providers should reconsider the way to tackle MiFID requirements
Currently, financial services providers use paper or electronic forms for the MiFID questionnaires. The MiFID questionnaires are particularly long and exhaustive (11 to 57 questions, depending on the bank). The time estimated to complete such a questionnaire is on average about 20 to 25 minutes. Moreover, the client may have some difficulties in understanding some questions, and this can lead to errors in the evaluation of the risk profile.

MiFID questionnaires can negatively affect customer experience if incorrectly implemented. Some common pitfalls include asking hard-to-understand questions or requesting too much information. In this context, chatbots can be used to improve experience for specific segments such as self-directed and digitally savvy customers.

A chatbot is a computer program that mimics conversations with users applying AI. Chatbots were initially limited to conversations about a specific topic but they are growing and diversifying with advanced functionalities. Chatbots can be used to tackle problems linked to the MiFID questionnaire. In the coming examples, we will see an application in relation to retail clients, however it is easily adaptable for professional clients or eligible counterparties.

Key functionalities of a chatbot
A chatbot can be embedded into any bank application. For example, when the customer has enough liquidity in his personal accounts, the AI-powered system will directly make the proposition to invest. The client has the possibility to interact with the chatbot to complete the mandatory MiFID questionnaire through an intuitive and user-friendly journey.

The solution synthetizes natural language text, extracting data from the user inputs at a rapid pace. The client's answers are stored in the database in order to create a full picture of client knowledge and experience, complete with risks and objectives. More precisely, the chatbot uses Natural Language Processing (NLP) to understand the customer's inputs.

Therefore, by chatting with the customer, the solution can gather information requested for the MiFID questionnaire and determine the profile of the investor.

Moreover, there is the potential to collect initial data directly from the user account in order to focus on questions that are more specific during the conversation.

The chatbot is a breakthrough in performing investment profiling by offering an innovative user experience for the MiFID questionnaire.

Main benefits of the chatbot

In this context, the chatbot is a breakthrough in performing investment profiling by offering an innovative user experience for the MiFID questionnaire. Indeed, it asks personalized and accurate questions to the client and from this is able to search for the available requested information and saves time by focusing on the client objectives. It can save time for financial services providers and for the customers by avoiding manual inputs of customers' answers but also because the chatbot can handle multiple conversations simultaneously. Moreover, this solution represents a key step toward paperless organizations.

The chatbot is very easy to adapt for financial services providers. It can be adapted to different kinds of questionnaires addressed to multiple types of customers (retail clients, professionals, eligible counterparties) and for different kinds of providers (retail banks, private banks). Its investor profile evaluation model can also be easily adapted if the provider wants to change the weight of one characteristic. This way, the chatbot is ready to handle any kind of change in the MiFID questionnaire.

User friendly and easy to adapt, this solution can be a real asset in the financial services industry by saving time for both financial services providers and customers, while providing digital and mobile solutions to their evolving habits, toward a simple and smarter interface. This endeavors to provide a great customer experience.

Key takeaways for CIOs

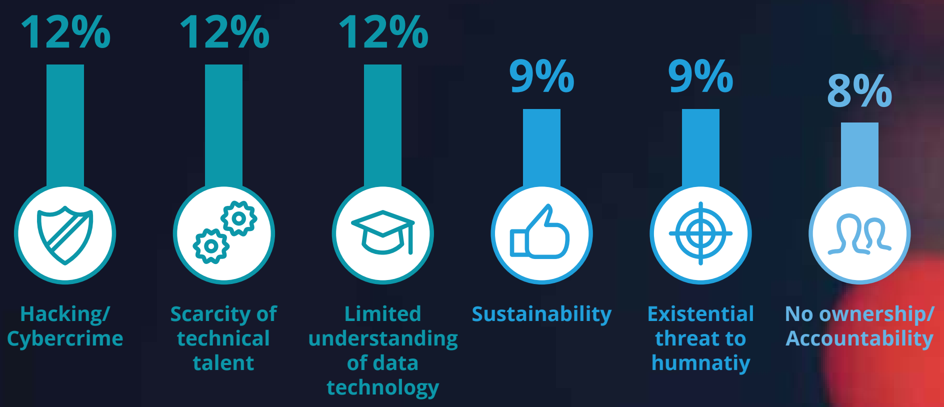
Major trends are profoundly affecting FSI, such as the exponential growth of data volume, evolving client expectations, the emergence of new risks, and increasing regulatory pressures. In this context, AI is reshaping the financial industry by enhancing customer experience, increasing the level of automation, and enabling organizations to derive deep and actionable insights to support decision management. Huge expectations are currently surrounding AI, and it could be the next breakthrough in the financial industry supporting digital transformations. Within the next three to five years, we expect an exponential increase in the number of AI-based applications.[6] Companies know the great potential that AI could bring. Most companies already started taking their first steps in their AI journey, by adopting technologies through proofs-of-concept to rapidly test new models for implementation.

Chatbots are becoming one of the most effective AI applications, which are becoming a privileged way to interact with customers across a large panel of industries, including FSI. They limit human intervention and the potential risk of operational errors. They can also provide a seamless customer experience, with natural language capabilities, sentiment analysis, and process automation. While providing a great customer experience with personalized advice and recommendations, chatbots also save time for financial service providers, enabling them to deal with the new challenges they are facing.

AI represents a key differentiation factor, unlocking benefits through operational efficiency and enhanced user experience. It is rapidly becoming a necessity to jump quickly onto the AI bandwagon to take advantage of this technological trend. Indeed, it enables to achieve competitive advantages through automation, cost optimization, insight-driven decisions, and customer experience enhancement.

Nevertheless, despite the disruptive potential of AI, key challenges need to be tackled in order to unleash its true power. Main concerns related to AI implementation in FSI are identified in a survey published in 2017 by EFMA and Deloitte,[7] such as hacking and cybercrime, scarcity of technical talent, and limited understanding of data technology.

Main concerns about Artificial Intelligence[7]



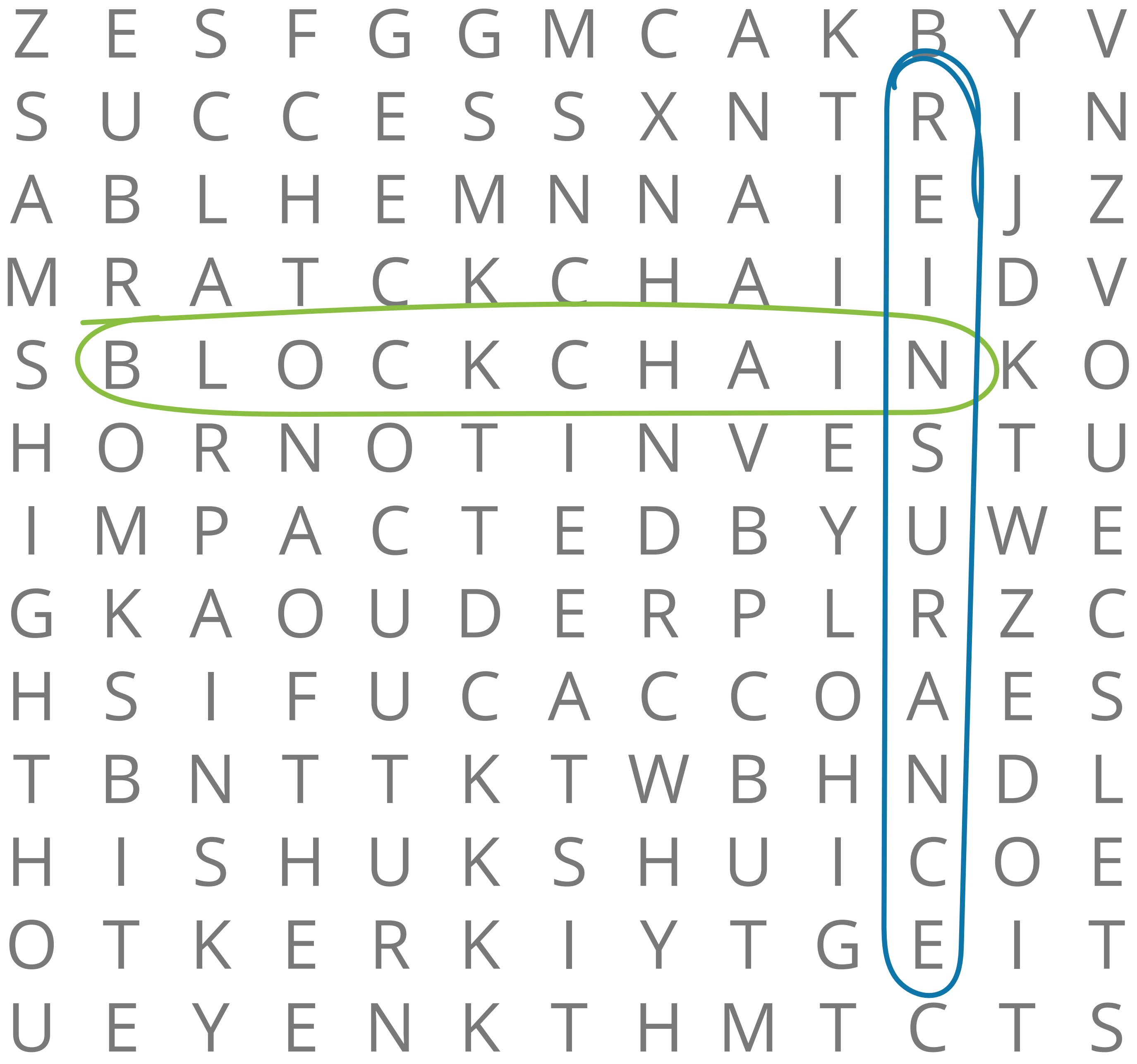
More generally, executives are concerned about the impacts of AI on their organizations and business models. Companies should start building knowledge and expertise and develop key competencies around AI in an attempt to better understand its implications in terms of security, compliance, and scalability. They could adopt a dedicated approach to start small and rapidly implement new prototypes into production. It is fundamental that key building blocks are implemented with the required capabilities to ensure proper data management across the firm. An initial step is to start testing AI through a first simple proof-of-concept, which enhances awareness and demonstrates its true potential. Given the role that CIOs play in security, data management, and digital operations, they are in the ideal position to lead the AI revolution, and to demonstrate its power and usefulness across the firm with concrete use cases. Successful projects require support from executives and accountable stakeholders; it is hence crucial to convince them by demonstrating its importance and benefits.

> Huge expectations are currently surrounding AI, and it could be the next breakthrough in the financial industry supporting digital transformations.

[6] Deloitte - Artificial Intelligence (AI) goes mainstream

[7] Deloitte – AI and you: Perceptions of Artificial Intelligence from the EMEA financial services industry

Blockchain meets reinsurance - A contract management system solution



Z	E	S	F	G	G	M	C	A	K	B	Y	V
S	U	C	C	E	S	S	X	N	T	R	I	N
A	B	L	H	E	M	N	N	A	I	E	J	Z
M	R	A	T	C	K	C	H	A	I	I	D	V
S	B	L	O	C	K	C	H	A	I	N	K	O
H	O	R	N	O	T	I	N	V	E	S	T	U
I	M	P	A	C	T	E	D	B	Y	U	W	E
G	K	A	O	U	D	E	R	P	L	R	Z	C
H	S	I	F	U	C	A	C	C	O	A	E	S
T	B	N	T	T	K	T	W	B	H	N	D	L
H	I	S	H	U	K	S	H	U	I	C	O	E
O	T	K	E	R	K	I	Y	T	G	E	I	T
U	E	Y	E	N	K	T	H	M	T	C	T	S

Dirk Siegel
Partner
Consulting
Deloitte

Peter Wiedmann
Senior Manager
Consulting
Deloitte

Christopher McDaniel
Specialist Leader
Consulting
Deloitte

Global financial companies continue to explore the new opportunities blockchain technology could offer, while continuing to evaluate the possible paradigm shift that it can trigger on their business. After an era of proofs-of-concept, the technology is now moving to the stage of live production and wide adoption.

Blockchain is one of the most promising innovations for financial services companies. According to the World Economic Forum,[1] financial services will be transformed by blockchain technology, with the expectation that at least 10 percent of the global GDP will be processed by blockchain platforms by 2025.

Over the last few years, the hype around blockchain has been growing. From its emergence as a technical experiment, blockchain now reaches toward wider adoption, ready to brandish its full potential. More than US$2 billion has been invested by venture capital companies and the number of blockchain technology-related startups are on the rise, with the more established companies starting to mobilize resources in an attempt to identify the full impact of blockchain on their business models. Some use cases are already live and many are awaiting their move into production.

Given that the advantage of the new technologies are greatest in a multi-player situation, numerous companies have entered into industry consortia to align on standards for implementation and identify areas of the value chain where blockchain technology can be applied to its greatest ability. Following the R3 consortium that gathered over 80 banks and was launched in 2015, the insurance and reinsurance industry has set up the B3i consortium as well as the RiskBlock consortium in the US.

[1] The Future of Financial Services – How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed. World Economic Forum June 2015

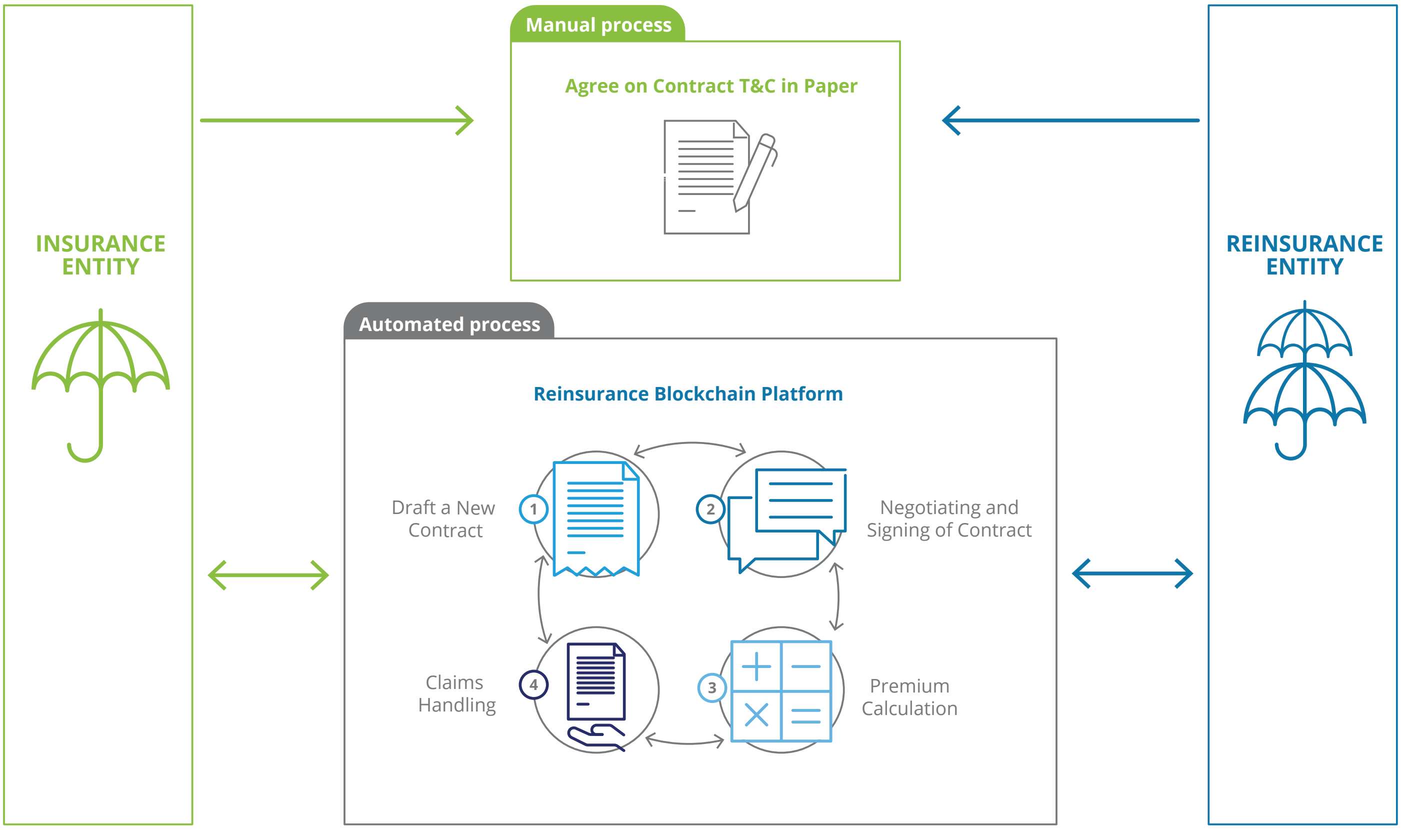
B3i consortium[2]

The Blockchain Insurance Industry Initiative (B3i) is a collaboration of insurance and reinsurance companies created in October 2016 to explore the potential use of blockchain and to increase efficiency in the exchange of data between reinsurance and insurance companies. Originally composed of five members (Aegon, Allianz, Munich Re, Swiss Re, and Zurich), the consortium welcomed ten new members at the beginning of 2017 (Achmea, Ageas, Generali, Hannover Re, Liberty Mutual, RGA, SCOR, Sompo Japan Nipponkoa Insurance, Tokio Marine Holdings, XL Catlin). B3i's vision is to jointly explore the potential of blockchain technology in industry-wide use cases to better serve end-clients.
The starting point was to develop a first proof-of-concept for Property Cat XL reinsurance contract management. The proof-of-concept was announced during an insurance summit in Monte Carlo in Septemper and opened for market testing.

We are confident that blockchain will play a pivotal role in the insurance industry in the upcoming years. As outlined in various Deloitte publications, blockchain will form the foundation of the industry's next-generation infrastructure. It will redraw processes and call into question orthodoxies that are fundamental to today's business models. Deloitte has already started to build real enterprise focused cross-industry blockchain frameworks with several use cases, both for property & casualty and L&A insurance. Examples include subrogation, proof of insurance, first notice of loss, and parametric insurance.

It is in this context Deloitte supported a large global insurance company in the development of a proof-of-concept in the reinsurance business. The client had already done one proof-of-concept with blockchain before and was one of the first big insurance players exploring blockchain technology. In 2017, in addition to their participation in B3i, the large global insurance company and Deloitte agreed to work together in order to implement a smart contract platform for a complex reinsurance program, focusing on the overall contract handling processes between the reinsurance entity and the primary insurance operating entities.

Blockchain enabled Reinsurance platform



[2] Reinsurance News. B3i to launch blockchain reinsurance platform at Monte Carlo RVS 2017. 20.07.2017

Reinsurance processes are famously inefficient. It is a complex business and still involves many manual processes. Blockchain technology offers great potential in initiating, processing, and settling transactions between primary insurers and reinsurers through its shared ledger, being able to track and trace every event and transfer value without needing a central database. For the proof-of-concept, the client identified several business objectives:

- Minimize the extent of manual collaboration required between the primary insurer, reinsurer, and retrocessionaires in creating contracts and claims
- Create transparency between the primary insurer, reinsurer, and retrocessionaires around contracts and claims
- Facilitate the processing and application of claims in real time
- Facilitate the automated processing of settlements
- Explore the capacity to interface with legacy platforms

In order to fulfill these functional requirements, the Deloitte team proposed and agreed on a series of technical requirements with the client:

- Build an extensible and modular platform for deploying blockchain-based reinsurance smart contracts
- Implement a user interface (UI) for the collaborative creation of contracts and the application of claims
- Implement connectivity of the UI to the blockchain through the use of application programming interfaces (APIs)
- Determine and assist the client in implementing an infrastructure to support the final proof-of-concept
- Build user profiles and capabilities for the primary insurer, reinsurer, and retrocessionaires

Smart Contract

A smart contract is a software algorithm integrated into a blockchain with trigger actions based on pre-defined parameters. The term can be misleading as it is not formally a contract (nor is it particularly smart). In this proof-of-concept, it is encrypted and time-stamped into a blockchain when created, and executes itself without the need for trusted third parties. This is one of the blockchain functionalities where companies see the highest benefit as it can drastically reduce the time and cost of actual contract processing. As an example, all terms and conditions of an insurance contract can be integrated as parameters of the algorithm and trigger reimbursement in the case of a claim.

In order to build this PoC as effectively as possible, an agile approach was formulated. The three sprints below were required to develop all defined functionalities and related interfaces:

- Sprint 1 focused on the creation of the contract processing module
- Sprint 2 developed the claims processing module
- Sprint 3 set up the multi-layer processing, settlement, and contract and claim exporting

Reinsurance is a complex business and still involves many manual processes.

After approximately two months of development, we delivered a fully functional proof-of-concept to the client. This PoC proved the hypothesis that blockchain can be very effective in managing complex and large reinsurance contracts. The smart contract platform implemented as part of the PoC allows insurers and reinsurers to interact securely and quickly across the contract lifecycle, utilizing a number of selected, pre-designed contract templates. Any one party can create a new contract on the platform and compile the various terms and conditions; negotiation over terms and conditions is handled directly on the platform, while providing a secure audit trail, guaranteed by blockchain technology. Upon contract signage, all information is directly saved in the blockchain, and can be "called upon" automatically once the relevant claims are applied against it, whereupon the payments resulting from the claim are then automatically redistributed to the participants in the contract.

The platform notably reduces the manual reconciliation efforts and applies a management-by-exception methodology for controlling activities. Looking forward, a full integration with core insurance systems, which was not part of this PoC, will undoubtedly benefit the overall management of reinsurance contract processes, guaranteeing increased security, transparency, and efficiency.

Blockchain for core insurance systems

Blockchain technology will act as the catalyst of a profound restructuring for insurers, as it will have a major impact on all steps of the core insurance value chain. We see the following three potential use cases as most relevant:

01. People: Based on Smart Identity, insurers can verify identity and enlist new customers much faster and at lower costs.
02. Contract: Through blockchain, all different parties of a contract will benefit from a joint platform that will reduce costs, errors, and the duration of the process.
03. Claim: The creation and processing of claims based on smart contracts ensures a transparent, responsive, and irrefutable process.

This PoC demonstrates that blockchain technology will have the potential to innovate not only the reinsurance business, but also the entire financial services sector through three mechanisms.

Blockchain technology will cause a paradigm shift for the financial services industry. Business data, rules, and processes relating to a single contract can be put integrally into a smart contract, which is audit-trailed by design. APIs interacting with the independent contracts can be set up, facilitating integration into a micro service architecture. This opens various new roles or changes existing ones within financial companies; so much indeed that over time, blockchain-enabled business could be the backbone of an industry-wide shared services center for selected processes.

> Upon contract signage, all information is directly saved in the blockchain, and can be "called upon" automatically once the relevant claims are applied against it.

> An obvious trend is that customers lean toward more customized products and services.

Despite the peer-to-peer nature of the system, validators will still be needed to authenticate participants and to be arbitrators in case of disputes. In a pure blockchain ecosystem, anyone could run the code and act as validator, but taking into account the current regulatory framework and existing trust models, we expect the emergence of regulated validators under the authority of existing entities, which financial companies best embody due to their market position.

An obvious trend is that customers lean toward more customized products and services. Blockchain, together with Big Data, artificial intelligence, and the Internet-of-Things, is one of the technologies that will be the driving forces for future innovation. In a blockchain-inspired insurance world, superior access to customers and risk assessment tools will continue to be key in running a successful business. Blockchain can serve as the infrastructure to orchestrate the complex ecosystem required in addressing specific needs of customers, which often go beyond the traditional insurance-focused business platforms. On top of this infrastructure, other innovative technologies might act as modules, e.g., create a tailored customer journey experience with artificial intelligence and the Internet-of-Things, balanced risk models for user based insurances with Big Data, or automated handling of business workflows with blockchain.

Adoption of Blockchain by Corporations

Technical progress is not yet fully satisfactory, both for public and private blockchains, especially over scalability, privacy and security.

