Digital Innovation: The Evolution of Financial Technology
# Table of Contents

- Introduction — The Evolution of Fintech ................................................. 1
- Digital Innovation: From the Boardroom to Execution ......................... 3
- Innovating Payments ............................................................................. 5
- Prepare for Blockchain Disruption ......................................................... 9
- Regtech: A Confluence of Opportunities ............................................... 15
- Enabling Speed of Innovation Through Effective Third-Party Risk Management ................................................................. 21
- Digitalisation Meets Risk & Compliance .............................................. 35
- Contacts ................................................................................................. 41
Financial technology is evolving at an extraordinary pace; driving historic changes in consumer behaviour and expectations globally. These changes are predicted to accelerate even more over the coming years as consumer preferences toward electronic channels and emerging technologies disrupt current financial industry business models and services.

Technology and innovation are advancing differently in jurisdictions around the world. In the USA, progressive steps are being taken by fintech and financial services firms however, regulators tend to move more slowly with necessary regulations governing new technology than their European or Asian counterparts. For example, open API projects are more widely supported by the regulators in the UK than in the USA, as demonstrated by the recent changes in the Payment Services Directive and Regulation (PSD2). In the large financial centres in Asia, regulators are keen to promote innovation and technology; Singapore was the first country to launch a regulatory sandbox for fintech firms.

The development of fintech also varies between countries in the Asia–Pacific region:

- **Japan** is one of the leaders in artificial intelligence (AI) and holds more patents in AI than any other country in the world. Japan is set to have a designated “Drone City” built for the 2020 Olympics with over 200 flying drones delivering goods from warehouses to apartments with built-in landing ports. Banks in Japan have introduced robotic tellers to replace human counterparts. Regulators are also beginning to get on board with innovation — the Financial Services Agency of Japan (JFSA) announced in July 2017 that it is setting up a hub for fintech startups to test new services. While this is progressive, it lags behind Singapore and Hong Kong, which set up regulatory sandboxes in June 2016 and September 2016, respectively.

- **Hong Kong** is often billed as a leading fintech centre. In September 2016, the Hong Kong Monetary Authority (HKMA) launched a regulatory sandbox, and by June 2017, ten fintech pilot apps had launched successfully, with eight more fintech apps completing regulatory trials. Ten out of these 18 cases involved a fintech company that was collaborating with an existing bank in Hong Kong.

- **Singapore** has dubbed itself a “Smart Financial Centre,” and lives up to its name. One leading bank in Singapore now offers real-time portfolio analytics services on a personalised basis to all of its high net worth clients, making use of big data and cognitive computing. The Monetary Authority of Singapore (MAS) launched a regulatory sandbox in June 2016. MAS has not announced the number of (Continued on Page 1)

---

5. Plenty of chatter, and even some action, as Hong Kong makes progress on fintech, South China Morning Post, June 28, 2017: http://www.scmp.com/tech/start-ups/article/2100298/plenty-chatter-and-even-some-action-hong-kong-makes-progress-fintech
6. DBS leverages big data analytics to reduce trade anomalies, DBS, September 1, 2016: https://www.dbs.com/newsroom/DBS_leverages_big_data_analytics_to_reduce_trade_anomalies
applications in the sandbox, but it did note that 80% are standalone fintech firms not associated with any banks in Singapore. In addition, MAS has partnered with R3, a distributed ledger technology company, and a consortium of financial institutions, on a proof-of-concept project to conduct inter-bank payments using Blockchain technology. The regulator is also consulting on robo-advisory services.

As these examples show, technology is advancing rapidly and financial institutions must keep pace to remain competitive. Adopting new technology gives firms the ability to reduce costs, more securely protect data and retain customers, whose demands are evolving constantly. The existence of legacy systems, regulatory hurdles and outmoded existing business models can make the extraction of business benefit from innovation projects difficult for the more traditional financial services firms.

This publication brings together a sample of Protiviti’s thought leadership on financial technology products and services, as well as issues relating to digitalisation projects, which share ideas on how firms can embrace innovation and remain competitive while maintaining sound risk management.

In this volume:

- Digital Innovation: From the Boardroom to Execution
- Innovating Payments
- Prepare for Blockchain u/c Disruption
- Regtech: A Confluence of Opportunities
- Enabling Speed of Innovation Through Effective Third-Party Risk Management
- Empowering Second Line Functions to Enable Innovation: Digitalisation and the Second Line of Defence

For more information about how Protiviti can help with digitalisation and innovation projects, please contact one of the subject matter experts below:

George Brown
Managing Director
+852.2238.0481
+852.6318.2902
george.brown@protiviti.com

Suneet Gorawara
Managing Director
+852.2238.0486
+852.5630.5080
suneet.gorawara@protiviti.com

Tyrone Canaday
Managing Director
+1.212.603.5435
tyrone.canaday@protiviti.com

Ronita Dutta
Director
+65.6309.5950
ronita.dutta@protiviti.com

Takehito Yamada
Managing Director
+81.3.5219.6600
takehito.yamada@protiviti.jp

---


Digital Innovation: From the Boardroom to Execution

The pace of innovation is increasing exponentially. For traditional financial services firms, partnerships with new technology companies are now essential for driving digital change and staying competitive in today’s environment. The move toward a distributed economy and digital transformation in companies is manifesting differently in jurisdictions around the world. The United States and Europe are driving early ideation, while companies located in the Asia-Pacific region and the United Arab Emirates are gaining strong momentum boosted by a pro-innovation regulatory environment.

Many firms are embarking on digital initiatives to stay competitive and to respond to customer demand, but few begin with a clear plan for deriving value from these often significant investments. Protiviti Managing Director Tyrone Canaday provides some insights on how firms can drive business outcomes, realise benefits, and better mitigate risk through digital investments by understanding and implementing digital transformation programmes effectively.

Now more than ever, the right investments made in technology and innovation have serious and material implications to the long-term success and viability of a business. Missing opportunities to capitalise on new technology to enhance capabilities, products and services could result in lost market share, reduced ability to participate in upside gains of new business models, inability to capture the customers of the future, and in the worst case, extinction altogether. Institutions that are able to re-imagine their business, maximise investments in technology and evolve their business effectively to harness the current innovation cycle will determine the next generation’s winners and losers.

Typically, firms have approached digital innovation or large-scale technology change projects facing their organisations with a “build versus buy” philosophy. Today, with the emergence of innovative fintech companies, which are more nimble and faster to market than legacy financial institutions, the transformation decision has expanded to encompass build, buy, invest or invent. Each option must be evaluated in the larger context of the ultimate business strategy and desired target state. Navigating through the optionality, complexity and uncertainty to ensure optimal choices are made is no easy feat. Further complicating matters are budgetary constraints, board members who don’t understand how technology can enable the business objectives and turnover of executive leadership driving the multi-year transformation. Similarly, business change projects have primarily focused on three elements within the organisation: people, processes and tools. For digitalization in today’s environment, this approach needs to ensure an agile, actively managed and risk-aware approach around six key elements:

1. Strategic alignment
2. People
3. Processes
4. Technology
5. Customer Experience
6. Partnerships

All of these aspects need to align to drive business value and outcomes, which need to be orchestrated meticulously for a digital transformation project to succeed. Few companies are integrating and delivering all five aspects well across the dimensions for their digital transformation and innovation.
projects. Consequently, such projects often fail or the desired outcomes aren’t realised due to the high interdependence of the elements working in unison. This results in delayed projects and large investments where the business is realising value far below expectations, which leads to a loss of board advocacy and support from the business. This in turn leads to reduced future investment that only puts the organisation at even more risk. In contrast, successful companies are able to work across those five dimensions seamlessly in a manner that is more efficient, risk-sensitive, regulatory-compliant, well-controlled, and enabled by leading technology and data and emerge as the digital leaders of the future.

Technology is the future, and the ability to enhance and unlock new capabilities through digital channels can drive tremendous value for industries. Being able to discern value-added investments in innovation that complement the business and preserve the value through the transformation process versus just chasing the “new shiny objects” will be increasingly important to do well. Furthermore, the ability to effectively measure against value drivers such as revenue growth, simplification, speed-to-market and competitive positioning will help to validate return on investment. In reviewing the upside potential, it is also important to be aware of the risks and consequences if digital transformation programmes aren’t implemented effectively.

With proper planning and execution, organisations can drive business outcomes, realise benefits, and better mitigate risk through digital investments by understanding and implementing digital transformation programmes effectively around these five elements.
Innovating Payments

Financial technology, or fintech, firms are promising to revolutionise the person-to-person (P2P) and business-to-business (B2B) payments industry, and are already causing a seismic shift in this sector. Unburdened by regulation and legacy IT systems, new entrants focused on providing payment services are claiming to provide faster and cheaper transfer of monies, both domestically and across borders, than the established players.

Swelling the already established ranks of traditional banks and fintech payment firms such as PayPal, technology companies Google, Facebook and Apple are all entering this space and are expected to grow rapidly. ClearXchange is a growing B2B payments provider, which was established by a collaboration of banks seeking to counter the fintech challenge. The traditional firms providing cross-border payment services, including Swift, Visa and MasterCard, are also under threat from new entrants and are working to improve the speed, transparency and predictability of cross-border payments to stave off further encroachments by fintechs. Protiviti managing director Tyrone Canaday and director Jason Goldberg share their views on how disruptive new entrants have been in the payments space so far and how firms can begin to realise further benefits from innovation in payments technology.

What major innovation has taken place in P2P/B2B payments?

