

# Inside

Insights  
from Deloitte

---

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

---

**Part 01** | From a strategic  
and regulatory perspective

Page 07

---

**Part 02** | From a digital  
perspective

Page 31

---

**Part 03** | From a governance  
and compliance perspective

Page 77



**Deloitte.**

CCO  
CISO  
CRO  
CIA  
BOD

EDITION  
2 0 1 8

# Contents



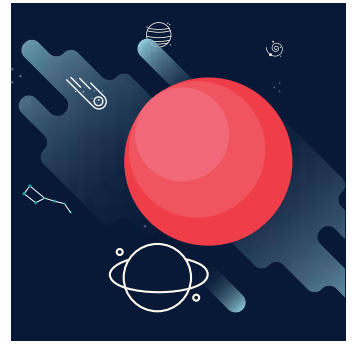
Page 09



Page 15



Page 24



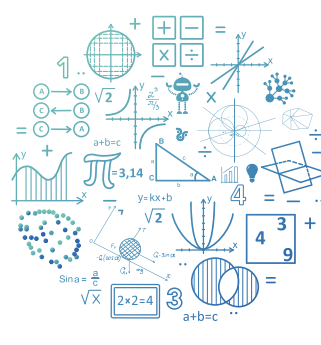
Page 33



Page 40



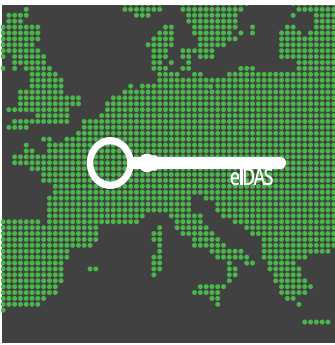
Page 47



Page 54



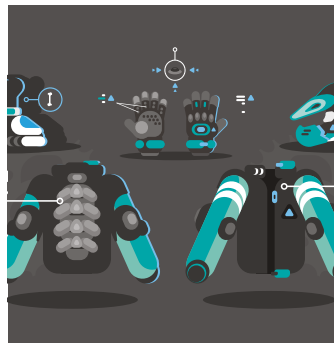
Page 63



Page 71



Page 78



Page 88



Page 94



Page 102



Page 110

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

Part 01   From a strategic and regulatory perspective	07
Part 02   From a digital perspective	31
Part 03   From a governance and compliance perspective	77

09

**Bringing it all together**  
Financial Markets Regulatory  
Outlook 2018

15

**The view from the industry**  
Deloitte Banking Union  
Supervision Survey

24

**Dealing with divergence**  
How banks can build a strategic  
response to the uneven  
implementation of Basel  
standards

33

**Using RegTech to transform  
compliance and risk from  
support functions into  
business differentiators**

40

**Blended learning**  
Combining digital and  
classroom training to achieve  
maximum results

47

**Hope is not a strategy**  
Confronting tomorrow's cyber  
threats today

54

**The algorithmic revolution  
is here**

63

**Fight fire with fire**  
Cyber response training  
through immersive simulation

71

**eIDAS**  
The EU as a forerunner in  
boosting the digital economy

78

**Risk, reward, and the  
realities of doing business  
right**  
Insights from the Deloitte Risk  
Conference

88

**Global Risk Management  
Survey**

94

**The future of risk in  
financial services**

102

**You and I were meant to fly**  
The rise of managed services

110

**What's next for bank board  
risk governance?**  
Recalibrating to tackle new risk  
oversight expectations

# Editorial



Dear readers,

Welcome to the fourth international edition of Inside, dedicated to governing bodies and internal control functions. Our objective is to provide professionals involved in governance, risk, compliance, and internal audit with thoughtful insights in order to overcome the main challenges they are likely to face.

Last year was expected to be a period of uncertainty for the financial services industry. Looking ahead to 2018, it seems that most of the challenges and uncertainties remain. First of all, 2018 has a concentration of regulatory deadlines, which, in combination, touch all sectors of the financial services industry.

Moreover, the economic environment, fierce competition, and regulatory and technological change will continue to put pressure on traditional business models across the industry.

In this edition, we explore important topics such as:

- Dealing with the complexity of the 2018 financial services regulatory landscape
- Building a strategic response to the uneven implementation of Basel standards
- How the EU regulation on electronic identities and trust services for electronic transactions will boost the digital economy
- How the future of risk management in financial services will likely look different than the current risk capabilities many are familiar with
- The rise of managed services to respond to the heightened pressure on risk and compliance operating models
- The evolution of bank board risk governance to meet new risk oversight expectations



- Using RegTech to transform compliance and risk functions
- Confronting tomorrow's cyber threats
- Managing the risk arising from the algorithmic revolution

In the current environment, financial institutions are now urged to rethink and transform the way they manage risks to leverage new technologies, and increase risk and compliance management efficiency and effectiveness.

You will find all that and more in these pages. We hope you will enjoy this publication.

Sincerely,



**J. H. Caldwell**  
Partner  
Deloitte US  
Global Risk Advisory Leader  
Financial Services



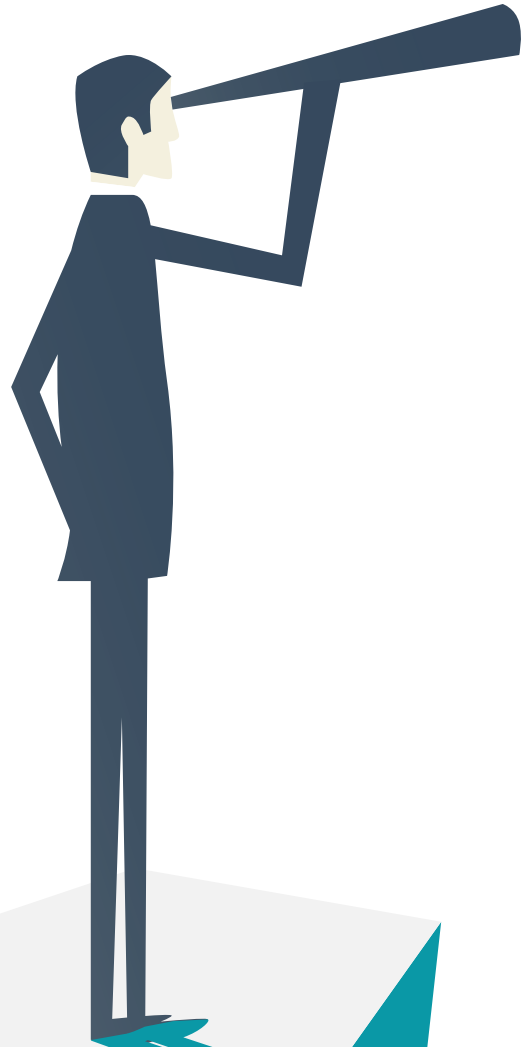
**Laurent Berliner**  
Partner  
Deloitte Luxembourg  
EMEA Risk Advisory Leader  
Financial Services



# Part 01

---

From a strategic  
and regulatory  
perspective ▶



Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018a](http://www.deloitte.com/lu/InsideRisk2018a)

Printed with permission of Deloitte UK



Bringing it all together

# Financial Markets Regulatory Outlook 2018

**David Strachan**

Partner  
EMEA Centre for  
Regulatory Strategy  
Deloitte UK

**John Andrews**

Senior Manager  
EMEA Centre for  
Regulatory Strategy  
Deloitte UK

The year 2018 heralds numerous challenges for European financial services, particularly in the arena of regulatory reform. The industry must grapple with the implementation of multiple new EU directives and regulations, while simultaneously preparing for Brexit, and guarding against the ever-increasing competitive and operational challenges posed by the development of new technology. This article provides a whistle-stop tour of these and a number of other themes that we identified in our 2018 Financial Markets Regulatory Outlook as strategically important for all sectors of the financial services industry in the year ahead. [➤](#)

This time last year, we expected 2017 to be a period of uncertainty for the financial services industry—among other things, there was a lack of clarity over the final shape of post-crisis reforms, and the implications of Brexit to deal with. We also saw pressures on the industry from sluggish economic growth and low interest rates, as well as competition from new entrants. Looking ahead to 2018, it seems fair to say that most of these challenges and uncertainties remain.

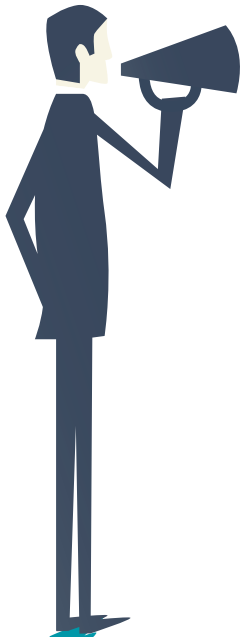
### Meeting multiple regulatory deadlines

2018 has a concentration of regulatory deadlines, which in combination touch all sectors of financial services. There is MiFID II, PRIIPs, the EU Benchmarks Regulation, the Insurance Distribution Directive, the revised Payment Services Directive, and the General Data Protection Regulation.

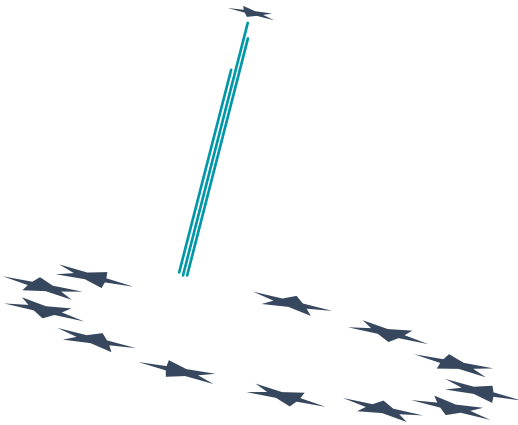
The focus on meeting these in such a short space of time will come with a significant opportunity cost. Firms will not have been able to exploit the potential synergies that exist between several of these regulations, and have had to divert resources from other strategic priorities. In a number of areas, we are expecting some firms to have to undertake significant remediation work after the deadline to make compliance more efficient and effective.

Some implementation work will inevitably overrun regulatory deadlines. Firms need to act swiftly to identify areas where they may be at risk of not being fully compliant and plan accordingly. Moreover, although some regulatory authorities have publicly recognized the challenges of getting over the line in time, there is no room for industries to relax.

Many firms will have to make ongoing changes to implementation plans throughout 2018 to ensure that they are working toward strategic solutions that will deliver optimal operating models. This means that controls optimization is likely to be a multi-year program.



Although some regulatory authorities have publicly recognized the challenges of getting over the line in time, there is no room for industries to relax.



## Brexit

as part of their Brexit preparations, we expect firms operating in the UK to start building their presence in EU27 countries on a sliding scale of intensity throughout 2018. We are yet to see whether a transitional period might be agreed, or what shape it might have. We expect some firms to press ahead with certain parts of their plans, including new authorizations and model approvals, even if a transitional agreement is reached.

With respect to two of the fundamental industry-wide issues in need of early resolution, namely the treatment of derivative contracts and of cross-border insurance contracts with durations beyond the UK's exit date, we expect legislative (or equivalent) solutions, especially given the risk of customer and counterparty detriment. These issues are clearly on regulators' radars.

We expect a degree of supervisory "learning by doing"—supervisors' expectations may well evolve over time as they better understand the specific challenges in relation to restructuring work brought on by Brexit. In the EU27, industry can expect to see a strong drive for consistent treatment of restructuring firms, led by the European Supervisory Authorities (the EBA, ESMA, and EIOPA) and the ECB.

