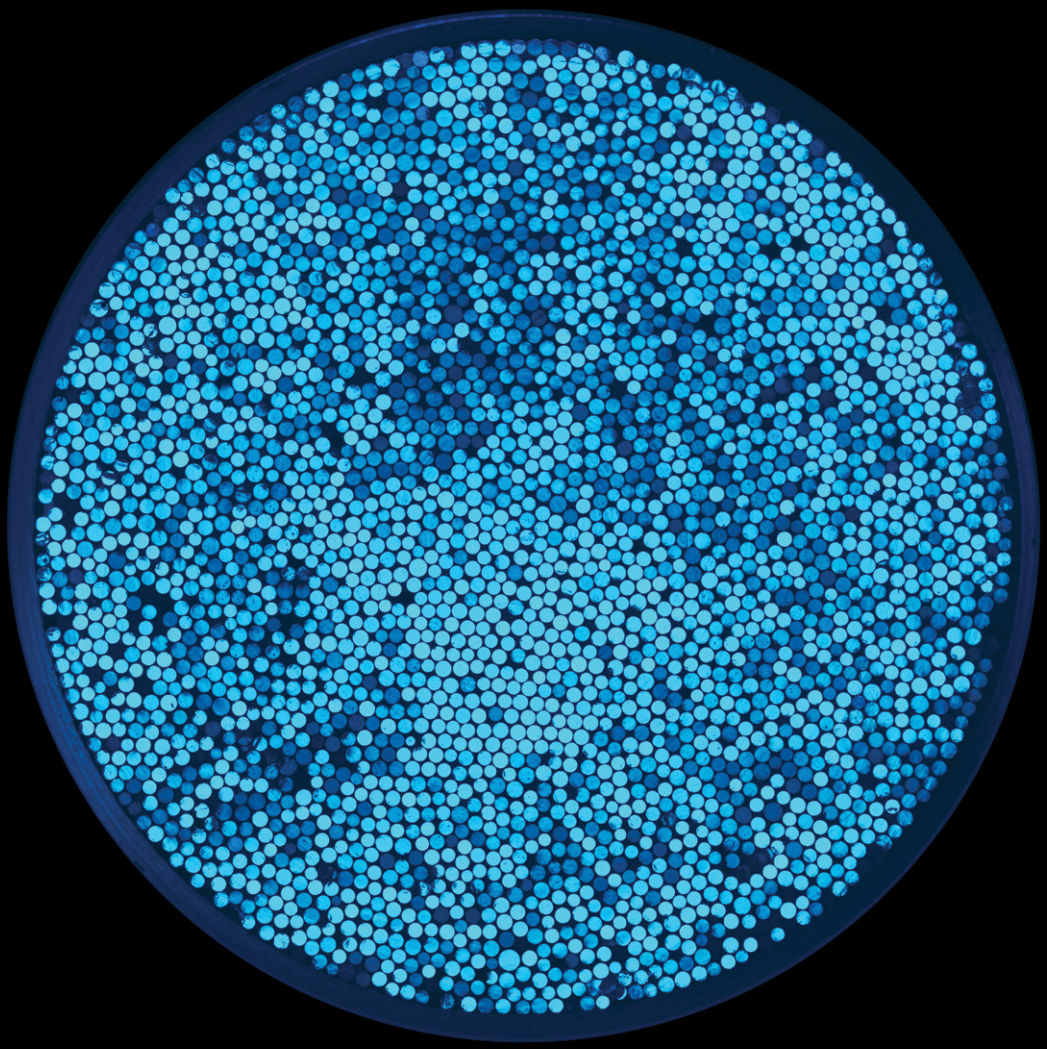
Deloitte.



Decoding the future

IT Risk Management. Disrupted.

Exploring the future of IT risk management

By Chris Recchia, Tom Bigham and Rob Dighton

IT Risk Management. Disrupted.

With fragmented IT architecture and legacy infrastructure still widespread across the financial services industry, many organisations are already struggling to get IT risk management right. A wave of change is coming that will make this challenge even more complex. Current approaches to managing IT risk, developed in an era focused on establishing controls for financial reporting, are no longer fit-for-purpose and need to be redesigned.

Now is the time for senior financial services risk professionals to begin preparing for the array of changes that are altering the world in which we all operate and compete.

The need for effective risk management is rapidly increasing in response to the rise in threats and the unprecedented wave of innovation spreading across the financial services industry. Robotics, Fintech, artificial intelligence, cognitive computing and blockchain are some of the emerging trends that are expected to reshape the financial services industry and have a substantial impact on firms of all sizes and geographical spread.

Financial services firms employ many more risk managers than they traditionally did, yet risk management teams remain on a reactive footing with a predominant focus on traditional IT general controls and risk assessment techniques, and are limited by the processes, systems and wider business insight with which they have been equipped.