Jason Goldberg, a director in Protiviti's Financial Services Business Performance Improvement practice:

Domestic business-to-business (B2B) payments have traditionally been made in the U.S. by check, wire transfer or ACH. Over the last decade, the large credit card networks — Visa, MasterCard, American Express — have developed e-payables rails and solutions that allow firms to issue invoices through a digital platform where their creditors can pay electronically. This has made payments faster but there are still delays. Cross-border payments are typically made via Swift and interbank transfers using decades-old technology, which is very expensive, slow and provides inadequate tracking capabilities. It is unsurprising that cross-border payments in particular have been targeted by fintech companies utilising distributed ledger technology (DLT) such as blockchain and virtual currencies to speed up the process. The use of DLT allows companies, such as Align Commerce, to transfer funds faster, cheaper and with a trackable mechanism. Where a Swift transfer may take four or five business days, new entrants can promise transfers within two days and for about half the cost. Services such as these are a major disruptor to the payments sector, and more companies are launching new payment platforms every day.

The most noticeable innovation has occurred in the P2P payments space, which has been driven by strong customer demand to pay via their mobile devices. Apple Pay is well known, but newer technologies include Venmo, PayPal.Me and Canadian firm Mobeewave which has rolled out an app called PayMeTap, which allows users to pay and receive funds by a tap of their NFC-enabled mobile phone. Apple Pay is also rolling out this sort of tap-and-pay technology and Facebook Messenger is also new to the scene. There are many different types of eWallets and nobody really knows which one is going to be most successful but they have all made payments easier.

These innovative payment products all offer faster speeds and an enhanced user experience by reducing friction in the payment process. Although some also
These innovative payment products all offer faster speeds and an enhanced user experience by reducing friction in the payment process.

offer reduced fees, none have discovered a way to bypass the traditional rails when making payments or transferring funds. ACH and credit cards remain the primary methods used to validate mobile devices or to transfer funds. The company that overcomes that hurdle will significantly disrupt the market.

A major disruption in the payments space to date is occurring in the lower end of the market, which services the under- and unbanked. Prepaid card companies have moved beyond their core service to allow funds from prepaid cards to be transferred to other people. This change is effectively encouraging the use of prepaid cards as an alternative banking mechanism. Individuals can have their pay directly deposited onto a prepaid card, which can be used to pay bills and for goods, etc. However, even here, the card still needs to be loaded with funds using credit card rails or EFT/ACH.

Blockchain is a major disruptive technology and it has the potential to reinvent and disrupt areas such as international payments.

Is the use of credit and debit cards in decline?

From an innovation, disruption and protection perspective, Visa and MasterCard have been way ahead of their competitors in preparing for the future. I don’t envision credit cards and debit cards going away. If anything, the major change is likely to be the elimination of the notion of the plastic card and a move to a mobile account. We have mobile and wearables now, but in the future this may move to implantables and injectables. Biometric payment devices are already in development. So although the notion of a card goes away, the network stays.

The technology behind those networks will likely shift, eventually. Blockchain is a major disruptive technology and it has the potential to reinvent and disrupt areas such as international payments. But for domestic payments, for now at least, blockchain is slower than the existing networks, which can process payments in a millisecond and are available almost everywhere in the world. This is not likely to change in the next few years.

How may payments become commoditised and how will that impact existing business models?

Tyrone Canaday, managing director in Protiviti’s Financial Services Industry IT practice:
The global payments landscape has transformed dramatically with the rise of innovative technologies and fintech. From capital markets, banking, cross-border and credit card payments, the existing transaction processing systems operate in disparate and complex configurations, often involving intermediaries that charge fees across the value chain. The rise of mobile and online payment methods, peer-to-peer transactions and distributed database technologies, coupled with demographic shifts to younger segments, has increased utilisation, adoption and the acceptance of digital and disruptive commerce. As adoption trends continue to strengthen, organisations become increasingly challenged to upgrade legacy systems to support the demand of heightened customer expectations and experiences through digital channels. Innovation in payments is occurring in the back end of financial services in clearing and settlement services, as well as on the front end, revolutionising the customer experience — all of which threaten to disrupt traditional players throughout the payments lifecycle.

Fintech and innovative third parties tend to operate in these high-value, high-friction process areas and execute them better, faster and cheaper compared
to the status quo. Transactions supported through innovations can deliver superior experiences, such as in-app purchases, peer-to-peer payments and cross-border fund transfers that are processed at a fraction of the cost and at near real-time speeds, which can threaten the existing transaction infrastructures, particularly when these new methods become ubiquitous. Innovation is occurring both at the user experience and back office layers of the value chain. As a result, traditional players are at risk for disruption and there will be new intermediaries involved whereby profit margins derived from the existing payment processing channels will be redefined. Digital payment business models allow better capabilities in customer acquisition and retention through enhanced products, services and experiences that may also drive new forms of revenue.

**What further change can we expect to see in the next two to three years?**

**Goldberg:** In the next two or three years, more P2P payments will move onto mobile, which offers a frictionless form of payment. There will certainly be some consolidation in the payments space, with some eWallets being absorbed by peers and even by the more traditional players. Banks are responding to this fintech threat, and responding aggressively. Banks are not likely to be disintermediated; they are more likely to embed real-time, P2P functionality within their secure banking apps and earn fees from other payment interfaces. Some of the more innovative payment offerings, such as Mobeewave, where you can make a payment by tapping two phones together, will be more resilient to this renewed attack from banks. A greater innovation will be to be able to transfer funds in the same way between different apps. There is great promise for that network technology. In the B2B payments arena, blockchain technology is very likely to be a truly disruptive force, especially for cross-border payments, because it makes it so much faster. One of the issues holding this sector back, however, is regulation. Because some of the new entrants do not hold funds nor transmit money, they do not require banking licenses. But this is likely to change, and they will need to answer to the same regulations as banks and existing money transfer companies.

**Banks are responding to this fintech threat, and responding aggressively. Banks are not likely to be disintermediated; they are more likely to embed real-time, P2P functionality within their secure banking apps, and earn fees from other payment interfaces.**

**What regulatory compliance challenges and issues does this create?**

**Canaday:** Innovation in payments will introduce regulatory compliance challenges in a number of ways, but the immediate areas include emerging technology regulation, third party risk management and transaction monitoring (for anti-money laundering, AML and know your customer purposes), which will manifest differently depending on the jurisdiction. Historically, regulators have been challenged to keep pace with the speed of innovation, which has created an education imperative for the regulatory bodies to understand the emerging technologies that exist and to evolve or create new regulation, collaborative environments among the various players, to proactively govern and shape their development. In the European Union (EU) and countries like Singapore and the UK, a number of strategic regulatory initiatives have been launched to lead, promote and support pro-innovation projects. The Monetary Authority of Singapore (MAS), in an effort to create the world’s first “SMART nation” and cashless society, has created a climate to encourage experimentation in partnership with banks and fintechs to safeguard new product development with the right oversight to ensure controlled boundaries but also not stifle innovation. In the UK and the EU, progressive legislation around the Second Payment Services Directive (PSD2) allows for more innovation and competition by near and non-banks...
to gain access to customer account data traditionally only held at banks. However, this regulation is counterbalanced with increased scope and rigour around the handling of personal data in the form of the General Data Protection Regulation (GDPR) and additional mandates of increased transparency into pricing of transferring money to further protect consumers. The U.S., with a more complex regulatory structure, is in the nascent stages of emerging technology regulation, but regulators are moving forward with fintech charters that attempt to balance innovation latitude with the right levels of oversight.

As technology further decentralises operating models toward a distributed “api-economy”, increased risks reside in the co-collaboration space between banks and third parties. Critical business processes that are supported and operated by third parties must ensure that customer data is protected not just internally but at the api-level and external to the institution. Additionally, new products and services offered by fintech and the continuity of business processes must be well controlled, while risks arising from fourth party dependencies must also be considered. As with GDPR in the UK and FFIEC Appendix J in the U.S., requirements for institutions are becoming “borderless” and are now being extended to encompass the third parties that consume and process consumer data on behalf of the institution. Managing technology risk in the digital age requires fresh new approaches to keep pace with the rapid change.

With shifting regulation, increased usage of digital payments and the emergence of cryptocurrencies, regulators are challenged with several new AML/KYC-related issues that raise questions on how best to adapt to these emerging trends. As innovation in digital payments grows, usage and access to new customer bases and detection, monitoring and investigating suspicious transactions from bad actors becomes progressively challenging, especially when proper tools and techniques are not readily available. For example, legacy methods of handling alert lookbacks, data aggregation for regulatory reporting and detection of SARs depend on heavy manual and semi-automated processes whereby error and inefficiency become major factors. This has led to the advent of regtech and robotic automation around processes to help perform these tasks with more efficiency and accuracy.

What kind of support should governments, central banks and regulators provide to help innovate payments safely?