Regulation authorities mainly adapted a wait-and-see approach. Although they are in principle open-minded about blockchain, global initiatives are not yet launched, i.e., intensive stakeholder management needed.

Legal enforceability continues to be uncertain, with special focus on e-signature acceptance and the true court value of smart contracts.

Social acceptance of such a new paradigm is all but certain, as significant and potentially painful disruption will need to occur, including job losses and failing businesses.

Blockchain technology is gaining momentum across all insurance market stakeholders. The technology is positioned to become a strategic imperative for large companies. Industry-wide consortia, such as B3i and RiskBlock, aim to maximize the potential benefit of blockchain. The presented blockchain proof-of-concept provides strong evidence that the technology is very effective in managing complex and large reinsurance contracts. Blockchain technology is positioned to become the industry infrastructure backbone of the future, enabling a paradigm shift in many ways. It provides the opportunity to positively affect the products and services provided to the customer, improves business processing, and evolves the role of existing industry market players. The time when the blockchain initiative was mainly about proofs-of-concept and experimentation is over. The era of blockchain as a key strategic value creator is upon us now.

Sources:

Deloitte Germany Blockchain institute Point of View: "Banking on a public platform - How Blockchain can change banking"

Digital onboarding for financial services

A must-have for digital natives

In the financial services industry, the level of service offered to customers coupled with a strong branding are key to attract and retain clients. Arrival of new players on the financial services market like neo-bank a few years ago and FinTechs more recently, reshaped the landscape of financial services providers and accelerated digitization of many processes and services. Customers expect from their financial institutions (e.g. bank, insurance) a high level of services and personalized communication as they enjoy in other areas of their lives. In addition, the PSD2 regulation encourages competition between financial services providers and facilitates change from one provider to another. Combined, these factors are making customers less loyal to their current financial services providers and highlight the importance of the onboarding process.

Ronan Vander Elst
Partner
Deloitte Digital
Deloitte

Maxime Heckel
Director
Operations Excellence
& Human Capital
Deloitte

Nicolas Vauclin
Manager
Technology & Enterprise
Application
Deloitte

Any customer who has tried to open a current account or become a new client knows how unpleasant the experience can be: either in a branch where they have to follow old paper-based onboarding processes or online where they are often redirected to a local branch.

Every customer's onboarding journey is different but the experience of opening accounts with traditional financial institutions leads to many common friction points like being re-routed to different channels, the need to provide physical identification, answering the same questions multiple times, and long delays to access the account. Improving the customer onboarding experience should be a priority for financial institutions, especially as new regulations like the PSD2 will enable customers to change their financial service provider more easily. The account setup should now be a formality and should therefore be completed in minutes, similarly to other common services (e.g. Facebook, Spotify).

Onboarding represents the first customer interaction for the financial institution and will set the tone for the entire relationship. A move from a lengthy, paper-based and inconvenient process to a smooth and genuinely omni-channel customer experience would be a true game changer, not to mention it could potentially save significant process cost.

Increasing cost pressure, evolving customer needs and market transformation require a profound rethinking of the client onboarding process.

Client onboarding encompasses the end-to-end process, from the time the client is looking for information on a financial institution to the time his or her product (e.g. bank account) is activated, as well as the follow-up activities performed by the financial institution to ensure a smooth start of the customer relationship (e.g. first contact with a customer representative).

Three main forces are challenging today's traditional onboarding process:

Decreasing cost/income ratio is a major challenge for most of the traditional financial institutions in Europe, especially with the threat of new market entrants (e.g. FinTechs) and increased regulatory burden. In particular, the traditional in-branch onboarding process is time consuming and could be automated and improved to provide a better customer experience and enable cost reduction and revenue increase.

Customers' behavior is evolving: they have become more international and mobile and thus expect simpler, quicker and more flexible interactions with their service providers. They also expect to be able to perform all types of services at any time, regardless of location. They are strongly reducing face-to-face interactions for their financial activities and look for institutions that can provide them with an easy access and personalized experience. Today, 38 percent[1] of customers drop out of the onboarding process because of frustration with paper or the volume of information required.

New market entrants are reshaping the landscape of financial services providers. On the one hand, new purely digital companies provide great customer experience and increase competition between traditional institutions, but on the other hand, new disruptive technologies allow the latter to keep up with change and meet client expectations.

[1] 2017 Deloitte Global Mobile Consumer Survey

Digitizing the onboarding process enables financial institutions to transform these challenges into opportunities
Digital onboarding enables a new and personalized customer experience by simplifying the access to financial services while reducing processing time and cost for financial institutions due to optimized processes:

Improved Customer Experience

- Faster and more flexible access to banking services
- Be perceived as innovative and reinforce brand image
- Possibility to switch between in-branch and online onboarding
- Onboarding in a matter of minutes
- Enhanced digital user experience
- Structured file archiving
- Reduce document loss
- Reduced paper usage

Reduced Cost/Income Ratio

- Reduce cost-to-serve
- Improve sales effectiveness
- Reduce failed client acquisitions
- Automate and accelerate processes to increase operational efficiency and to reduce operational costs
- Increase Assets under Management and revenues
- Free up employee time that can be spent on more valuable activities

In the banking industry, 38 percent of customers stated user experience (UX) as the most important criterion when choosing a digital bank.

01

Customer experience is one of the most important success factors of the onboarding process. Financial institutions use more and more customer-centric methodologies to redesign the target customer experience.

Customers need to see onboarding as a single process, no matter how many channels they use. To avoid losing customers during the process, the onboarding strategy must offer cutting-edge personalized experiences that accompany the customer during the onboarding process across multiple channels.

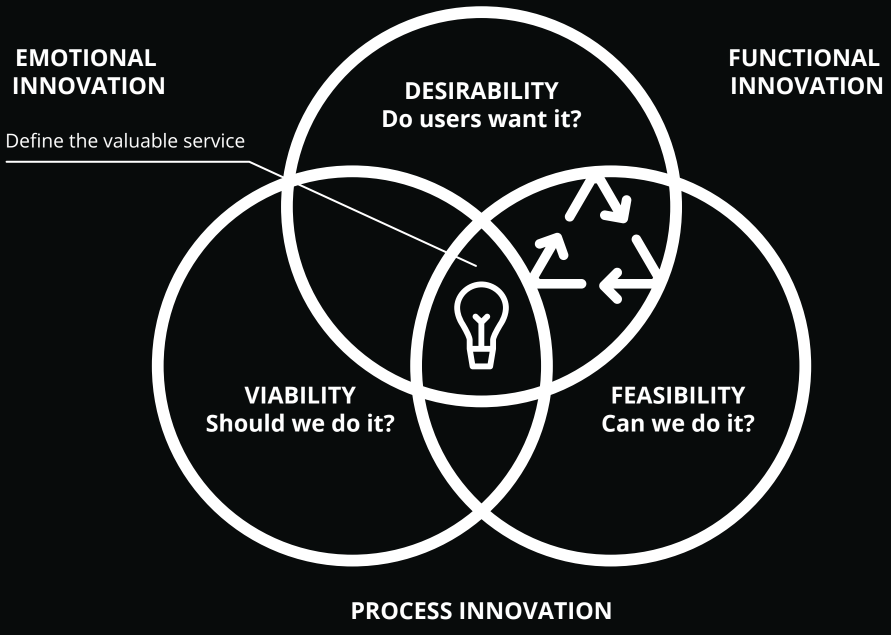
In the banking industry, 38 percent[1] of customers stated user experience (UX) as the most important criterion when choosing a digital bank, and 26 percent stated the easy enrollment and login is the most important one. Giving customers the choice of interacting via multiple channels at any time makes the process much more convenient and requires an omni-channel strategy upfront. This means giving customers the flexibility to start their onboarding process using one channel and switch to another one at any time to pick up where they left off. Customers who experience "anywhere" onboarding with consistent information across channels are likely to think that this convenience would extend to their day-to-day experience.

In order to design great omni-channel customer experience during onboarding, service design techniques enable an organization to understand customers' needs and empathize with them. It aims to ensure that service interfaces are useful and desirable from the client's point of view, as well as effective, efficient and distinctive from the financial institutions' point of view.

Service design approach should be iterative, user-centric and co-creative: prototypes are designed together with customers, not only for them. This approach is also more holistic as it considers the service context and formalizes the onboarding before, during, and after the process itself.

Nevertheless, service design should not only focus on customers, but should aim to find the "sweet spot" between the three following dimensions:
Desirability: Do users want it? This question links onboarding to target customer segments
Viability: Should we do it? This question assesses the alignment of new service to the strategy
Feasibility: Can we do it? This question makes the link with capacity planning and architecture

Service design is an iterative approach aiming at finding the "sweet spot"



Service Design is a disruptive method based on group work and customer focus

USER CENTERED
It is all about people

CO-CREATIVE
Design with, not just for

SEQUENCING
Sequence of correlated actions

EVIDENCING
Physical touchpoint interaction

HOLISTIC
Considering the service context

Onboarding is a specific process that requires identifying customers and verifying their identity with high level of security and low level of risk.

02

To start implementing a new onboarding process, financial institutions need to consider their overall business architecture
Onboarding represents the process by which a customer establishes a relationship with the financial services provider. This journey encompasses all activities performed by the institution or the customer, from information display, data capture, and product activation to key follow-up activities (e.g. first instalment on the account, first contact with an insurance agent). The goal is to ensure a valuable onboarding for the financial institution, not only by developing a new mobile app or website.

Some specific steps of the digital onboarding process require dedicated technologies
Onboarding is a specific process that requires identifying customers and verifying their identity with high level of security and low level of risk, as required by KYC and AML regulation. Five elements need particular attention:

01
Collecting potential clients' static data and identification documents, and checking the accuracy of the information provided through different methods.
It can be OCR (Optical Character Recognition), that extracts textual data from documents or document validation, that verifies the authenticity of the customer's identity documents (such as passports, driver's licenses or national ID cards) scanned by customers.

02
The anti-impersonation step ensures that the customers applying for the product are "who they say they are", i.e. their identity matches the identity indicated on the documents and data that have submitted. There are two main types of anti-impersonation solutions: Knowledge-Based Authentication (mainly used in the UK) and Facial Recognition.

03
Verification of the customers' identity and compliance (AML/CTF - Anti Money Laundering / Counter Terrorism Financing) is performed by running background checks on inputted static data (e.g. name, gender, date of birth, country of residence, nationalities). The "Know Your Customer" background verification will assess the potential risks a customer could represent (i.e. counterparty risk).

04
The electronic signature ensures that a contract is duly signed between the customer and the financial institution.

05
Orchestration is a key element of the process, as it enables a smooth and transparent experience for the customer who does not see all systems used during the process. Determining a basic real-time onboarding status is not trivial and still considered as a goal to achieve by many financial institutions.

In order to cover these activities, a large number of applications are required and need to be perfectly integrated to guarantee great customer experience.
Digital onboarding requires financial institutions to implement the following capabilities:

- Provide a customized and ready-to-use front end
- Capture customer's static data and identification documents
- Perform OCR on documents to enhance user experience
- Ensure advanced photo and video facial recognition (i.e. comparing photo and video from smartphone built-in camera and identification documents)
- Perform basic AML/CTF background checks (e.g. official list, politically exposed persons, adverse media)
- Provide electronic signature services, to enable contracts to be signed between the customer and the financial institution

Implementing a large number of different applications within the existing landscape brings traditional IT challenges like incompatibility between technical frameworks, difficult synchronization of release cycles, etc. The complexity is further increased by the limited scope of the onboarding process and the high-level of service required to provide great customer experience. This complexity comes with additional costs that need to be anticipated in the business case of the project. Implementing Service Level Agreements with external providers is one example of activities to control costs.

Designing architecture for digital onboarding requires a trade-off between easy customer experience design and IT complexity
Depending on several factors such as channel strategy, the existing technology landscape, and flexibility in the continuous improvement of the process, financial institutions can implement onboarding solutions following two alternatives.

The first alternative is to orchestrate the digital onboarding process with a dedicated end-to-end solution that comes with already integrated technology components. A single external vendor orchestrates the whole onboarding process using several sub-FinTech vendors. In this case, the financial institutions only contract with one vendor and benefits from an integrated and end-to-end technological solution. Multiple vendors, and in particular new FinTechs, flourish in that domain. Integration within the financial institutions' IT landscape is limited to back office and CRM systems.

The second alternative is to orchestrate the digital onboarding process using a mix of internal and external technology components (when necessary). In that case, the financial institutions leverage existing components (e.g. front-end development tools, document management) and orchestrate all services in-house. The only missing components that would need to be added are photo and video recognition capability and electronic signature.

In both alternatives, financial institutions exclude the development of all applications in house. For instance, performing onboarding via video identification requires a multilingual 24/7 video call center. Similarly, OCR capability is a component that is mature on the market and not worth developing from scratch.

> The complexity is increased by the limited scope of the onboarding process and the high-level of service required to provide great customer experience.

03

IT efforts do not represent the most complex and time-consuming part of digital onboarding projects
Digitization of the onboarding process in financial institutions are complex in terms of architecture and technology. However, IT does not represent the most complex part.

Many regulations are applicable in the onboarding process and must be carefully analyzed before launching the new digitized process. These regulations encompass Anti-Money Laundering/Counter Terrorism Financing (AML/CTF), data protection and guidelines provided by local regulators (e.g. BaFin in Germany, CSSF in Luxembourg).

The difficulty is not limited to a deep analysis of the regulations. As digitizing the onboarding process is a relatively new type of project, regulations are not explicit about all the steps of the process. Moreover, regulators pay particular attention to these digitized processes and authorize projects after careful analysis of the submitted files. These challenges need to be taken into account at the beginning of the project and be incorporated in the planning.

In addition, depending on the customer target group, local regulations apply and shall be considered in the process. For example, the number of documents to provide is different between a digital onboarding in France and Belgium. ●

> Many regulations are applicable in the onboarding process and must be carefully analyzed before launching the new digitized process.

Specific case: Onboarding experience with N26

Number 26 ("N26") is a bank created in 2013 in Germany that allows customers to run their entire financial life from their smartphone. N26 processes the entire account opening in less than 10 minutes, and offers the possibility to withdraw cash from any ATM and receive real time push notifications after every transaction. Moreover, customers can send and receive money instantly to and from other N26 users. As of August 2017, the bank was available in 17 European countries, and claimed it had 500 000 customers, with 1500 new clients per day on average.

N26 announces a full online onboarding in less than 10 minutes, including ID verification and anti-impersonation performed via live video chat. Customers are guided through the process on a simple and clear interface:

- Fill in the online application form by entering personal details
- Provide personal legal data (e.g. tax country)
- Verify your identity and collect your ID document via a video chat with a video agent, available in multiple languages
- Receive an SMS with a unique code to pair your smartphone to your bank account

The fast success of this fully digital bank highlights that many customers are ready to change to new players when the experience of change is satisfying, and the level of services provided afterwards at least equal to that of traditional financial institutions.

The onboarding process represents the first interaction a customer has with a financial institution. This is a unique opportunity to create long-term loyalty. Moreover, it is the starting point enabling the digitization of other digital financial services such as online loans, insurance or investments.

Re-designing existing onboarding processes is a complex activity that involves many processes, providers and systems. The complexity increases due to customers' high expectations of top-notch user experience (UX) and their demand for omni-channel use. A customer-centric approach during the design phase should make it easier to achieve these goals. Today, numerous FinTech and non-FinTech providers are able to assist with both end-to-end and standalone solutions. Even if most of the underlying technology has a proven-track record, financial institutions still need to assess integration feasibility (i.e. considering specific internal constraints) and local legal requirements. Indeed, some of these requirements can be unclear and require special attention. For instance, photo/video identification and electronic signature requirements (e.g. advanced vs qualified according to eIDAS regulation), AML/CTF background checks and underlying customer due diligence duties need a specific focus.

Re-envisioning the customer banking experience

Olivier de Groote
Partner
Financial Services
Industry Leader
Deloitte

Cedric Deleuze
Partner
FS Deloitte Digital
Deloitte

Deloitte's digital bank solution is fundamentally changing customer relationships with new ways to create value. The solution is designed to build in-depth client relationships, enhance productivity, and enable banks to engage more holistically with clients anywhere and on any device. Built on the Salesforce Financial Services Cloud, Deloitte Digital has created a pre-configured digital banking accelerator that will help to enable banks to create value by offering customers banking solutions that are tailored to their individual needs, behaviors, and patterns.

Many banking customers' expectations are changing the way banks interact with them on a daily basis. As a result, new technologies, non-traditional competitors, and regulatory changes are disrupting the banking world, pressured by more and more sophisticated customers. To compete in today's shifting landscape, it is important for banks to wow their customers with experiences that are genuinely surprising in both their function and appearance. Addressing these changes may require speed and innovation to maintain exceptional customer loyalty and advocacy.

Many banks that are succeeding in today's digital world are transitioning from a product-centric approach to a need-based customer model so that they are well positioned to add value anytime, on any device, as if it were a human interaction.

The evolving nature of digital is dynamically changing the banking experience. For too long retail and commercial banks have been dependent on single applications, which typically offer limited personalization and no context, limited services insights and assistance, and tend to be disconnected from the customer "hub" with little sharing across channels.

With emerging trends and technology advancements moving to the cloud, digital banking offers new opportunities for creating greater customer value as well as new entry points for competitors. As these competitive online services move up the financial services value chain, digital is rapidly redefining the banking experience and forcing many banks to adapt to customers' needs that are ever more demanding.

What your Customers Expect?

Your customers expect you to provide them with the same easy, personalized, transparent, fast, simple and secure digital experience as in other industries and aspects of their lives.

Easy to consume
Across channels and devices

Personalized and unique
Context-driven solutions, designed to meet client needs

"Appification"
Products and services that can be updated easily and quickly

Easy to integrate
Solutions that integrate and onboard easily with legacy systems

Pricing and value transparency
Clear definition of costs and benefits of products and services

Security and protection
Safe and secure solutions

Predictive solutions
Products and services that actively anticipate what lies ahead

To win customers and keep them, banks may need to reimagine their customer relationship and find new ways to:

- Engage their customers – genuinely surprise them with services that offer function as well as appearance
- Know them – know their behaviors and patterns to tailor their experience
- Make it easy for them – provide a customer service without barriers to make it simple and easy to do business
- Earn their trust – pro-actively do the right thing to build strong digital relationships

Deloitte Digital Bank built on the Salesforce Financial Services Cloud is designed to help banks create value and address the emerging retail and commercial banking trends and requirements for:

- Frictionless experiences – allowing customers to interact with banks efficiently and easily across a growing array of internet-connected devices, remembering these interactions, and aligning capabilities across those touch points
- Personalized services – adopting smart devices when dealing with bank staff online, by phone, or in-branch, providing personalized, informed advice and guidance
- Transparency when comparing products and services – making it easier than ever for customers to evaluate competitive banking service quality in real time
- Making sense of financial data – helping customers understand data by providing engaging, intuitive, and useful experiences and insights

Deloitte Digital is using innovation and a consultancy model to fundamentally change bank-customer relationships by providing the technology, skills, and experience to help banks successfully realize a digital transformation that removes traditional barriers, so that they can better serve customers in a simpler, frictionless way.

Where to Focus?

Digital capabilities are in a continuous process of evolution, proliferation, and adoption. Leading banks realize that it's not enough to seek incremental enhancements to remain competitive; they innovate understanding that differentiating capabilities will quickly become table stakes.

1

Table Stakes
Customer's demand this just to do business. Many which at one time were innovative are now today's standards.

- Online and Mobile Banking
- Mobile Check Deposit
- Text Banking
- Branch Locator
- Mobile Bill Pay

2

Competitive Offering
Semi-unique features which ensure you are up to date with competition.

- Streamlined P2P Mobile Payments
- Virtual Wallets
- Credit Monitoring

3

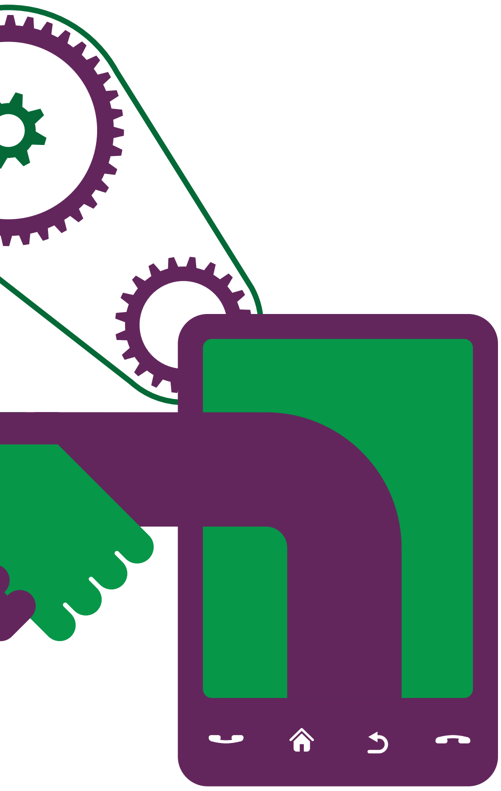
Innovate
Emerging capabilities which customer's never imagined were possible going beyond their expectations.

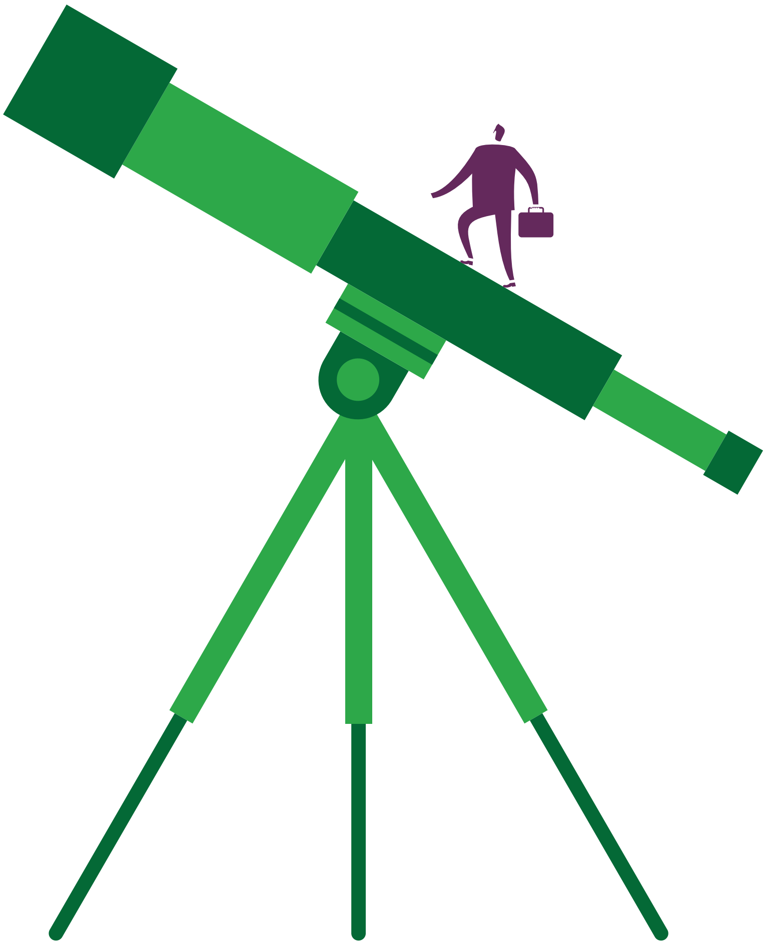
- Biometric Banking / Voiceprint
- Digital personal financial advisors
- Automated product recommendations
- Cross-border P2P Payments
- Automated customer service - Chat Bots
- Automated and actionable insights

4

Differentiate
Unique capabilities which delight your customers and remember why they bank with you.

- Fingerprint Sign-on
- Personalized mobile banking
- Mobile enabled branch appointment scheduling
- Mobile enabled rewards systems
- Online Portals
- E-Signature
- Analytics Driven Budgeting / Savings tools
- Social Media Integration





The pre-configured accelerator helps enable banks to rapidly create and enhance customer value. The solution comes integrated with a wide range of leading cloud vendors and FinTechs—helping banks to benefit from pre-integrated technologies.