For incoming firms to the UK, the FCA has said that it will set out more details in the new year of its approach to a potential temporary permissions regime, for which the UK Government will legislate if necessary. The PRA meanwhile has clarified its stance on the post-Brexit treatment of UK branches of EU firms, most notably for systemic wholesale bank and investment bank branches, for which the PRA will expect to have a degree of influence and visibility over the supervisory outcomes for the relevant firm as a whole. The PRA also made clear that it will retain the option of requiring subsidiarization of such branches where it cannot meet its objectives through other regulatory measures. With respect to insurance, the PRA has said it is likely to press insurers to subsidiarize if they are servicing material volumes of retail insurance business, with £200 million of FSCS-protected liabilities given as a benchmark for this assessment.

## Data protection and innovation

We are in an increasingly data-heavy world, with more and more tools at our disposal to analyze that data in novel ways. For financial services firms, this creates opportunities, but also risks. In particular, we see increasing concerns about the use of personal data and data privacy, and as a result, the industry can expect greater supervisory scrutiny of the way in which it uses and controls personal data. This is particularly true of those firms whose business models rely on wholesale processing of customers' personal data.

Most significantly this year, the EU's General Data Protection Regulation will come online in May. This will give consumers additional rights to understand and take control of how firms are using their personal data. Firms will have to carry out Data Protection Impact Assessments, not only to satisfy supervisors, but also to enable them to respond to customers' enquiries in a meaningful, transparent, and understandable way.

Still, GDPR compliance is not the end of the story. Conduct supervisors will be paying attention to any unintended consequences of the automated processing of large data sets—for instance, the potential for financial exclusion and discrimination, and what this means for customers who might be considered vulnerable. ➔

### Business model sustainability

The macro-economic environment, competitive forces, and regulatory and technological change continue to put pressure on traditional business models across the financial services industry, and in some cases are driving significant changes to business models, risk appetite, and strategic positioning.

From supervisors' perspectives, deeper analysis of regulated firms' business models enables them to think more broadly about their approach to supervision. Supervisory business model analysis played a more prominent role in supervisory activity in 2017, and will only intensify this year. The result is that business model analysis will increasingly provide a lens through which supervisors will view the competence and effectiveness of the board and senior management.

Firms need to be ready for this, and they may find themselves under scrutiny from two polar opposite ends: on one hand, they may ask themselves whether they are making sufficient and sustainable returns. On the other, they wonder where they are making good returns, and if they have considered the competition and conduct issues around pricing, fees, customer suitability, transparency, and so on. Either way, firms will need to develop their own internal capacity to analyze their business models and their vulnerabilities.

### Customer vulnerability

Regulators are increasingly recognizing that legislation, products, and services are often built for the "average" consumer. While that means that things work well enough for many, supervisors have a responsibility to consider customers whose situational vulnerability may mean that they are less able to look after their own interests and hence are at greater risk of suffering harm.

As a result, we are seeing a general shift in conduct supervision strategy. The starting point remains firms' responsibilities to

treat all customers fairly, but conduct supervisors will increasingly look to focus their resources on groups of customers at greatest risk of potential detriment or harm. At the same time, those supervisors are broadening their understanding of what it means for a customer to be vulnerable.

Essentially, regulators are recognizing that an individual's vulnerability is dynamic and a function of many variables—it is not just a case of someone's income, but will be based on health, age, life events, and other factors that may change over time. The industry will need to adapt to this broader definition of vulnerability, and factor it into their governance and interactions with customers. Building the capability to monitor vulnerability factors over time will be crucial and will need to be supported by strong board and senior executive engagement and enhanced data analytics.

Supervisory business model analysis played a more prominent role in supervisory activity in 2017, and will only intensify this year.



## Cyber resilience

Clearly, the regulatory focus on cyber risks is not new, particularly in light of technological change and increasingly digital business models. Nevertheless, in 2018 we are likely to start to see regulators articulating clearer priorities for what firms need to prepare for the inevitable cyber threats they face.

One shift of emphasis we expect in 2018 is driven by the heightened risk of cyber attacks with the potential to threaten financial stability. The increasing interconnections between financial services firms and their outsourcing partners—particularly technology partners—add to the challenge of dealing with what are increasingly becoming jointly owned systemic cyber risks, especially when you consider the cross-border element to many firms' arrangements.

In the insurance industry in particular, prudential supervisors will take a close interest in stress testing and reserving practices, with EIOPA having indicated that it will look to incorporate qualitative elements relating to cyber risk in its 2018 stress test. Conduct supervisors, on the other hand, will be alert for signs about whether policyholders have concerns about the coverage of policies they have already bought, and whether they provided adequate cover any for cyber events they experienced.

## Model risk management

It seems clear that regulators in Europe continue to see value in modelling as a part of the regulatory framework, even if they do so with differing levels of enthusiasm. However, there remain general concerns in some quarters as to whether models are fulfilling their intended role in adequately capturing and calibrating risks. There are also concerns as to whether model risks are well understood and managed by boards and senior executives.

In the light of this, firms need to demonstrate that they have considered the inherent limitations of their models, and that they understand the circumstances in which key model assumptions and dependencies might break down.

There are two immediate drivers for supervisory interest in models. The first is the ECB's fieldwork for its Targeted Review of Internal Models, which will be substantially complete by the end of 2018, and as a result, some banks can expect to be asked to carry out remedial work. The second is forthcoming guidance from EIOPA on internal model convergence for insurers.

These things all point to the importance of model risk management frameworks—that is, the governance and oversight of the deployment of models, and the management of risks that arise from their use. We expect supervisors to scrutinize firms in this area; firms will need to demonstrate that they have identified all models generating material risk, and that they have a clear understanding of risks posed by their models, including those outside the scope of regulatory approval. Supervisors will be particularly interested in the information provided to boards and risk committees that lead them to their decisions over how and where to use models. ●

## Conclusion

We titled this year's Financial Markets Regulatory Outlook "bringing it all together." So what are some of the common threads in our analysis?

First, it is clear that the industry is under significant resource constraints, with numerous competing priorities. With business models under pressure, it can be difficult for regulated firms to do the bare minimum, let alone become the best in class.

Second, this is not helped by considerable uncertainty about the future regulatory environment. Irrespective of this, firms will have to act on several fronts in 2018.

Third, the ecosystem of financial services is clearly changing. The capital markets landscape is being changed by MiFID, but we are also seeing old and new players forge new connections, particularly through technology.

Fourth, these new technologies create opportunities, but also risks, particularly for firms whose business models may be challenged, and risks for consumers where the use of technology is not well understood or controlled.

Last, but not least, and on the subject of customers – their relationships with the financial services sector are changing. Firms are looking to use technology and data in new ways, but customers are also set to gain stronger rights over how their data is used.

All in all, the financial services industry faces a complex landscape as it enters into 2018.



Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018b](http://www.deloitte.com/lu/InsideRisk2018b)

Printed with permission of Deloitte UK, Germany



# The view from the industry

## Deloitte Banking Union Supervision Survey

**David Strachan**

Partner  
EMEA Centre for  
Regulatory Strategy  
Deloitte UK

**Hans Jürgen Walter**

Partner  
Banking Union Centre in  
Frankfurt  
Deloitte Germany

**Simon Brennan**

Director  
EMEA Centre for  
Regulatory Strategy  
Deloitte UK

**Thomas Grünwald**

Director  
Banking Union Centre in  
Frankfurt  
Deloitte Luxembourg

Deloitte's annual Banking Union Supervision Survey asks banks about their experiences of the Single Supervisory Mechanism (SSM) and the changing supervisory and regulatory landscape. The resulting insights enable banks to benchmark their strategies for responding to the SSM and understand best practice, and provide supervisors and policymakers with a clear industry perspective. [▶](#)

This year, the survey examined in particular how supervisory relationships have continued to evolve; the organizational impact on banks; and technical issues regarding supervisory activities and regulations, as borne out by the Supervisory Review and Evaluation Process (SREP) and on-site inspections (OSIs). The results of the survey highlight in part the continuation of trends observed last year, as supervisory processes have matured, and banks have refined their supervisory engagement strategies. At the same time much remains in development, not least because of the growing importance for banks of supervisory actions as the regulatory framework stabilizes.

This article sets out highlights from the survey and puts them in the context of broader developments—in particular, through the lens of the supervisory approach, business model analysis (BMA) and supervisory priorities for the year ahead—three topics that we keep coming back to in our conversations with clients.



For this second edition of Deloitte's Banking Union Supervision Survey, more than a third of banks directly supervised by the European Central Bank (ECB) participated. The survey was carried out between February and May 2017.



### Target banks

All directly supervised SSM banks within the Eurozone



### Participating banks

45 directly supervised out of 19 Eurozone, 13 countries



• Countries that participated in the survey



# Key messages from survey participants



## Impact

- Half of survey participants report that their supervisory spending has increased by more than 50 percent on average over the first two years of the SSM
- Supervisory priorities have driven targeted investment in operations across a number of areas, most prominently governance
- Data requests continue to be a particularly significant draw on resources and distraction for management
- Progress still needs to be made in establishing a level playing field



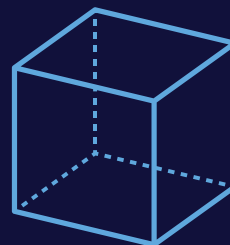
## Relationship

- More than 60 percent of survey participants are satisfied or very satisfied with their supervisory relationship
- Coordination on messaging and policy between supervisory teams is felt to need improvement, as are the clarity and timeliness of supervisory communications



## OSIs

- Most survey participants considered themselves to have been well-prepared for inspections
- From the perspective of survey participants, supervisors' planning, resourcing, and operations for OSIs could be improved
- The ECB's draft guide on OSIs and internal model investigations published after the survey was completed will help with this



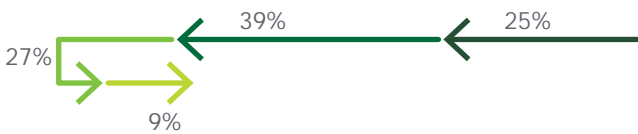
## SREP

- The continued low interest rate environment is by far the most significant factor affecting banks' business models. Focusing on profitable products and increasing cost efficiency are seen as the main drivers for restoring or increasing profitability
- Despite positive developments in supervisory relationships, survey participants think there is insufficient transparency about the results of the SREP, and significant uncertainty about supervisory BMA

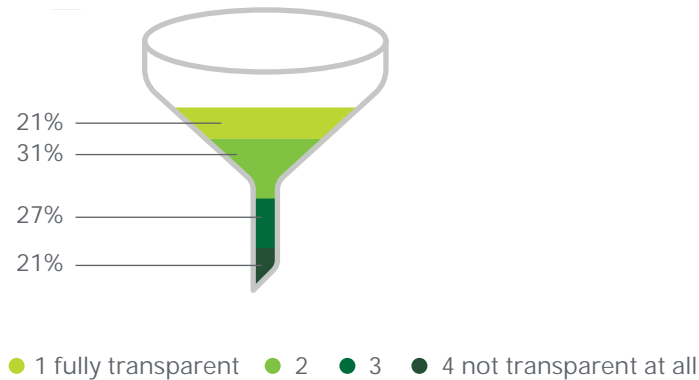
# Evolution of the supervisory approach

**During the 2016 SREP, conducted by the ECB, did you feel that there was sufficient transparency in terms of the methodology used and the results it produced?**

## Methodology



## Results



**Two years after the ECB took control as Eurozone banking supervisor, to what extent do you think that the level playing field has been achieved?**



Reflecting on the evolution of supervision in the SSM over the past year, it is tempting to conclude that not much has changed. Survey participants report that the supervisory approach continues to lack transparency and consistency. That is despite relationships with supervisors—a key communications channel—having stabilized. Banks wonder if the much-heralded level playing field will ever become a reality.