As technology transforms banking and insurance and shifts the risk landscape, organisations will need to develop an entirely new approach to IT risk management.

Drivers for change

The integrated model is evolving

For the majority of the last four decades most financial services firms have been creating and distributing end-to-end products and solutions without having to communicate and connect as they now need to in a mobile, device-driven world.

The emergence of integrated technology platforms, so far primarily outside financial services, will further change the financial services ecosystem, enabling users to consume banking services provided by multiple firms on a single platform.

Looking ahead, processes may increasingly rely on utilities or shared-service companies, involving more and more third parties (external and inter-entity) in a move away from the traditional banking model.

Emerging technologies driving innovation

The emergence of new technologies, as well as increased collaboration across the industry and between regulators, is driving innovation like never before.

Among the technological advances originating within the industry is the Utility Settlement Coin recently proposed by a number of large banks. This would allow financial institutions to pay for securities without waiting for completion of traditional money transfers and would rely on digital cash being directly convertible into cash at central banks. It would also speed up post-trade settlement and clearing.

Among the technological advances prompted by regulators is the Payment Services Directive 2 (PSD2), which will require banks to grant third-party payment initiators and aggregators access to online accounts by January 2018, enabling Payment Initiation Service Providers (PISPs) to initiate payments on behalf of clients.

Increased regulatory scrutiny

As the financial stability of firms becomes increasingly linked to technology, regulators are taking more interest in the effect of technology transformation on business.

Many firms are struggling to manage the technology changes required to meet regulatory requirements and the current UK Financial Conduct Authority business plan highlights Technology and Innovation among its seven priorities for the next financial year. The UK Financial Stability Board is also assessing the implications of financial technology innovations and the systemic risks that may arise from operational disruptions.

Cost focus at the top of the corporate priority list

Political and economic uncertainties are currently focusing corporate priorities on cost reduction and improved cash flow. This trend is expected to continue for several years, driven by low interest rates, increased capital requirements and the low-growth environment predicted after the UK voted to leave the European Union.

This cost focus is shining a light on the value being delivered by current approaches to IT risk management, whether that is investment in business-as-usual capabilities, or funding large-scale control remediation programmes.

Figure 1. Key milestones defining the evolution of IT risk management

As established banks instil innovation across their cultures, challenger banks grow market share, and digital banks emerge, we will see a step change in the role, responsibility, and profile of the IT risk management function.

What does this mean for IT Risk functions?

Whilst technology was initially an enabler to the business, it is now a key differentiator in terms of cost, speed, innovation and customer experience.

As the role of the Technology function has changed over the last 50 years, the role of those charged with IT risk management has evolved too (see Figure 1).

As banking and insurance technology becomes more efficient and more automated, the ecosystem in which firms operate will grow vastly more complex. The IT Risk function will need to take the lead in driving a coordinated approach to dealing with some of the big issues:

Redefining the accountability model

Accountability for risk and control will need to be revisited in this new evolving world of technology driven innovation, new business models, and further regulation.

As technology becomes more prevalent and ingrained, the scope of risks and controls becomes more blurred, where they begin and end is less distinct and responsibility is not always clearly defined.

Embedding the right accountability model for ownership of risks arising from Technology, both within IT and the wider enterprise, will be a critical factor in redesigning the approach to managing IT risk.

Rationalising the control framework

More preventative, real time controls need to be designed and built into systems up front, enabling risks to be identified in a continuous manner, rather than hours, days or months later. Given the speed at which data can be created, accessed, shared, and processed, traditional detective controls are increasingly identifying incidents and issues too late.

Over the last 10 years, responding to the wave of regulation has in part layered complexity upon complexity within the control environment. With the overall number of controls reliant on technology expected to increase (see Figure 2), this complexity needs to be addressed.

Risk management professionals need to play their part in championing risk intelligent design across new systems, technologies and control frameworks. This role will be more critical than ever so that the risks associated with new products, systems and processes are better understood and can be integrated into the existing risk landscape, rather than being layered as an afterthought.

Figure 2. Our view on how adoption of new technologies will impact the make up of an IT control framework

Overall # of controls reliant on IT	# of automated IT processes	# of automated application and IT controls	# of controls executed without human intervention
	# of controls that are manual in nature	% of controls derived from IT general computer controls	% of detective controls relative to preventative controls

Deloitte recently evaluated 302 operational controls at an organisation and identified that 74 percent of the controls could be eliminated. This involved eliminating duplicate, identical and redundant controls, checker-type controls and those that didn't add value or mitigate risks within processes. For this organisation, controls could still be automated without major infrastructure changes, shifting the majority of controls from manual to automated.