Canaday: Governments, central banks and regulators should develop policies and foster environments that allow startups, academia, banks and/or innovative third parties to take risks overseen appropriately to balance speed of payments innovation with sound risk and compliance management. Oversight should be “fit for purpose” and adjusted to provide appropriate guidelines tailored for the type of fintech or innovation and the product or service being considered. Innovation initiatives should be encouraged to push the boundaries in developing new technologies such as blockchain, artificial intelligence and cryptocurrencies, and be allowed to fail in safe havens. This allows all parties to learn while at the same time permits regulators to proactively guide policy and mitigate broader risks to consumers. As the use cases mature and reach specific milestones and inflection significant, regulatory requirements can then become more prescriptive. Innovating payments safely and with efficacy will also involve embracing new technology to help with oversight of new policies that are put in place. Changing existing regulations to allow banks to utilise cloud-based regtech solutions in robotics automation, artificial intelligence and blockchain, would help to evolve regulatory structure toward the 21st century at the similar pace as emerging technology. There is a need for regulatory consistency across jurisdictions, however, to eliminate uncertainty for innovators. The emergence of best practices and standards would also benefit all players in the payments space.
Prepare for Blockchain Disruption

Blockchain, the secure distributed ledger of digital events that uses consensus and cryptography to validate each transaction while also protecting the identities of all participating parties, is more commonly associated with cryptocurrencies such as bitcoin, but it has applications elsewhere that could disrupt the established financial services industry. In this paper, part of Protiviti’s series exploring how new technologies are disrupting financial industries, Protiviti’s Ed Page, Tyrone Canaday, Jason Goldberg, Vishal Ranjane and Nirav Shah discuss the impending impact of blockchain technology.

What are the main uses and advantages of blockchain today?

Tyrone Canaday, managing director in Protiviti’s Financial Services Industry IT practice: Blockchain’s applications are still being determined, but the ability to facilitate transactions without the need for a central authority, combined with the speed and cost benefits, are among the features that have so many interested in the technology. It is essentially a decentralised distributed ledger in which individual transactions are digitally signed and confirmed by a consensus of the network. Individual transactions are grouped to form blocks, and the data captured is rendered immutable.

Whether it is open ledger or closed ledger, all the participants in a blockchain can view current and historic transactions. With the use of smart contracts, business rules can be applied that can facilitate transferring anything of value.

Ed Page, managing director and Financial Services Industry IT practice leader at Protiviti: Blockchain is one of the more disruptive technologies available today, and it has broad implications for the payment space. There are many opportunities for blockchain to disintermediate some of the payment networks in place today. In so doing, blockchain has the promise to streamline much of the arcane processing that has evolved over time.

There are many challenges, however, including regulation and integration with the existing payment ecosystem. The regulatory response to blockchain will be something to watch carefully. Despite the promise of transparency that blockchain brings, there are questions about how things like Know Your Customer (KYC) and anti-money laundering (AML) compliance will manifest in a blockchain context. These will be solved over time, but how they will be resolved is still uncertain.

Blockchain is one of the more disruptive technologies available today, and it has broad implications for the payment space.
How susceptible is blockchain to hacking?

Jason Goldberg, a director in Protiviti’s Financial Services Business Performance Improvement practice:

Blockchain is based on a mathematical proof, which makes it very difficult to hack, and it takes the majority of the network to try to game the system. The issue is more around control. In an open ledger system, a user with 51 per cent or more of the aggregate computing power within the open blockchain could influence the chain. In a closed-ledger, or private, blockchain, the owner would have a bit more control because it would control all the participants involved.

Besides cryptocurrencies, how can blockchain technology be used in financial services systems?

Canaday: Blockchain technology can be leveraged to facilitate person-to-person (P2P) payment transactions and the exchange of value between any two parties. It can also be used to provide simple and efficient post-trade clearing and settlement services. In addition, there are applications around security and privacy, since the underlying protocol accomplishes requirements around authentication. Because a historic record is kept for all transactions on the blockchain, there are also potential uses for compliance risk management as well as internal audit groups that have access to the ledger.

Page: Blockchains can also be used to facilitate the digital documentation transfer of legal documents and property titles. Indeed, any legal document that must be securely and verifiably transmitted between entities can benefit from blockchain technology. There is great potential for these “smart contracts,” particularly in the legal and accounting space.

Canaday: Risk and compliance executives could use blockchain technology and smart contracts for providing electronic sign-offs, which could aid in better controls for a bank’s environment and overall governance efficiency. For example, maker-checker validations around processes such as funds transfers could be made more transparent and streamlined. Some firms have pilots in place to test use cases around an internal permissioned ledger to manage systems.

Any legal document that must be securely and verifiably transmitted between entities can benefit from blockchain technology.

Goldberg: Blockchain won’t immediately replace the payment networks Visa, MasterCard and American Express have built, because they are already secure, fast, inexpensive and ubiquitous. Blockchain is slower in terms of approval or verification than a traditional network-based payments transaction. Where it will more likely have near-term impact is in money transfer. Blockchain will likely disrupt the worlds of cross-border wire transfers, ACH and P2P payments.

Most small businesses and middle-market businesses pay their international suppliers through wire transfer, or through ACH, electronic checks or e-payables solutions for domestic transactions. For international payments, which are increasingly common, unless the payee wants to accept credit cards, the payor has to go to a bank or log on to the bank’s website, and it has to use a complex routing mechanism. The money is transferred out of its account using Swift, there are correspondent banks in the middle and, eventually, it winds up in the destination account. But the process is slow and expensive, and you can’t track your money during the funds transfer; it is 30- to 40-year-old technology.
One company uses bitcoin to speed up international money transfers. Using local money transfer rails, such as ACH in the United States, it moves money out of an account, then instantly transfers the money to bitcoin (but it could use any blockchain-oriented currency or mechanism). Within milliseconds, it transfers the funds out of bitcoin and into the destination currency in the destination country — currently, they support approximately 30 countries. Finally, the money is deposited into the recipient’s account using the local rails. This is relatively low risk, because the transfer into and out of bitcoin happens in less than a second, and the entire process is trackable. It takes half the time and a fraction of the cost, and it is starting to disrupt cross-border payments.

Does blockchain also offer advances for internal audit as well as security and privacy?

Canaday: The ability to view historic transactions and associated counterparties on the blockchain holds many potential uses for internal audit and security and privacy. Audit is essentially built into the blockchain itself, as a user is able to see a log of all transactions and who has committed them. We are starting to see companies analysing the blockchain for irregularities in activity and adopting it for security and privacy.

There are banks experimenting with using blockchain to track transactions at the device channel level. For example, electronic payments initiated from a mobile device or via a website are monitored as endpoints on the blockchain of a closed-loop system. Combining those capabilities with additional multifactor authentication facets such as tokenisation (the process of replacing sensitive data elements with nonsensitive elements), geolocation or biometrics allows even more layers of security. This is already happening at some organisations.

The blockchain has business continuity and disaster recovery built into its design, as all participants have a copy of the ledger and there is redundancy in the network in case a portion of it goes down. Furthermore, there are different analytics tools on the blockchain so firms can investigate other attributes of the transaction, such as currency types, frequency and location of payment origination, as well as the type of customer channel utilised. Analytics applied on this data could provide powerful investigative tools for security and privacy teams.

How quickly do you expect blockchain to gain further traction in the financial services markets?

Goldberg: People are still trying to figure out its applications. The adoption of blockchain technology hasn’t moved more quickly because there remains a general lack of understanding about it. The teams working on it have deep expertise, but they are not necessarily the ones making adoption decisions. Blockchain will not be additive; it will replace something that exists today. There needs to be more understanding and simplification about it so senior-level decision-makers have comfort in moving from the tried-and-true to something disruptive.

Canaday: Penetration around blockchain will largely depend on how it is adopted by the various players in financial services. Consortiums like R3 are experimenting cross-bank to test various use cases. There seems to be a lot of interest in capital markets, especially around post-trade clearing and settlement applications.

1 The processing of bitcoin (blockchain) is powered by the network performing calculations to validate transactions. All participants have access to the blockchain ledger. If there are 10 participants in the ecosystem, there needs to be consensus across the 10 participants on a particular calculation to confirm that the transaction is valid. If two or three of those participants are removed, the remaining seven or eight members can still validate transactions.

2 R3 is a blockchain technology company that leads a consortium of 45 financial companies in research and development of blockchain usage in the financial system. The main members include Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, JP Morgan, Royal Bank of Scotland, State Street and UBS.
We are starting to see that already; Nasdaq has successfully completed trades using blockchain, and there are efforts in Australia and China to do the same. Janet Yellen, governor of the Federal Reserve Board, is encouraging the central banks to study blockchain. If this technology can be applied to find revenue-generating applications and move top-line growth for firms, there will be an even more rapid adoption.

*Nirav Shah, director, Protiviti:*

It is certainly more development in these areas. A research lab that determines how you could use the ledger or transaction analysis in KYC would show you how to build that into your monitoring processes, but such applications are in an incubation space right now.

Security is inherent in the ledger, but it could do a better job on normal payment systems to use the type of security-of-privacy controls that are required to see how they line up when firms use blockchain technology. They will certainly gain more clarity, since they will not only be screening in the traditional way; they will also screen information that may be buried inside. How they do that will present some challenges.

*Ranjane:* Looking ahead to a blockchain-enabled financial world, the transaction monitoring process may need to change, because transactions are occurring more on the network using multiple institutions. In this more connected global marketplace, the regulatory approach to AML, KYC and transaction monitoring may need to change from being focused on an individual institutional level to being conducted at a state or even at a global level.

**Page:** Some senior AML executives are already discussing the idea that, rather than continuing to spend billions of dollars on partially effective compliance activities while still risking billions in AML enforcement fines, the industry would be better off simply paying an “AML tax” to the government, transforming AML requirements into a pure data-reporting regime and letting government staff handle transaction monitoring.