Much has changed though. The reality is that the SSM is faring better against higher industry expectations. The ECB has made significant strides in clarifying its expectations on key topics—through bilateral discussions between banks and Joint Supervisory Teams (JSTs), publications, and speeches—and supervisory processes have matured. Perhaps most notably, the ECB has made changes to how it implements the SREP, against the backdrop of a broader discussion about the process at the EU level. The split of the SREP capital requirement into a Pillar 2 Requirement and Pillar 2 Guidance is intended to improve comprehensibility. Further, the ECB has worked on its qualitative approach and is consulting on its multi-year plan on SSM guides on the Internal Capital Adequacy Assessment Process (ICAAP) and Internal Liquidity Adequacy Assessment Process (ILAAP),<sup>1</sup> which provides details of what the ECB expects from annual submissions.

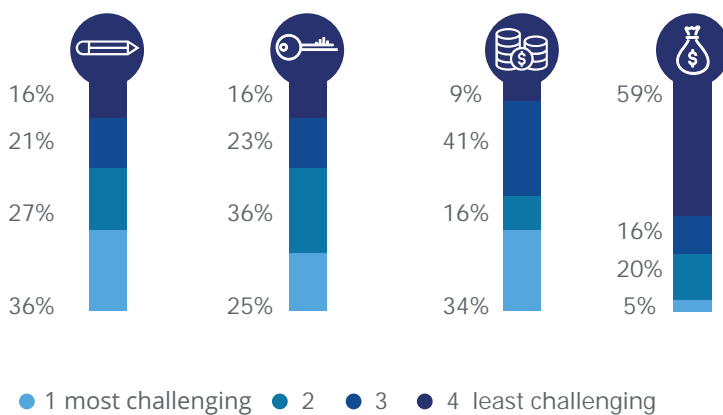
Of course, there remains more to do. Banks are hoping for greater clarity around supervisory methodology and also other topics such as stress testing and risk data. Only 9 percent of survey participants think that the SREP methodology is sufficiently transparent, while only 21 percent judge the SREP results to be sufficiently transparent. The relatively more favorable response on transparency of results may reflect improvements in disclosures in SREP letters, while aspects of the underlying process remain challenging to understand. The ECB is, however, ultimately likely to be reluctant to provide more insight into its

methodology, in order to not encourage banks to game the approach. However, unless banks fully understand why their capital requirements are being increased, their ability to remedy the supervisory concerns that gave rise to them will be limited.

In addition, while JSTs have stabilized and banks' meetings with them have become more frequent over the past year, banks perceive there to be some problematic differences between formal and informal communication. While banks can sometimes wait months for formal communication (e.g., the final results of OSIs or approval for model changes), informal communications can be much faster, but by definition less certain as the outcome can be changed as a result of the ECB's internal challenge process. Banks would value a more coordinated and tailored approach across the ECB, in particular between policy and supervision teams. ➔

While banks can sometimes wait months for formal communication, informal communications can be much faster.

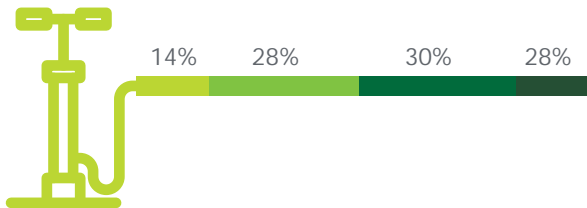
**Which pillar of the SREP assessment was most challenging for your organization in terms of effort and resources (staff and management)?**



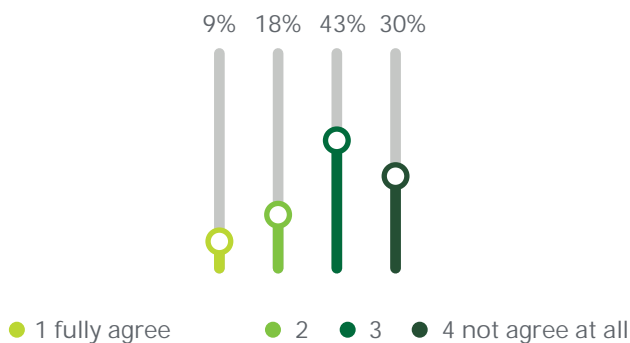
1. "Multi-year plan on SSM Guides on ICAAP and ILAAP," letter from Daniele Nouy, Chair of the Supervisory Board, ECB, February 2017, [https://www.bankingsupervision.europa.eu/ecb/pub/pdf/170220letter\\_nouy.en.pdf](https://www.bankingsupervision.europa.eu/ecb/pub/pdf/170220letter_nouy.en.pdf)

## Business model analysis

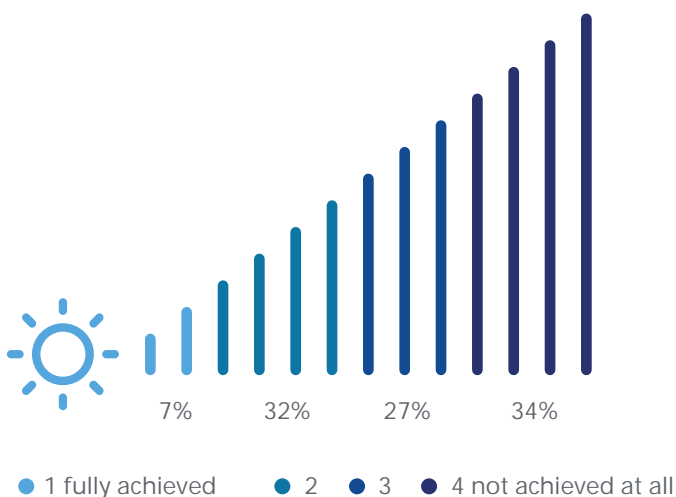
**Do you think that the SSM's supervisory activities are putting you under pressure to adapt your business model beyond changes that the board would make in any case?**



**To what extent do SSM requirements and requests play a role in driving adjustments to your business model?**



**Are SSM business model expectations communicated in a clear and understandable manner?**



Supervisory BMA has been a priority for the ECB since the beginning of the SSM. Three years on, we often hear about an increase in the intensity of supervisory scrutiny of business models and it is a topic currently mentioned regularly in speeches by the ECB Supervisory Board. Supervisors are exploring, in particular, banks' ability to generate their cost of capital, against the backdrop of protracted low/negative interest rates and disruption from new technologies, and the challenge of responding to the UK's withdrawal from the EU. There is a stated expectation that the Eurozone banking sector needs to consolidate,<sup>2</sup> although the mechanism for making this happen remains unclear.

That level of activity suggests banks should be very focused on understanding their business through the lens of supervisory BMA, in particular whether or not they are outliers in the quantitative horizontal analysis. However, any concern that supervisors will try to intervene and tell banks how to run their business is probably unfounded. In fact, the SSM approach has remained rather quantitative, and as a result banks are asking themselves if and when BMA will become more influential in the supervisory process. The majority of survey participants (61 percent) find expectations on BMA unclear or difficult to understand. Overall, banks do not report much pressure to change their business strategy or their approach to managing their business model in response to supervisory activities. Only 14 percent of survey participants are definitely planning such changes, while 28 percent are considering them. The perceived lack of potency of BMA as a "lever" for supervisors may be addressed, in particular as follow-up discussions with supervisors become more frequent.

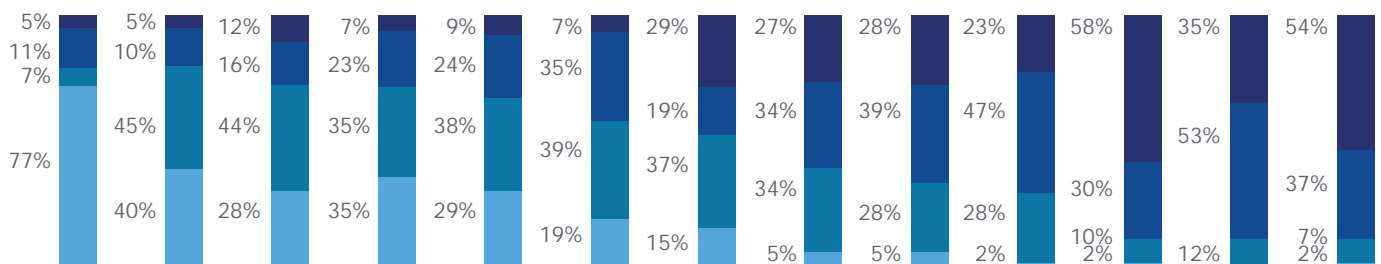
2. "Interview with Mannheimer Morgen", Sabine Lautenschläger, Member of the Executive Board and Vice-Chair of the Supervisory Board, ECB, July 2017, <https://www.bankingsupervision.europa.eu/press/interviews/date/2017/html/ssm.in170729.en.html>

That is not to say that banks are not themselves focused on challenges to their business model. The impact of the low interest rate environment is considered to be the key driver of any change to business models. Survey respondents, however, ranked both competition from outside the banking market and Brexit at the lower end, with only 2 percent considering each to have a significant impact on their business model. Meanwhile, 28 percent ranked new competition from outside the banking sector second and another 12 percent ranked new competition from the banking sector second. The fact that the perception—or prioritization—of issues appears to diverge between banks and supervisors reflects differing perspectives. That banks' and supervisors' perceptions differ so much when it comes to the priority topics may prove problematic and aligning these different perspectives may have to become a priority in its own right. ➔



The impact of the low interest rate environment is considered to be the key driver of any change to business models.

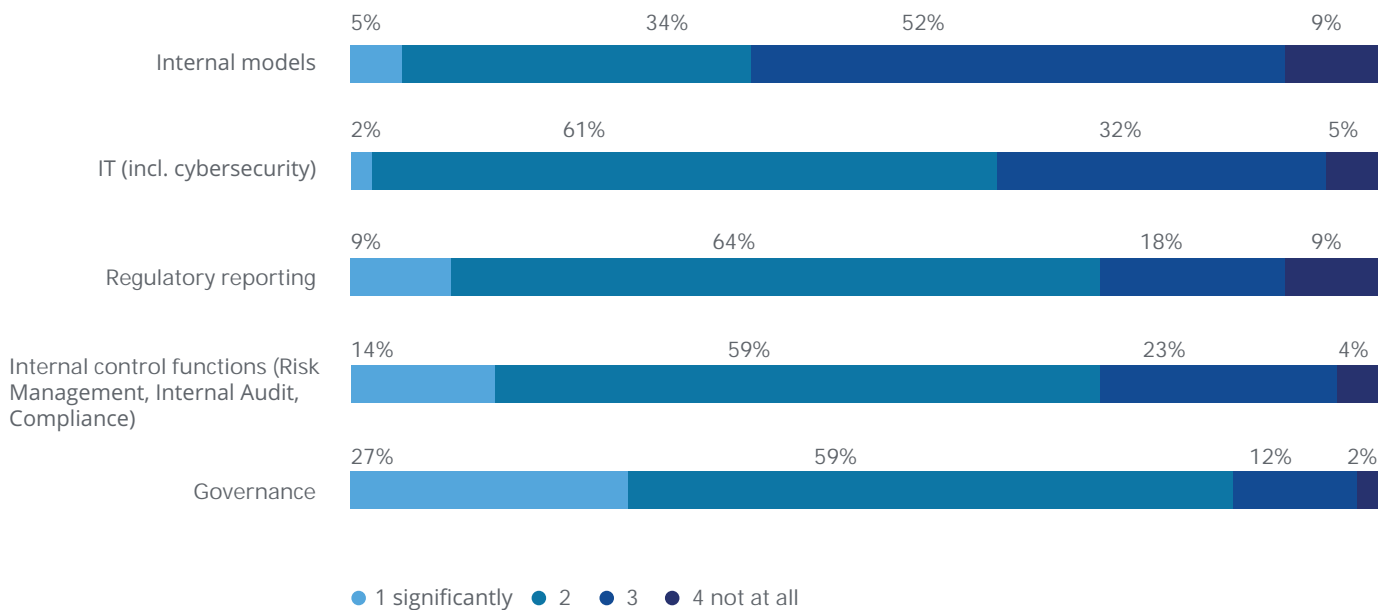
**To what extent do the following factors affect your business model?**



● 1 representing a significant impact on your business model ● 2 ● 3 ● 4 representing no impact at all

## Business model analysis

**To what extent do you think that your bank has improved/the operations of your bank have improved in the following areas over the last year?**



At the start of 2017, the ECB set out its supervisory priorities: business models and profitability drivers; credit risk, with a focus on non-performing loans (NPLs) and concentrations; and risk management. Survey participants report that they have made significant investments over the past year in operations aligned to areas of supervisory scrutiny. Most notable is the extent of investment in governance, which ranked second highest in terms of number of inspections as reported by the ECB in its latest annual report on the SSM. It also could be interpreted as a response to the ECB's thematic review on risk governance. Banks seem to be reactive rather than proactive in that sense. Given the amount of new regulation they have to implement, this is a pragmatic approach. The danger, though, that this will backfire some day in terms of banks falling short of supervisory expectations in a particular area remains.