By utilizing the Deloitte Digital banking solution, banks can benefits from:

- A flexible, open, and adaptable software platform that delivers cutting edge digital banking experiences to help drive differentiation, innovation, and outstanding customer and employee experiences
- A cloud-based digital solution that is designed to lower risk and increase value, tailored to the ever-changing banking industry landscape
- An approach that can increase speed and agility to meet the increasing needs of sophisticated customers and deliver exceptional customer loyalty and advocacy – while meeting the regulatory needs of the industry
- A consultancy vision and platform that allows for broad-based transformation or incremental models that can deliver rapid value and expand across line of business or channel as needed to deliver on their strategy
- An implementation starting point that can get banks in-market quickly and generate ROI faster

Many banks that are succeeding in today's digital world are transitioning from a product-centric approach to a needs-based customer model so that they are well positioned to add value anytime.

Exponential Technologies

Engage

Advice

Onboard

Service

Customer Engagement

- Customer Communities
- Social Media listening and publication
- Video Call and co-browsing
- Chatbot
- Mobile App integration

Banking Functions

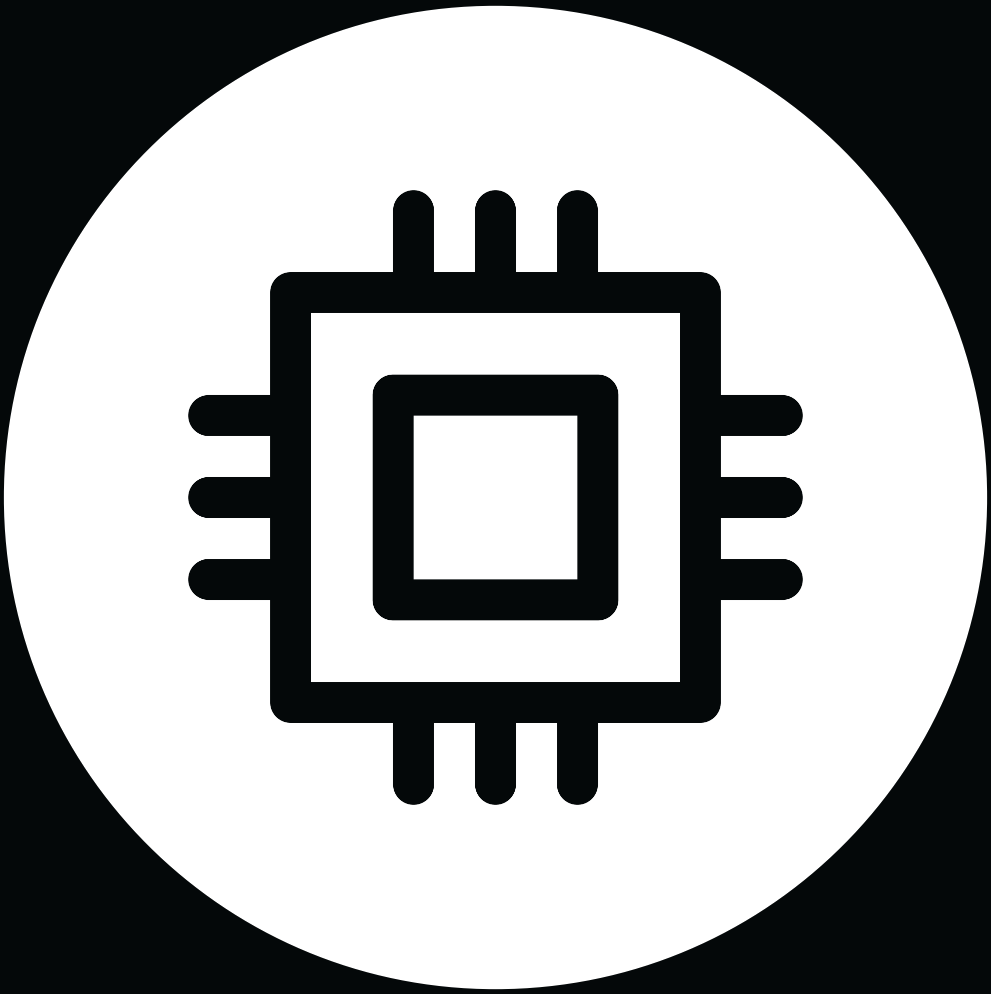
- Client Onboarding
- Households and Relationships
- KYC and Compliance
- Loan origination
- Product Portfolio Management

Sales and Marketing

- 720° B2B and B2C Client View
- Offer management
- Next Best Action and Next Best Offer
- Campaign Response Tracking
- Segmentation and Targeting

Service and Support

- Activity and Interaction Management
- Complaint Management
- Online assistance
- Satisfaction Surveys
- CTI Integration



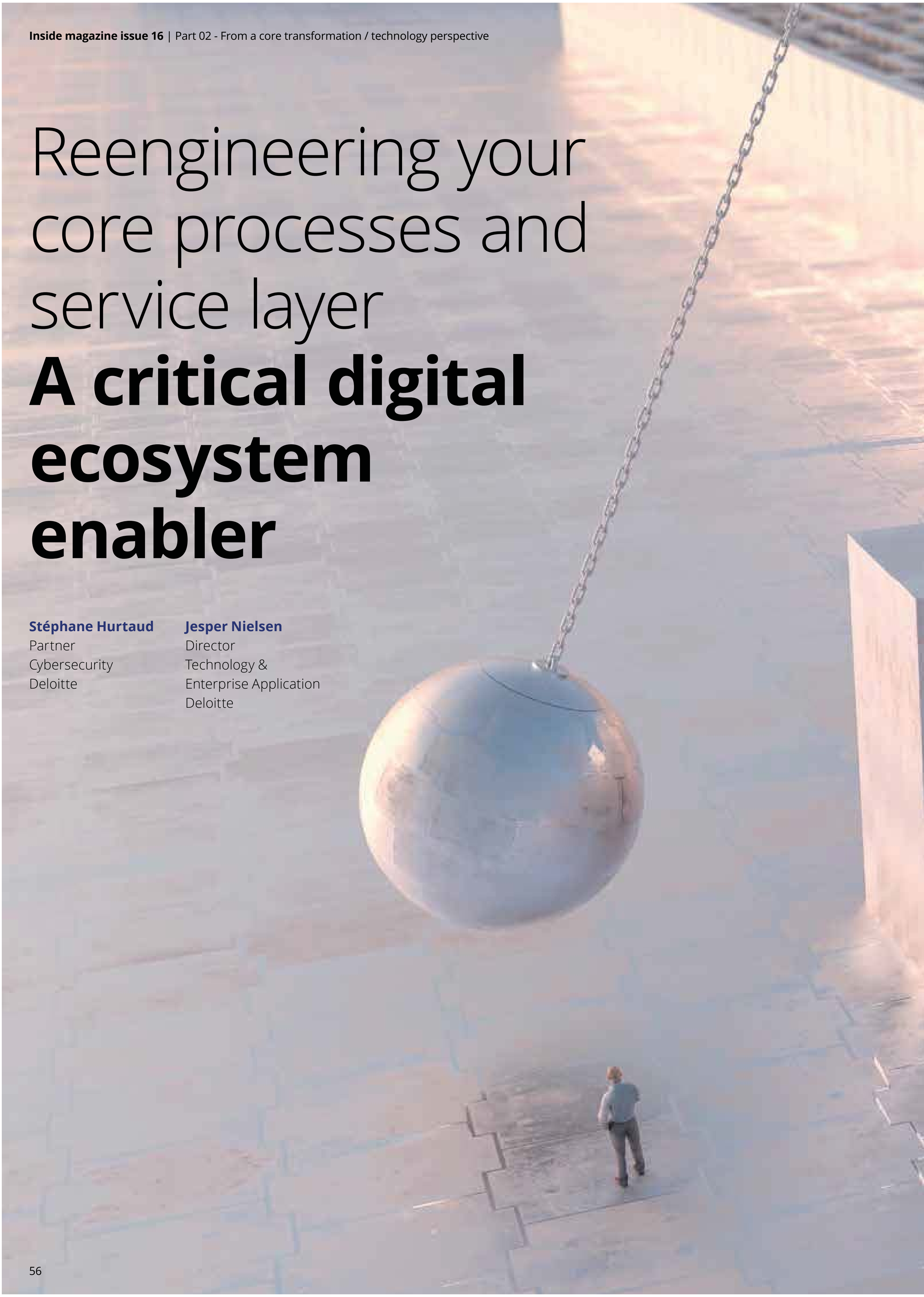
Part 02

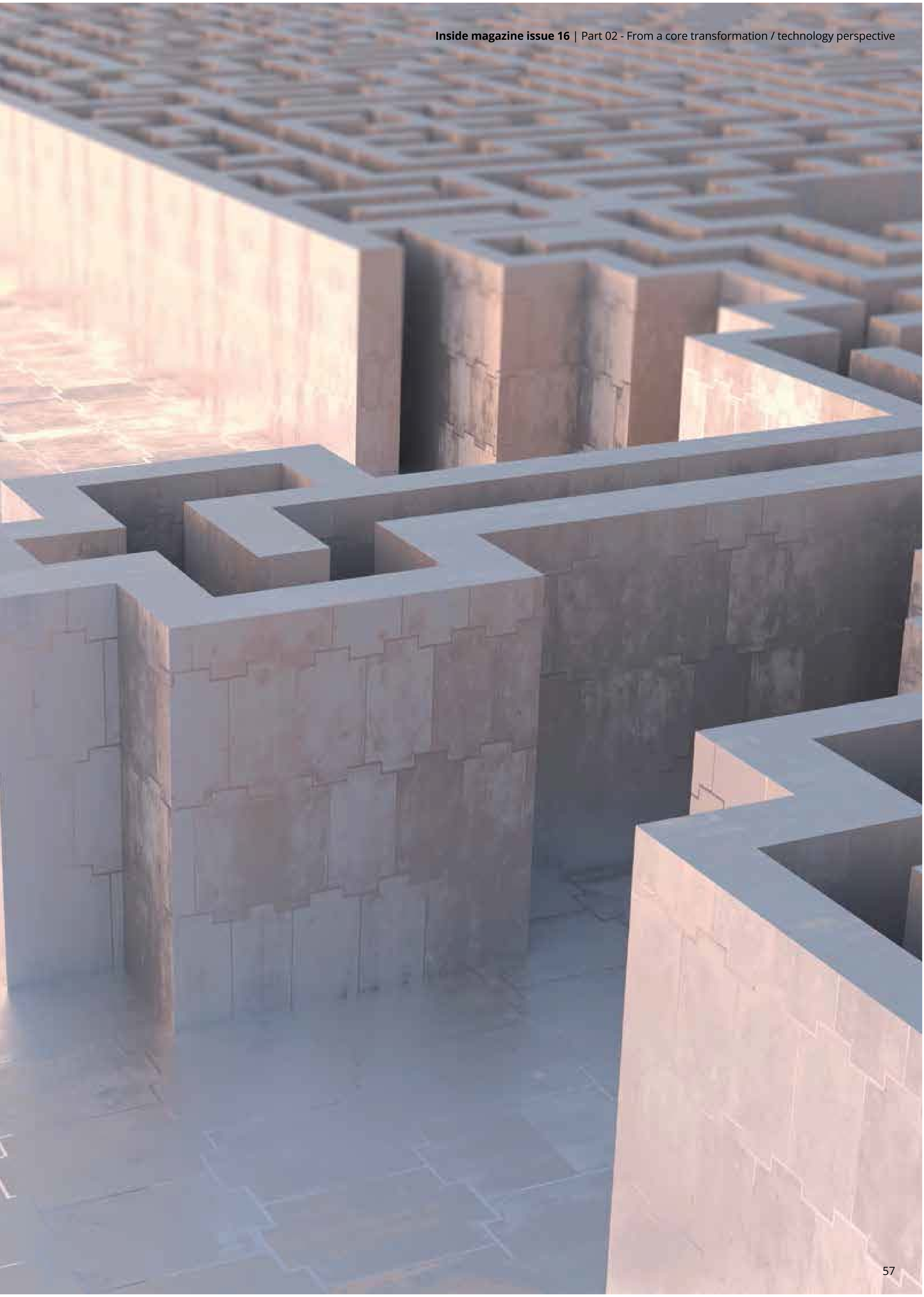
From a core transformation/ technology perspective

Reengineering your core processes and service layer **A critical digital ecosystem enabler**

Stéphane Hurtaud
Partner
Cybersecurity
Deloitte

Jesper Nielsen
Director
Technology &
Enterprise Application
Deloitte





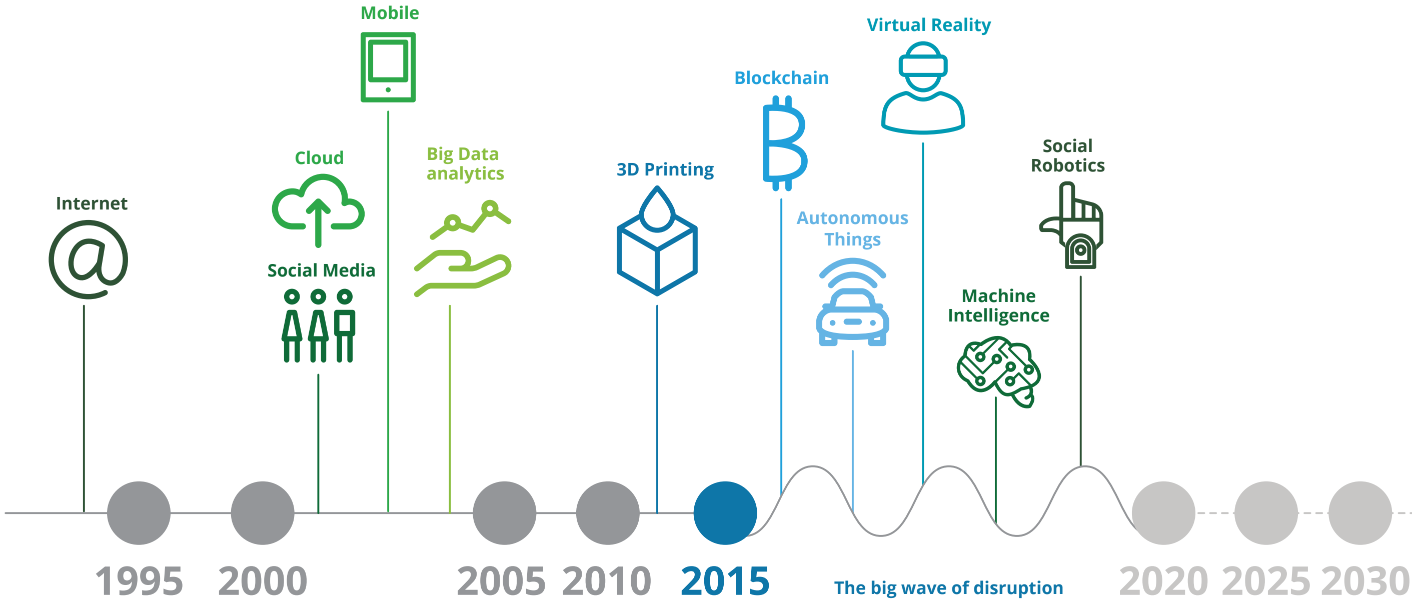
Digital services require a flexible and readily adaptive service layer to manage the multitude of core processes within an organization, as well as providing a seamless and efficient service structure. Without such a service layer, it becomes increasingly complex to build, manage, and supply services layered upon internal (core) systems, external cloud services and FinTech service providers.

Utilizing a modern cloud-based offering for the service layer—preferably a true open-API platform—will become a key differentiator for improving or building new products and services, as this will increase the go-to-market speed, provide the necessary flexibility, and be flexible enough to cope with unplanned events and changes. Done well, the enterprise service management layer becomes your internal digital enabler.

Requirements from the digital economy

The digital economy is storming ahead and changing industries, businesses, and organizations alike. However, some of the technologies that are expected to be most transformational are still in their infancy and the disruption caused by them is hence still ahead of us. However, this disruption is approaching fast!

The economy is turning digital, and as a result, digitalization and automation affect all parts of businesses. In this digital economy there are several big shifts taking place. We see 16 different dimensions being radically affected by these shifts due to new digital technology and digital transformation with critical questions about processes, capabilities, sourcing, and locations to be addressed.

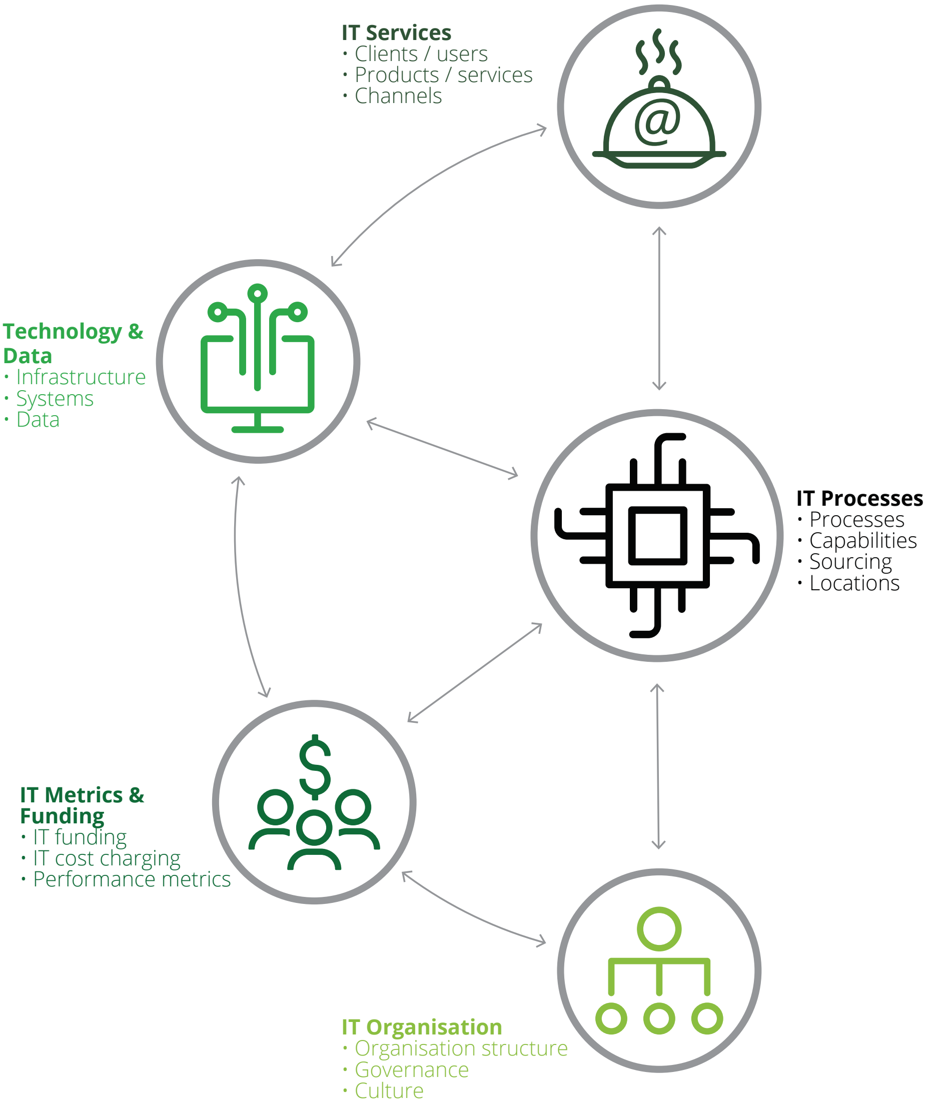


Source: Digital Era IT Operating Models - Deloitte Point of View

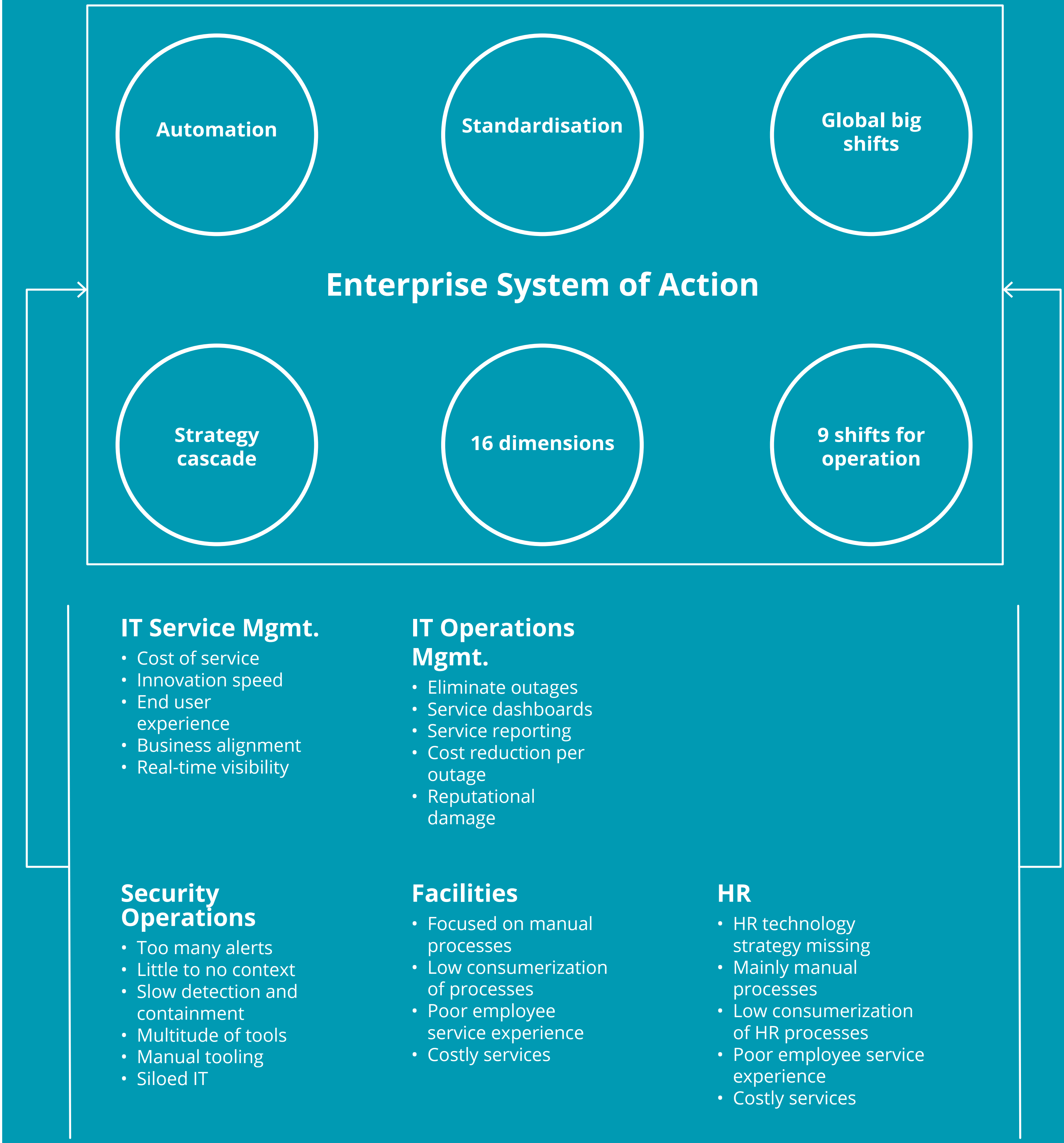
A "System of Action" is a necessity for organizations to adapt to the digital economy, where the pace of innovation and transformation of business value propositions is changing rapidly. It is not news that the digital economy is upon us, but it is now definitely time to act!

"We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten. Don't let yourself be lulled into inaction"

Bill Gates



Today's organizations are typically using a multitude of not-scalable applications for delivering services, whether internally or externally.