Although this is unlikely to happen — at least, not anytime soon — it demonstrates the fact

---

**Vishal Ranjane, a managing director in Protiviti’s Risk and Compliance practice:** People are experimenting and innovating using blockchain, but it is difficult to predict what that technology will look like six months from now. There is certainly a lot of hype. All the top-end banks are innovating or have innovation labs created around blockchain — and they are collaborating. These firms will probably release blockchain technology first into some of the lower-risk products before expanding applications rapidly.

**Ranjane:** Applications for KYC and risk and compliance are conceptual at this point. It is difficult to see how this will be applied to AML compliance and risk management as a whole.

**Blockchain will not be additive; it will replace something that exists today. There needs to be more understanding and simplification about it so senior-level decision-makers have comfort in moving from the tried-and-true to something disruptive.**
that it is becoming increasingly difficult for any given institution to get a full picture of who they are really doing business with and what types of activities are behind the end of a transaction being monitored. Today, there is some degree of cross-institution information sharing as a result of the 314(b) provisions of the USA PATRIOT Act, but it is not universally adopted by all firms, and even for those that have signed on, it is done in a very ad hoc manner — there is no centralised or systemic data exchange, for example. I could certainly see something like that being set up as an interim step between where we are now and the fully centralised industrywide monitoring system of the future.

The blockchain cheerleaders say that AML monitoring will actually be easier and more effective under blockchain than legacy rails because of the ability to perform networkwide and cross-institutional behavioural monitoring, which adds more value than the limited KYC information subtracts. That said, even after significant investments and decades of development, behavioural monitoring remains in its infancy.

What are the main challenges for firms looking to implement blockchain?

**Goldberg:** Adoption must occur industrywide to gain the perceived efficiencies and the additional security of leveraging blockchain. That means creating partnerships with competitors, with upstream and downstream processing or data providers to implement blockchain simultaneously.

**Canaday:** The advent of blockchain is similar to the changes that occurred to entire business models when the internet was invented. People and organisations don’t yet know the impact and the promise of blockchain and which types of business models will spawn from it. From a change-of-management perspective, as with any new technology, new business processes are impacted, as well as the skills needed to support them.

**Ranjane:** Integrating blockchain within the ecosystem internally and externally is a significant challenge. Add to that compliance activities and operational nuances, as well as the engineering perspectives.

What is the current regulatory response to blockchain, and how could future regulations impact its development?

**Goldberg:** Regulators around the world are telling firms to innovate with caution, but that means they haven’t figured out how to regulate blockchain and what the regulatory implications will be. Whatever innovation financial institutions create, they must be in step with the regulators, working closely with them so they understand the implications of the change to come.

---

**Canaday:** Firms can adopt blockchain technology without having to make wholesale changes to their legacy systems, but it would require careful consideration of where and how to apply the technology, and how to couple it to existing systems and processes. There may be specific business processes in organisations that could be made more efficient by using smart contract structures, however. Blockchain is definitely going to be disruptive. Banks will likely create new blockchain functionality in environments that run parallel to their existing production environments, and as they start to prove the concept out, they can start to roll it out more broadly. But this will need to be closely managed.

---

**Goldberg:** Firms can adopt blockchain technology without having to make wholesale changes to their legacy systems, but it would require careful consideration of where and how to apply the technology, and how to couple it to existing systems and processes. There may be specific business processes in organisations that could be made more efficient by using smart contract structures, however. Blockchain is definitely going to be disruptive. Banks will likely create new blockchain functionality in environments that run parallel to their existing production environments, and as they start to prove the concept out, they can start to roll it out more broadly. But this will need to be closely managed.
Canaday: Emerging technology firms, by their very nature, tend to operate in new spaces where regulation likely does not exist or where it is emerging. Because of this, organisations may appear to be operating under the radar of regulation. There needs to be better collaboration between banks and regulators so as not to hamper innovation.

Goldberg: In some cases, there would be no regulation: Using blockchain for credit card payments, for example, wouldn’t be regulated per se, because the entities running it aren’t processing companies — they are technology firms. But the companies they plug into, such as banks and other financial services firms, will be regulated, and as such, new entrants need to understand the implications for those companies. For example, in 10 years, the major credit card companies could collectively decide to replace their existing rails and implement a blockchain-oriented system. Every card issuer, processor and merchant acquirer would need to work within that framework, and all those entities would be regulated.

Can firms predict the value of blockchain today?

Canaday: There is a time-cost benefit in certain areas of the market. Blockchain could reduce the cumbersome back-end processes (like clearing and settlement) from a number of days to real time. Firms would benefit from having a better sense of their real-time liquidity positions, which could provide better intelligence to make business decisions. Clearly, efficiency is one benefit, and reduced fraud could be another.

Shah: Blockchain could help a clearing corporation solve how derivative transactions are moving back and forth, but it could be used in tracking the movement of investments as well.

Blockchain could reduce the cumbersome back-end processes (like clearing and settlement) from a number of days to real time.

How will the expansion of blockchain impact the financial services market in the short-, middle- and long-term?

Canaday: It really depends on the sector of the market. At one extreme, clearinghouses could become obsolete if the trading and investment banks all switch to use blockchain technology. This would make the process more transparent, because all the parties will participate in those activities, as well as transact in real time. There have to be clear value propositions with tangible outcomes and benefits for blockchain expansion.
Regtech: A Confluence of Opportunities

A new phrase has crept into the lexicon in recent times — “regulatory technology,” or, more simply, “regtech.” Like many neologisms that emerge on a wave of hype and marketing spin, the phrase is poorly defined currently, but it is rapidly being attached to a disparate range of new business models, technologies and business-change projects that at first glance can appear a little incongruous.

The difficulty is seeing through the marketing rhetoric to gain an appreciation of the confluence of ideas underpinning the range of regtech offerings that gives them substance. There is a need to understand emerging thinking from a business perspective, to identify evolving trends more broadly. More important, however, is the need to translate all of this into practical and pragmatic action and to understand how ideas can be brought together and applied to real-world business problems.

Regtech has reached the point where business leaders need to sit up and consider their next actions and test the waters or risk being overtaken by competitors operating in the same industry that are facing the same challenges.

What Is Regtech, and Why Is It Important?

Protiviti adopts a relatively broad definition of “regtech.” From our perspective, regtech is the innovative application of technology and new business concepts to the challenges firms face in managing regulatory risk and compliance.

The escalating cost of regulatory compliance is a key driver for innovation, and the most costly element is the level of human capital applied to the issue. An example of this escalating expense is the $2.2 billion spent by one leading bank on regulation and compliance in the first nine months of 2015, an increase of 33% year-on-year. Noncompliance is even more expensive, with financial institutions in the U.S. paying out more than $160 billion in fines for noncompliance over the last five years. Any innovation that has a possibility of putting a dent in these costs is worth understanding better. Regtech and innovation go hand in hand. Finding areas where innovation can cut through increasing levels of regulatory complexity and where it can replace the fallibility of human activity is critical. This is the regtech frontier. Regtech is not a specific and well-defined set of technologies and innovations — the “tech” part of “regtech” is simply the enabler. Individual technologies provide new and interesting capabilities that can be brought together in novel ways to tackle issues previously solved through a range of traditional techniques and human endeavours.

The truth is that none of these techniques is perfect. They all have their flaws and imperfections. Combining them is helpful in terms of the delivery of an outcome where the primary goal is ensuring compliance; however, this is at the expense of armies of people processing information and making myriad decisions in an increasingly complex regulatory landscape.

Existing businesses have been built over time, and the way they address risk and regulatory compliance is ingrained in their systems, policies, processes, procedures and controls. These are very rarely swept...
aside and are reinvented with the advent of new or changing regulations. Changes are applied piecemeal over time, adding to the level of complexity. It becomes increasingly difficult to take on board further change without making processes more rigid or more costly.

Innovation dissects problems and inherent flaws within the traditional techniques to find new ways to deliver the same outcomes for a reduced cost which are more flexible and less prone to human frailties.

**Traditional Approaches**

To help identify regtech technologies, it is worthwhile, considering the range of techniques currently employed, to address the challenge of regulatory compliance in a large corporate entity.

A non-exhaustive list of these techniques includes:

1. **Process Standardisation** — Forcing all transactions through well-defined, prescriptive and rigid processes to ensure that all the right boxes are ticked.

2. **Pooling of Expertise** — Organisational structures which concentrate technical knowledge and experience within well-defined areas so that valuable and expensive capabilities can be shared and applied sparingly, while the costs of maintaining and retaining this expertise are carefully managed.

3. **Corporate Bodies of Knowledge** — Expressing policies, procedures, culture, behaviours and controls in the form of written documentation so that tacit knowledge can be captured, codified and retained to provide corporate memory.

4. **Training and Accreditation** — Techniques to transfer essential information to individuals participating in business processes to ensure that they are aware of relevant regulations and their individual obligations.

5. **Quality Control and Assurance** — Recognising the inherent fallibility of people and processes and building in additional checks and balances to increase the likelihood that an organisation is complying with relevant regulations to spot exceptions.

6. **Structured Data Collection** — Capturing a limited set of key data points to provide an authoritative data source and to act as a definitive record of transaction.

7. **External Validation** — Enhancement or comparison of data with curated sources of information from outside the organisation to support decision making.

8. **Audit Trails** — Evidence gathering and documentation to prove that processes and rules have been followed.

These techniques are so ingrained in the psyche of business and best practice that they have been applied as the default response to regulatory compliance challenges across a number of industries and at all scales of organisation.

Innovative technologies can also be applied to this set of challenges alongside the need for regulatory compliance. Organisations which are positioned to better understand and manage their business risks in a cost-effective manner are able to both outpace and outprice their competition.