Looking forward, these topics are likely to remain important, but the aspects that supervisors focus on will evolve. Most

importantly, work on business models will focus on Brexit preparedness. The ECB is closely monitoring planning by banks with operations in the UK, as well as banks relocating operations to the Eurozone. The ECB has to ensure that the banks it currently supervises have adequate plans in place to be able to continue operations without major disruption. For banks moving to the Eurozone, the ECB needs to handle more authorizations, and the number of banks to be supervised will increase. Given the attention on Brexit and the resources required, it remains to be seen how far the ECB will be able to pursue other efforts (even with its stated intention to increase resources). Brexit will stretch its resources and the ECB will potentially need to be more selective as to which initiatives to push forward, as well as reconsidering timelines.

The Targeted Review of Internal Models (TRIM) program has picked up and the in-depth on-site review cycle has started. The program is up and running for all risk types

in scope with the key objectives being to reduce the variability of risk-weighted assets (RWAs) stemming from internal models, to improve consistency across banks' methodologies, and to restore the credibility and adequacy of capital requirements. The work on NPLs, IFRS 9 implementation, and risk governance is also proceeding. Elsewhere in the banking union, the resolution cases during 2017 have provided important lessons for the SSM and Single Resolution Mechanism, and will drive changes to supervisory and resolution approaches over the coming months.

We also expect to see more work on topics such as cyber risk and outsourcing. Both have become more prominent on the EU supervisory agenda. ●



# Dealing with divergence

## How banks can build a strategic response to the uneven implementation of Basel standards



**David Strachan**

Partner  
EMEA Centre for  
Regulatory Strategy  
Deloitte UK



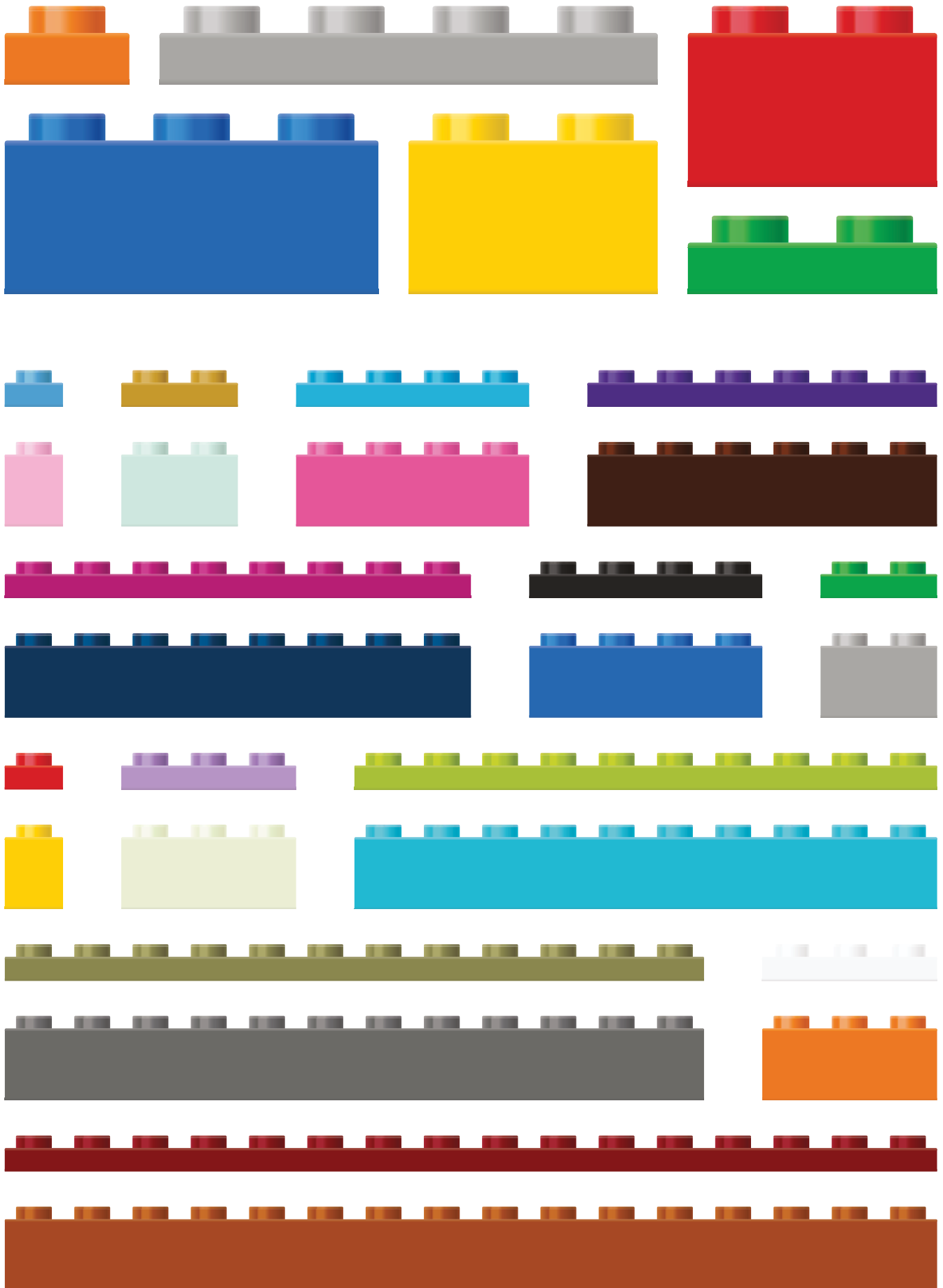
**Scott Martin**

Senior Manager  
EMEA Centre for  
Regulatory Strategy  
Deloitte UK

Since the Pittsburgh G20 Summit in September 2009, regulators around the world have been committed to strengthening capital, liquidity, and leverage standards for banks. The agenda is well-known; embedded within it has been an equally strong commitment to addressing the unevenness and complexity of the global capital framework for internationally active banks. Regulatory convergence initiatives such as Basel III were intended to pave the way for an increasingly consistent banking rulebook in most jurisdictions. This drive to increase regulatory convergence is now under pressure. Almost 10 years on from the onset of the financial crisis, and with governments keen to stimulate economic growth, there are signs of “regulatory fatigue” setting in, and several countries are questioning the need to adopt additional common global regulatory standards for the banking sector.

The European Union’s approach to Basel implementation in the last year has been instructive. Although in the past it has been prepared to amend international standards to reflect European specificities, the European Commission’s November 2016 proposed review of the Capital Requirements Directive and Regulation (CRD V/CRR II) demonstrated a growing willingness to depart from an implementation of global post-crisis banking rules either in full or on time. This was particularly evident from the proposed implementation of the Basel Committee on Banking Supervision’s (BCBS’s) Fundamental Review of the Trading Book and Net Stable Funding Ratio. The time it now takes for EU institutions to pass major banking legislation alone indicates that similar timing departures are in store for the implementation of Basel III’s remaining elements (often referred to as “Basel IV”). In short, the global regulatory landscape for banks looks set to become increasingly divergent and fragmented and the implementation of Basel III is becoming a prime example. ➔

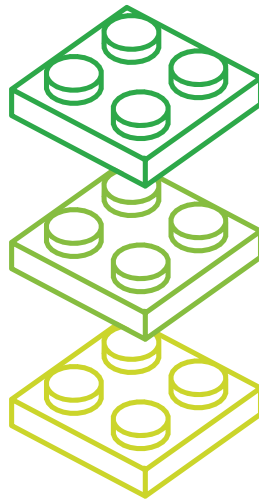




### Why internationally active banks should be concerned

Left unchecked, these developments will have very real implications for banks with substantial operations in multiple jurisdictions. Many regulators will hope that December's international-level agreement on Basel III will draw a line under the post-crisis regulatory agenda, but the inconsistencies arising from jurisdictions charting their own course in implementing it may substantially increase the complexity faced by regulatory and risk managers at these banks.

This added level of complexity will multiply the costs and challenges already associated with more manageable levels of regulatory change. This will, in turn, generate substantial pressure to increase headcount, will demand more cumbersome processes requiring more frequent manual intervention, and may complicate the understanding of the future state capital, liquidity, and risk environment. We believe this could significantly increase the risk of strategic paralysis for banks as they struggle to assess the cumulative impact of regulation on the profitability of their products and services and operate without a clear understanding of their costs and binding constraints. As a result, they will be less well-equipped to make the best business and resource allocation decisions. In our view, the challenges associated with regulatory divergence give rise to three types of questions, which the management and boards of internationally active banks should consider as a matter of urgency.



**Strategic:** Does divergence affect the sustainability of business models and the ability of managers to plan and make well-informed regulatory and business decisions?

**Operational:** To what extent an inconsistent Basel III implementation increase the complexity and costs of risk processes, and can bank governance structures, controls, and regulatory capabilities cope with this complexity?

**Technological:** How will divergence increase the pressure on banks' data management systems and do these challenges strengthen the case for making additional IT capability investments?

Almost 10 years on from the onset of the financial crisis, and with governments keen to stimulate economic growth, there are signs of "regulatory fatigue" setting in, and several countries are questioning the need to adopt additional common global regulatory standards for the banking sector.

### The blueprint for a strategic approach

These strategic, operational, and technological considerations, in our view, further justify the case for banks to make targeted investments now to enhance their risk management and regulatory strategy capabilities in order to operate more efficiently in an increasingly fragmented environment.

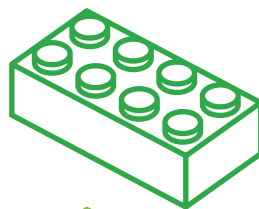
We call this developing a “divergence-resilient” approach to regulatory complexity, and we believe that the risk of a fragmented implementation of Basel III makes a greater business case for such an approach now more than ever.

Our view is that regulatory technology (RegTech), which is becoming increasingly available, can allow such a divergence-resilient approach to be designed flexibly enough to control for the uncertainty around Basel standards that can still be modified by national legislatures and regulators. As part of this, there are a number of capabilities that banks can develop or extend to support ongoing risk and regulation processes, most notably stress testing and capital planning.

For most banks, this will require a significant re-thinking or acceleration of changes to their regulatory operating models, which may nevertheless take years to fully implement. Such models, however, would not only help enhance the functionality of banks’ regulatory processes, but also transform the way that they integrate regulatory and commercial

considerations—what we see as the real crux of “regulatory strategy.” This will allow them to manage their risk and regulatory capital operations more centrally, embed the multiple demands they face into routine scenario planning, and produce more meaningful information on the costs of capital and liquidity to enable better business decisions.