Automation

Standardisation

Global big shifts

Enterprise System of Action

Strategy cascade

16 dimensions

9 shifts for operation

IT Service Mgmt.

- Cost of service
- Innovation speed
- End user experience
- Business alignment
- Real-time visibility

IT Operations Mgmt.

- Eliminate outages
- Service dashboards
- Service reporting
- Cost reduction per outage
- Reputational damage

Security Operations

- Too many alerts
- Little to no context
- Slow detection and containment
- Multitude of tools
- Manual tooling
- Siloed IT

Facilities

- Focused on manual processes
- Low consumerization of processes
- Poor employee service experience
- Costly services

HR

- HR technology strategy missing
- Mainly manual processes
- Low consumerization of HR processes
- Poor employee service experience
- Costly services

What is a service layer and why is it necessary?

Enterprise Service Management is defined as *"an integrated view of core service business processes, often in real-time, using common databases. ESM systems track business resources—people, parts, assets—and the status of customer commitments: service requests, orders, repairs, and SLAs. The applications that make up the system share data across various departments (customer service, technical support, sales, field service, etc.) that use the information for their work. ESM facilitates the information flow between departments and coordinates activities with external resources involved in the service business process."*

Today's organizations are typically using a multitude of not-scalable applications for delivering services, whether internally or externally. Here you typically think of email requests, phone calls, and escalations (perhaps by adding a manager on an email). These systems have a very low satisfaction level for users, and typically only work well for senior people in the organization and long-term employees. New employees are generally struggling.

These non-scalable applications mean a massive loss of company productivity as resolution times are slow and require more interactions. In other words, operating costs are higher. In the consumerization of IT we are also seeing more and more workload handed back to the employees. The time an employee uses on processes and requests varies depending on the seniority and experience level, but it is a regular occurrence and takes an increasing amount of employees' time.

The best way to improve the situation is through an enterprise system of action. Such a system delivers a uniform user experience, making it easy for users to navigate the company services, no matter what kind of services are considered. By standardizing and integrating the company processes, it becomes possible to set and deliver more formalized service levels, which in return yields better overall economics.

ESM systems track business resources—people, parts, assets—and the status of customer commitments: service requests, orders, repairs, and SLAs. The applications that make up the system share data across various departments (customer service, technical support, sales, field service, etc.) that use the information for their work.

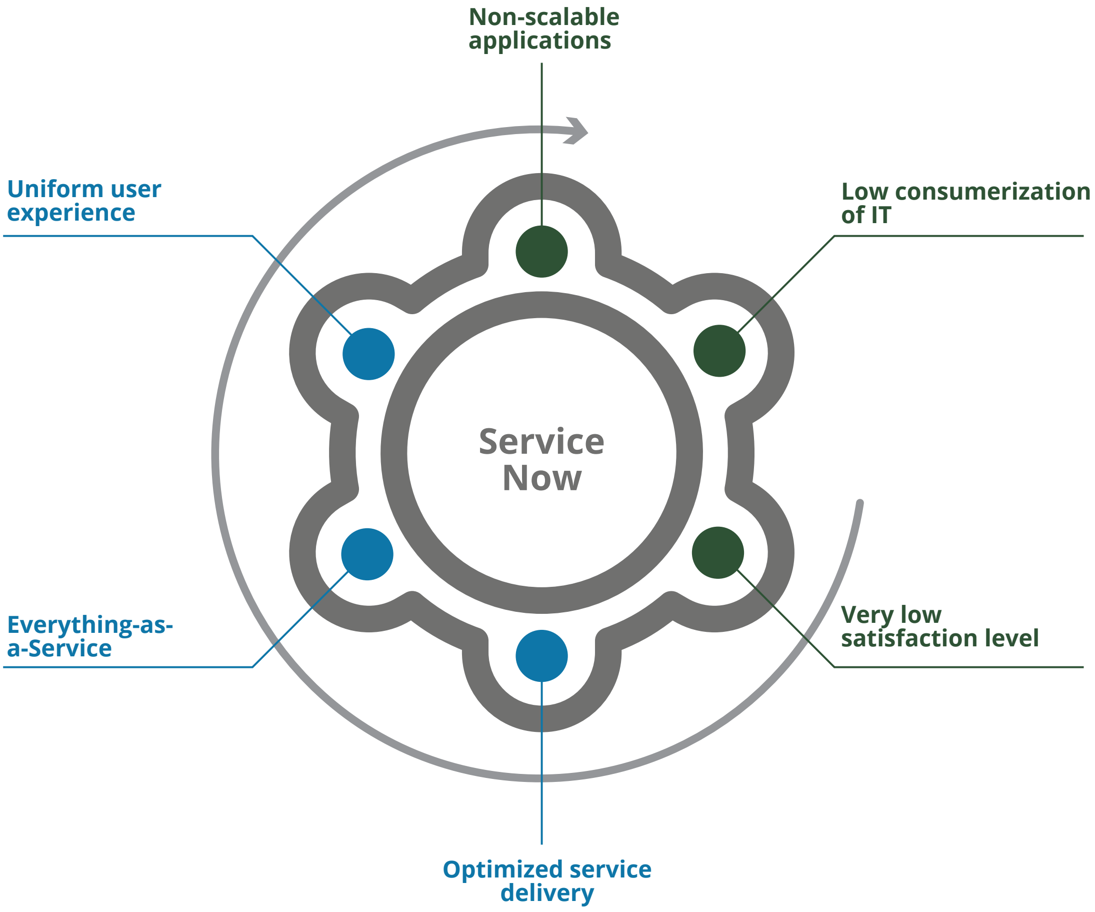
"The secret of change is to focus all of your energy, not on fighting the old, but on building the new"

Socrates

Think "Everything as a Service".
Any complex—or less complex—business process can be mapped and structured and is therefore able to become a managed optimized service. This is the enablement of internal digital delivery—supporting business agility and speed, enabling data driven decisions, and maturing the organizational processes in anticipation of the "Big Shifts."

Enterprise Service Management must assist organizations to deliver digitally internally; employees today expect the same service internally as they are used to receiving externally.

Digital delivery


Non-scalable applications
Uniform user experience
Low consumerization of IT
Service Now
Everything-as-a-Service
Very low satisfaction level
Optimized service delivery

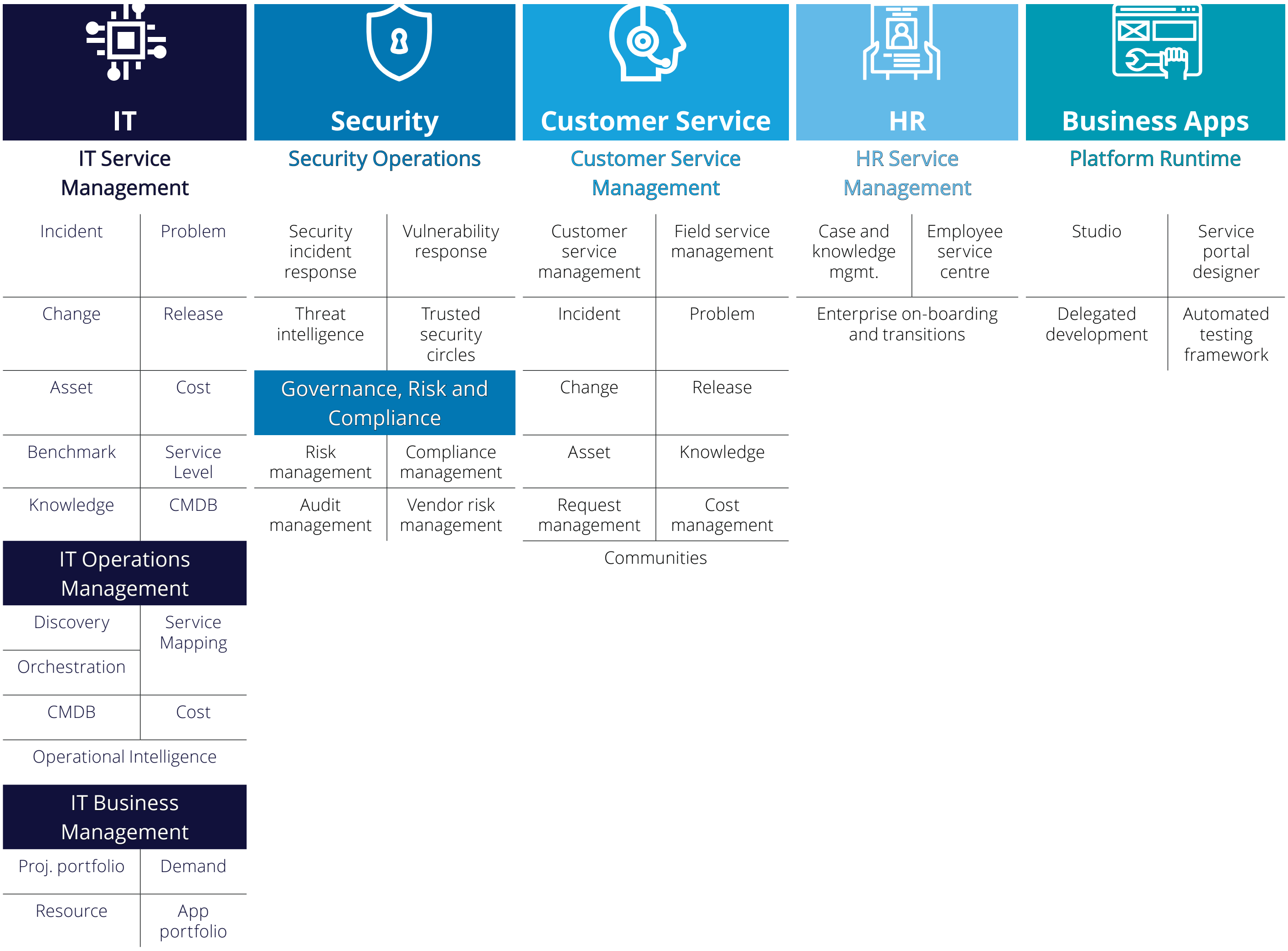
● Challenges today ● Target situation

What are the best options for implementing a service layer?

There are several solutions on the market that can be used to build the service layer. The market leader for Enterprise Service Management is ServiceNow with their cloud platform covering IT as well as business service management. ServiceNow is recognized as a leader for their innovative solutions, due to the flexibility and ease of use of their cloud-native platform. As an ITSM solution provider, ServiceNow is market leader (see Gartner magic quadrants; e.g. for IT Service Management Tools). They currently have several other additional areas covered by the platform, mainly security operations and GRC, facilities, and HR.

Organizations that intend to achieve maturity level 3 (or higher) should consider such an advanced service management platform to ensure the possibility of end-to-end business context in combination with an adaptable platform. Combining the rapid pace of innovation and development of the platform from ServiceNow, with the possibility to download applications or build their own developments directly on the platform where needed, the possibilities for the creating and implementing of such a service layer with a fast pace is a real opportunity for all organizations.

ServiceNow Products Suites



IT

IT Service Management

- Incident
- Problem
- Change
- Release
- Asset
- Cost
- Benchmark
- Service Level
- Knowledge
- CMDB

IT Operations Management

- Discovery
- Service Mapping
- Orchestration
- CMDB
- Cost
- Operational Intelligence

IT Business Management

- Proj. portfolio
- Demand
- Resource
- App portfolio

Security

Security Operations

- Security incident response
- Vulnerability response
- Threat intelligence
- Trusted security circles

Governance, Risk and Compliance

- Risk management
- Compliance management
- Audit management
- Vendor risk management

Customer Service

Customer Service Management

- Customer service management
- Field service management
- Incident
- Problem
- Change
- Release
- Asset
- Knowledge
- Request management
- Cost management
- Communities

HR

HR Service Management

- Case and knowledge mgmt.
- Employee service centre
- Enterprise on-boarding and transitions

Business Apps

Platform Runtime

- Studio
- Service portal designer
- Delegated development
- Automated testing framework

What benefits will this service layer ultimately provide?
The main benefits this service layer will provide is standardization and automation; which ultimately delivers performance improvements in part due to clear data management and analytics within this layer (limited information offers low visibility in most organizations today).

Some direct improvements organizations regularly experience are:

Improved efficiency and reduced operational costs
Optimized processes and workflows, by automation and alerting, can remove unnecessary manual work. This is amplified when self-service capabilities are implemented.

Self-service efficiency and workload reductions
Employees can get to the solutions they need quicker through self-help. This means fewer telephone calls to the service desks or other business (support) functions.

A better ROI on the corporate ITSM solution investment
The more service portals are used the better the ROI on a per user basis becomes. Some existing systems may be phased out, hence there is further upside for additional technology cost savings through rationalization.

Improved effectiveness
Using a market leading ITSM solution and Enterprise Service Management all employee processes, incidents, cases, and requests are dealt with in the most effective manner.

Improved performance visibility
The use of a modern ITSM and ESM solution ultimately gives insight into the value of each business function and enables communication to customers and other business stakeholders.

Increased control and governance
ESM workflows can be used to implement internal controls, which in turn can provide insight into workflow actions as well as reporting.

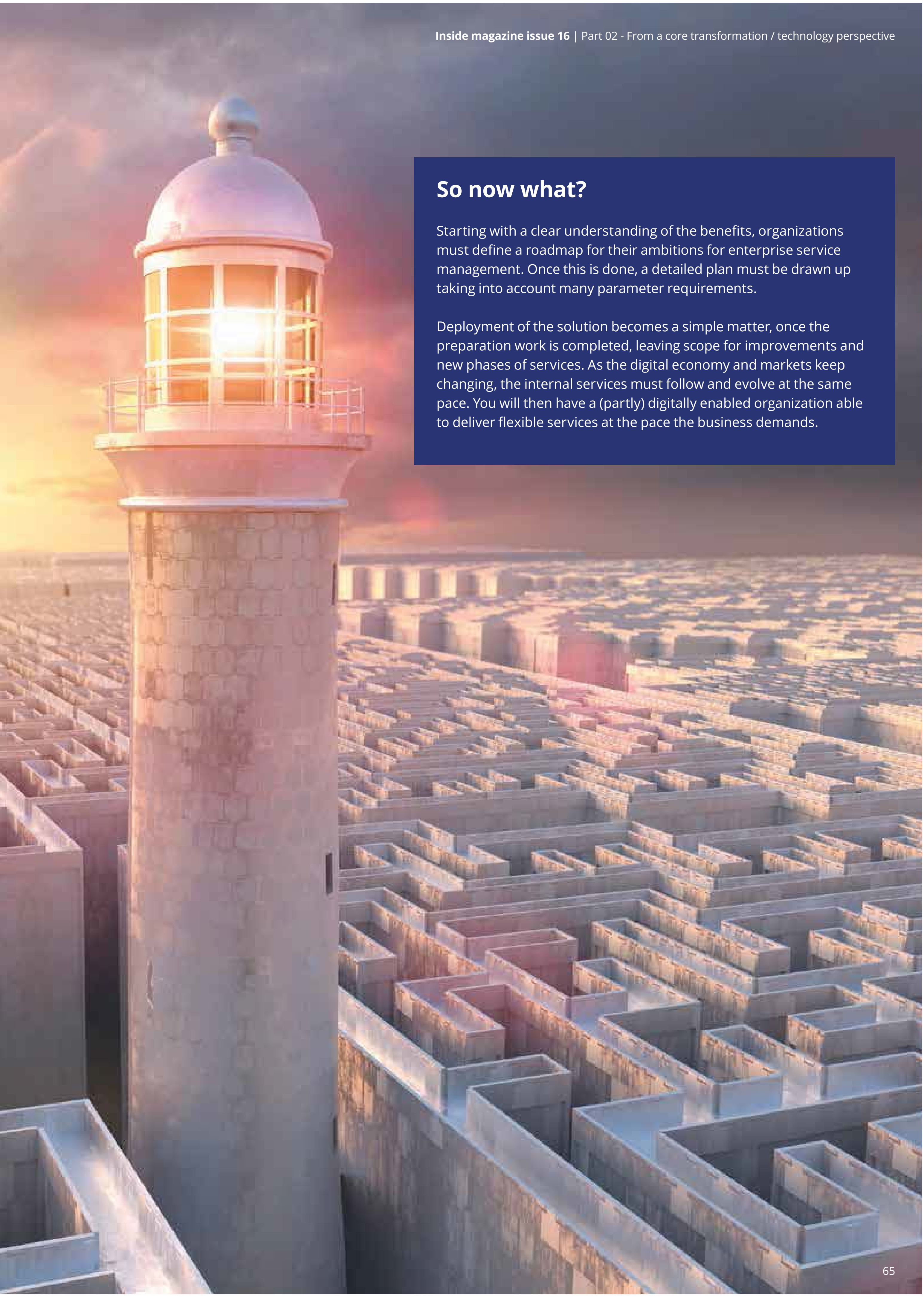
Better service and customer experience
ESM improves the corporate service provider game by better delivery against employee expectations across:

- **Ease-of-use**
- **Self-service**
- **Service request catalogues**
- **Knowledge availability and self-help**
- **Social or collaborative capabilities**
- **Anytime and anyplace access**
- **People or customer-centric support**

Improved access and communication channels, plus more effective communication
ESM solutions bring a choice of access and communication channels. Escalation and alerting capabilities also help to ensure that no ticket or communication goes un-actioned.

Cross business-function enablement
ESM solutions make it easier to combine business functions, e.g. the onboarding of new employees as well as the exist-process.

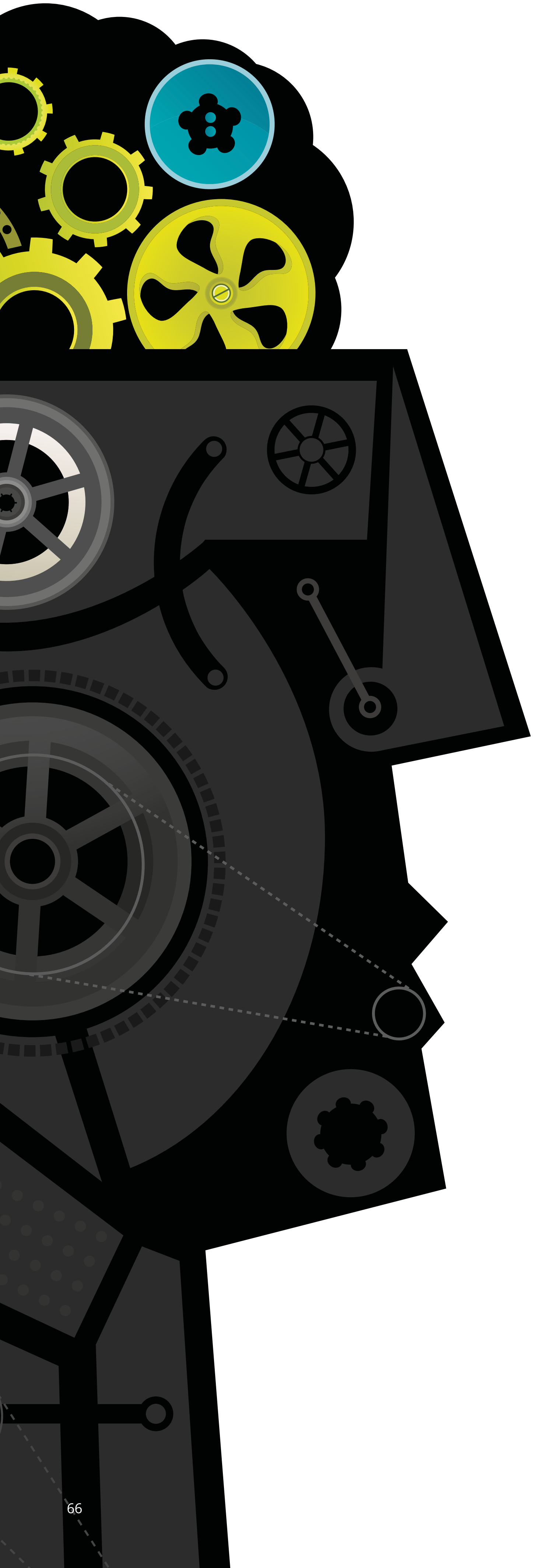
Standardization
Optimized processes is a common way of working with a common look and feel, and a common service model for employees. It offers the potential to provide a single point of service, no matter the service provider, companywide.



So now what?

Starting with a clear understanding of the benefits, organizations must define a roadmap for their ambitions for enterprise service management. Once this is done, a detailed plan must be drawn up taking into account many parameter requirements.

Deployment of the solution becomes a simple matter, once the preparation work is completed, leaving scope for improvements and new phases of services. As the digital economy and markets keep changing, the internal services must follow and evolve at the same pace. You will then have a (partly) digitally enabled organization able to deliver flexible services at the pace the business demands.



Your RPA Journey
From an idea to a fully functioning robotized center of excellence

Patrick Laurent
Partner
EMEA FS Technology Leader
Deloitte

Benjamin Collette
Partner
Strategy, Regulatory & Corporate Finance
Deloitte

Bernard Lecaillon
Senior Manager
Operations Excellence & Human Capital
Deloitte

Colm Cannon
Senior Consultant
Operations Excellence & Human Capital
Deloitte

Andrej Hocevar
Consultant
Operations Excellence & Human Capital
Deloitte

RPA represents a low-cost solution for process improvement. It is a relatively simple and inexpensive software-based technology, it sits on top of other applications, requires no special hardware, and works well in almost any IT environment. The immediacy of the gains can be attractive in comparison with a lengthy system overhaul or the cost of a globally sourced employee, whereby a "fully loaded" robot may equal about one-third of the cost of a globally sourced employee. RPA is particularly suitable for processes with a high human error rate, helping to avoid rework and aiding to produce 100 percent accuracy as well as other error implications like reputational or regulatory risks. For example, a process with an error rate of 10 percent done by 20 FTEs, would equal the savings of two FTEs.

RPA is an optimal solution for managing highs and lows in workloads. A process performed by robots is much easier to manage than one performed by a human. Multiple robots operating on a certain process can easily be redeployed or reassigned depending on workload, avoiding temporary hiring, training, and relying on a traditional learning curve.

Fast progress of digital technology and business models will also continue to shift the balance of global economic power, putting more pressure on CIOs to stay ahead of existing and emerging competitors. The many tools at the disposal of CIOs make up a long and comprehensive list. This paper will look at the journey a CIO would take if he or she settled on robotics as a tool to stay ahead of the technological curve.

Use of robotics

Robots used in RPA work by interacting with applications mimicking human actions, and can perform many of the mundane tasks such as rekeying data, logging into applications, moving files and folders, copying and pasting, and much more. Robots can be seen as a virtual workforce and can be assigned to middle and back-office processing centers. There are also front-office processes that robots can perform, for instance prompting contact center agents during customer interactions and automatically capturing call close notes. These types of activities and processes have been adopted in industries with intense manual or administrative processes, in sectors such as financial services, insurance, and healthcare.

One of the common features among financial service providers is that of dealing with large volumes of data and transactions. In the banking industry, there are simple processes like deposits and transfers that make for perfect RPA targets. For those businesses in the financial sector who have already adopted RPA, it has effectively transformed this transaction-laden industry into one that is fast, effective, and reliable. This has helped to improve customer service, as well as made the lives of those who work behind the scenes much easier and more efficient.

In the insurance industry, there are many processes that can be automated; examples include managing policies, filing and processing claims, underwriting, and the countless other administrative tasks. RPA enables insurance providers to manage all the necessary tasks across multiple platforms with ease. It also provides the scalability necessary to deal with the many changes and challenges businesses in this industry face on a regular basis.

The administrative side of healthcare involves lots of paperwork, large quantities of file and data management, and mostly manual repetitive tasks. RPA has helped encourage an already forward-thinking industry by streamlining the backend of operations to maximize efficiency levels, reduce errors, and reduce costs.