The business case for regtech is even more easily made where the technologies being deployed are applied to a range of business risks, not just the challenge of regulatory compliance.
Beyond Regtech to Risktech

Before identifying the range of technologies which can help to address regulatory challenges, it is worthwhile standing back a little from the “regtech” phrase to give it wider consideration. Regtech specifically addresses regulatory risk — i.e., the risk that a business may not be fully complying with all relevant regulations and legislation across all of its dealings with customers, suppliers and other counterparties. This is only one aspect of risk management that needs to be addressed by businesses on a day-to-day basis. There is a whole range of additional risks that need to be assessed and addressed when undertaking a business transaction. For example:

1. Credit Risk — If I am lending money to a customer, how certain am I that the customer will repay the debt based upon the agreed terms?
2. Fraud Risk — How do I determine that the customer I am engaging with is genuine and isn’t in the process of undertaking a criminal act which could lead to a loss?
3. Acquisition Risk — How do I ensure that a customer doesn’t decide to buy from a direct competitor after I have spent a lot of time and effort vetting and assessing the customer?
4. Defection Risk — How do I ensure that my customers don’t begin to move to my direct competitors because they are simply much easier to interact with?
5. Execution Risk — How do I ensure that my high degree of reliance upon people and manual data entry within my complex business processes doesn’t lead to issues and an increased level of risk?

Innovation Opportunities

The list of technologies associated with regtech solutions will develop over time. There is, however, a set of technologies and innovations that have already reached a point where they are robust enough to have real-world applicability. No single technology or innovation provides the entire answer. The skill lies in selecting the right individual components to address key elements of a problem. Solutions may require the combination of a number of distinct innovative approaches in order to develop a flexible and agile business platform, integrated with current line of business systems.

The current technologies demonstrating the most promise in relation to regtech and risk management fit into the following broad categories:

- Cognitive Systems & Artificial Intelligence — The ability to capture and apply human knowledge and experience.
- Data Analytics — Analysis of high volumes of structured and unstructured data to identify patterns and provide business insight.
- Machine Learning — Inference of business rules from analysis of large sets of data.
- Robotic Process Automation — Replication of human interaction with computer systems via existing user interfaces.
- Speech Recognition — Real-time translation of spoken language into a form that can be interpreted by software based systems.
- Natural Language Processing — The ability to infer context and meaning from human language.
- Biometrics — The identification of an individual based upon recognition of physical and behavioural characteristics.
Why Has Regtech Gained Prominence?

A number of factors have led to the increasing use of technology in relation to regulatory compliance. Technologies previously confined to the academic sphere have begun to spin out companies and products which are now being applied to real-world problems. Most notably, these include various forms of artificial intelligence and data analytics.

The world has entered a digital age. The rapid and almost ubiquitous deployment of smartphone technologies across the globe has put sophisticated technology in the hands of consumers. Businesses can now anticipate that a large proportion of their customer base will have access to video cameras, geolocation systems, fingerprint recognition technology and instantaneous connectivity to people and information across the globe. The ability to utilise biometrics on a large scale has leapt dramatically through the use of smartphone-based technology. Consumers now expect businesses to be able to take advantage of this new environment in the way they engage with their customers.

The adoption of cloud-based technology has put enormous computing power and scalability in the hands of even the smallest of companies, providing cost-effective ways to quickly try new ideas and to pay for processing and data storage based upon usage as opposed to up-front capital investment.

Off the back of the financial crisis, financial technology, or fintech, firms have picked apart the business models underpinning a variety of banking- and insurance-related products. They have fundamentally reimagined business models by starting with a blank sheet of paper and questioning everything they do from a customer and value perspective. This includes solving regulatory challenges in a novel way by applying the latest thinking and a range of new technologies. These organisations are consequently more agile; they are configured to adapt quickly to change from both a market and a regulatory perspective.

A combination of these factors, along with a number of wider digital transformation and economic trends, has focused attention on regtech as a topic, which is continuing to gain traction.

What Action Is Required?

“Regtech” does not refer to the implementation of technology to simply play with the latest set of toys. Regtech is providing real-world solutions for today’s high-cost business problems in areas that cause the biggest issues in terms of business agility and competition. Our list of regtech solutions extends to around 80 suppliers, with new solutions being identified on a frequent basis. It is true to say that many of the technologies Protiviti is tracking in this space are leading edge; however, adoption rates for successful solutions are climbing rapidly as early business cases are verified through proof-of-concept launches followed by rapid deployment.

The world of artificial intelligence and analytics around which much of regtech revolved is changing fast with the advent of new deployment models. A shift from apps to bots is creating the opportunity to string together a range of new capabilities to increase the level of automation within processes which were traditionally the preserve of human operators. Combining human capabilities with autonomous agents can provide a massive uplift in productivity.
accompanied by greater certainty that regulatory obligations are being fulfilled. Despite all the points noted above concerning the power of technology, individual technologies must not be seen as magic bullets. There is still a need to address people- and process-related issues in parallel. Technology deployed within existing processes must work alongside human operators. Businesses still need to rely upon human interaction and empathy to manage customer relationships and to spot exceptions that need a degree of flexibility and human ingenuity. Organisations need to be careful to choose the right technologies and to consider their impact on the business. Considerable skill is needed to access existing expertise within the organisation and to undertake the required knowledge engineering to match human capabilities with automation.

Investment risk needs to be carefully considered. Selecting the right business problems to solve and the business processes with the greatest opportunity for improvement is fundamental to success. Identifying the technologies that should be considered and which have the best chance of making a significant difference is critical when considering where and how to invest.

To survive and thrive, businesses need to carefully assess their options; invest time, effort and resources in the activities most likely to deliver value; and be prepared to learn quickly from failures as well as rapidly capitalise on every success. Facing the future with confidence is a trait which all organisations need to develop in our rapidly changing world.
This paper summarises key elements of an effective third-party risk management lifecycle and how to manage the elements of an R&D process adapted for innovation to support and streamline growth and adopt new technology.
Enabling Speed of Innovation Through Effective Third-Party Risk Management

Technology is evolving at an extraordinary pace, driving historic changes in consumer behaviour and expectations. These changes are predicted to accelerate even more over the coming years as preferences toward electronic channels increase and emerging technologies disrupt current business models and services.

This technological evolution is impacting the financial services industry significantly. Increasingly, customers are shifting from physical locations to digital channels, with financial technology, or fintech, companies accelerating the speed of innovation to unprecedented levels, challenging traditional firms and regulators to keep up.

Each year, fintech companies are offering a wider range of financial services and products, including peer-to-peer payment services, mobile wallets, lending, treasury management services, robo financial advice and many more. Fintech companies are applying innovative technology and new business concepts to the challenges firms face in managing regulatory risk and compliance, with products now referred to as regulatory technology, or regtech, which aims to make regulatory compliance more streamlined, integrated and less costly.

To remain competitive, many financial institutions are adapting their research and development (R&D) processes and capabilities in response and are developing more advanced products and services to meet changing customer demands. Legacy financial institutions are forming partnerships with fintech companies or are acquiring specialty start-up firms to collaborate on the development of new technology. Such partnerships bring many benefits, but they also subject the fintech company to the same rigorous third-party risk management practices as financial institutions, and potentially to direct oversight by financial services industry regulators. This calls for rigorous, comprehensive third-party risk management.

This paper summarises key elements of an effective third-party risk management lifecycle and how to manage the elements of an R&D process adapted for innovation to support and streamline growth and adopt new technology. By integrating these components, fintech companies and financial institutions can face the future confidently by navigating a highly complex regulatory environment while maintaining speed and flexibility to innovate responsibly.

Legacy financial institutions are forming partnerships with fintech companies or are acquiring specialty startup firms to collaborate on the development of new technology. Such partnerships bring many benefits, but they also subject the fintech company to the same rigorous third-party risk management practices as financial institutions.
To succeed in today’s competitive marketplace, banks are embracing innovation in numerous ways, primarily by increasing their reliance on third parties and developing in-house solutions to provide the critical products and services necessary to stay competitive. The fintech expansion has increased regulatory scrutiny, whereby regulators are seeking to bring some of these companies under their supervision.

The U.S. Office of the Comptroller of the Currency (OCC) has issued several papers focused on the need for responsible innovation, including proposals for fintech companies to be granted special-purpose charters to operate within the financial system and be subject to the same rigorous standards of safety and soundness, fair access, and fair treatment of customers that apply to all national banks and federal savings associations.

Granted, these are only proposals, but financial services organizations entering into partnerships with fintech companies still must deal with numerous external factors and regulations impacting the industry and the risks associated in dealing with third parties. In the U.S., various regulatory agencies responded to the global financial crisis that began in 2006 with a series of pronouncements governing how banks and other financial institutions should manage technology and outsourced providers, and ultimately extended this to all vendors and third parties.

The OCC, the Federal Reserve, the Federal Financial Institutions Examination Council (FFIEC) and the Consumer Financial Protection Bureau (CFPB) have all released updated guidance on requirements for robust third-party risk management practices at financial institutions. Deficiencies in third-party risk management practices, including weak oversight by financial institutions, have come under close regulatory scrutiny, with some facing severe penalties in fines and reputational damage.

The impact of regulatory guidance was widespread and continues to increase today. As recently as January 2017, the OCC published Bulletin 2017–7, Supplemental Examination Procedures for Third-Party Relationships. The latest document from the U.S. regulator further raises the bar and expectations on how banks must manage the entire lifecycle of third-party relationships.