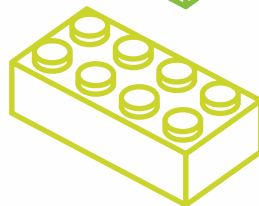
In order to support the development of regulatory strategy capabilities, the core elements of the divergence-resilient approach that we propose include:



Making targeted investments in **technology, data, and modelling** to allow risk and regulatory processes, such as capital calculations, to be conducted more quickly and cost-efficiently



Aligning **governance structures** and regulatory processes to support greater flexibility and functional integration; for instance, greater risk and finance alignment for capital planning and stress testing purposes has yielded strong dividends for many firms



Developing a new or enhancing an existing **central regulatory strategy group** with the mandate and analytical capabilities to assess the impact of Basel standards—both those in force and those forthcoming, and related divergence—on business strategy and profitability.



## A divergence-resilient approach to managing regulatory complexity

### Regulatory strategy capabilities

#### Central regulatory strategy group

A central function responsible for identifying the bank's current and future regulatory demands, interpreting the need for resources this will create, identifying and in some cases directing investments in technology, data, and governance needed to support the divergence-resilient approach and providing regulatory insights for business strategy planning.

#### Scenario-based analytical capabilities

Embeds an ongoing process of scenario analysis that provides a more granular understanding of the impact of forthcoming or probable regulatory developments. When mature, the use of data analytics can eventually provide a deal-by-deal view of the likely regulatory costs to the business and identify optimal strategies.

### Enhancing core functionality

#### Technology, data and modeling

Investing in technology, modeling and data remediation to enable capital and liquidity calculations and controls to be varied in a short period of time. Allows for the greater use of robotic automation to reduce the time and cost-intensity of regulatory processes.

#### Governance and operating model

Creating clear responsibilities, processes, and lines of communication to facilitate quicker and more flexible risk management capabilities. Includes executive-level sponsorship of the divergence-resilient approach and intervention, where needed.

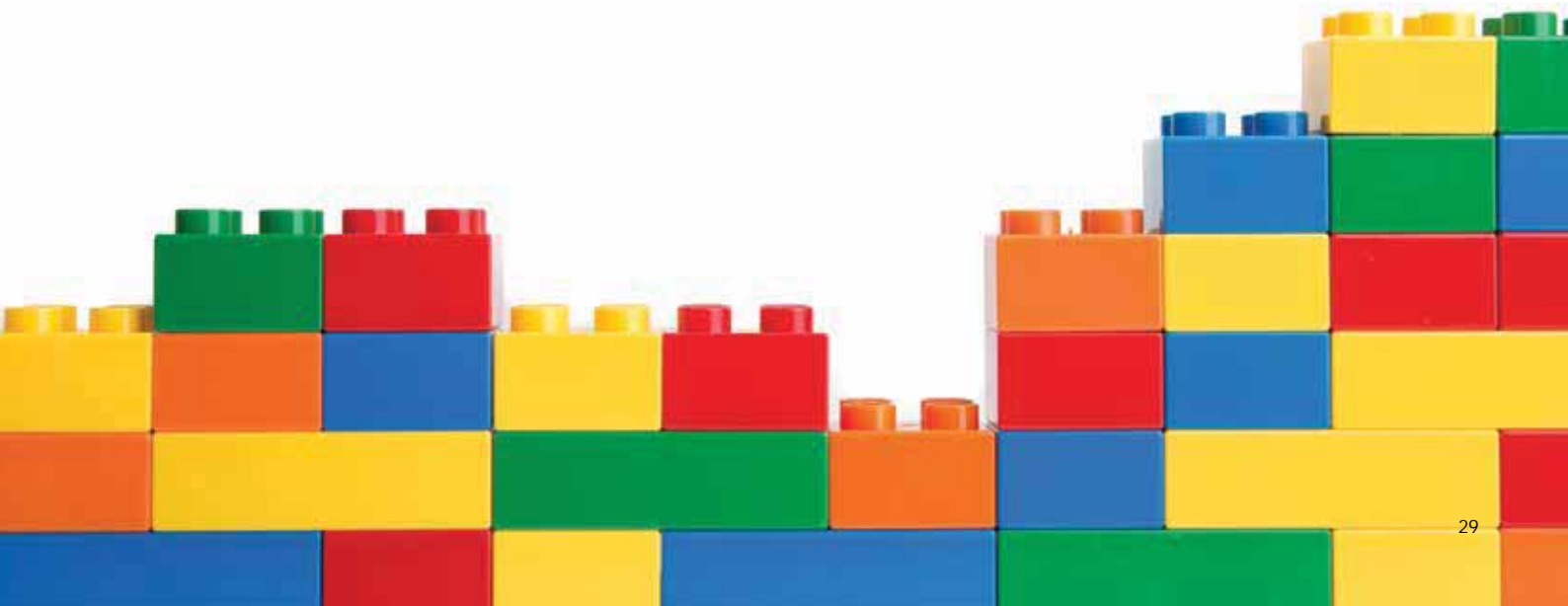
### Thinking further ahead

For most internationally active banks, maximizing profitability while also contending with multiple regulatory constraints on the allocation of capital is an increasingly challenging task. Combined with the never-ending imperative of reducing costs, the temptation to take a piecemeal or tactical approach to regulatory capital management, as opposed to an integrated and strategic one, is strong. However, given the trend toward regulatory divergence and the already foreseeable delays in the implementation of Basel III, we believe that a minimalist approach could set banks on a medium-to-long-term course toward incurring higher costs arising from an increasingly complex regulatory landscape.

Greater divergence in the eventual implementation of Basel III's final components also threatens to undermine the confidence that regulators and supervisors have in each other's efforts to manage risk in the banking sector. As a result, reduced trust between a bank's home and host supervisors could cause hosts to take further measures to ring-fence the capital and liquidity resources of banks in their jurisdictions. This has already been seen with the Intermediate Holding Company requirement in the United States and the EU's similar Intermediate Parent Undertaking proposal. These developments run the significant risk of creating even greater trapped pools of capital and liquidity than already exist in the global banking market.

Developing regulatory strategy capabilities to deal with this will be neither simple nor cheap. But regulatory spend to enable more efficient capital and liquidity management should not be viewed as a "deadweight cost" that adds little value to the broader business. It is clear that Basel III's requirements have emerged as some of the most decisive regulatory variables for a global bank's profitability since the financial crisis. The capabilities, flexibility, and foresight gained through a divergence-resilient approach to dealing with regulatory fragmentation can support commercial decision-making and ultimately contribute to the creation of a more sustainable business model. From this perspective, we consider that the case for such an approach, which generates a positive return on investment, is to be made. Looking ahead to the prospect of an increasingly uneven and unpredictable implementation of Basel III underlines this urgency. ●

For most internationally active banks, maximizing profitability while also contending with multiple regulatory constraints on the allocation of capital is an increasingly challenging task.

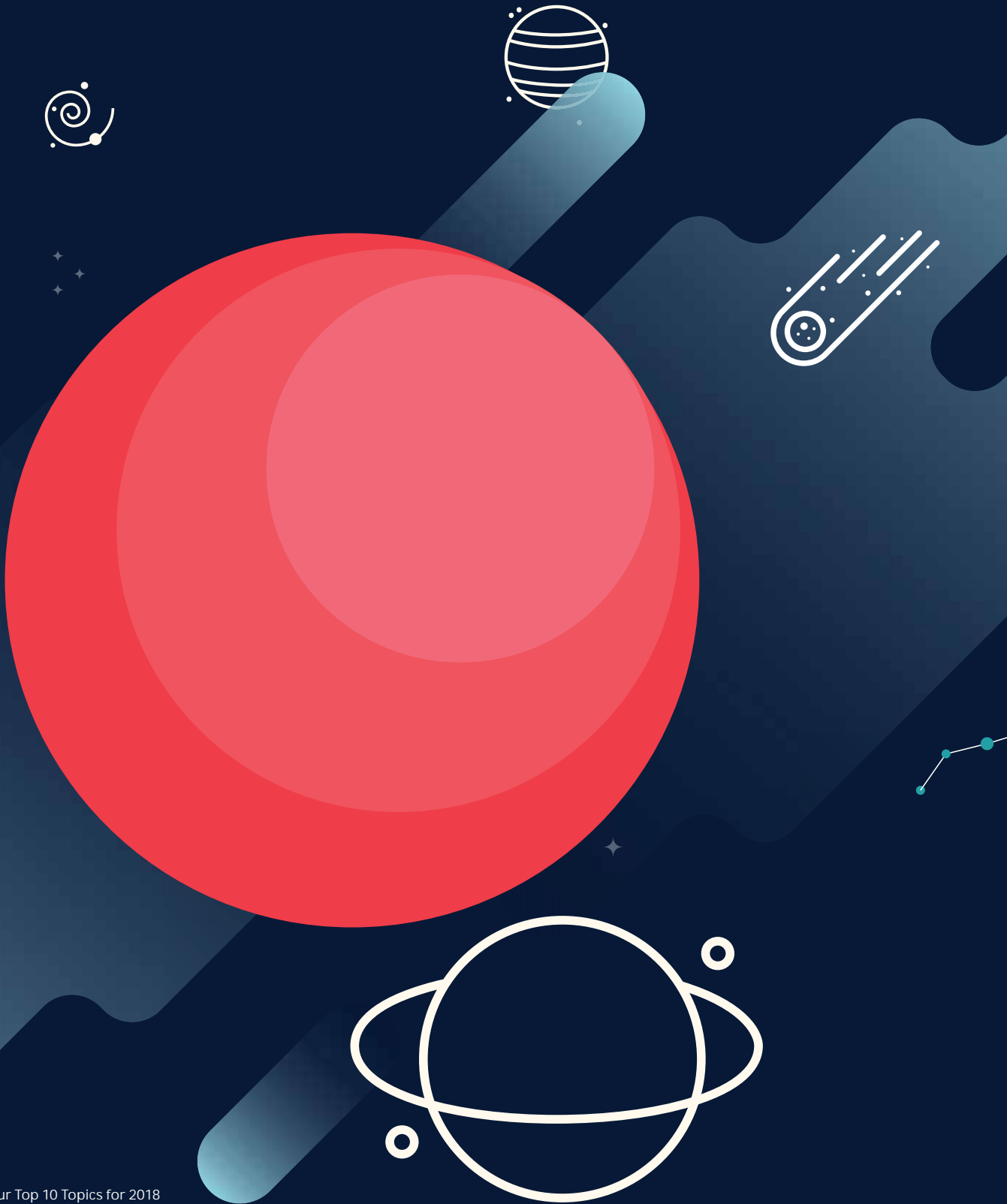




# Part 02

---

From a digital  
perspective ▶



Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018d](http://www.deloitte.com/lu/InsideRisk2018d)



# Using RegTech to transform compliance and risk from support functions into business differentiators

Technological innovations continuously emerge, offering new risk and compliance solutions to help financial firms to comply and manage their risks at lower cost.

**François-Kim Hugé**  
Partner  
Financial Industry  
Solutions  
Deloitte Luxembourg

The sheer volume and complexity of new and existing regulations have had the unintended consequence of encouraging financial service providers to focus on compliance rather than innovation. Regulations such as Packaged Retail and Insurance-based Investment Products (PRIIPs), the Payment Service Directive 2 (PSD2), the fifth Undertakings for Collective Investments in Transferable Securities Directive (UCITS V), the Markets in Financial Instruments Directive (MiFID), the fourth Anti Money Laundering Directive (AMLD IV), the Capital Requirements Directive and Capital Requirements Regulation (CRD and CRR), the European Market Infrastructure Regulation (EMIR), and the second Market Abuse Directive (MAD II) are just a few examples of the systemic shift in terms of compliance and risk, capital and liquidity requirements, and governance and supervision with which all investment management actors must comply.

In parallel, firms have been cautious to innovate due to the regulatory uncertainties underlying the development of new products and the deployment of pioneering technology. However, in the context of the ongoing digitalization of our day-to-day life and the consequential redefinition of the way we live and work being driven by technology, the last years have witnessed the emergence of promising and innovative companies targeting the regulatory environment to support efficient compliance management from an IT perspective—the so-called RegTech companies (RegTechs). Put simply, RegTechs offer solutions that use technology to solve compliance and regulatory issues. ▶



Regulatory pressures require fast implementation, which often conflicts with financial firms' development and transformation calendars.