In summary, RPA can be used as a tool to increase engagement and satisfaction, and is an enabler of ongoing transformation that touches upon many dimensions of the workforce. It therefore needs to be connected to a broader talent strategy, and companies will need to change their operating models to maximize value. Simply put, the benefits of RPA easily transcend headcount and cost reduction. RPA offers great potential for businesses to become smarter and more efficient.

The RPA Journey

The successful implementation of RPA requires a comprehensive and inclusive approach. When it comes to leveraging RPA, companies generally fall into one of two camps: those that have launched pilots and are now trying to scale the technology, and those that are at the early stages of exploring its possibilities. One viable way to begin is with a prototype or pilot that will allow you and your organization to become familiar with RPA. It is important to identify sponsors with vision to promote the new technology and approve the future financing of the program in case of a successfully launched pilot.

Implementation begins by identifying the processes in your business that could benefit from RPA. To commence, conduct a high-level assessment of the potential process candidates for automation, document the resulting efficiencies and cost-saving opportunities to confirm whether RPA is a good fit. Not every process in the company may be suitable for RPA implementation. This savings baseline confirms a business case and is the starting point for internal discussions with sponsors and stakeholders to spark interest and obtain direction. Most importantly, this phase includes technology demonstrations of selected RPA vendors to serve as a proof-of-concept and platform for knowledge gathering.

Once the scope for applying this technology has been defined, the crucial next step is to define the objectives of the RPA initiative. The biggest mistake companies make during this phase is trying to avoid risk by selecting smaller processes without significant business impact. In fact, the main finding of the sixth MIT Sloan Management Review and our Deloitte Digital Global Study was that risk-averse companies struggle most with any kind of digital transformation. This will result in an unattractive business case for stakeholders and sponsors who approved the initiative.

Overall, RPA represents an opportunity to accelerate business strategy and maximize both growth and organizational performance through the automation of select processes and the redeployment or removal of excess capacity. As with any large-scale business transformation, the implementation of RPA should be considered holistically, covering business strategy, people strategy, process, and technology.

Integrating RPA into your organization’s DNA

The demand for implementing emerging technologies no longer poses most organizations much concern, however scaling and a clear strategy often prove difficult for less digitally mature organizations. Establishing a clearly defined vision is the first step when designing a strategy. Understanding the company’s holistic objectives and desired automation capabilities (e.g., RPA, machine learning, cognitive automation), will help to define the actual purpose of RPA implementation—reducing costs, accelerating growth, or other drivers. In order to meet the set objectives, an organization should define the delivery model, operating model, business case, and roadmap to deliver scalable robotics across the organization.

Re-envision corporate culture

A move to RPA will likely require a shift in working norms to enable the effective use of virtual teams, increase trust in technology, and embrace innovation and analytics. Technology has become a fundamental part of business, however the advantage and disadvantage of technology is that it constantly changes in order to further improve and create value. A flexible and changing corporate culture that can be easily shaped and enhanced plays a vital part of technology acceptance. RPA is no exception; in order for RPA to be truly successful and produce sustainable results, it has to be integrated into the corporate culture of an organization and fully embraced across the entire company. Stakeholders must be aware of how RPA will benefit them directly—providing them with additional flexibility, enhancing autonomy, or enabling them to focus on more demanding and value-adding tasks. Only then can RPA become an integral part of the work environment.

Organizational design

The necessity to understand the future state of human/robot interactions will have implications on organizational target design, changes to roles and responsibilities, spans of control, and workforce planning, among other things. Digital governance is a framework for establishing accountability, roles, and decision-making authority for an organization’s RPA program. A complete governance framework is crucial to successfully execute a RPA implementation, manage organizational change, redesign processes, manage future RPA demand, and communicate with stakeholders. Workforce planning and talent strategy will also play a key role in the success of an RPA implementation. Based on the outputs of workforce planning, organizations will need to reconcile the capabilities they have with the ones they will need, and devise a plan to develop and acquire the latter. An end-to-end review of the organization’s talent lifecycle, from recruitment through to transition, will be required.

Overall, RPA represents an opportunity to accelerate business strategy and maximize both growth and organizational performance through the automation of select processes and the redeployment or removal of excess capacity.

Change management

Successful change management is essential for a successful incorporation of new technology into corporate culture, but can be challenging, especially when trying to redefine a company's DNA. A good assessment of the potential obstacles is the first step to take. For example presenting employees with the possibilities of RPA will encourage their acceptance rather than resistance. It is critical that employees understand any and all impacts on their roles and how RPA will contribute to the bigger picture. A clear communication strategy will play a definitive role in the success of change management and RPA acceptance. All employees involved in and affected by RPA implementation will most likely have to deal with a role change, role elimination, or capability change. A targeted transition plan that addresses each of these types of change at both the individual and department levels will mitigate unnecessary confusion and enable a quicker arrival at a "steady state." It is important to identify and close the skill gaps. An end-to-end review of the organization's talent lifecycle, from recruitment through to transition, will be required.

Working with RPA

Once RPA is firmly incorporated into the organization's DNA, it is important to incentivize the use of RPA and aim at continuous identification of further RPA opportunities. Not all processes fit for RPA will be identified or implemented from the very beginning. Companies can set up different initiatives to accelerate the growth of RPA, including asking for suggestions from employees and set up a demand management process in order to forecast, plan, and manage the future ideas and demand for RPA.

Performance management set during the implementation phase focused on the RPA will help track the lessons learned through documenting prioritized opportunity business cases, including robot process design, challenges, complexity, dependencies, and benefits enabling easier and smoother expenditure of RPA technology on other processes. Capacity management on the other hand will ensure that IT resources are properly allocated and sized in order to meet current and future RPA requirements in the most cost-effective manner.

RPA Maturity cycle

A center of excellence (CoE) is frequently used when an organization needs to adopt and manage a new technology. Establishing CoEs for RPA will contribute to effectively deal with a rapidly evolving business environment and embed RPA into the organization's DNA. The CoE should have senior sponsorship who believes in RPA, champions RPA, and gets buy-in throughout the organization. The creation of a CoE should be considered from the very beginning when setting up the RPA vision with all the anticipated future technological changes and strategy in mind. To avoid the future rework or any quality issues it should be set up before any delivery has been started. Onboarding IT to the CoE will help create internal buy-in while allowing IT to build the knowledge and expertise of running and maintaining the robot workforce as RPA is scaled across the business.

Companies can set up different initiatives to accelerate the growth of RPA, including asking for suggestions from employees and set up a demand management process in order to forecast, plan, and manage the future ideas and demand for RPA.

How to move from RPA to RCA

RPA should be viewed in the full context of where it sits on the automation continuum. Organizations that have successfully integrated RPA will inevitably ask, "What's next? How do we traverse the path to more advanced cognitive automation?" Whereas for some organizations it may make sense to leapfrog RPA and go straight to cognitive automation; it does not have to be a linear progression.

Some companies are beginning to combine RPA with other technologies to automate not only human actions but human judgment, and eventually, intelligence. By combining RPA with cognitive and artificial intelligence capabilities, natural language processing, generation, and other emerging technologies, companies can create toolsets that can tackle processes that include judgment-based processes, predictive decision-making, and conversational user interfaces. Seen through this lens, RPA becomes a foundational technology for a digitally transformed enterprise that can evolve in step with other quickly advancing technologies. ●

Sources:

1. Robotic Process Automation: Keys to a Successful Implementation
https://www.scottmadden.com/insight/robotic-process-automation-keys-to-a-successful-implementation/

2. Automate this The Business leader's guide to robotic and intelligent automation (Service Delivery Transformation)
https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-sdt-process-automation.pdf

3. 8 Benefits of Robotic Process Automation
http://virttia.com/2015/09/benefits-of-robotic-process-automation/

4. Top 10 Strategic CIO Priorities For 2017
https://www.forbes.com/sites/oracle/2017/01/17/top-10-strategic-cio-priorities-of-2017/#29e3f8d94e42

5. Robotic process automation - A path to the cognitive enterprise
https://dupress.deloitte.com/dup-us-en/focus/signals-for-strategists/cognitive-enterprise-robotic-process-automation.html

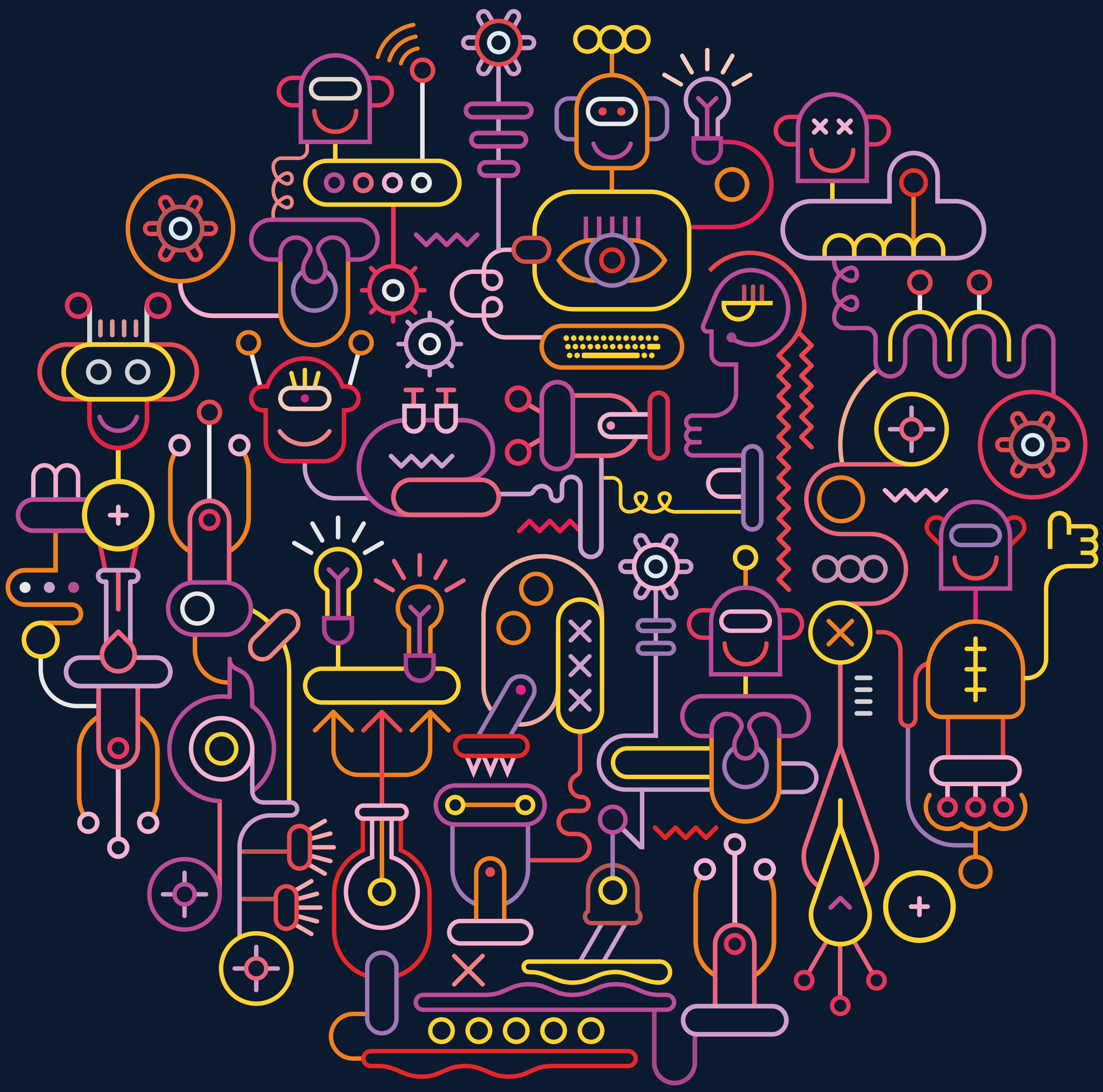
6. Automation is here to stay... but what about your workforce?
Preparing your organization for the new worker ecosystem
https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-fsi-automation-here-to-stay.pdf

7. Digital Finance: Why (and How) Robots Are Joining the Team
http://deloitte.wsj.com/cfo/2017/07/18/digital-finance-why-and-how-robots-are-joining-the-team-2/

8. Sixth Annual MIT Sloan Management Review and Deloitte Digital Global Study Finds Risk-Averse Companies are Struggling with Digital Transformation
http://www.prnewswire.com/news-releases/sixth-annual-mit-sloan-management-review-and-deloitte-digital-global-study-finds-risk-averse-companies-are-struggling-with-digital-transformation-300487650.html

9. Building a Digital Governance Program
http://m.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/GW2016/0808%204pm-SWiedman-Digital%20Governance.pdf

10. Centers of Excellence: Managing organizational skills
http://searchmicroservices.techtarget.com/tip/Centers-of-Excellence-Managing-organizational-skills



Yves Van Durme
Partner
Global Human Capital
Leader for Strategic
Change
Deloitte

Jean-Pierre Maissin
Partner
Technology &
Enterprise Application
Deloitte

Kris Van Steenberghe
Director
Human Capital
Deloitte

Roxana Moise
Senior Manager
Human Capital
Deloitte

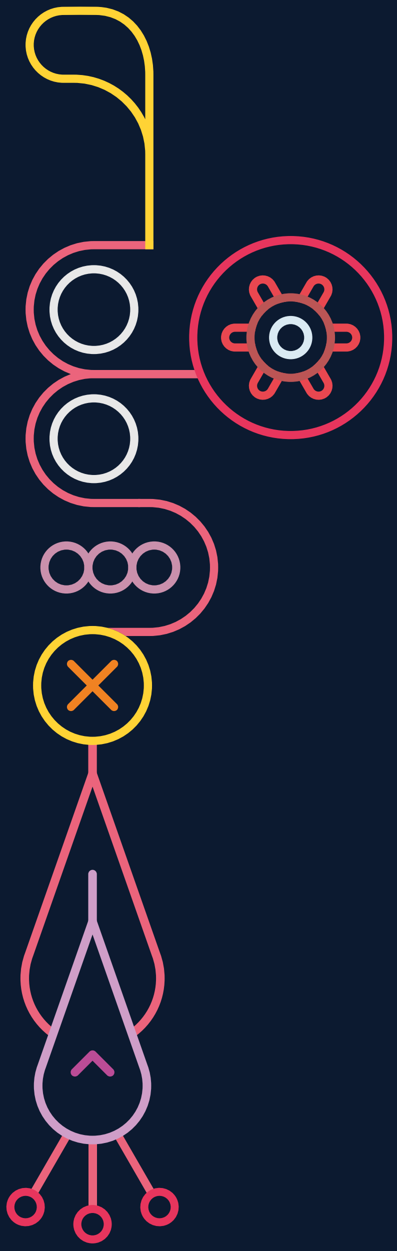
Accelerate the value of **technology-enabled business transformations**

Taking advantage of improved user experience is not as straightforward for corporate technologies as it is in our daily private life.

Leveraging technologies in a corporate context requires fully embedded technologies in the DNA of the organization, on top of technology adoption. Taking into consideration the new, disruptive, and innovative environment we are living in today, it is by mastering the art of change adapted to the ways we are living today that new ways of working are embedded faster and more effectively amongst the employees.

In response, Deloitte has Spotified the experience that drives value and accelerates measurable business results. It has Youtubed leaders, to enable them to deliver on the purpose, and has Uberized an experiential journey that is enabled by high impact engagements combined with digital technology. Deloitte has FitBited targeted behavioral interventions, to nudge and shape successful change adoption, and has Wazed people analytics throughout the lifecycle, driving a focused effort.

From Vision to Value: A new framework to accelerate technology-enabled business transformations
Improvements in customer experience, business growth, and reduction in operational costs are key drivers of technology initiatives taken by many organizations today. However, technology-enabled business transformations are famous to surpass budget and timing. Some of the main reasons are often not the quality of the technologies or processes deployed, but a variety of risks related to the way the leadership tackles the "people side of change." A technology-enabled transformation is not just about implementing more and better technologies, it involves congruence; aligning your company's culture, people, structure, and tasks to match disruptive and agile business-wide technology initiatives. Change is then more about the results extracted from congruence, than about the success of a series of isolated initiatives. ›



Typically leaders consider the "people side of change" around the start of the technology implementation process. Based on our experience we notice that successful technology-enabled business transformations embed the "people side of change" from the start of the transformation journey.

This poses the question of who is ultimately responsible for embedding the technology around the day-to-day of an organization's employees—in a sustainable and stimulating way. We see that in successful transformations it's the executive board who takes the responsibility and not only the CIO, HR, or the business.

In terms of allocating the responsibility, research has pointed out that soft skills such as having a transformative vision and solving problems are considered as critical success factors for a technology-enabled transformation. Purple people—those who possess a mix of business and technology skills—therefore seem to be the right candidates to counter major risks such as an unclear vision, lack of stakeholders' engagement and alignment, missing sponsorship, and inconsistent and irrelevant messaging, which all undermine the technology implementation success.

In this context, Deloitte developed From Vision to Value as a new change management framework based on psychology, design thinking, behavioral economics, scientific evidence, and Deloitte global-wide experience in driving transformational programs to support leaders in effectively managing the "people side of change" throughout the entire transformation journey in the technology-enabled world.

Many organizations struggle to deploy successful technology-enabled business transformations. They tend to treat change management as a separate project, which is poorly linked to the expected business results, inadequately led by its leaders, lacking a personalized and insightful application of behavioral science, as well as change adoption analytics.

The Deloitte From Vision to Value framework takes these lessons learned and generates value by the application of five key principles that were crystalized through the experience of several transformations.

From Vision to Value principles

Accelerated Business Value
An experience that drives value & accelerates measurable business results...

Leader Led
Leaders are enabled to deliver on the purpose...

High Touch, High Tech
An experiential change journey that is enabled by high impact engagements, combined with digital technology...

Underpinned by behavioral science
Targeted behavior change interventions to 'nudge' and shape successful change adoption...

Precise and measurable through analytics
People analytics throughout the change life cycle drives a focused change effort...

To highlight the From Vision to Value approach and the key benefits of the From Vision to Value principles in deploying successful technology adoption initiatives, we describe two case studies.

Case Study 1: Context
Consider the experience of a large organization in the financial industry that embarked on a CRM transformation with Salesforce to cover overall sales processes to be able to structure and capture customer information across different touch points and use this information for a personalized proactive approach anytime and anywhere. Over 5,000 employees have been estimated to be impacted by the new technology and need to adopt the new ways of working. Given that the institution was challenged to let go of a significant amount of people and new operational and risk procedures needed to be implemented, an innovative yet sensitively adaptable change approach was needed.

Case Study 2: Context
A worldwide organization in the life sciences industry implemented SAP as a result of a merger between two companies that needed to work as a single business. The goal of the SAP implementation was to integrate the production and distribution facilities. About 400 employees were heavily impacted by the new way of working as a result of the SAP implementation.

The challenge was to make sure that the impact on the business and the clients at go-live was as low as possible (i.e., products are still produced and shipped toward the right customers).

Accelerate value of the technology-enabled business transformation
Most project leaders find themselves relieved to leave elaborate business cases behind and start the practical “sleeves rolled up” work. However, it is exactly at the start of a project where efforts are needed to define how the business value that was put forward will be materialized, and, more importantly, accelerated throughout the project delivery.

Accelerated impact on the purpose is experienced through design thinking and immersion techniques such as change labs. Traditional and non-traditional change and communications activities are delivered to ready your business. You experience change activities that start up front but continue to include the practical support an organization needs to deliver the behavioral shift that fuels and sustains new ways of working and delivers business results.

Let’s take the example of the financial industry organization (Case Study 1) who embarked on a complex Salesforce implementation. To create alignment and commitment early on, the project team applied From Vision to Value techniques to develop five design guidelines that would guide all decision-making and messaging around the CRM implementation. This is important because CIOs and other business leaders rarely use the same parameters to define the success of the technology-enabled transformation. To measure the results of a transformation in a uniform way, it is imperative that leaders sing from the same song sheet, which will create the visibility and transparency they need to demonstrate value throughout the organization.

Throughout the project, these principles played the role of a guiding light in trade-off situations. The project principles were collaboratively created and committed to by leaders during a change cockpit session. This is a particular setup where design thinking, psychology, and a time-boxed approach are used to empower those in the business that need to pilot the change with a roadmap and tools to do so. It is a one-day scripted session that takes place in a compelling and unique environment and is designed to build a sense of ownership and common language about the transformation. After the session, the leaders then actively lived these principles in their work streams and included these explicitly in communications toward affected end users. For example, during the opening of the annual leadership conference, the five principles were elaborated upon, rather than demonstrating the CRM platform itself, hereby setting the scene for project expectations. Moreover, when discussing a potential extra tool integration, the business case did not include the costs and benefits of the integration, but was based on the applicability of the five principles. Those five principles were:

I Keep a strong focus on the Meaningful Viable Product

II Clear leadership commitment

III Adoption over adaptation

IIII Co-creation and co-validation with empowered teams

𝍸 CRM for all, not for everything

even used during the backlog crunching and sprint configuration as these defined the user stories that were going to be delivered within a three-week span. It is thanks to a clear alignment on the five principles that the project was delivered on time and within budget—as no time was lost getting distracted long approval procedures and no money was wasted on features that were not core to what a CRM platform is aiming to achieve. The result is a platform that end users considered as meaningful as of day one, and more importantly, that was fully embedded in their ways of working thanks to a complete experiential change journey.

Enable leaders to deliver on the purpose
Leaders often underestimate the importance of their role in the context of a transformation. When leaders announce a major transformation initiative and delegate its execution, they are somewhat missing the (project) action. Employees listen to the leader, they look up to the leader, and they expect the leader to guide them throughout the overall journey.
Leaders are considered to be the engine of a successful technology-enabled business transformation, enabling and enhancing the speed of adoption. Their role is to inspire and support employees to get through the "roller coaster" of emotions inherent to ensure a seamless transformation initiative in order to shorten the transition period whereby productivity loss is significant:

- **Vision:** Leaders play a key role in developing a shared sense of direction – clarity on what is changing, why it needs to change, and how the organization will benefit.
- **Sponsorship:** Leaders demonstrate sustained, strong, unified sponsorship
- **Communication:** Leaders establish and communicate the business context and rationale; establish a climate of genuine openness to concerns
- **Ownership:** Leaders are responsible for goal setting, owning the business plan, and monitoring its progress
- **Risk Management:** Leaders mitigate resource allocation, timeline, and scope review
- **Celebrate:** Leaders support and encourage recognition to manage change fatigue

Consider the experience of the leaders in the Life Science organization in Case Study 2 above. The project sponsor gathered his project stream leads (all leaders in the organization), steering committee members, and senior leaders in a High Impact Session one month before go-live (More details on a High Impact Session can be found in the third From Vision to Value principle).

The objective of this creative and collaborative working session was to align and decide on the key actions for a successful SAP implementation. This was a critical milestone before go-live, as leaders were not attending steering meetings; they had no idea about the issues and risks identified by their teams. The outcome was an aligned team, with key actions defined and clear responsibilities assigned.

Equipping and empowering leaders with the knowledge and tools to effectively and efficiently drive, sponsor, and engage employees rather than acting as a silent partner of the transformation represents one of the key success factors of any technology adoption program.

When leaders announce a major transformation initiative and delegate its execution, they are somewhat missing the (project) action.