---


The Third-Party Risk Management (3PRM) Lifecycle

The Protiviti third-party risk management (3PRM) lifecycle, as depicted in the model below, can guide financial services organisations in building capabilities to manage their third-party risk with the rigour and level of detail needed to support effective, scalable and compliant programmes.

Following is a summary of the key elements of this 3PRM lifecycle.

The Third-Party Risk Management Lifecycle
The lifecycle begins well before a specific third party is identified in the R&D and planning process. It includes identifying and planning for any needs of the financial institution that cannot be met through internal resources and processes. This planning process involves considering the potential risks and exposures posed by the potential third party, what risks the contractual relationship might impose on the company, and how these risks will be mitigated, actively managed and monitored.

Once potential third parties are identified, typically through a sourcing process, rigorous vetting, risk assessment and due diligence should be performed as part of the third-party selection process. Such due diligence should include an evaluation and analysis of the inherent risk driven by the type of service (or product) being provided and the specific control environment of the third party providing the service or product. Combining these two factors should equate to a “residual” risk score that drives segmentation and risk tiering of the third-party relationships. The risk tier should ultimately dictate the contracting strategy and requirements (including inclusion of specific terms where needed) as well as the frequency and type of monitoring.

A critical component of due diligence is the risk assessment process. Using a “bilateral risk assessment,” companies can assess the category of what is being provided (inherent risk) separately from the vendor that is providing the service or product. These can then be combined to get a true picture of residual risk and to determine an overall third-party risk management tier. The risk assessment process should consider an array of risk domains, including compliance, concentration, reputation, legal, country, operational, strategic and credit risk. The type of product or service should drive the level of due diligence required for the provider. The higher the risk, the more due diligence is needed, taking a deeper dive into the third party’s financial reports, management background, reputational checks, security and privacy controls, business continuity management and compliance framework, among other areas.

Next, depending on the third party’s risk management organisational structure and ownership of third-party relationships, the business, as well as information security teams and the compliance department, can conduct individual deep-dive assessments. This process is generally managed centrally, either by procurement or by a central vendor management organisation.

By combining the category risk assessment with the provider risk assessment, the financial institution is able to set out specifics in the contracting and onboarding phase, which can stipulate important issues such as provisions around the protection of personal information, ownership of intellectual property and expectations for managing subcontractors, among others. In addition, leveraging a bilateral risk assessment to segment and prioritise third-party relationships provides additional rigour and opportunities to streamline the process through automated scoring.

Development, negotiation and execution of a contract with third parties is a key step in establishing the pricing, scope and performance expectations of the relationship, including deliverables, acceptance criteria, milestones and service level agreements. Contracts also serve as the foundation to establish expectations around key terms such as limitations of liability, indemnification, data security and privacy requirements, regulatory compliance, management of subcontractors (fourth parties), and termination rights. Contracts should take into account the key risk factors and have appropriate mitigating controls where possible.
Once the contract is executed, the most important activity in managing third parties begins, which is monitoring both performance and ongoing risk. The frequency and extent of monitoring should be dictated by the segmentation and risk tiering strategy and process. Many banks struggle to hand off a completed contract effectively (often drafted and negotiated centrally) to the business owner that will be responsible for managing and monitoring the relationship and contract. This “first line of defence” activity is crucial, yet it is often not seen as part of an individual’s day job and thus gets swept aside. In response to this challenge, many banks establish first-line vendor management offices (VMOs) to facilitate monitoring within the lines of business. There can also be secondary monitoring and reporting, either by procurement or the central vendor management function, acting as the second line of defence. Monitoring must include the periodic reporting through committees, which have delegated oversight responsibility from the board of directors, as well as continuous review of actual risks, emerging risks and early detection of performance deterioration. This also includes the development and review of a timely corrective action and, if required, the identification and mitigation of risks associated with the termination of a contract relationship.

Guiding Principles and Operational Improvements

Bookending the third-party risk management lifecycle are guiding principles and operational improvements, which help scale the process for different companies.

Some key considerations and guiding principles to consider when implementing or refreshing a third-party risk management programme include:

01 Compliant — More than just compliance, firms should consider all external and market factors. Whether the company is a national bank (governed by the OCC), a credit union or a state chartered bank (governed by the Federal Reserve Bank or FDIC), all the governing bodies have fairly consistent guidance, with some being more prescriptive than others. Insight can be gained by looking at leading practices as well as the regulatory guidance.

02 Effective — Simply stated, does the third-party risk assessment process function as intended and as designed? Translating a process on paper into practice can be the most challenging part and the area where many companies struggle. How do you actively engage the lines of business and consider the needs of individuals in the first line of defence that own the relationships? Does the process work for them?

03 Scalable — Scalability is not always about technology, but it certainly helps. Scalability also considers the robustness of the processes and controls, and whether they are automated. Does the company have the right process infrastructure to carry the weight of double the volume? Firms need to ensure that workflow, queue management, control reporting, exception management, and efficient and streamlined processes are in place. Without these, current processes may collapse over time.

04 Fit for purpose — A third-party risk management program for a bank with $25B in assets looks a lot different from that of a $100B bank. Even though it contains all the same components, the level of rigour and detail — and the amount of automation through workflow — changes with the size and risk profile of the company. The foundations need to be in place, but it is generally something addressed in phases over time as the bank grows.
Benefits can be gained through operational improvements by following these guiding principles throughout the third-party risk management lifecycle. As an example, by monitoring and managing procurement and contracting more closely, as this process dictates, the organisation will be consolidating a number of vendors for each type of category to limit its risk exposure. It is less risky to do business with a few firms than with 50 separate vendors, which need to be monitored individually. It has obvious cost benefits, but, more importantly, fewer vendors can be monitored much more closely for performance against contracted service-level agreements, billing and pricing, as well as accuracy, enabling improvements.

Underpinning the lifecycle are leading practices that include organisational design; governance, policies and procedures; supporting methodology and frameworks; and enterprise visibility. These are areas that the more mature organisations should consider as they evolve their lifecycle process.

Additionally, the enhanced regulations encompass all vendors that provide a service to the financial institution in exchange for a fee. The third-party risk management lifecycle framework therefore should apply to all third-party providers, affiliates (such as credit card providers to a bank that scrape a fee off the revenue the bank earns), joint ventures, fintech companies and outsourced providers — not just traditional “vendors.”

_The third-party risk management lifecycle framework should apply to all third-party providers, affiliates (such as credit card providers to a bank that scrape a fee off the revenue the bank earns), joint ventures, fintech companies and outsourced providers — not just traditional “vendors.”_
Adapting the R&D Process for Innovation

Speed-to-market in such a rapidly evolving environment is essential. Many financial institutions are leveraging customary third parties, while others have created open platforms where they invite innovative vendors as well as fintech companies to curate their product and service offerings. Although speed is important, and fintech firms typically accelerate the software development lifecycle through more modern ways of working, it must be achieved by establishing certain “guardrails” to protect both parties. In many cases, fintech firms are not simply contracted directly by the financial institution, but rather are becoming engaged early in the business development or R&D stage and, in some cases, evaluated as potential acquisition targets for the bank depending on the strategic nature of the capabilities sought. Financial institutions are increasingly setting up investment arms, where they own an equity interest and are providing a customer base to the fintech firm, which subject the innovative third parties to the scope of the regulations indicated in the framework.

The Fintech Research and Development Lifecycle

As fintech companies progress through each stage gate of the R&D lifecycle, there should be increasing rigor applied to due diligence activities to understand inherent and residual risks.
Driving responsible innovation in the R&D process requires effectively integrating fintech companies into a partner firm’s existing third-party risk management programme at an earlier stage in the innovation process. Our recommended R&D methodology sets out a process where the fintech company is integrated into the traditional institution’s third-party risk management programme at the beginning of the relationship.

The objectives of the R&D activities mirror those of the planning and due diligence activities — to identify viable and qualified business partners. The benefit of this approach for both firms is that the third-party risk management due diligence is applied consistently throughout the R&D process. It also allows operational processes to be reviewed on both sides, which can subsequently lead to more rapid integration.

It is important that innovation and speed are not inhibited by a heavy third-party risk management programme; however, this approach enables both firms to consider carefully any large-scale operational and technology changes the partnership may require at the beginning of the process, saving time and resources further down the line.

By taking a risk-based approach, an organisation can tailor such changes to fit the specific risk posture and unique environment of the contracting party. This may include integrating products and services based on new technology into existing core systems and processes that could require modernisation and/or transformation to work optimally. This process can also be used to flesh out and communicate to senior management proactively how the risks of such partnerships may impact the financial institution’s overall risk profile and appetite.