**Financial firms must embrace innovative solutions to face the heightened risk and compliance challenges**

Diving a little more into the regulatory requirements, financial institutions are currently managing ever-changing regulations while being increasingly exposed to complex multi-jurisdictional facets. In practice, regulators now demand much more transparency—meaning an increasing amount of data needs to be produced by financial institutions to improve their vision of systemic risk and the behavior of different agents involved in the financial ecosystem. To gather, analyze, and compute all the required data, institutions make use of a variety of technology systems, but the truth is that much of this work still heavily relies on manual processes and interventions. It goes without saying that these processes are the main cost drivers for firms. As such, the greater demand for transparency and rigor has brought the role of technology to the forefront, leading companies to simply ask themselves the following question: how should a financial institution address compliance in a more efficient and less resource-consuming manner while improving the quality of the data reported to regulatory supervisory authorities?

Historically, financial institutions have had the choice of using large, well-known vendor systems or building an in-house solution. In selecting and implementing such technologies, different challenges arise. Firstly, the chosen solution must fit into the often complex and heterogeneous internal architectural IT environment of the company. Secondly, reporting and visualization tools are typically used on a very local level within different departments, and not always governed centrally. Finally, regulatory pressures require fast implementation, which often conflicts with financial firms' development and transformation calendars, thereby creating additional operational challenges.

Once the technology has been selected, development and configuration needs to be done in a proprietary language while adapting the solution to dovetail into an already complex existing IT architecture, which in turn leads, among others, to high lead times. Add in high price tags and it is clear that an agile alternative is required.



## Main technology supporting RegTech solutions



### Cloud computing

Cloud, open platforms and networks for sharing data, format standards, and common processes.



### Blockchain

Technology allowing the creation and verification of transactions on a network instantaneously without a central authority. Used to track and speed up the transaction life cycle and cut costs while lowering the risk of fraud.



### Application program interface

Software solution that allows off-the-shelf RegTech tools to interact directly with regulatory reporting systems.



### Machine learning

Technology that learns from data and allows automatic reassessment and refinement of processes in reaction to input from users.



### Big Data

Real-time processing tools/ techniques of Big Data to create value out of the massive amount of available heterogeneous and textual data.



### Data mining and analytics

Use of machine learning and behavioral analysis that offers the potential of powerful data mining and simulation techniques for enhanced decision making and artificial intelligence.



### Predictive analysis

Solution that looks to identify patterns of activity, such as unusual use of communications, non-routine patterns of leaving the office, non-completion of training, or missing mandatory leave, which may flag potential conduct concerns.



### Smart contracts

Computer programs to enforce the negotiation or performance of a contract. Smart contracts aim to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting through automation.



### Visualization solutions

New technical solutions for a user-friendly data presentation to make sense of and to speed up the understanding of complex, heterogeneous, and abundant data.

Technological innovations continuously emerge, offering new risk and compliance solutions to help financial firms to comply and manage their risks at lower cost. Stepping out from the shadows into the light, regulatory technology (RegTech) solutions present themselves as being able to tackle several of the aforementioned issues by providing agility, speed, and data-driven outputs. These attributes are enabled through multiple emerging technologies. Generally, such solutions tend to be cloud-based, meaning that data is remotely maintained, managed and backed up. This provides enhanced flexibility through the ability to customize control over not only the access to but also the sharing of the data. In addition, simplified addition and removal of service features provides for enhanced performance and scalability while end-to-end data encryption provides the necessary security. Cost-wise, the cloud is especially interesting as it provides the ability to offer pay-as-you-go pricing.

Besides cloud features, a variety of RegTech solutions have advanced analytical and machine learning/artificial intelligence capabilities. Evidently, data is meaningless unless it is organized in a way that enables people to understand it, analyze it and ultimately make decisions and act upon them. As such, analytics is beginning to help the industry rapidly and automatically understand not just the explicit meaning of the regulation but also the implicit meaning or "nuance" that is so often the greatest challenge to digest and assess. Advanced analytics and assessment techniques can start to "learn" and support by accelerating the review of new and emerging regulation based on what has been seen previously and how that has been interpreted in the same way that neural networks have helped predict fraud or customer behavior. Intertwined with analytics is the use of artificial intelligence. This technology combined with in-depth learning capabilities may be used as a continuous monitoring capacity, providing close to

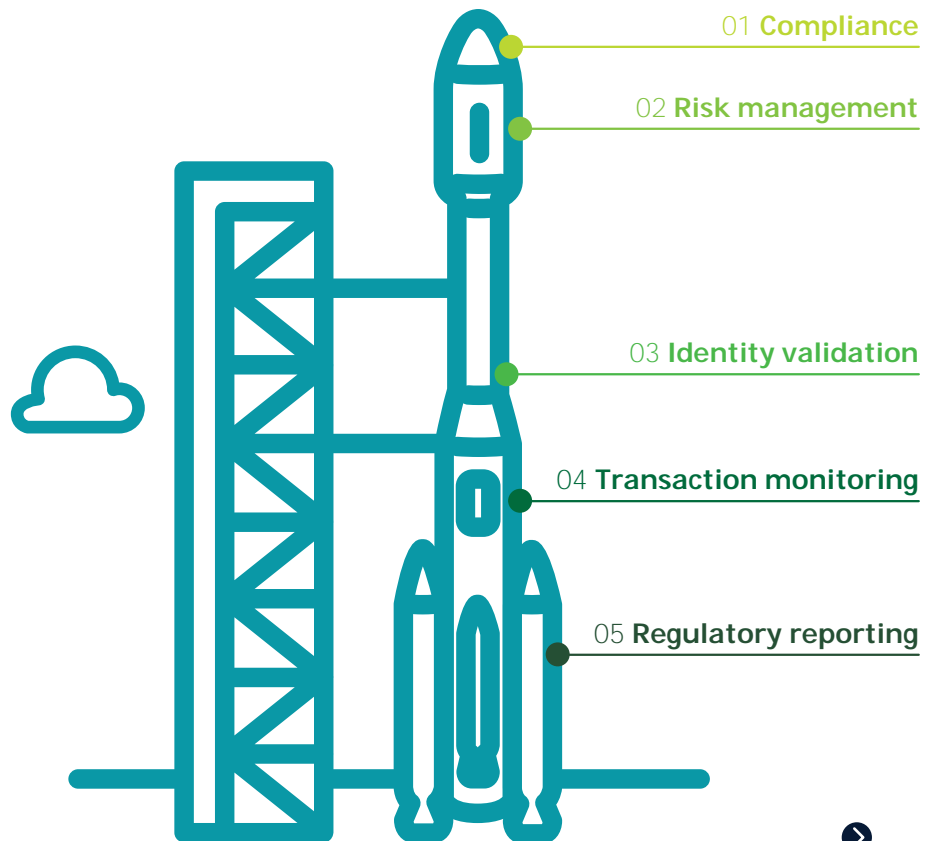
real-time insights into the functioning of global markets, and identifying problems in advance rather than simply taking action after the fact.

Lastly, some RegTech solutions use Blockchain – a record or ledger, of digital events distributed between many different parties that collectively guarantee the scalability and integrity of the said ledger. It can only be updated by a majority consensus of the participants in the system. Once entered, the information can never be erased, only amended. Blockchain contain different types of information such as transactions but also smart contracts. Through the Blockchain's near real-time settlement capability achieved through automation and global consensus, RegTech solutions can automate compliance aspects in cases such as identity management and transaction processing, settlement, and reporting.

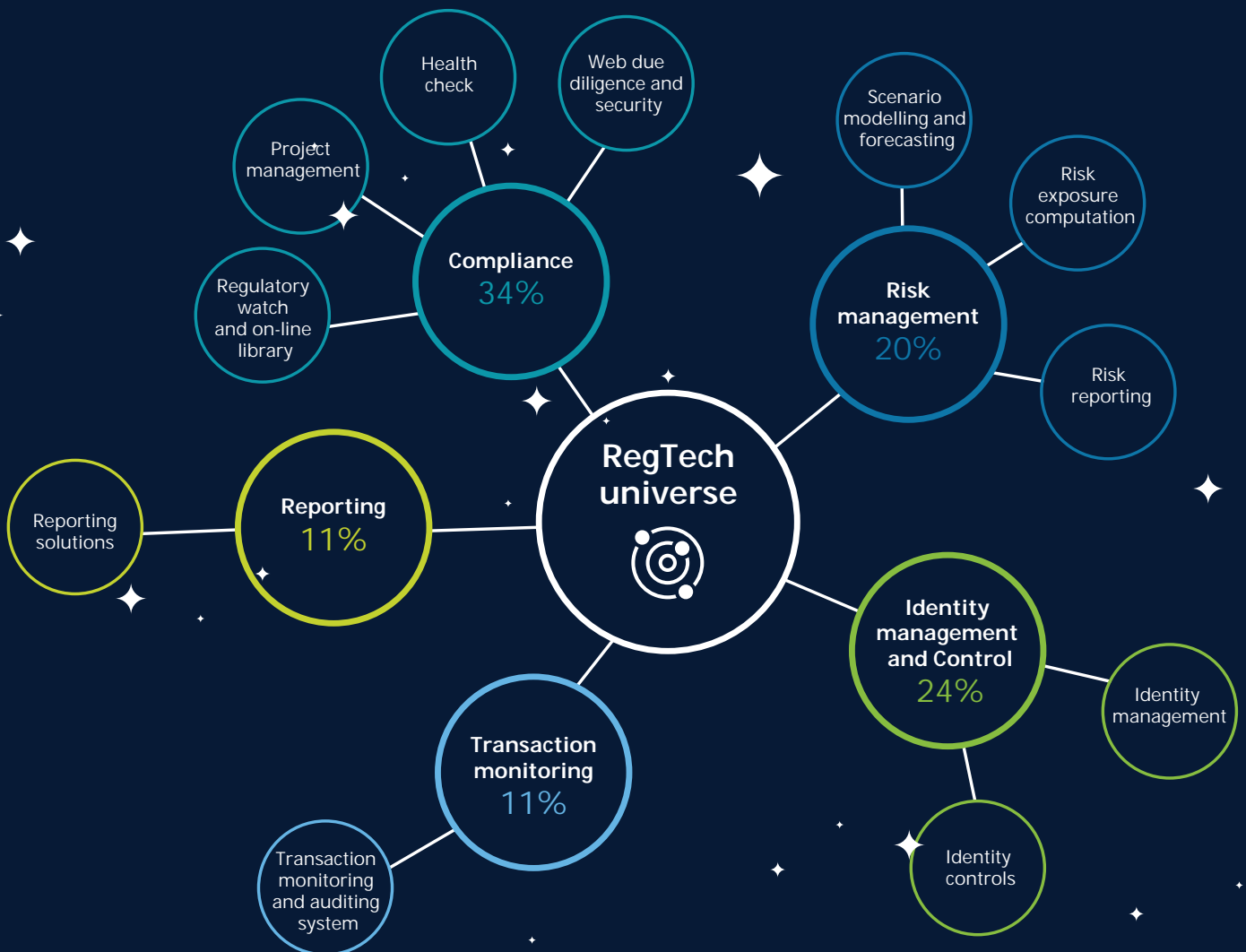
### What to expect from RegTech

Activities and processes covered by RegTech solutions are much broader than regulatory reporting and present themselves in many forms. Yet, they all have one thing in common: the targeting of a very specific niche.