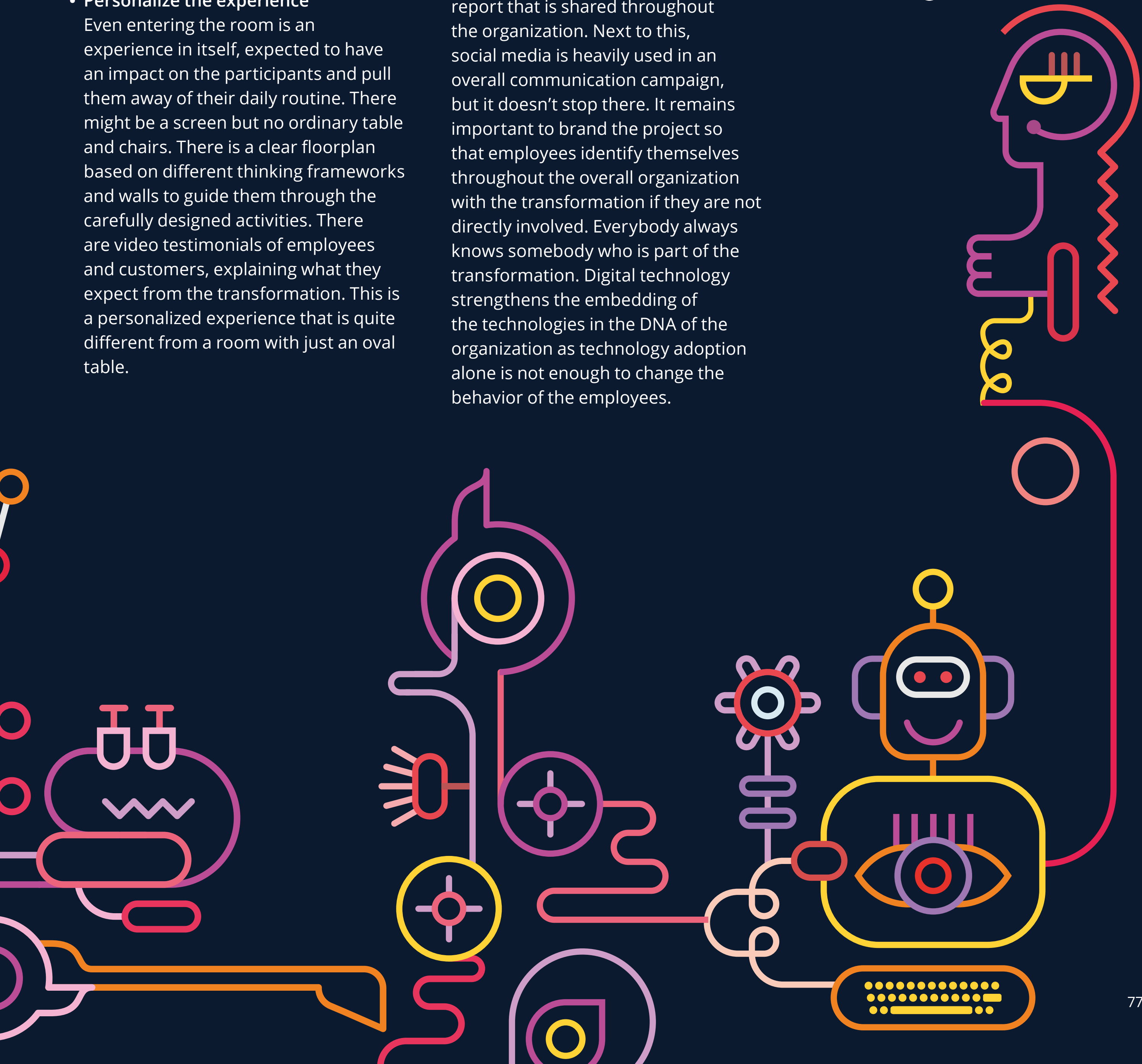
Design an experiential change journey that is enabled by high impact engagements, combined with digital technology
How many of you have been involved in one of those meetings where you are sitting at an oval table, being presented with carefully designed slides capturing critical points on the transformation journey while you are picking up on business emergencies through your smartphones or emails? In reality, embedding technology-enabled business transformations in the DNA of the organization is all about achieving impact and involvement.

- **Personalize the experience**
  Even entering the room is an experience in itself, expected to have an impact on the participants and pull them away of their daily routine. There might be a screen but no ordinary table and chairs. There is a clear floorplan based on different thinking frameworks and walls to guide them through the carefully designed activities. There are video testimonials of employees and customers, explaining what they expect from the transformation. This is a personalized experience that is quite different from a room with just an oval table.

- **Build engagement and shared purpose**
  Participants are taken along a disruptive and intense journey. They are actively involved in the delivery of the session using scripted scenes tailored to the challenges of the specific organization. They learn from each other, co-create their business future, and align on how to manage their project. The results are pragmatic and fully owned outcomes, with a clear vision, action plans, and communication activities.

- **Use digital technology**
  Furthermore, all this hard work is translated into a video and a visual report that is shared throughout the organization. Next to this, social media is heavily used in an overall communication campaign, but it doesn't stop there. It remains important to brand the project so that employees identify themselves throughout the overall organization with the transformation if they are not directly involved. Everybody always knows somebody who is part of the transformation. Digital technology strengthens the embedding of the technologies in the DNA of the organization as technology adoption alone is not enough to change the behavior of the employees.

In case of the Life Sciences organization (Case Study 2), branding supported increased awareness of the transformation and buy-in, for example branded mugs, beach flags at every plant entrance at go-live, branded sweets, and users wearing t-shirts with the project logo to make it easy to find them in case of questions. The creation of an overall project identity is key to deliver a smooth go-live and to embed the new way of working into the DNA of the organization. In terms of communication, a technology adoption project is not any different from a business project: You need to speak with high touch and use high tech to make it stick.



Underpin your technology transformation by behavioral science
Arthur Bracks's quote, "Software doesn't build relationships, people do," often passed through the floors at the financial industry organization during their journey for the Salesforce implementation (Case Study 1). When spending significant amounts on a customer relationship platform, this might not be the quote that one wants to hear. But there is a truth to it: The new platform should be used by the employees to build relationships, for it to be worth the investment, and so it did. In a first release of 325 users, 100 percent user adoption has been reached after only three weeks and 8,400 interactions and more than 3,400 opportunities have been created by end users after one week. In the weeks following the key feature, usage increased with 50 percent. Leads are now resulting in 20 percent more business generation and more than 10,000 contributions to the collaboration platform, indicating the increased collaboration to generate business. Finally, end users now only use two tools instead of four to five tools to support their customer engagements, which results in significant time saving. These results are materialized thanks to a multitude of learning initiatives. The key is to design the learning experience keeping the shift in the ways of working (what and how) for the impacted end-user population in mind.

This goes beyond knowing system functionalities and features. It is all about painting a compelling picture of the key activities that the end-user will need to do differently.

Using insights in behavioral science, moments that matter (i.e., key moments in the working life of an end-user where the technology would have a significant impact) have been identified. For example, preparation of client conversations, managing an open opportunity to results, selecting attendees for an event, etc.

These key activities showcase how end-users need to act differently. They were also used as a basis for developing training sessions. Trainings should not be focused on what the platform can do, but rather on what the platform can do for the end-user (i.e., how the platform will add value to her day-to-day work), focusing on the events where behavioral changes will be most critical for the success of the technology.

Likewise, moments that matter can be leveraged in different circumstances during the project lifecycle such as a leadership conference or a communications campaign to showcase what the new technology means for people in the organization

Adoption analytics can boost your organization's chances for success in driving technology transformations. They replace hunches and guesswork with insights and quantifiable data about stakeholder issues and concerns.

Business Case

Leadership support & buy-in

Training

Communication

Culture

Customer orientation

Use analytics to measure and tailor technology adoption.
Adoption analytics can boost your organization's chances for success in driving technology transformations. They replace hunches and guesswork with insights and quantifiable data about stakeholder issues and concerns.
In the financial services organization case (Case Study 1), before the launch of the CRM platform, the readiness for adoption of the technology has been estimated per region at the end-user and manager level. The assessment entailed both quantitative data—which can be compared to post-go-live and with other audiences—as well as qualitative data, related to six dimensions:
The assessments showed the side effects—both positive and negative—of the CRM implementation.

On the one hand, the CRM platform significantly contributed to the planning of the agenda for the customer-facing personnel, even though it was not designed for such purposes. This allowed a more efficient scheduling of customer appointments to make the best use of each interaction with the client.
On the other hand, the results of the data analysis pointed to a leadership problem in one of the regions that caused the conditions to be suboptimal before launching the platform.

True magic happens when pre-go-live readiness is combined with adoption figures post-go-live, both as assessed by the end-user group, as well as extracted from the technology platform itself. This is when preparatory work is fully materialized and the perception of the platform can be compared to the actual use. For example, the results of the data analysis showed a gap between managerial speech—supportive of the platform benefits—and their actual use. These insights allowed the organization to focus their change efforts on the right initiative and the right stakeholders at the right time to ensure efficient technology adoption.

To improve customer experience, leaders need to consider the "people side of change" at the start of the transformation journey. Next to this, not only the CIO but the complete executive board need to take the responsibility of turning the transformation into a success. This happens when the new way of working is completely embedded in the DNA of the organization, on top of technology adoption.

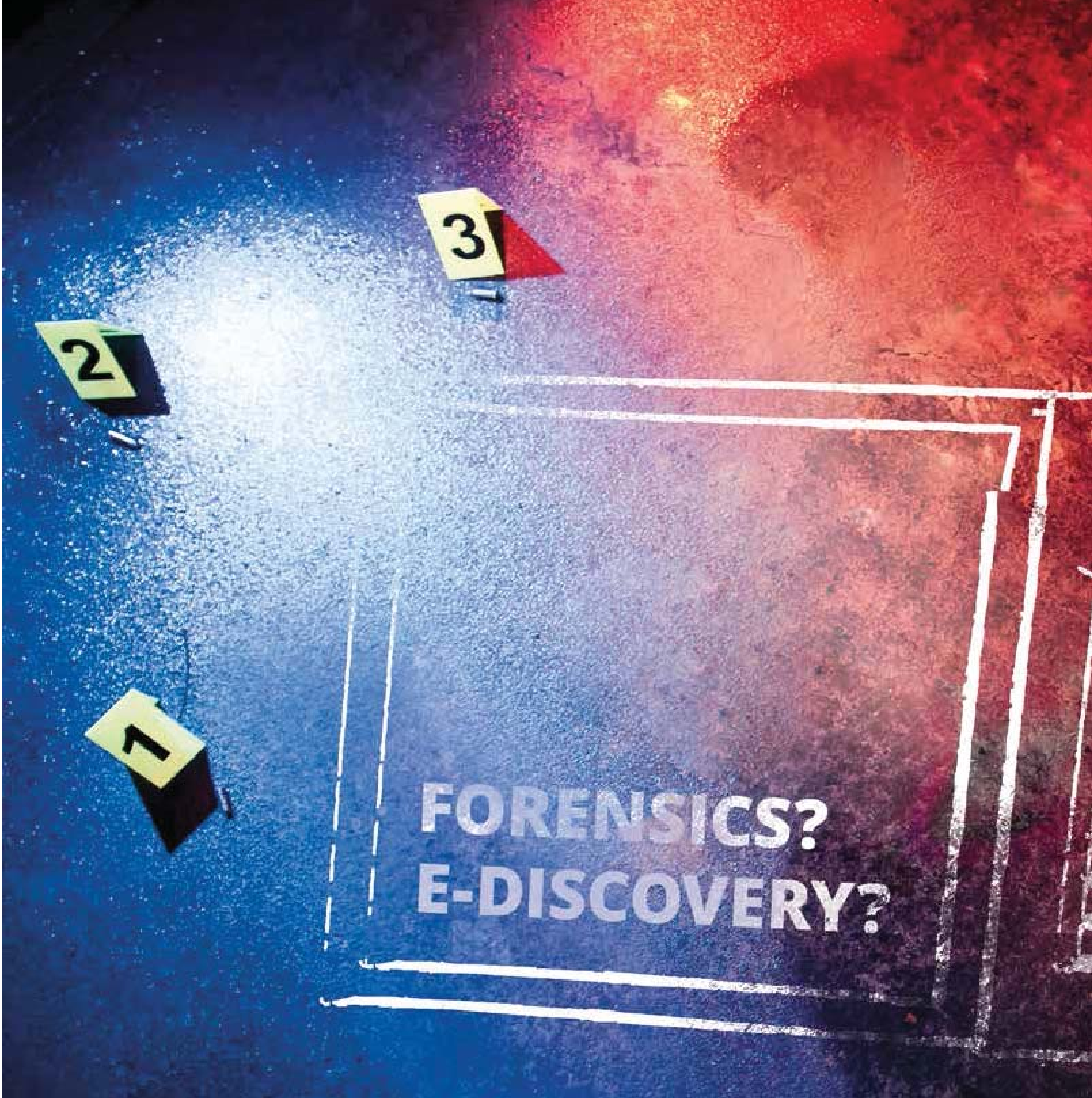
Making it happen efficiently and matched with the new technology trends in a disruptive, innovative, and agile environment requires more than traditional ways. It encompasses a series of methods and a distinctive and compelling approach, which fueled the creation of the "From Vision to Value" Deloitte framework.

If your organization is struggling with effectively delivering change through technology adoption programs, you might want to ask yourself the following questions:

01. Do you, as a CIO, have the same explicit aligned definition of success of the transformation as the business leaders? Case Study 1 strived toward a successful go-live within time and budget versus improved customer experience. The definition of clear "guiding lights" enabled the leaders to work together on the same goal to increase the potential of the technology investment. A clear dashboarding approach is key to track progress and increase common understanding.
02. How do you work with new methods like Agile, UX, or sprints? These methods should drive acceleration yet it cannot only be a program or project related way of working. The main change is the way of working and not the implementation of the new technology. CRM software doesn't build relationships, it enables people to accelerate at getting better at doing it (Case Study 1). Also SAP will not create new materials, it will enable the employees to speed up the process from production to end-user (customer).
03. How do you design the change journey for technology implementations? Building engagement and shared purpose are essential. To make this happen, avoid assumptions (e.g., they know what is happening or why we are doing it). They are dangerous while open and transparent communication will increase overall awareness and understanding about the business transformation. ●

Part 03

From a risk and cyber perspective



Roland Bastin
Partner
Risk Advisory
Deloitte

Gunnar Mortier
Senior Manager
Risk Advisory
Deloitte

THINGS YOU NEED TO KNOW BEFORE DELVING INTO THE WORLD OF DIGITAL EVIDENCE

Businesses are increasingly facing growing risks involving digital evidence, which puts them in considerable jeopardy if these risks are not adequately anticipated and managed. These range from fraud, theft of assets, complex litigation to disputes that include accusations of financial mismanagement and malfeasance, to name but a few. Legal actions can be taken both by and against organizations and involve parties such as regulators, shareholders, competitors, customers, employees, and hackers. These activities can consume significant resources across legal jurisdictions in multiple areas of the world, and if not handled correctly, risk may be further compounded.

As an example, a civil e-discovery investigation could be looking at emails of employees and how certain business deals were conducted.

E-discovery and digital forensics

Digital forensics, also sometimes called cyber forensics or computer forensics, is concerned with techniques applied to the process for collecting, examining, analyzing, and presenting evidence originating from digital data sources to courts. The term “computer forensics” is becoming less appropriate to describe digital or cyber forensics activities, as what a computer can be has changed and the scope of digital data sources has become increasingly large. Data sources typically do not only include the various types of computers one easily thinks of (desktop, server, laptop, tablet, mobile phones etc.), but also computers such as the ones in GPS systems in cars, in the cars themselves, and as was recently shown in a US court case, a pacemaker! One should also not forget that digital data sources that can be forensically examined include any type of media that will store digital information (including the cloud) and computer networks.
Digital forensics may seem highly similar to e-discovery, and there is an overlap, but there are differences between digital forensics and e-discovery that are important to understand. However, different sources may not always concur on the subject.

E-discovery typically pertains to civil cases and refers to a well-defined process that will identify and preserve what is often defined as Electronically Stored Information (ESI) in order to determine if this information is relevant or privileged and will produce this information to be used in court. As with digital forensics, these activities can obviously also be conducted for internal purposes, i.e. without the certainty that there will eventually be a court case of some sort.

Digital forensics on the other hand will mostly relate to criminal cases and is typically linked to detailed analysis and investigation of digital evidence, including metadata, that is not normally used or visible. More often than not, a determination will be made of how devices and data were used by the defendant in the criminal case, which includes distinguishing user-generated data as opposed to system-generated data.

As an example, a civil e-discovery investigation could be looking at emails of employees and how certain business deals were conducted, while digital forensics could try to find out if an employee had been using his laptop to exfiltrate customer information for their future private use.

E-discovery and forensics require different tooling, though the lines are blurred. For instance, information received on a hard disk may be imaged using the same tools in both cases. There are however specific tools for e-discovery that are related to the workflows for counsel for the culling of selection of data and eventually production. There are also different tools for digital forensics, used for detailed investigation, such as toolkits for the collection of data from mobile devices or tools for disk analysis that will attempt to recover information from deleted files or re-formatted disks. Even more importantly, in addition to different tooling, the two domains require specialists with different expertise.

Common challenges

The general requirements for evidence, including digital evidence—whether in the context of digital forensics or e-discovery—are that evidence should be relevant and admissible. This implies that digital evidence has to relate to the case and has to have been properly obtained and preserved, because evidence must be reliable. Properly obtaining means that breaches of law to obtain evidence, which may include breaches of privacy law, have to be avoided. It is quite important to be able to rely on the advice of legal counsel in order to avoid cases where evidence has not been properly obtained and can therefore not be used. Organizations should also be aware that stumbling on a crime in progress can require immediate notification to law enforcement authorities. Admissibility of evidence requires evidence to have been correctly preserved and not tampered with or accessed and potentially modified under unproven circumstances, which means there could be doubts about the integrity and therefore the validity of evidence—making it unreliable and therefore unsuitable for use. This is called continuity of evidence in the UK, or chain of custody in the US.

The role of legal counsel in these matters is vital because they will give advice on the relevance or admissibility of evidence, which will include looking at proportionality when privacy law is applicable. Obviously, legal counsel also plays a key role in the defense of any organization when litigation is involved. It should be clear that good collaboration between counsel and technical teams is vital throughout the entire process of digital forensics and e-discovery, as it will be explained later on. One of the things that makes this hard is that evidence is now rarely located on a single device; multiple devices and especially the cloud make identification of relevant sources of data and data collection more challenging.

Digital evidence is also fragile. Accidental or deliberate change, partial or complete destruction and relocation easily happens and can turn evidence into something unusable. Criminal acts add further complexity because attacks can be hidden through the use of botnets and all kinds of counter-forensic techniques.

As if these problems weren't enough, technology can make things harder. Computer media such as SSDs (Solid State Disks) can potentially destroy parts of the evidence of their own volition, without instructions to do so from the computer or user. The use of some technologies can also make data collection without modification impossible, for instance during the capture of live memory or of collaboration tools where multiple users can be working on documents as the capture is executed, to name but a few. Arguably, information glut is also part of the technological challenges because of the evolution in media sizes and cloud storage. Volumes of data that need to be handled have become formidable (potentially even for a single person under investigation) and without integration and product expertise, the majority of off-the-shelf forensics and E-discovery products can simply not handle the demands of high volume projects.

Criminal acts add further complexity because attacks can be hidden through the use of botnets and all kinds of counter-forensic techniques.

Basic principles for the handling of digital evidence

The ACPO (Association of Chief Police Officers) guidelines provide guidance for the handling of digital evidence under four principles in their good practice guide. These principles are also highly relevant for other parties than the police.
Those principles can be summarized as:

01. Any action taken should not change data on computers/media. This means integrity of evidence should be preserved to the greatest extent possible.
02. If it is necessary to access computers/media, the person doing so must be competent and be able to give evidence regarding the relevance and implications of what they did.
03. There should be a record of processes applied to any evidence and these records should be kept. One of the key reasons for this is achieving reproducibility, i.e., if the evidence is provided to a third party, the third party should be able to obtain the same results or outcomes based on the same evidence. The principle of reproducibility also links to integrity (under principle 1). If the evidence has been modified, then it may no longer be possible to obtain the same results from the original evidence.
04. The final principle relates to having a person in charge of the investigation to ensure laws and regulations as well as that the above principles are adhered to. It is important to note that properly obtaining evidence is addressed under this principle as well.

Applying the principles – process makes perfect

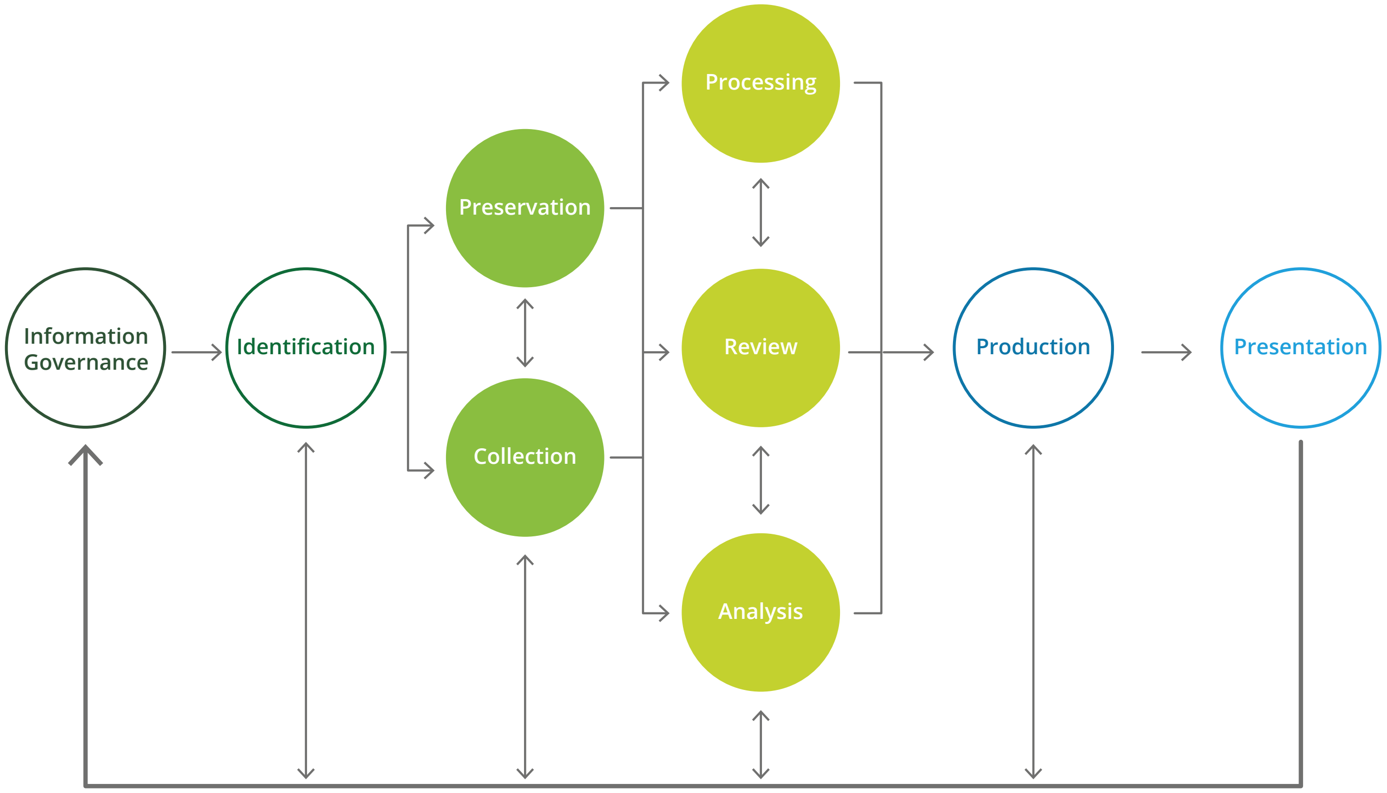
In order to keep evidence admissible and more generally manage risk and increase the likelihood of achieving the intended results, it is important to follow a predictable process for carrying out any investigation.

Typically such a process is described as containing the following steps in the digital forensics domain:

01. **Collection:** often called the "data collection," concerns the collection of digital evidence
02. **Examination:** the examination focuses on early case assessment, data reduction, removing duplicates, and irrelevant information
03. **Analysis:** the data obtained after the examination stage has to be analyzed in order to be suitable for presenting in court. The matter of wrongful acts and intent come into play at this stage
04. **Reporting:** the last stage concerns the preparation of reporting suitable to be used in a court of law

In the context of E-discovery, the EDRM model is used. This model essentially contains the same components as the previously described model, but offers more detail.