71 percent of respondents to the recently published Deloitte EMEA IT Risk Management survey "Foundations in a technology driven world" said that finding suitable candidates in the market is a struggle.

Leveraging opportunities for automation

Control execution by robotic software is now a reality. IT Risk functions should define their own automation strategy to guide investment of time and resources in the automation of processes, controls and risk reporting. Consideration should be given to how automation can be used to reduce the 'risk administration' burden, and to improve the timeliness, accuracy and usefulness of IT risk reporting data such as metrics and exception reports.

Large scale adoption of robotic process automation (RPA) software will need careful oversight from IT Risk given the inherent risks associated with automating key control processes.

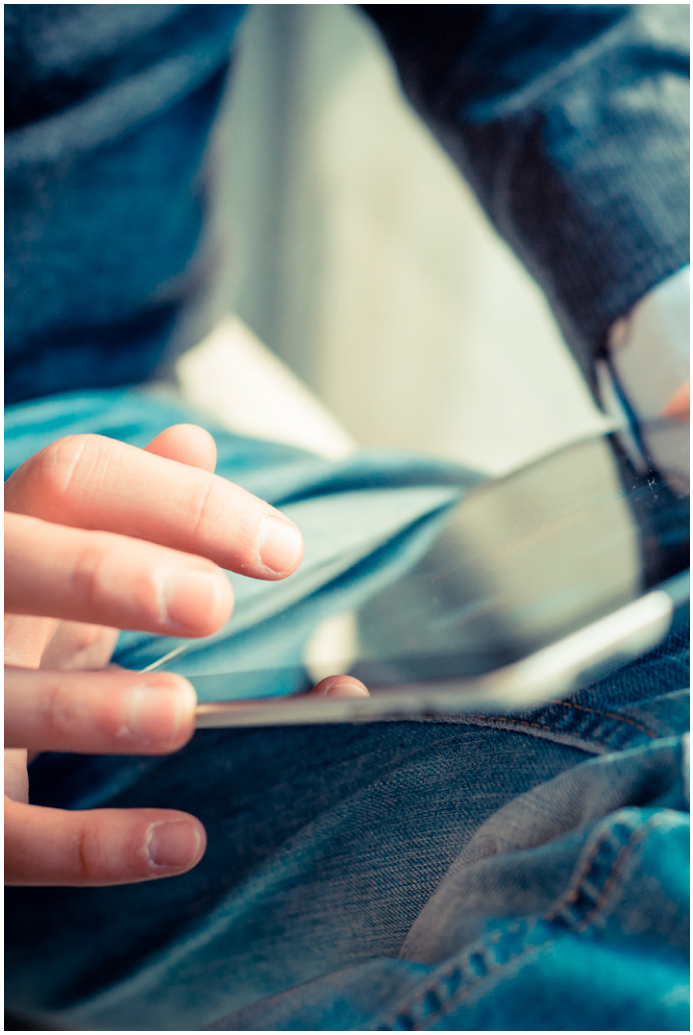
Reassessing the new risk and threat landscape in an 'open world'

As technology accelerates business automation and innovation, the risk landscape is rapidly evolving. Responsibility for understanding the risk implications of new technologies should be allocated to specific individuals who can coordinate the appropriate risk management response and help IT understand the implications. Three immediate examples of topic areas are:

- **Application Programme Interfaces (APIs)**: APIs will be an agent for further change for financial services, throwing open the doors to the payments world that has previously been the domain of a few large players. Customer data will have new value for all but will also pose new data protection and data privacy risks. Risk functions will need the technical expertise to be able to identify and manage the associated risks.

- **Management of third party risk**: As integrated banking platforms emerge, it is feasible that a proliferation of third-party relationships will emerge where no contractual relationship exists between the parties. The traditional method of financial compensation in the event of an incident, contractual clauses, will be redundant, and this will need to be factored into risk management and mitigation techniques.

- **Blockchain**: As blockchain emerges as a feasible financial services building block, the implications for risk management and governance functions are considerable. Shared chains inherently establish new relationships, and promote the concept of 'real-time' monitoring, control assessment and auditing. Several global regulators are considering how to implement a regulatory 'node' that will provide them a window into banking transactions which they have never had before and which only parties to the transactions have previously been able to see.



Rethinking the IT Risk talent strategy

In order to meet the growing demands being placed on it over the next five to seven years, the IT Risk function will need to develop and nurture a pipeline of talent that has operational IT, business knowledge and risk and control experience in equal measure.

As the environment becomes increasingly complex, Risk staff will have to assess, analyse and respond to the new landscape alongside business risk management teams. Consideration should be given to the additional skills required for managing IT risk in the future, and how they differ from the skillsets management have at their disposal today.