Deloitte has mapped more than 200 RegTech companies offering various solutions that we have attributed to five main categories, these being:



## From business needs to RegTech features



Each category encapsulates various subgroups. For instance, "identity validation" encompasses both identity management and various controls, whereby tools target customer or counterparty onboarding. Based on biometrics and access to a multitude of information databases at the same time, Know-Your-Customer (KYC) processes can be facilitated. Identity controls form a key ongoing part of the relationship with a client and may include Anti-Money Laundering checks based on big data reports. In risk management, several tools provide scenario modelling and forecasting for regulatory requirements such as stress testing by computing future data and allowing automatic reassessment and refinement of processes in reaction to input from users.

The essential role of regulators for supporting innovations While we anticipate a very strong interest by financial firms in RegTech solutions due to the resultant competitive advantage, the adoption of RegTech solutions is currently slow due to a variety of underlying challenges. As such, the legitimization of these innovative products by enforcement authorities and regulators is a key driver to stimulate their adoption.

As the RegTech space is in its infancy and is developing rapidly, it is difficult for financial firms to identify and commit to a particular technology or solution. In addition, several constraints remain, such as those related to the sharing, storing, processing of, and access to data. A general wariness of banks and other financial actors to implement.

RegTech solutions mainly originates from the need for enforcement authorities and supervisors to approve the use of such innovative products and services as well as apprehensions resulting from such solutions being as yet unproven. For instance, as the financial ecosystem moves toward increased data utilization, the relevant regulatory framework to perform analyses through the use of advanced algorithms will need to be assessed.

Indeed, how data will be handled in terms of ownership, analysis, maintenance, and security will be a non-negligible aspect of the evolution of RegTech.

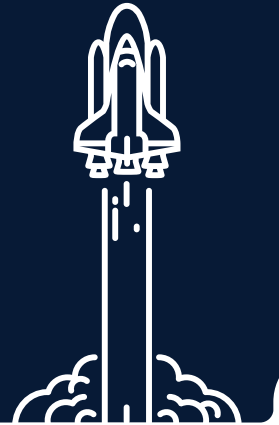
Recently, a progressive approach has been adopted by regulators such as the Financial Conduct Authority in the UK (FCA), the Monetary Authority of Singapore (MAS) and the Australian Securities and Investments Commission (ASIC). Being the first worldwide to offer a "regulatory sandbox," the FCA aims at providing a safe place where businesses can test new services and business models in a live environment alongside the regulators who are tasked with assisting these innovators. The FCA has established a framework of application as well as relevant safeguards for the operation of its sandbox. The FCA's stated market objectives for the sandbox are to reduce time to market at a potentially lower cost, provide better access to finance, and foster more innovative products reaching the market. Essentially, for the RegTech ecosystem to grow, the need for collaboration is required from key industry stakeholders.

Currently, RegTech solutions are in the process of understanding business and regulatory engagements to allow them to align their solutions with current regulatory frameworks, while some financial institutions are working on the development of their RegTech strategy and roadmap. On the educational front, we see professional services firms which can, in the future, become a dynamic center of the ecosystem through their wide-ranging relationships and business understanding across industries, start-ups and—rather critically— regulators.



As such, regulators play a contributory role in fostering innovation, create common integrated standards and proactively drive efficiencies in the RegTech ecosystem. With such development and further innovation in the RegTech space, both regulators and financial institutions would be able to monitor and analyze real-time financial information from all parts of the global financial services sector thereby facilitating a more efficient and safer financial system. The FCA is one of the regulators spearheading innovative initiatives, e.g., through their regulatory sandbox, which provides a unique opportunity to pilot this novel kind of regulatory architecture and eventually make it viable. Looking ahead, the challenges for regulators on a global level will be to conceptualize and assist the industry in implementing the far-reaching possibilities of RegTech to further develop the ecosystem into a foundational base underpinning the financial services sector.

Currently, RegTech solutions are in the process of understanding business and regulatory engagements to allow them to align their solutions with current regulatory frameworks.



## IN SUMMARY: MANAGING REGULATORY RISKS HAS RISEN TO BECOME AN ESSENTIAL BUSINESS MANAGEMENT PRACTICE

RegTech can no longer be labelled as a buzzword as it is most certainly reality now. On the one hand, there is a need from financial institutions to drive compliance programs with greater efficiency, while on the other hand, new technologies foster the creation of innovative solutions.

The importance of regulatory risk management, always a critical challenge for the financial industry, has reached new levels of importance in the aftermath of the financial crisis. Financial stability is the new motto, and deficiencies identified in regulatory compliance gave rise to enhanced frameworks, obligations, and risks. 492 percent is the rate by which regulatory change volume has increased between 2008 and 2015.<sup>3</sup> Across the world, a variety of financial blue chip companies have been subject to heavy fines and penalties for failing to be compliant. According to Reuters, 20 of the world's biggest banks have paid out more than US\$235bn (£151.71bn) in fines and compensation between 2008 and 2015 for breaching various financial regulations.

To put this number in perspective, it is roughly equivalent to the current gross national product of Ireland. The preventive steps taken by many firms encompass shifting resources to mitigate regulatory risks, i.e. allocating of up to 15 percent of their workforce to governance, risk management and compliance departments and spending an extra €1 billion on controls in 2013 alone.

The fact is that there is no sign of this trend slowing down; the financial industry must live with the fact that regulation will continue to expand and deepen. A consequence is the changing focus of the classic business model, which now needs to integrate regulatory risk management as a key enabling business practice together with product profitability and meeting customer needs. In this context, RegTech solutions will certainly be instrumental in helping investment firms to cope with such change. ●



# Blended learning

Combining digital and classroom training to achieve maximum results

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

**Paul Schilling**  
Director  
Operations Excellence  
& Human Capital  
Deloitte Luxembourg

**François Bade**  
Senior Manager  
Strategy Regulatory &  
Corporate Finance  
Deloitte Luxembourg

**Sonia Ben Abdelhafidh**  
Manager  
Deloitte Learning Solutions  
Deloitte Luxembourg





Our professional environment is in constant evolution: the market is becoming increasingly regulated, employees' focus areas change rapidly, and it is essential to both gain knowledge and understand how to apply it in practice. In the midst of this stands the individual employee—an individual who needs to understand what changes the second Markets in Financial Instruments Directive (MiFID II) entails for her and her clients; an individual who needs to understand how the new General Data Protection Regulation (GDPR) will affect him; an individual who constantly needs to learn new things to remain up-to-date on all emerging regulatory changes.

Besides these mandatory knowledge requirements, companies are increasingly training in "softer" areas: raising awareness around a cultural shift, boosting the use of feedback, or helping their employees understand how to fight against cyber-attacks in the workplace. Given the complexity of many of these topics, dedicated tailored programs are becoming increasingly common. The plethora of planned training programs may frighten certain employees, but it is key to their continuous professional development. ➤



Employers, on the other hand, are generally looking at these challenges from a much more pragmatic and often economically driven perspective; they understand that the company needs to be compliant on some of the above-mentioned topics and they may define a number of other areas that they consider strategic for their own development or for that of their staff. The corporate learning department—often working closely with the corporate compliance team—then seeks the most effective and efficient way to skill up the company's workforce.

At this juncture, the company must adopt an approach to professional training and development that ensures the maximum possible response to the outlined needs, while also being reasonable in terms of cost—two criteria that may seem inherently contradictory at first glance. If we consider the evolution of the classroom training market over the past few years—both in Luxembourg and abroad—it is clear that these conflicting forces have shaped two major clusters of players.

At one end of the spectrum, we find a large set of Learning Solution Providers operating in the reasonable-to-low price segment, offering fair learning services to the local market. Standard content is used, developed once, and redeployed to be delivered to the broadest possible audience. Trainers or facilitators are often limited in their knowledge to what they have in their script. Such programs generally contain the standard theory and give examples on how it is applied in a general context. In order to make this a viable business, these Learning Solution Providers often cover a broad range of topics, but have a limited depth of knowledge of each topic.

At the other end of the spectrum, we find Learning Solution Providers with extremely extensive expertise on the topics they teach, generally delivering programs across regions, or even globally. They often cover a limited number of topics in detail but are able to elaborate on these topics way beyond their scripts, building on a true understanding of the field. They can

elaborate on specific situations and needs raised during their training sessions. They view themselves as facilitators instead of mere training providers, and see their role as facilitating a proper adult learning experience where training participants discover and internalize the knowledge themselves and understand how to apply it afterwards. While this option certainly sounds appealing, it obviously comes with a very different price tag—training programs of this kind often cost up to eight times the price of entry-level training programs.

Over the years, these two types of player have carved a niche for themselves in this market and succeeded in co-existing with their respective client bases—indicating that neither model is better or worse in terms of the perceived price/return ratio. Alongside the outlined classroom learning offering, digital learning has established itself and evolved over the past decade. In terms of meeting demand for affordable staff training, this has proven to be a viable option when training large numbers of people on standard topics. At a time when most training on business topics involved PowerPoint, it seemed obvious to use content slides and deliver them through a Learning Management System to the employee. While this proved to be a highly cost-effective way of training employees, academic rigor was somewhat lacking. In many cases, the interaction between the learner and the system was rather limited, and employees tried to finish the mandatory electronic lessons as quickly as possible by clicking through the content rather than focusing on developing their knowledge. Whereas Learning Solution Providers in the high-end segment were affected relatively little by this new way of training, eLearning put additional pressure on the low-price segment as it suddenly started to be seen as a replacement for face-to-face training sessions.

In this context, today's employers are confronted with the challenge of finding the best possible learning and development solution—tapping into both the different types of classroom and digital training offerings—yielding the highest possible impact for both the company

and the employees while being cost effective. It is a tough challenge, but it is not insurmountable if varying training needs are properly understood.

To that end, training needs can be split into three broad categories:

- Standard knowledge and theory
- Mastery of technical skills and their application in day-to-day work
- Attitudinal and behavioral traits

These different categories of need can be met by the various learning solutions as follows.

Standard knowledge and theory do not necessarily require high-end classroom training. This type of knowledge can easily be taught through adequately designed reading materials or in a more engaging way in eLearning modules. Rather than spending precious classroom time to train people on what they could learn by themselves, eLearning modules are likely to be the solution with the highest impact at the lowest cost if conceived with the right expertise. Unlike early eLearning programs that were a mere compilation of content on a specific topic, high-end eLearning modules are now conceived by experts in both the topic and industry as well as in learning design. Only in this way it is possible to ensure the highest possible quality of the content while ensuring an engaging learning experience. ➔

The plethora of planned training programs may frighten certain employees, but it is key to their continuous professional development.



When it comes to the mastery of technical skills, it is clear that eLearning alone is not the best solution. Company-specific examples should be used to make the lesson more memorable, while guided exercises help learners to not only understand the content but also internalize it and develop an ability to apply it. For such topics, companies do not necessarily need to call upon high-cost training facilitators; nonetheless, they should make sure that the Learning Solution Provider is adequately equipped to tailor the classroom experience to the context and needs of the organization.

For training people on their attitudes and behavior, it is not only essential that this is done in a classroom setting, but also that it is facilitated by trainers who have extensive expertise on the topic and are properly trained on facilitating such learning experiences. Regardless of whether you are trying to improve your employees' practical sales skills or whether you would like to support them in better coaching and developing their teams, this type of message only has the expected impact if delivered properly. Saving on training costs by choosing an inadequate training delivery format or facilitator might actually create more frustration than benefit. For example, a sales expert might have a hard time completing an eLearning module on generic sales best practices in which she believes she is already an expert, not learning much and rushing through the three-hour eLearning pain, whereas she could have considerably benefited from a thoughtful exchange among experts in a classroom session.

Pinpointing the blended learning approach that best suits your needs may seem like a daunting challenge, but smartly combining digital learning with professional classroom solutions yields enormous value for the evolution of an organization. Taking the basic knowledge and theory out of the classroom and providing employees with the opportunity to learn these things

## Saving on training costs by choosing an inadequate training delivery format or facilitator might actually create more frustration than benefit.

through highly informative eLearning modules saves both time and money. Ensuring that field and topic expertise is combined with in-depth knowledge of learning design leads to learners staying highly engaged throughout the eLearning program and makes sure that the content is in line with the latest market trends and regulations.