Electronic Discovery Reference Model[1]



[1] EDRM data model as per http://www.edrm.net/frameworks-and-standards/edrm-model/ © EDRM.NET

The EDRM model is composed of the following steps:

- **Information Governance:** Adequate management of information – raises the issue of E-discovery/forensic preparedness
- **Identification:** Identify where relevant data may be located and determine its nature
- **Preservation:** Same principle as in forensics, ensure evidence remains admissible
- **Collection:** Gathering evidence for further use in the E-discovery (forensics) process
- **Processing:** Reducing the volume of evidence (e.g., de-duplication), eliminate irrelevant data and potential conversion for review and analysis (text extraction, indexing etc.)
- **Review:** Evaluating for relevance and privilege
- **Analysis:** Evaluating evidence for content and context, including key patterns, topics, people, discussions etc.
- **Production:** Delivering results/outcomes in an appropriate form (may be specified in detail, see for instance the United States Attorney's Office specifications)
- **Presentation:** Present the results

In order to keep evidence admissible and more generally manage risk and increase the likelihood of achieving the intended results, it is important to follow a predictable process for carrying out any investigation.

E-discovery/forensics preparedness

Organizations are often not well prepared for cases where forensics or e-discovery is required, which can be highly detrimental to them. Preparedness consists of proactive activities which make the essentially reactive activities of digital forensics and e-discovery more predictable and reliable. The lack of preparedness may convey an unfavorable impression to courts and authorities, which can hamper successful litigation (e.g. mishandling of [potential] evidence). Lack of preparedness also negatively impacts (information security) incident handling capabilities. All of these factors increase levels of risk and cost.

It is a mistake to think that all of this only affects larger organizations, medium size (and even small) organizations can be affected as well, because threats that require forensics or e-discovery preparedness remain quite similar irrespective of organization size. Organizations of any size should achieve an appropriate level or readiness, i.e., a capability to adequately handle the different stages of the forensics/e-discovery process, in order to be able to use digital evidence for its intended purposes.

Some of the examples we encounter include:

- Organizations that have issues determining where their data is, which includes data on backups (how many, when, mechanism used to backup, exclusions), in the cloud, and any other instances of data. This can be a surprisingly hard nut to crack. It can cause significant delays in the process of e-discovery or digital forensics and may cause potential evidence to be overlooked or neglected
- Problems in producing data in bulk; often nobody has wondered how all transactions can be "pulled out of application X." The inability to produce data in bulk can be worse in cases of cloud services
- The IT department (and other parties) prodding around on a device of an employee can easily destroy all chances of using it as evidence
- Lack of authoritative information on who is the present "owner" of a device (inventory), including basic things such as the signature of the device owner for receipt of a device
- Unauthorized processing of information, i.e., prohibited by laws or regulations, and therefore not admissible
- Lack of policies that clarify what an employee is allowed and not allowed to do

Digital forensic and e-discovery readiness will maximize the ability to use digital evidence, thereby reducing the risk and cost of investigation while increasing the probability of a successful litigation. This involves more than ensuring adequate levels of (information) security.

Information security is more concerned with the protection of the properties of confidentiality, integrity, and availability of information, which normally will not include comprehensive forensics and E-discovery preparedness. Key activities will include the following:

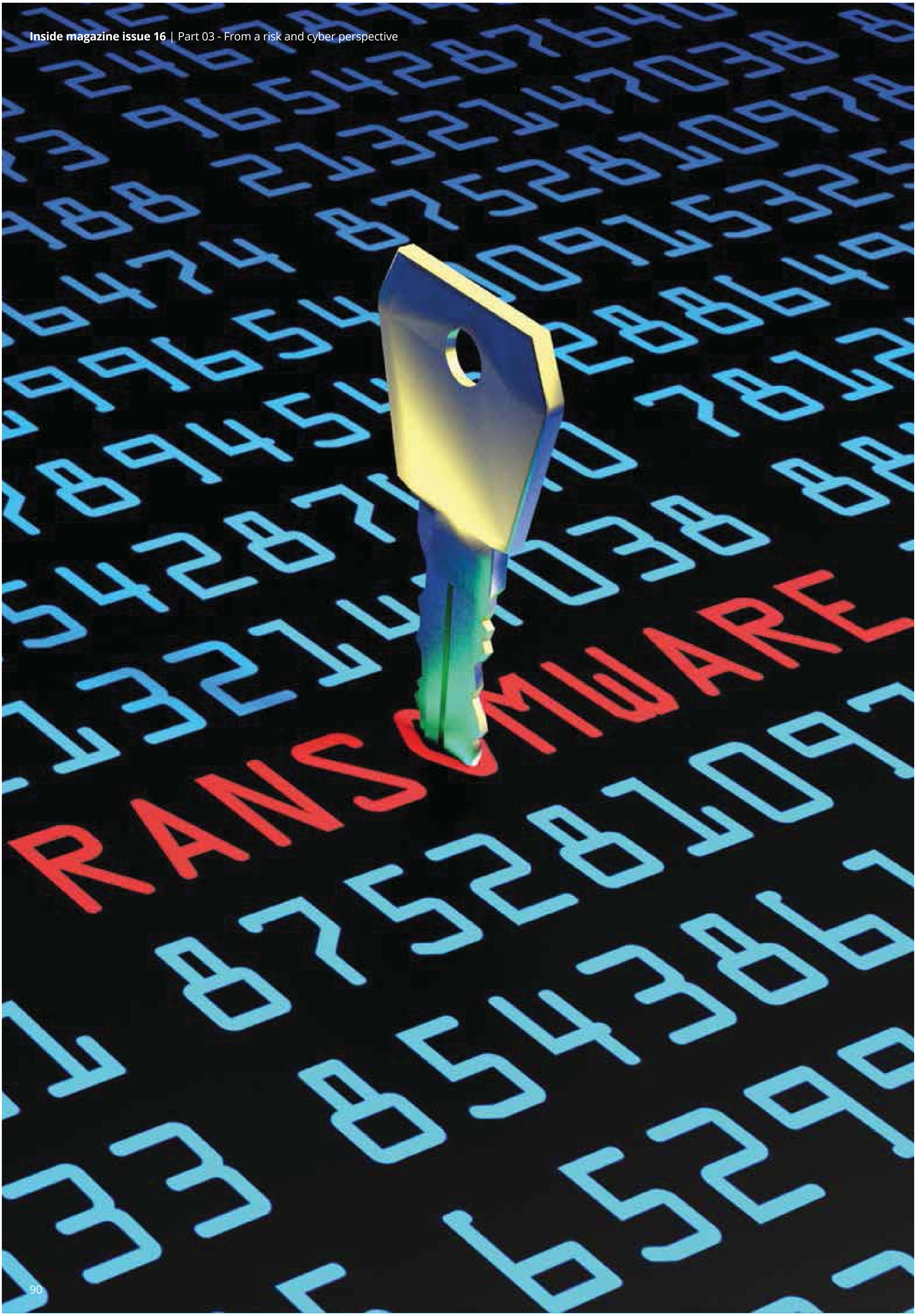
01. Define scenarios that require digital evidence. This is a practice that is extremely similar to preparing scenarios for (information) security incident handling, but concentrates on digital evidence scenarios such as when an organization has been hacked, data breaches, regulator/law enforcement requests, etc. There will be overlap between scenarios for security incident management, business continuity, and these scenarios; it is important to ensure integration.
02. Identify the sources and types of evidence. Even for smaller organizations this is becoming more complex. It is important to know where your data is and how this data can be exported (including bulk export). Data properties are also important to know, as is their relation to business processes.
03. Determine the requirements for gathering the evidence (collection/preservation); this includes addressing continuity of evidence.
04. Determine the requirements for the rest of the e-discovery/digital forensics workflow (see EDRM model).
05. Document and ensure the necessary resources can be made available in the required time frames. Documentation including policies (digital forensics/e-discovery readiness policy), standards, and integration in existing processes is key. Resources, also if these are external, are highly important to consider. This ranges from skilled and experienced staff to special purpose digital forensics infrastructure.

It is important to never forget there is not only a technical but also a legal angle to readiness. Readiness therefore not only requires support from e-discovery/forensics specialists but also from legal counsel with experience in such matters. ●

It is a mistake to think that all of this only affects larger organizations.

In conclusion

It is easy to get things wrong when digital evidence is involved. Applying good practices for handling digital evidence is required. In order to achieve this, the best approach is a proactive one that includes forensics/e-discovery readiness as a mechanism for not only ensuring digital evidence is handled correctly, but also reduces risk and cost by ensuring there is an ability to make informed decisions. Doing so involves striking the right balance in committing resources for digital forensics/e-discovery readiness in order to achieve a sufficient level of readiness capabilities. This involves addressing both the technical and the legal angle.


RANSOMWARE

The aftermath of ransomware

Stéphane Hurtaud
Partner
Cybersecurity
Deloitte

Laurent de la Vaissière
Director
Risk Advisory
Deloitte

Yasser Aboukir
Manager
Risk Advisory
Deloitte

The first six months of 2017 have seen an evolution of ransomware, producing more viral variants unleashed by cybercriminals and alleged state sponsored players.
In May 2017, we experienced an unprecedented ransomware attack (WannaCry), which affected a significant number of organizations globally across a wide range of industries.
A new bar has been set for cybersecurity teams across financial services institutions to defend their mission-critical information assets in the coming months. While the occurrence of new cyberattack methods is not going away, there are immediate lessons that can be learned and proactive steps to be taken by organizations to keep their businesses resilient against ransomware threats.

In today's current technological climate, most people are familiar with ransomware one way or another. This is no surprise considering the recent increase in outbreaks of ransomware and malware, with examples including WannaCry on 12 May 2017 and NotPetya (or Nyetna) on 27 June 2017. Nearly every day there is another story about a ransomware attack in the news. The US Department of Justice reports[1] that an average 4,000 daily ransomware attacks have taken place since January 2016. Ransomware has become a sizable international business, and it is now estimated that the global cost for organizations will reach US$5 billion by the end of 2017, up 400 percent from 2016 estimates. The average ransom requested has risen to US$2,500,[2] but this number pales in comparison to the hours of lost productivity businesses suffer, and the resources spent trying to recover the data, as well as the time and effort needed to determine the extent of the breach to ensure that the damage has been contained.

[1] How to Protect Your Network from Ransomware, US Department of Justice, 2017

[2] The Rise of Ransomware, Ponemon Institute LLC, January 2017

The significant risk magnitude of ransomware

The untold cost of ransomware to business

Ransomware's aftermath can be more costly than the ransom itself. For instance, a global logistics provider from the US reported the NotPetya ransomware attack amounted to US$3 million and a global manufacturer from France reported the same attack would drain about US$290 million in sales this year. A few months after the NotPetya ransomware attack, the public reports of financial losses in the press or SEC filings amounted to several hundred million dollars and this could be just the tip of the iceberg.

Unless good backup procedures are followed, recovering data after a ransomware attack is time-consuming and in some cases impossible. During a ransomware attack, stress, downtime, and system recovery can cost users and organizations weeks—even months—of productivity. Small business owners can lose customer trust, intellectual property, vital records, and at times direct reputational damage. In terms of profit, a ransomware attack cost can range from a few hundred euros to millions in fees, penalties, and lost or a drop in sales.

The ransomware landscape in FSI

The breadth of information that financial services store about their customers makes them prime targets for ransomware attacks. Financial services firms and banks agree: 55 percent list ransomware as the biggest cyberattack threat vector. Nearly one third of them also say they have lost between US$100,000 and US$500,000 due to ransomware attacks.[3]

Credit unions and small banks are seeing significant jumps in ransomware attacks. They experienced 81 percent of total incidents in financial services and banking in 2016, up from 54 percent in 2015[4]. This is largely due to the fact that they traditionally have smaller cybersecurity budgets and resources than larger counterparts.

Ransomware under the GDPR radar

The General Data Protection Regulation (GDPR) focuses on strengthening and unifying data protection for all individuals within the European Union. Concerned organizations are busy preparing their compliance in respect to this new regulation. A big part of it is related to avoiding and responding to personal data breaches.

The definition of a personal data breach based on the GDPR document means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

This broader definition can include many different security incidents, including ransomware attacks. This means that, in the context of compliance with GDPR, organizations might be obliged to notify ransomware infections to the relevant authorities, as well as to the affected individuals should it result in a high risk to the rights and freedoms of these individuals[5].

Incident response plans need to be updated and include checks to determine whether the GDPR notification obligation is triggered by different incidents, related or not to ransomware attacks.

Major trends of ransomware

In early 2017, a growing number of cybercriminals are turning their attention from attacks against private users to targeted ransomware attacks against businesses. The trend is alarming as ransomware players start their crusade for new and more profitable victims. There are many more potential ransomware targets in the wild, with attacks resulting in even more disastrous consequences.

Phishing is the number one delivery vehicle for ransomware. The motive behind this is that phishing emails are easy to send and lead to a faster return on investment (ROI). Phishing, as part of social engineering schemes, lures victims into executing actions without realizing the malicious drive. The less aware the targeted user is, the more fruitful the attack. Likewise, in case of targeted attacks (also known as spear phishing), phishing emails are created to look like they come from a trustworthy sender, but link to or contain malicious content that executes as soon as users click it, encrypting their data and asking for a ransom.

[3] G. Mark Hardy, "From the Trenches: 2016 Survey on Security and Risk in the Financial Sector," SANS Institute, October 2016.

[4] "Cyber Attacks on Financial Firms Up; Ransomware Attacks Way Up," Insurance Journal, July 22, 2016.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), articles 33 and 34

Sophisticated phishing attacks are harder to detect by nature and sometimes even careful users can still fall into the trap.

Several studies and media headlines are confirming the following major trends:

- The main purpose of most phishing emails today is to deliver, directly or indirectly, some form of ransomware
- Phishing campaigns with the highest click rates use content that targeted users would assume to come across during their everyday job tasks

The unavoidable controls

(Re)building the "Human Firewall"

Anyone who uses a laptop, workstation, smartphone, or connected device can be targeted by some form of ransomware or other cyber threats. The good news is that we are seeing a growing realization across the financial industry that their workforce needs to be educated about cyber threats in general and about ransomware specifically. There is a variety of best practices that organizations should follow in order to minimize their exposure to ransomware.

Organizations should implement a strong security awareness program that will help users to make better decisions about the content they receive through email, on what they view or click in social media, how they access the web, and so forth. It is essential to invest in employee training so that the human firewall can provide an adequate first line of defense against increasingly sophisticated ransomware.

Furthermore, organizations should occasionally test all users to determine if their security awareness training is effective throughout phishing simulations. Those tests should trigger an action plan and measure the organization's successes and failures.

In early 2017, a growing number of cybercriminals are turning their attention from attacks against private users to targeted ransomware attacks against businesses.

mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_z = True
add back the deselected mirror modifier object
active = modifier_ob
str(modifier_ob)) # modifier ob is the active ob
0 10 1
10 1

Backup remains the best protection against data loss.

Reported entry points of the ransomware

4% Social media

7% Business application

9% Unidentified

16% External URL

27% Phishing-Link in an email

37% Phishing-Email attachment

The perils of not patching

The WannaCry ransomware attack underscores the importance of keeping software such as Windows operating systems up to date and patched, and the fact that many organizations do not do so. The WannaCry attack affected around 200,000 users in 150 countries exploiting a known vulnerability in various Windows operating systems. In June 2017, a South Korean web-hosting group paid about US$1 million to unlock more than 3,400 websites running under unpatched Linux servers that had been infected by a ransomware variant called Erebu. This case is believed to be the largest payout ever following a ransomware infection. Another ransomware variant called Samsam specifically attacks a vulnerability in the Red Hat JBoss software. In each of these instances, the respective software vendors were aware of the vulnerabilities and had published patches to address them. However, if organizations are not taking the necessary steps to patch their systems on a regular basis in order to keep them up to date, targeted ransomware attacks will continue to take advantage of these vulnerabilities.

Keeping software up-to-date seems like a simple task and a given for any security-conscious organization such as firms in the financial sector. Understanding the current patch management structure of your organization begins with answering important questions:

- Have we assigned clear roles and responsibilities?
- Do we know our IT assets?
- What are the capabilities of our patch management technology?
- What are the inputs to our security monitoring process?
- Do we measure effectiveness and efficiency?

CIOs and CISOs should be aware that good patching practices are not enough to prevent ransomware. The next attack after all, could involve a zero-day exploit for which a patch has yet to be issued. Defending financial services institutions against ransomware, like almost any cyber threat, requires a layered defense.

If you don’t have a Plan B, you don’t have a plan

Backups remain the best protection against data loss. As a fail-safe, organizations should implement enterprise endpoint backup for laptops and workstations. They must set recovery point objectives (RPOs) for each server deemed to be at greater risk to ransomware according to organizational requirements based on a data loss period acceptable to the organization.

Even keeping backups does not necessarily secure business data from attacks, as recent ransomware strains scan for backup files and delete them.

Your optimal controls

Ransomware brought cybersecurity back to the boardroom

The recent outbreaks of ransomware and the high-profile data breach brought cyber security at the forefront of board meetings. CIOs and CISOs can make this opportunity fruitful by focusing on the following key messages:

- Presenting the emerging threats: Who is attacking our organization or industry peers? What are the latest trends? How can this affect our organization?
- Sharing your top cyber risks: What are the results of your last risk assessment related to current business challenges? What are the mitigation controls? What are the management actions?
- Explaining your program maturity: How are we positioned in terms of maturity level to face the evolving threat landscape? What is our maturity comparing to the industry peers?
- Leveraging on internal and external opportunities: Are there any open audit issues or regulatory updates relatable to the threat landscape?

The ransomware threat should be handled with a comprehensive assessment of the organization's countermeasures to understand whether they are capable of responding to the latest threats.

Rethink your protection against ransomware
A cybercriminal ally is complacency. Traditional protection methods relying on malware signatures and basic rules for protection has revealed to be ineffective against ransomware threats. Indeed, threat players design their ransomware to bypass traditional web and email protections, which are prone to have set-and-forget configurations.

The ransomware threat should be handled with a comprehensive assessment of the organization's countermeasures to understand if they are capable of responding to the latest threats. We have previously emphasized the importance of user awareness, vulnerability, and patch management processes and backup and recovery strategies, but this comprehensive assessment includes the following:

- Use of privileged accounts and access controls
- Content and whitelist filtering
- Security configurations of endpoints
- Use of threat-intelligence solutions
- Network segmentation and layered security
- Robust business continuity planning and exercising
- Crisis and incident response planning and exercising
- Testing the business resiliency, using targeted exercises such as "red teaming" and threat simulation

Future trends and predictions
The profitability of ransomware is flourishing due to the simplicity of its business model and the ease of use of its operating model. According to the latest cyber threat intelligence, there have been significant improvements in ransomware variety and functionality to increase damage and accelerate the need for response:

- Ransomware will continue to be the number one malware type used by cyber-criminals
- Given the signs of growing competition on the ransomware market, Ransomware-as-a-Service is also becoming more and more popular, attracting new players
- Ransomware is growing in sophistication and diversity, offering many ready-to-go solutions to cybercriminals with fewer skills, resources, or time
- A change in the targeted platforms may also be on the horizon. Experts believe that mobile devices, Internet-of-Things (IoT), point-of-sale systems, and ATMs are all seen as new potential targets
- More comprehensive and targeted damage, including back-up files, databases, and web pages
- Use of security vulnerabilities to increase the rate of infection
- Methods to increase ransom in case users delay payment, such as stealing and selling data on the black market
- Change of communication methods with victims to better negotiate ransom amount (e.g., through chat rooms instead of fixed banners)
- Stealthier encryption of infected computers and improved techniques to evade detection

Conclusion

- Recent ransomware attacks demonstrated the potential damage on organizations and that it can even halt some businesses
- Regulators will address more and more challenges around ransomware threats (cloud resources, patch management, backups, etc.)
- Phishing is the main vehicle for ransomware
- People are the first line of defence that should be trained to face the challenging new threats
- Ransomware coupled with unpatched vulnerabilities and "flat" networks demonstrated that patch management and in-depth security are crucial to reduce ransomware infections
- Effective backup and recovery strategies are the plan B in case of ransomware attack
- Organizations need to take a comprehensive approach to ensure they can be secure, vigilant and resilient against ransomware threats

The psychology of ransomware

Social engineering is defined as an act that influences targeted people to act in a way that may or may not be in their best interest.

A recent study[6] based on the analysis of splash screens—the initial warning screens of ransomware attacks—demonstrated that key social engineering techniques are used to intimidate or influence victims.
Common trends include the following:

- **A race against time:** In over half, the samples featured a ticking clock device. Deadlines are ranging from 10 hours to more than 96 hours.
- **Consequences reminder:** Should the deadline not be honored, the encrypted files will be lost. Some screen featured threats made to publish the locked files on the internet. In this instance, we can talk about a "doxware." Doxing is a cyberattack where the threat players expose and publish an individual's or an organization's private or identifiable information online.
- **Varity of imagery:** Official trademarks and emblems (e.g., the crest of the FBI) are used in the splash screens to instil the notion of authority and credibility to the request. One of the most prominent pop cultural images used was Jigsaw—a character from the horror movie Saw.
- **Ransom payment assistance:** Three in four ransomware notes asked for payment in Bitcoin. The average amount asked was 0,47 BTC (approximately €1321 in the first week of August 2017). Over half of splash screens included some aspect of a help desk, such as instructions on how to buy Bitcoins or frequently asked questions (FAQs).

[6] Dr Lee Hadlington, De Montfort University, URL: https://sentinelone.com/wp-content/uploads/2017/06/Psychology-of-Ransomware-Report-Final.pdf

EduChain

Validating your Educational Identity

David Dalton
Partner
EMEA Blockchain Lab
Co-leader
Deloitte

Eric Piscini
Partner
Consulting
Deloitte

Lory Kehoe
Director
Consulting
Deloitte

Lisa Simpson
Manager
Consulting
Deloitte

Blockchain is fast becoming more than just a buzzword. As organizations continue to educate themselves on the technology and its capabilities, the number of potential use cases where blockchain can play a real and disruptive role is rising. With bitcoin cryptocurrency as the first use case, the main focus has been on the financial services industry; particularly around payment, capital markets, lending, and regulatory reporting. However, there has been a recent shift to looking beyond these use cases and identifying other areas or processes across industries where blockchain would have an impact. One such area is education qualifications.

Deloitte's EMEA Blockchain Center of Excellence based in Dublin has developed a blockchain solution around the collection, validation, secure storage, and sharing of education qualifications. This increases the efficiency of the onboarding process of new employees along with tracking the continuous development of employees across the organization. This platform was originally designed to address a regulatory requirement within the financial sector, and can be leveraged across industries, sectors, and geographies to manage qualification requirements of all potential and existing employees.

Identifying the use case

Regulatory compliance is a key focus area and pain point within the financial services industry. Over the past number of years, increased regulatory pressure and related fines have had a major impact on the industry, resulting in a reshape of strategy and investment focus in many organizations. Several use cases have previously been explored around regulatory reporting and the ways in which blockchain can be used to improve the efficiency and minimize the effort in this process. Deloitte was approached by our client who was searching for a more efficient and innovative approach to handling one such regulatory requirement in Ireland—the Minimum Competency Code (MCC).

The Minimum Competency Code (MCC) is a directive issued by the Central Bank of Ireland, effective from 1 December 2011. The code sets down the minimum standard of competence required of persons carrying out certain functions regarding financial products, particularly around providing financial advice to customers. Each staff member in a role under the MCC scope must have a validated qualification from the Institute of Bankers and additionally must carry out and log 15 hours of continuous professional development activities on an annual basis. Failure to do so can result in a membership being revoked, as the person would not be legally qualified to carry out this role. This carries huge repercussions for the financial institution and there are regulatory penalties in place for failure to comply with the MCC code.