**R&D Stage Gates in the Innovation Process**

The collaborative R&D lifecycle approach consists of four primary stage gates:

- Exploration/discovery
- Prototype
- Pilot
- Production

As partnership fintech firms progress through each stage gate of the R&D lifecycle, the financial institution enhances its understanding of the specific controls the fintech entity will continue to operate once a product or service launches. If the fintech firm has been acquired by the financial institution, however, the controls should have been integrated into its infrastructure and environment after the initial stage gate. In such an instance, the continued due diligence would focus on the ongoing monitoring of those controls to identify any new issues fleshed out through more robust end-to-end testing prior to “going live.”
### R&D Stage Gates

#### Research and Development Lifecycle
- **Exploration**
  - Sandbox environment with sanitised data (quarantine)
  - Unstructured development
  - No system integration
  - No access to production

- **Prototype**
  - Controlled data (quarantine)
  - Structured development/use cases
  - No system integration
  - Friendly users (consenting employees or customers)

- **Pilot**
  - Limited customer data
  - Limited access to production
  - Some "live" customers
  - Defined use cases

- **Production**
  - Access to sensitive data
  - Access to production/core systems
  - Offered to customers

#### Stage Gates
- **Exploration to Prototype**
  - ID of viable third-party use cases for innovation and first-line approval
  - Internal pass/fail diagnostic to ensure controlled data and system access parameters
  - Third-party compliance screen

- **Prototype to Pilot**
  - First-line approval of testing and definition for larger pilot program
  - BCM internal pass/fail diagnostic
  - IT controls established on data exchange containing sensitive personal information
  - Compliance approval on third party

- **Pilot to Production**
  - First line of defence go/no-go decision on production
  - Holistic governance, controls and policies to mitigate BCM risk
  - Fintech and fourth-party BCPDR testing, compliance and sign-off

#### R&D Phase Attributes
Exploration

There are many fintech firms in the financial services ecosystem, ranging from the small startups at the nascent phase of their development to larger, more developed firms that have secured funding and a growing client base. During the exploration phase, traditional firms can examine a number of potential fintech partners to assess which products and services would best fit their business strategy and integrate well into their existing infrastructure. Only a short list of candidates is selected to advance to the prototype and pilot stages.

During this stage, firms need to align a strategy of how they will be able to integrate the new product into their existing systems, while also considering the control environment, which will mitigate risks of the developmental product from the rest of the organisation. This is also the time to evaluate the fintech firm’s own security and control environment, which can inform how the company should work with the organisation.

Based on the level of maturity, this could lead to a decision to develop a product in a contained “sandbox” — a controlled in-house environment with live testing — or accelerate a move toward a full-scale roll-out to customers. This allows the level of review from a compliance perspective and a cybersecurity perspective to be scaled to an appropriate level with sufficient controls, which will need to be put in place ahead of a full-scale rollout of the end product.

Completing a full due diligence compliance assessment requires a much longer period before a product is ready for production. Typically, emerging fintech firms are not at a level of maturity to be able to prepare for or respond effectively to the full due diligence programmes demanded by large financial institutions. Therefore, at this stage, the institution should determine whether it needs to assist the fintech with the development of appropriate internal processes, procedures and controls if they are lacking. Depending on the strategic nature of the product or service being considered, the business may decide to acquire the fintech outright to ensure governance and ownership over all aspects of security and compliance.

Promotion to the next stage gate would require the fintech firm’s products and services to meet qualifying criteria such as passing internal diagnostic tests to ensure data and system access parameters, successfully completing a third-party compliance screening programme, and receiving approval from the business on the viability of the product and/or service.

Prototype

The selected products and services identified during the exploration phase are progressed to the prototype phase, where the product is developed using controlled data in a quarantined environment. More structured and robust use cases for the product or service are developed to ensure the viability of the technology, guaranteeing that it continues to meet the requirements of the business. This might include satisfying base operational process cases and unit and integration test cases and assessing projected demand and revenue, which can be achieved through small tests with consenting employees or certain customers.

Until the client base increases, the collaboration should avoid processes, controls and workflows that add to overhead costs and that are specific to client-vendor relationships that do not contribute to the rapid development of the product or service. Instead, both companies should look to integrate working teams’ capabilities and processes to strive to create a software development lifecycle closer to that found in a single, agile company.
In addition, the organisation should identify any business-continuity issues with the new technology in failover scenarios, detailing the process of recovery. This process will assist with the identification of any missing controls and system requirements, such as disaster-recovery processes and protecting sensitive data. All these controls need to be defined and built, and then need to pass through a compliance approval process before this product is deemed suitable for advancement to the pilot phase.

**Pilot**

Once a product enters the pilot phase, the organisation can address more specific compliance considerations. These could include data security requirements, financial due diligence and the legal ramifications around the legal structures shared between the bank and the fintech firm (for example, some are joint ventures, while others are pure third parties). Live data can be introduced at this stage to further test controls with a broader range and number of customers. The organisation also can test more detailed and intricate end-to-end integration at this point, along with user acceptance testing from the business.

Companies should also increase the coverage of both automated and manual tests involving representatives from the business, as well as compliance and information security teams. Data-driven automated tests should be used to validate multiple scenarios in a single pass, and if the business includes first- and second-line representatives during these tests, a better evaluation and analysis of the inherent risk driven by the type of service (or product) provided by the third party can be fleshed out and addressed. The “residual” risk that drives segmentation and risk tiering of the third-party relationships can then be adjusted accordingly.

For manual testing, firms should strive to achieve complete coverage and surfacing of all defects within a specified time frame. A risk-based approach should be used that leverages the existing test cases to determine which tests will be run for each release. Firms should introduce tests based on whether the top-level business process has been impacted.

This phase also enables the larger firm to regression review the fintech company’s control environment and conduct further testing of business-continuity management and disaster-recovery policies. Only once end-to-end testing from the user acceptance testing meets “go/no go” criteria, the holistic governance business-continuity management structure has been signed off and a thorough review of the fintech company’s fourth-party risk management controls is deemed to be satisfactory can the product be passed to the production phase. This phase also requires final approval from the business to move ahead.

**Production**

Once the organisation makes the decision to “go live,” fintech companies that are working with banks will ultimately have to complete the full scale of due diligence activities of a bank’s third-party risk management programme before going to market and having access to the full scale of customer data or other sensitive access. At this point, the product...
will have access to sensitive live data and will be fully integrated into the company’s systems and infrastructure, which is then offered to customers as a valid product via various marketing campaigns.

If the financial services organisation fully considers all the control and compliance aspects throughout the early prototype and pilot phases, the due diligence burden is alleviated once the product reaches this final stage of the R&D lifecycle, as it has essentially completed all the necessary steps along the way. This not only provides the business with confidence on the safety and soundness of new products and services but also gives the organisation a distinct competitive advantage with quicker and more streamlined new service launches.

Similarly, the R&D and planning process detailed above provides fintech companies, particularly smaller startup firms, with a more flexible and nimble approach to the rigorous requirements of standard third-party due diligence that is required by the regulators. Once this stage is completed, the startup company is better positioned to comply with the process. Then, once the fintech firm has made it past the pilot stage and into production, the expectation is that it will be more prepared to respond to the due diligence pressure applied by the larger institution.

However, many fintech companies will not be mature enough to push to the production phase without additional assistance. In these cases where the product or service has a strategic interest by the business, the larger institution has the option to step in and help the fintech firm establish more mature capabilities in risk management, compliance and controls, facilitating the launch of a compliant and successful product to the market.

The R&D and planning process provides fintech companies, particularly smaller startup firms, with a more flexible and nimble approach to the rigorous requirements of standard third-party due diligence that is required by the regulators.
Final Thoughts and Evolving Considerations on the Fintech Phenomenon

The trend of collaboration between traditional firms, innovative third parties and regulators will continue to increase, as will expectations to manage risk in distributed environments. Therefore, firms need to modernise responsibly. Collaboration between financial institutions and fintech firms should follow the responsible innovation R&D and third-party risk management best practices set out in this paper.

Traditional financial institutions must proactively look at innovation as both an opportunity and an emerging risk, and respond accordingly, either by developing their own fintech subsidiary companies or through acquisition. Large banks have set up fintech innovation labs or accelerators, which are testing disruptive technologies for their customers, with some firms also funding proof-of-concept tests for startup firms with fintech partners.

In addition to avoiding the crosshairs of the regulators, implementing an effective third-party risk management programme can yield significant operational improvements. The increased focus on third parties often leads to vendor rationalisation, greater spend leverage, better contractual alignment and reduced costs, as well as driving improvements in performance delivered from vendors and third parties.

Many organisations are seeking third-party partnerships to develop innovative products and services in an increasingly competitive environment, focused on speed-to-market and providing a better, and more accessible, service for consumers. As more and more customers demand “always-on and on-the-go” services via myriad smart devices and access points, developing innovative services quickly demands that traditional firms partner with more nimble financial technology firms in an effective manner that drives value creation. By taking advantage of their composite strengths, partnering firms can achieve competitive advantages through balancing speed of innovation with product safety and soundness.

*By taking advantage of their composite strengths, partnering firms can achieve competitive advantages through balancing speed of innovation with product safety and soundness.*
Risk and compliance teams also need to recognise that they too have a role to play in ensuring organisations are able to benefit from digitalisation projects and embrace new technologies.
Digitalisation Meets Risk & Compliance

In response to the growing cyberthreat, rapid technological change and opportunities for digital innovation, second line functions are beginning to recognise that their mindset needs to change. Technological advancement is an unstoppable force. Customers will demand innovation. It is therefore essential that risk, compliance and security teams are not viewed as too risk averse and rather become enablers of innovation. There is always a balance between risk and reward. Risk and compliance teams have a critical role to play in ensuring the organisation gets this balance right. For many, the medium-term risk of not innovating may be more significant than the shorter-term pain associated with adverse events arising from the risks that the business is controlling tightly.

Over the past few years, security teams have acknowledged that their mentality has had to change. They used to be seen as a function that blocked requests from the business; they now acknowledge that their role is much more about working out how to best manage the risk while embracing changes the business leaders want to push throughout the organisation. “Bring your own device” was a classic example of something that many security functions looked to block before recognising that their role was to help manage the risk. The majority of organisations now allow these devices and manage the risk to a greater or lesser extent.