5 emerging themes executives can start to address NOW

Redefine the accountability model

Consider how changes in the external environment, including changes to business models, further innovation or new regulation, will affect the risk landscape and the blend and balance of controls required. Determine how these changes will affect existing accountability models for risk and control and be clear about how these changes can be embedded within the operating model.

Rationalise the control framework

Champion risk intelligent design across new systems, technologies and control frameworks. Delayer the control framework with more preventative, automated controls built into systems up front, enabling risks to be identified in real time, rather than hours, days or months later.

Reassess the new risk and threat landscape

Assign responsibility for understanding the risk implications of new technologies to specific individuals who can coordinate the appropriate risk management response.

Three immediate examples of topic areas to be addressed are: Application Programme Interfaces, blockchain, third party risk management.

Leverage opportunities to automate

Define an automation strategy and the principles for process, control, and reporting automation.

Consider reducing time spent on low value 'risk administration' activity and increasing time spent on removing layers from the control environment by implementing a consistent and scalable set of automated controls. Identify quick wins to drive adoption and to demonstrate, with little investment, the benefits to be gained.

Rethink the IT Risk talent strategy

Review the IT risk talent strategy and develop and nurture a pipeline of talent with the right skill sets to meet the growing and more widespread demands that will be placed on the function over the next 5 – 7 years. Consider the spectrum of skills required now, and in the future. Consider the interface with other business risk management teams and how these functions can work together in a more integrated and resilient manner, reflecting the direction of travel for the supporting technology platforms and operational processes.

The opportunity

The financial services industry has never faced the combination of political and economic stresses it is currently facing.

Many organisations have a legacy of multiple and layered controls, sequentially put in place over time to meet a series of governance and policy mandates. Many have inefficient and poorly controlled change, security and operations processes, which are inherently expensive to run. Yet more organisations have a number of long-running and costly control remediation programmes, often bringing with them additional project management overheads.

Reducing this spend by improving up front IT risk management processes presents an opportunity for financial services firms. Firms that seize the opportunity to act now and get on the front foot will not only reduce costs, but will also increase their knowledge of front-to-back risk and reduce time-consuming manual interaction and control management activities.

Furthermore, new technologies present opportunities for risk management simplification, improving risk management efficiency and embedding control automation. Tapping into these opportunities will enable firms to redeploy resources they currently expend on reactive 'risk administration' activities.Fostering a cultural shift towards forward-looking and business-aligned IT risk management will also better position firms to meet the long-term IT risk challenges that haven't yet emerged or been identified.

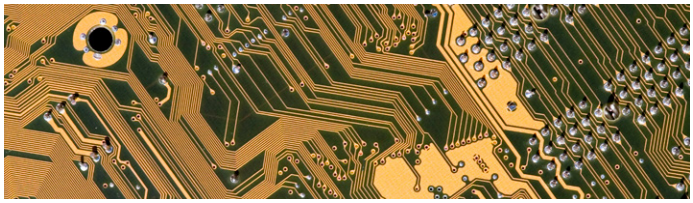
Conclusion

Given the current political, economic and regulatory environment, the short to medium term focus should continue to be on driving better value from IT risk management, without exposing firms to an increased level of risk.

Technology will grow more sophisticated in response to consumer and regulatory demands, further intensifying competition across the industry.

As established banks instill innovation across their cultures, challenger banks grow market share and digital banks emerge, we will see a step change in the role, responsibility, and profile of IT risk management.

Acting now to address the drivers and considerations we have summarised here will enable the IT Risk function to play a leading and value adding role in shaping the way in which technology drives the industry in the future.



Chris Recchia is a Partner within our Risk Advisory practice in the UK with over 15 years' experience leading global assurance and advisory engagements across clients within the financial services sector. His relationships span across all levels – the board, executive management, 1st and 2nd lines of defence, internal audit, external audit, and the wider extended enterprise.

He has a detailed understanding of technology risk management, business processes and IT risk and control environments, with additional specialisms in the execution and delivery of the technology components of large scale regulatory investigations.

Tom Bigham is a Director in our Risk Advisory practice with over twelve years' experience in governance, risk, and control advisory services. Tom leads our IT Risk Management campaign for the UK Firm, and also runs our annual EMEA Financial Services IT Risk survey.

Tom has built up extensive experience in designing and embedding process, risk, and control frameworks, as well as managing complex governance, risk and compliance projects.

Rob Dighton is a Senior Manager within our Technology Risk & Controls team and is responsible for leading the delivery of our IT Risk proposition across financial services.

He has 10 years' experience in delivering large-scale governance, risk and control projects across the financial services sector. His core areas of focus are the design, implementation and enhancement of 1st and 2nd line risk management processes and operating model design for Technology Risk functions.

Deloitte.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. J10236