The existing MCC process within our client's organization is a completely manual process with reliance on data stored in static spreadsheets, passed around the organization and validated by 10 internal teams. Each request, update, or amendment made to the data requires the manual and time-consuming process of merging, updating, extracting, and maintaining the data. The process also carries a large regulatory risk and there is currently no single view of the MCC status within the organization.

Developing a secure shared data platform would allow for the automated extraction and access of data from multiple independent organizations. However, a key difficulty with developing and implementing this solution revolves around companies and organizations trusting that their sensitive data will be secured, maintained, and available in the appropriate and reliable manner.

Where blockchain fits

Blockchain is a disruptive technology that provides the capability for multiple users to securely share information through a distributed ledger without the need for any central database maintenance or management. Specific blockchain characteristics enable the realization of concrete use cases, leveraging three core applications:

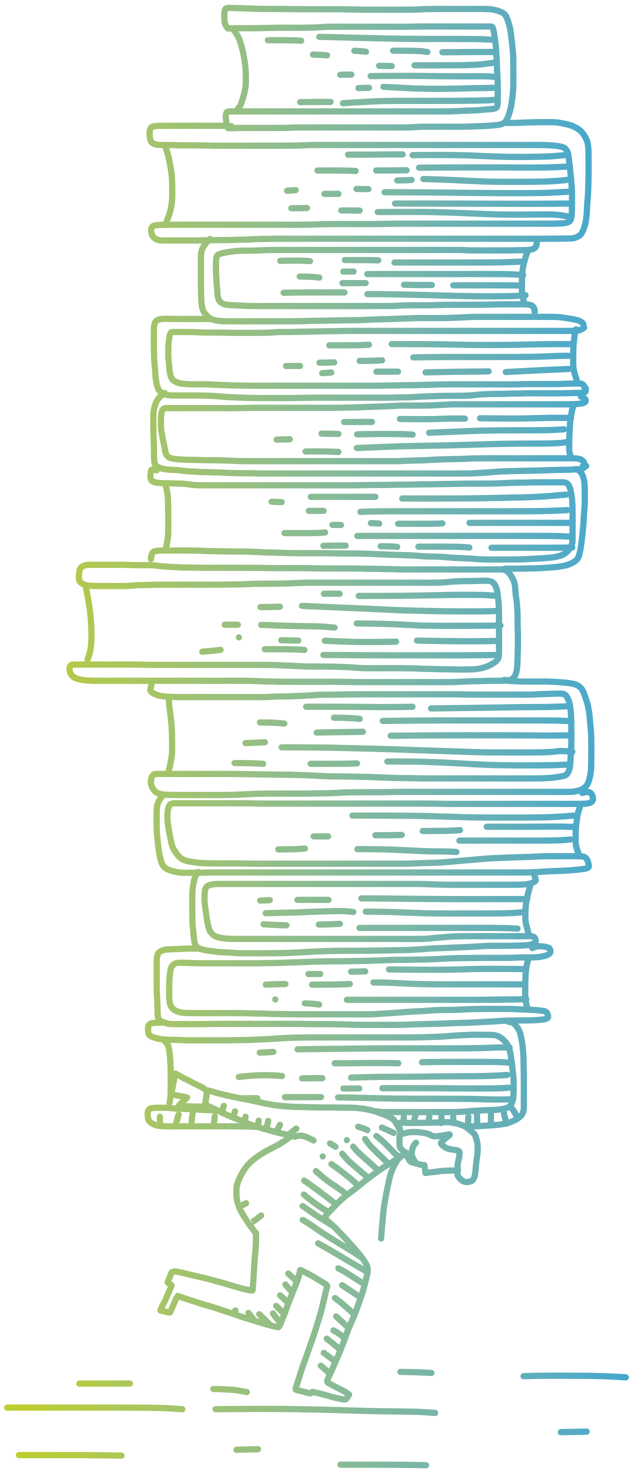
01. Immutable data storage – decentralized consensus to track and store information
02. Value Exchange – transactions among peers within a network
03. Smart contracts – distributed workflow and automatic execution of pre-written logic

A valuable example could be where a university may simply assign a qualification to a user's identity that can be accessed and shared as necessary and is globally available, thereby eliminating the need for independently verifying qualifications with the host organization. The data written to this common platform is digitally signed and encrypted.

Using blockchain technology in this manner to deliver the secure sharing of data across multiple organizations, where the data is fully authenticated through the organizations' private key has not been attempted before. Blockchain was identified as a good fit for this MCC process, as it provides:

- An immutable, trusted source of information, to ensure the accuracy of the certificate issued
- Permissioned access and visibility of the stored data to multiple internal and external parties and user groups
- Ease of integration with multiple systems and data sources
- Scalability and catering for multiple types of data, beyond certificates

> Over the past number of years, increased regulatory pressure and related fines have had a major impact on the industry, resulting in a reshape of strategy and investment focus in many organizations.



In this scenario, multiple organizations could access certifications in real time, where the data may be segregated into multiple secured compartments by implementing specific cryptography rules. This would allow for the seamless onboarding of multiple certification organizations.

However, the nature of the blockchain technology means that it will always be slower than interacting with centralized databases and is not designed for use on applications that require large-scale, real-time data access. For each transaction processed, a blockchain must perform all the same validations and checks as a regular database in addition to:

- Signature verification: Since transactions propagate between nodes in a peer-to-peer fashion, every blockchain transaction must be digitally signed using a public-private cryptography scheme. The generation and verification of these signatures is computationally complex, and represents significant challenges and technological uncertainties that must be overcome. By contrast, for centralized databases, once a connection is established, requests can flow over it with signature verification.
- Consensus mechanisms: In a distributed database such as a blockchain, it is necessary to ensure that nodes in the network reach consensus, which may involve significant back-and-forth communication and dealing with forks or rollbacks. In a centralized database dealing with conflicting or aborted transactions is much less frequent since transactions are queued and processed in a single location.

Supporting our client

From idea conception, Deloitte undertook a collaborative approach. The transfer of knowledge and exploration of the potential of blockchain within our client's organization was a focal point and a key deliverable. We developed an end-to-end solution, providing both technical and business expertise, mapping out the requirements and identifying the savings and improvements. Our technology team developed a functioning prototype, based on Ethereum code, including user interfaces for four different types of users.

As disruptive technologies accelerate, we must deliver projects with higher flexibility and agility. Deloitte approached this engagement using agile and SCRUM methodologies, which enables rapid collaboration, feedback, and iteration from our client to ensure the solution was fit for purpose. In order to truly embrace shared learning and knowledge transfer, the client team was co-located in Deloitte's EMEA Blockchain Lab in order for the project team to really be involved in the development of the solution.

The solution impact

The output from the proof-of-concept (PoC) phase was a working demo prototype that proved the capability of blockchain to provide a viable and trusted solution to the tracking and tracing of education qualifications within the financial services industry. The use of blockchain in the MCC process enabled our client to have a single view of the organization and also assure their compliance with the regulatory code. It showcased the dramatic reduction in man hours and manual input that was required in the process, which thereby would enable staff to spend more time focused on value added tasks within the organization. It also alleviated the pain and the effort involved in onboarding new staff; improving the process for the HR function and improving the employee experience. Moreover, it provided a potential industry-wide solution to the MCC process; creating a strengthened ecosystem in the financial services industry.

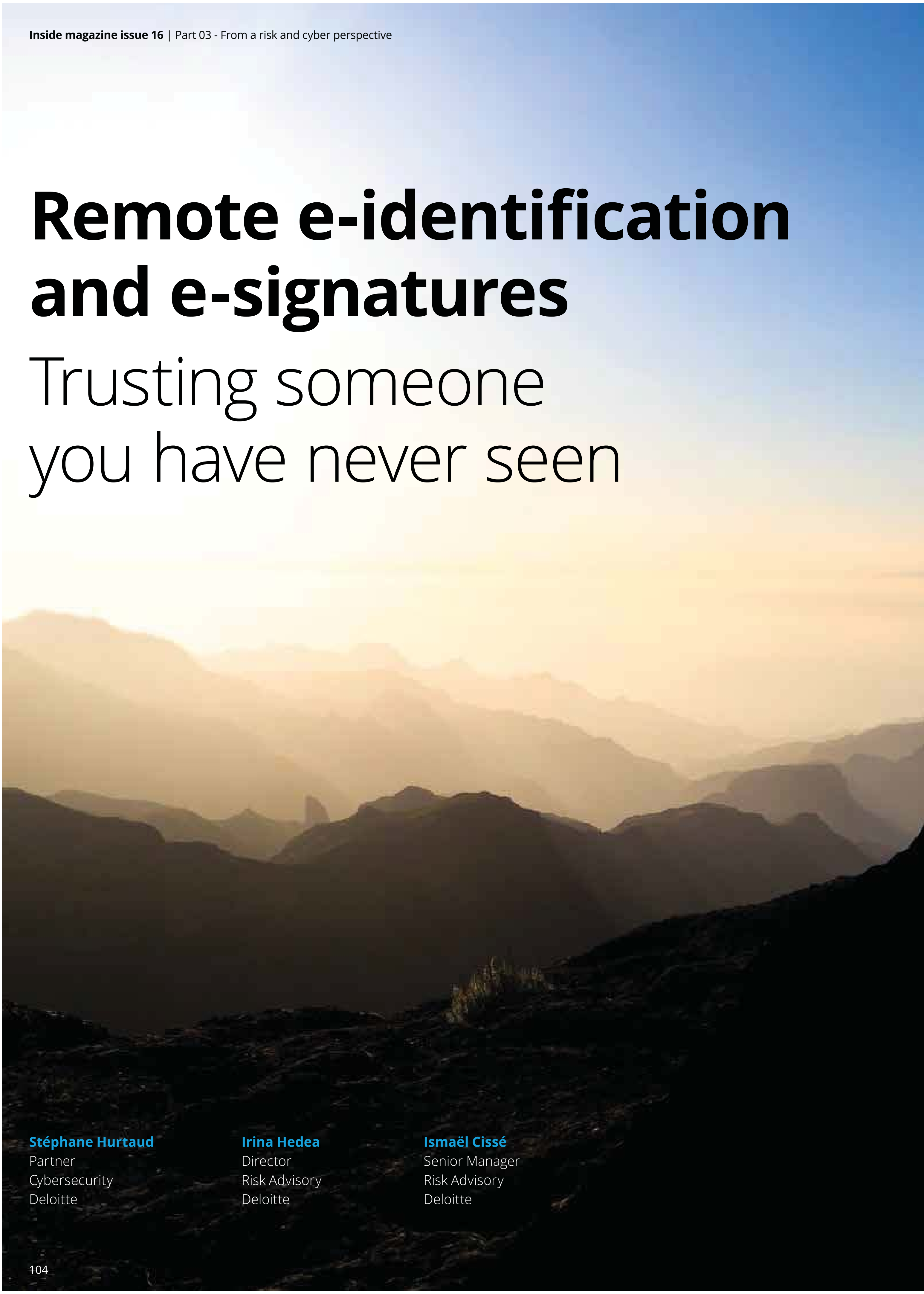
However, what was unique about this use case was the potential it has to be leveraged and replicated across industries and sectors. It provides a trusted way for organizations to ensure the validity of new staff qualifications and their ability to carry out their role. It also allows organizations to monitor the skillset of their staff, which can present opportunities for redeployment of capabilities. Finally, it provides employees with control over their qualifications as they can ensure the qualifications they receive are safely stored in one place, and with permission can share these qualifications as required.

Moving forward

This use case has opened up the conversation around where blockchain can play a role in transforming traditional business models and processes. In fact, the key lesson learned from this short effort is that when it comes to disruptive technologies and their potential impact, the sky is the limit.

We have also proved that traditional functions can unlock their ability to truly innovate and create new ways of working. As we move forward to the pilot stage, we will explore the legal, regulatory, and compliance considerations associated with blockchain platforms. ●

As disruptive technologies accelerate, we must deliver projects with higher flexibility and agility.



Remote e-identification and e-signatures

Trusting someone you have never seen

Stéphane Hurtaud
Partner
Cybersecurity
Deloitte

Irina Hedea
Director
Risk Advisory
Deloitte

Ismaël Cissé
Senior Manager
Risk Advisory
Deloitte

Over the past 20 years, the rise and rapid evolution of information and communication technologies has led to new digital services and usages responding to customers' need for mobility, convenience, efficiency and rapidity in the services response time. In the banking industry for example, this evolution was reflected by the development of services such as online and mobile banking and their rapid adoption by the customers.
However, as these new electronic services grow in magnitude, the risks related to cybercrime, identity fraud and leakage of personal data are also increasing. As a consequence, many organizations have the same concerns:

- How can I ensure the identity of a counterpart (natural or legal person) during an electronic transaction?
- How can I perform digital business or administrative transactions in a convenient, secure and seamless manner while maintaining the legal value of these transactions?

In this context, allowing citizens and businesses to identify remotely when performing electronic transactions is key for answering this need for mobility and convenience.
Consequently, the digital world needs to be protected by strong security measures.

Use case and challenges

Part of the trust in the digital world, remote electronic identification is the process of identifying a person only based on data in electronic form, without any face-to-face meeting.
In the financial sector, remote electronic identification supports a wide variety of use-cases, for example, the bank account opening or the online credit subscription. Such a solution typically involves several stakeholders:

- The provider of the remote electronic identification technology, solution or platform
- The provider of the service itself, such as the bank for an online bank account opening

For example, opening a new bank account can be done if a person is physically within the bank's premises or if the bank provides the required technologies for proceeding with this service remotely.

Independently of how the account is opened, a process involving different checks related to "Know your customer" (KYC) and "Anti money laundering" (AML) has to be performed. Documents such as ID card or passport, proof of residence, employment contract and client's consent for terms and conditions have to be presented and validated. The client's signature on the contractual agreement also has to be received.

Electronic identification allows this process to be performed remotely and from any location, provided that the client has, among others, an internet connection (e.g. from the client's home or office):

01. The client connects to the bank's website and initiates the account opening process
02. Then, he/she provides the requested personal information and supporting documents online
03. He/she is then invited to download an application, based on which the remote

electronic identification is performed: A trained expert performs a live-video identification of the client (face verification and cross-checking with ID card)

After the remote electronic identification, the bank performs the verification of the provided documents and, should the results of the controls be successful, opens the account.

As a conclusion, for the same process, the remote electronic identification allows an increase in efficiency and rapidity while keeping the same level of trust.

Further examples can be given, in different industries, such as online life insurance subscription, online telephone subscription, online apartment, and house rent subscription etc.

Information security challenges

For providing the required trust during a remote electronic identification, ensuring the security of the data exchanged through Internet is mandatory. Consequently, the solutions and processes supporting the remote electronic identification have to be securely designed, implemented, and operated in order to ensure the confidentiality, integrity, and availability of these data. Appropriate security measures must be adopted to reduce risks such as data leakage and identity fraud.

Legal challenges – Focus on eIDAS and qualified trust services

Another challenge for ensuring trust is to use the remote electronic identification solutions that are aligned with the different regulations currently applicable for the digital services.

Depending on the risks related to the remote electronic identification and the legal value expected from the digital service, the regulation currently applicable is the European regulation (EU) No 910/2014 (the "eIDAS" regulation)[1].
The eIDAS regulation addresses the cross-border harmonization at the European level of the legal value of trust services such as electronic signatures, electronic seals, electronic time stamps, electronic registered delivery service, and website authentication.

The regulation also defines the status of qualified trust services, which benefit from the presumption of reliability in legal proceedings. In the specific case of the qualified electronic signatures, the regulation goes even further by bestowing a qualified electronic signature the equivalent legal effect of a handwritten signature.

In this context, a third player comes into the ecosystem: the Trust Service Provider, which provides a trust service (e.g., an electronic signature certificate) to the user at the end of the remote electronic identification process. In the context of the online bank account opening, this could allow the client to electronically sign a contract at the end of his remote electronic identification, which would successfully conclude the client on-boarding process.

The eIDAS Regulation in its article 24 addresses the requirements related to the remote electronic identification process for enabling the delivery of qualified trust services:

"1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued.
The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

a. by the physical presence of the natural person or of an authorised representative of the legal person; or
b. remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or
c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or
d. by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body."

In this context, in order to provide the highest level of trust, the main challenge for remote electronic identification providers and Trust Service Providers is to ensure that their identification methods (e.g. live video identification) are recognized at national level as providing an equivalent assurance as the physical presence.

Operational and technical challenges

Organizations choosing to benefit from remote electronic identification are also facing operational and technical challenges. They have to select secure and technically mature solutions to provide the best service to their customers; however, this is just the tip of the iceberg.

Other key considerations are the technical integration of the solution in the existing infrastructure and processes while assessing the organizational changes towards their employees, clients and partners this integration will create.

The solutions provided by remote electronic identification providers, supported by the Trust Service Providers try to tackle the challenges previously mentioned, while ensuring the quality of the digital services.

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Remote electronic identification allows processes such as bank account opening and credit subscription to be performed remotely and from any location, provided that the client has an internet connection.

A vision of the remote electronic identification market

Analysis of the market

The remote electronic identification market is still emerging. This can be explained by the fact that the technologies used to perform the remote electronic identification are quite recent.
In addition, the capability to meet the requirements of the digital services regulations (e.g. eIDAS), when applicable, is in its infancy.

However, from a technological perspective, video quality (particularly on mobile devices) and network bandwidth are now efficient, thus paving the way to creating a strong technological market in the mid-term.

In order to benefit from the added value related to trust services such as the electronic signatures, the remote electronic identification providers couple their solutions with services from Trust Service Providers such as LuxTrust, Namirial or Infocert.

A good example of collaboration between a remote electronic identification provider and a Trust Service Provider is the one between IDNow and LuxTrust for the provision of added-value services such as the online bank account opening.

Diversification of Trust Service Providers' services

In the context of a remote electronic identification enabling the delivery of trust services, the eIDAS regulation states in its article 13 that "Without prejudice to paragraph 2, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation."[2]
Consequently, for having a competitive advantage in the digital market, Trust Service Providers need to demonstrate that they meet the eIDAS regulation's requirements, need to obtain the related certifications and to ensure the information security.

Since eIDAS provides a pan-European framework for mutually accepted identities, this represents an opportunity for Trust Service Providers to diversify their service offering as a one-stop-shop for supporting remote electronic identification, identity management, authentication and electronic signing solutions.

Example of differentiators

As in every new market, it is key for providers to identify the features which will allow their solutions to differentiate from others. In the context of remote electronic identification, the following aspects can be considered as differentiators:

- User experience
- Compliance with applicable legislations (e.g. eIDAS, GDPR and PSD2 for payment services) and related certifications
- Information security
- Re-usability of the identification process for other added-value services allowing for data portability and gain in time and costs (as one avoids repeating the identification procedures)
- Multi and omni-channel service (available on any type of device or platform)

These differentiators in general, will drive partners and clients to trust the digital services offered and will open the way for a swift and steadily growing adoption of remote electronic identification.

[2] eIDAS article 13, paragraph 2 "Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations."

Conclusion

Remote electronic identification is not a new topic. However, the key challenges that should be addressed while offering the expected quality, efficiency and legal value are becoming more and more significant.

Nevertheless, the legal framework introduced by eIDAS (such as the qualified trust services) allows leveraging on digital services that sustain the cross-border digital market in a trusted, innovative and efficient manner.

Organizations choosing to implement added-value services based on remote electronic identification have now the ground towards a digital transformation in a trusted and secured environment. Their journey can start right now.

Contacts

Africa - East, West, Central and South

Thys Bruwer
Director - Deloitte Digital Africa
+27 112 096 440
tbruwer@deloitte.co.za

Belgium

Olivier De Groote
Partner - Financial Services Industry Leader
+32 2 749 57 12
oldegroote@deloitte.com

Cédric Deleuze
Partner - FS Deloitte Digital
+32 2 749 58 19
cdeleuze@deloitte.com

Yves Rombauts
Partner - Leader of Technology, Strategy and Architecture
+32 2 600 69 20
yrombauts@deloitte.com

Koen Vandaele
Managing Partner - EMEA Consulting Leader
+32 2 749 59 52
kvandaele@deloitte.com

France

Redouane Bellefqih
Partner - FS Technology Leader
+33 1 55 61 64 10
rbellefqih@deloitte.fr

Michel De La Bellière
Partner - EMEA FS Consulting co-Leader
+33 1 40 88 29 95
mdelabelliere@deloitte.fr

Serge Gruber
Partner - Head of division FSI SAB
+33 1 55 61 48 28
segruber@deloitte.fr

Daniel Sousa
Partner - SAB CoE
+33 1 55 61 68 20
dsousa@deloitte.fr

Germany

Dirk Guttzeit
Partner - Industry Lead FS Technology Germany
+49 22 1973 2414
dguttzeit@deloitte.de

Greece

Niko Aggouris
Partner - Technology Leader
+30 21 0678 1205
naggouris@deloitte.gr

Iceland

Gudni Gudnason
Partner - Consulting Technology Leader
+354 5 803 316
gudni.bjorgvin.gudnason@deloitte.is

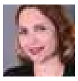
Ireland

David Dalton
Partner - EMEA Blockchain Lab Co-leader
+353 14 074 801
ddalton@deloitte.ie

Petri Heinonen
Partner - FS Technology Leader
+353 14 172 225
peheinonen@deloitte.ie

Harry Goddard
Partner - EMEA Technology Leader
+353 14 172 589
hgoddard@deloitte.ie

Israel



Meirav Hickry
Partner - Head of FS Technology solutions
+972 3 608 6187
mhickry@deloitte.co.il

Italy

Paolo Gianturco
Partner - Head of Fintech & FSI Technology
+390 283 323 209
pgianturco@deloitte.it

Luxembourg

Patrick Laurent
Partner - EMEA FS Technology Leader
+352 45145 4170
palaurent@deloitte.lu

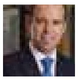
Netherlands

Timo Span
Partner - FS Technology Leader
+31 88 288 5164
tspan@deloitte.nl

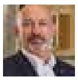
Poland

Warren Hatton-Jones
Partner - Temenos COE Co-Lead
+48 22 348 3391
whattonjones@deloittece.com

Portugal



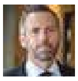
Joao Sales Caldeira
Partner - FS Insurance Technology Leader
+351 2 1042 2545
jcaldeira@deloitte.pt



Joao Carvalho
Partner - FS & Fintech Leader
+351 2 1042 2509
jocarvalho@deloitte.pt

Joao Luis Fonseca
Partner - FS Consulting Partner
+351 21 042 2541
joafonseca@deloitte.pt

Nordic



Marten Sellgren
Partner - FS Technology Leader, Sweden
+46 70 080 27 65
msellgren@deloitte.se

Spain

Antonio Crespo Ybanez
Partner - FS Technology and Strategy Leader
+34 91 438 1503
acrespoybanez@deloitte.es

Switzerland

Jan Seffinga
Partner - Head of FS Technology
+41 58 279 6928
jseffinga@deloitte.ch

UK

Keith Ashworth
Partner
+44 20 7303 4142
kashworth@deloitte.co.uk

Louise Brett
Partner - Fintech Leader
+44 20 7303 7225
lbrett@deloitte.co.uk

John DaGama-Rose
Partner - Head of Capital Markets COE – EMEA
+44 20 7007 7987
jdagama-rose@deloitte.co.uk

Richard Hurley
Partner
+44 20 7303 8912
richurley@deloitte.co.uk

Stephen Marshall
Partner - Global FS Technology Leader
+44 14 1304 5743
stephenmarshall@deloitte.co.uk

Richard Widdas
Partner - EMEA FS Consulting co-Leader
+44 20 7303 0966
rwiddas@deloitte.co.uk

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

Deloitte.

Deloitte is a multidisciplinary service organization that is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see **www.deloitte.com/about** to learn more about our global network of member firms.
Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on **Facebook**, **LinkedIn**, or **Twitter**.

Designed and produced by MarCom at Deloitte Luxembourg