Risk and compliance teams also need to recognise that they too have a role to play in ensuring organisations are able to benefit from digitalisation projects and embrace new technologies. At the same time, risk and compliance teams need to ensure that risks are understood, assessed and managed and that regulations are met. The key is recognising that there are many ways to embrace most technologies and manage risk together. Risk management does not always mean risk avoidance. The risk associated with a pilot or proof-of-concept project can often be managed without completely locking down the technology. It is also worth noting that many of the regulations are not as prescriptive as many might assume from the restrictive policies and standards that the business has put in place.

To add value, second line teams need to be actively engaging with the business leaders to provide guidance and advice during the planning phase of a project using emerging technologies. If they are not consulted, there is a significant likelihood that technology will be implemented without the risks and regulations being fully considered and without the appropriate controls in place. It is essential that when consulted, the second line does not make it difficult
for the business to be agile. To do this well, second line functions will need to anticipate the future demands of the business, and have an opinion on the use of the new technology and the associated risks. The team will be familiar with rules and regulations around the world and will be able to provide guidance to the business on how best to harness the new technology and manage the risks. The difficult questions will already have been asked, and the rules of engagement defined. When this process works well, the second line becomes a valued partner, which is empowering the business rather than being viewed as a barrier to change.

To date, many second line functions have not been good at anticipating the demands of the business and are not as well informed as they could be when fully engaged. Without adequate knowledge and preparedness, the risk and compliance function is forced to tilt more heavily toward risk mitigation, often at the expense of speed and innovation. Leaders are recognising the need for this to change, however. Without clearly defined policies, guidance and opinion on the risks new technologies poses, the business moves forward without realising the value of or need for consultation with the second line. It is critical that risk and compliance functions stay abreast of emerging technologies and ensure that they are engaged by the business as it looks to evaluate new technologies such as biometrics, AI, robotics, blockchain, virtual currencies and much more.

Key questions for risk and compliance functions to consider:

- Technological advancement is an unstoppable force. Customers will demand innovation. It is therefore essential that risk, compliance and security teams are not viewed as too risk averse and rather become enablers of innovation.

01. Do leaders of digitalisation initiatives actively seek out guidance and support?

02. If not, what can the second line of defence do to encourage, engage and dialogue with the first line?

03. Is there a cultural obstacle that needs to be challenged and transformed?

04. How can you improve collaboration and consultation on new technologies and their associated risks?

05. Has the function been able to provide guidance on new technology when asked?

06. Is the business aware of the policies and rules associated with research and development and the process to involve risk and compliance?

07. Is the function engaged enough with the leaders of digitalisation initiatives to promote trust and confidence?
With more advanced consultation and active engagement, the risk and compliance function can more effectively fulfil its mission to ensure that the organisation’s risks are managed and adequately controlled and avoid the internal and external consequences of failing to act.

- Consequences of Failing to Act

<table>
<thead>
<tr>
<th>Internal</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inability to embed an innovation culture</td>
<td>Loss of market share due to delays launching new solutions</td>
</tr>
<tr>
<td>Unnecessary and/or wasted expenditure on digitalisation initiatives that do not comply with policies and/or regulations that need to be either scrapped or rebuilt</td>
<td>Regulatory costs and penalties due to poor governance and lack of controls</td>
</tr>
<tr>
<td>Increased costs associated with research, development and investment in the new technology</td>
<td>Reputational damage from consumers, press and peers</td>
</tr>
<tr>
<td>Trust and reputational costs based on the relationship risk and compliance has with the business</td>
<td>Declining revenues and margins and failure to meet market expectations</td>
</tr>
</tbody>
</table>
When assessing the organisation's preparedness for pursuing each of the digitalisation objectives, they should consider the questions below:

**Digitalisation Objectives and Considerations**

### Customer Engagement
- What information is the organisation currently storing and using, and what types of information should it be collecting?
- What information would customers expect to be stored, and how would customers expect this information to be used?
- Other personal data often has more value on the black market, as it does not need to be exploited immediately to obtain the value. For example, it is hard to change biometric data. GPS data can also be misused, as it provides a lot of information about a person. What is the organisation's view on capturing and using GPS information on smartphones to learn more about the consumer? When is it allowed and appropriate to collect and use that data commercially?
- What is the organisation's view of customers using Siri and Alexa to access account information? Does the organisation have a view on access limits?

### Digitising Products & Services
- What is the organisational view on the use of robotics for risk-based decisions and at what stage do humans need to be involved?
- What level of understanding is required of the rules that are being applied by systems using AI to make decisions?
- Is there a limit articulated for when and how the organisation uses customer data?
- Have rules of engagement been defined when the business is looking to collaborate with technology companies that might become competitors? What information can we share?
- How will virtual currencies impact the business?
- Does the business have a clear view of the use of blockchain technology?
- Do any countries still require physical signatures to evidence contracts? How might this impact plans to use blockchains to replace traditional contracts?

### Business Analytics & Decision Science
- Does the company have policies around data sharing, data storage and the use of the cloud?
- What restrictions should the business put in place on the utilisation of AI? Are there ethical considerations? For example, would it be appropriate to train an AI engine to support recruitment decisions? Might AI result in an organisation unknowingly not selecting candidates on certain criteria that a business would never utilise against? Is not understanding the rules ever a defence?
- What policies and/or rules exist to ensure that all AI is subject to the appropriate validation and/or testing? What 'black boxes' exist in the organisation?

### Operational Performance
- Customers are demanding faster decision making and approvals for new products, which will require firms to undergo radical change. Is the business effectively assessing the risk of not making these changes, or is the focus only on the operational risks associated with making the change?
- Automating processes can improve operational efficiency but brings additional risks that need to be considered and managed. Does the organisation have a view on where those boundaries lie?

### Regulation
- Are there laws and regulations firms need to comply with that impact the digital strategy?
- How is the use of technology going to be regulated?
- How are regulators responding to new technologies, and what new rules are expected?
- How are regulations likely to vary between jurisdictions?
- Does the organisation have processes in place to consider the regulatory mood and direction for any products and services based on new technology?
Final Thoughts

The velocity and rate of change of digital innovation is an undeniable disruptor to many traditional businesses. New technology is enabling new products and service channels that adapt to changing customer behaviours, as well as driving efficiencies and creating competitive advantages.

Risk management and compliance functions need to evolve. They need to engage with the business, anticipate how technology could/will be used, understand potential implementation timelines, conduct more research and define policies and/or guidance where necessary.

Fundamentally, risk and compliance functions need to get to a point where the business is looking to engage with them because they value their advice. If leaders of digitalisation initiatives believe that the second line will guide them effectively on how to embrace technologies in a risk-managed way and not create barriers, they will consult. It is essential that the second line is seen as empowering and guiding, not blocking. In summary, they need to redefine the rules of engagement and advise the business how to do something rather than provide many reasons why it should not.
Protiviti is working with the leaders of risk and compliance functions to help them transform and become more forward-looking and prepared for the opportunities and challenges a digital future holds. These include:

- Educating risk and compliance functions on the latest technological trends
- Providing training on risks and controls within the digital arena
- Providing guidance on how to manage the digital risks and promote business innovation
- Helping organisations ensure that policies are fit for purpose in the digital age and not inadvertently stifling innovation

Digitalisation provides an opportunity for risk and compliance functions to engage with the right people and help their organisation embrace digitalisation in all its technological guises to face the future with confidence. It also provides the second line functions with opportunities to embrace these emerging technologies to improve performance and to manage escalating costs. These opportunities should also not be overlooked.

### How Protiviti Can Help

Protiviti has developed a digitalisation/digital transformation framework that provides a high-level overview of how we help our clients fulfil their goals and objectives. In the graphic below, the vertical columns represent the problems that we are seeking to help our clients solve; the horizontal bars explain how we help.

<table>
<thead>
<tr>
<th>Customer Engagement</th>
<th>Digitising Products &amp; Services</th>
<th>Business Analytics &amp; Decision Science</th>
<th>Operational Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploring new ways to build strong relationships with customers</td>
<td>Launching new, enhanced products and exploring new business models</td>
<td>Exploiting enhanced data analytics to improve decision making</td>
<td>Creatively using technology to improve performance</td>
</tr>
</tbody>
</table>

**Digitalisation Strategy, Governance & Execution**
Ensuring that transformation programmes are established, well defined and set up for success and that they support execution

**Functional Transformation & Improvement**
Using technology to reinvent finance, information technology, business operations, procurement, risk management and audit

**Enabling an Innovation Culture**
Ensuring that the unnecessary barriers to innovation and change that exist within organisations are eliminated

**New Technologies Assessment & Implementation**
Supporting organisations with decision making as they consider whether or not to embrace new or emerging technologies

- Advising on how to transform into a digital function that proactively collaborates with the business
- Helping with their digital strategy and forming an opinion on the latest trends
ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

ABOUT OUR IT CONSULTING SERVICES

In today’s rapidly evolving technological environment, a trusted adviser – one who not only provides relevant insights, but delivers a combination of strategic vision, proven expertise and practical experience – can enhance the value of your business with technology. Our global IT Consulting practice has helped CIOs and IT leaders at more than 1,200 companies worldwide design and implement advanced solutions in IT governance, security, data management, applications and compliance. By partnering with us, you ensure that your IT organization performs with the same focus and excellence with which you manage day-to-day business operations. We will work with you to address IT security and privacy issues and deploy advanced and customized application and data management structures that not only solve problems, but add value to your business.