Where eLearning is not the best choice—for instance if technical skills or changes in attitudes and behaviors are necessary—the learner should be taken into the classroom. Building on David A. Kolb's adult learning cycle, classroom sessions should be designed to encourage the learner to experiment with the knowledge in real-world examples and role plays, reflecting on the experience and planning how to use the knowledge going forward. And ideally this training should build on earlier eLearning programs to ensure continuity in the employee's learning experience.

In the end, there is no one-size-fits-all response to the challenge of training your staff. It remains essential, however, for each organization to properly understand the different contexts and topics on which it wishes to train staff, and to select the most suitable training delivery mode available in order to maximize return on investment. After all, this is all about an investment in one of the most important assets you have in your organization: your people. ●

Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018f](http://www.deloitte.com/lu/InsideRisk2018f)

Printed with permission of Deloitte Canada

# H O P E is not a strategy

Confronting tomorrow's  
cyber threats

# T O D A Y

**Nick Galletto**

Partner  
Research Leader  
Global and Canadian  
Cyber Risk Leader  
Deloitte Canada

Digital disruption and exponential technologies are creating unprecedented business opportunities, but they also bring risks. Having a strong cyber risk management plan in place can give your organization a competitive advantage and enable it to use cyber risk to power performance. >

In the World Economic Forum's The Global Risks Report 2017, cyber risk is recognized as one of the most significant sources of commercial risk, alongside the economy, the environment, and geopolitics.<sup>1</sup> The risks from cyber continue to skyrocket; according to a recent report, by the year 2020 the world will need to cyber-defend 50 times more data than it does today.<sup>2</sup> With new risks emerging daily, organizations must constantly devise new cyber strategies and defenses, and become more resilient as attackers figure out how to get past the cybersecurity that is currently in place.

The good news is that while digital disruption and cybersecurity present serious challenges, those challenges are not insurmountable. To protect themselves from both evolving and emerging cyber threats, organizations need to ensure they have established basic cyber capabilities that can repel today's threats, while at the same time investing in future-proof capabilities that can protect them and enable them to effectively respond to any threats that might emerge in the future.



### Digital innovation: a double-edged sword

In this new digital world, one of biggest threats facing organizations today, and for the future, is cyber risk. "We always refer to it as the duality of technology," says Nick Galletto, a partner at Deloitte and the Global and Canadian Cyber Risk practice leader. "The same technology that is used to create for good can, in the wrong hands, be used to mount cyber-attacks."



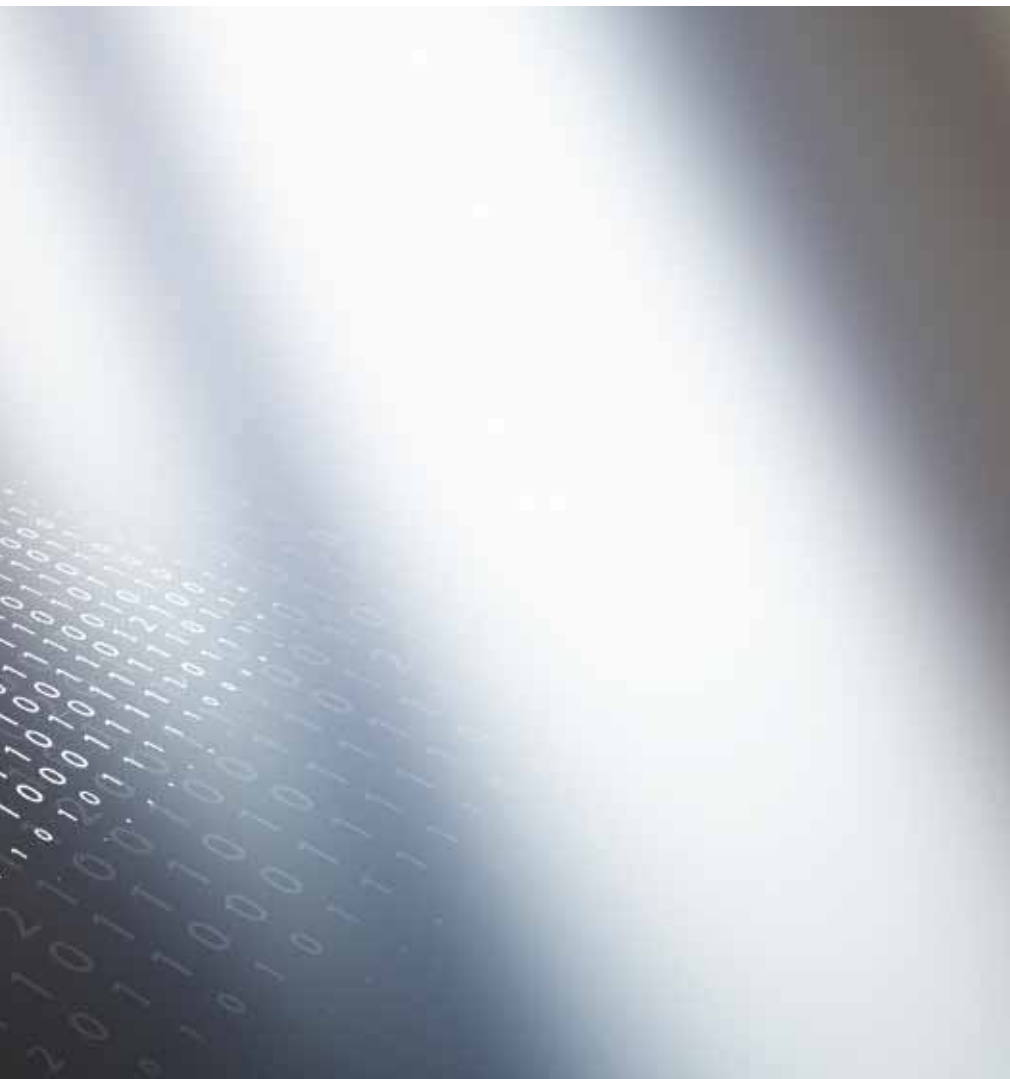
### More than an IT issue

Cybersecurity is no longer just an IT issue; it is a business issue and strategic imperative for organizations of all industries and sizes. Innovators in every sector must take the lead by constantly striving to strike a balance between protecting the organization from cyber threats and laying the groundwork for future success by capitalizing on digital technology. That is why taking the lead on cyber capabilities means doing more than addressing the threats that exist now.

1. World Economic Forum, "The Global Risks Report 2017", 12th Edition, [http://www3.weforum.org/docs/GRR17\\_Report\\_web.pdf](http://www3.weforum.org/docs/GRR17_Report_web.pdf) Accessed 9 May 2017.

2. Cybersecurity Ventures, "Cybersecurity Market Report," 2016 edition <http://cybersecurityventures.com/cybersecurity-market-report/> Accessed 9 May 2017.






The good news is that while digital disruption and cybersecurity present serious challenges, those challenges are not insurmountable.



### Prepare for tomorrow's threats today

As new technologies drive digital disruption, they introduce entirely new kinds of cyber threats and amplify existing ones—requiring additional next-level capabilities that companies must start building now.

Even threats an organization thinks it has under control today could threaten it again in the future as those threats evolve and grow in sophistication and complexity. For example, distributed denial of service attacks have been around for many years, yet they are now more prevalent, deceptive, and sophisticated than ever—often being used as a ploy to divert attention from secondary attacks such as data exfiltration, physical attacks, or the implanting of ransomware.

“Organizations are realizing that no one is immune to a cyber-attack, and in response to the increase in large and well-publicized attacks across a number of sectors, there is a greater sense of organizations now starting to better appreciate what the risks are and putting the appropriate measures in place to be better prepared,” says Galletto. “We’re definitely trending in the right direction.” 

Suppliers, vendors, partners, and even customers can all be points of entry for an attack—which means that even if an organization itself is highly secure, it could still be vulnerable.



#### Protect your crown jewels

Although a comprehensive cyber strategy that provides full protection for everything within an organization might sound appealing in theory, in practice it is simply not feasible. Cyber threats are infinite, but cybersecurity budgets and resources are finite. That is why it is essential to set priorities, with your "crown jewels" at the top. These include:

- People: key individuals that might be targeted
- Assets: systems and other assets that are crucial to your business and operations
- Processes: critical business processes that could be disrupted or exploited
- Information: data, information, or intelligence that could be used for fraudulent, illegal, or competitive purposes

Organizations that do not explicitly design their strategies around these crown jewels often end up allocating their resources haphazardly, investing too much in areas that are not very important while investing less in what matters most, leaving those areas dangerously vulnerable.



### Mind your ecosystem

Suppliers, vendors, partners, and even customers can all be points of entry for an attack—which means that even if an organization itself is highly secure, it could still be vulnerable. After all, a chain is only as strong as its weakest link. To stay aware, conduct ongoing cybersecurity assessments of your ecosystem to ensure outsiders are not creating unacceptable risk exposure. Also, be part of the solution, sharing information with ecosystem partners and fostering collaboration to fight common adversaries.



### Pay attention to the enemy within

Although external attacks get most of the headlines, the fact is many of the biggest cyberthreats are internal—originating from within an organization, or within its extended corporate network. These internal incidents can be even more damaging than attacks from outside. In many cases, the damage is done without malicious intent, and is simply the result of carelessness or poor controls and procedures.



### Prepare a resiliency plan

The middle of a crisis is no time to be figuring things out from scratch. To be resilient, you need a plan. You also need to establish effective governance and oversight to coordinate plans and response activities across all stakeholders—including board members and business leaders outside of IT. For most organizations, this comprehensive approach will require a mindset shift from thinking of cyber breaches as an IT risk to understanding that cybersecurity is a strategic business issue and should be addressed as an integral part of the organization's disaster recovery planning.

An effective resiliency plan needs to be developed well in advance, and should be clear and concise enough that people can quickly understand it when the bullets are flying, yet detailed enough to be immediately actionable. The preparation process is continuous—develop threat scenarios, test, evolve, repeat—with the goal of having a response plan that constantly matures and improves to keep pace with emerging threats and changes to the organization's threat landscape. ➤

Cyber threats are infinite, but cybersecurity budgets and resources are finite.



### Leverage best practices and cutting-edge insight

The most effective way for an organization to maintain the necessary levels of security is through partnering with external experts in cyber risk management to take the lead on cyber risk. "The threat landscape continues to change," says Galletto. "But the good news is that there are a lot of services out there that can help organizations maintain cyber hygiene basics, while also effectively managing their cyber risk profile."

Leveraging teams of global cyber risk advisers, these experts help organizations build effective cyber risk strategies based on a thorough understanding of their business and industry. The result is a secure, vigilant, and resilient strategy that enables organizations to grow, share, and trust without compromising on compliance.

It can also be useful to establish or join a cyber-threat intelligence (CTI) sharing community. These communities aim to help organizations improve their vigilance posture in a variety of ways, including: enabling cross-sector sharing with similar organizations; leveraging cybersecurity expertise; facilitating open group discussions; improving compliance with regulatory requirements; developing a funding framework; and initiating government relationships. Think of CTI communities as fighting fire with fire. After all, cyber attackers leverage online communities to strengthen their attacks; why not do the same to strengthen your defenses?

In the months and years ahead, digital innovations and exponential technologies will be key drivers of growth and success, providing tremendous opportunities for businesses around the world to create value and gain a competitive advantage.

To thrive in this increasingly digital world, businesses need a robust cyber strategy that can help them become secure, vigilant, and resilient. Hope is not a strategy.

- Recognize that cyber risk is a strategic business issue, not just an IT issue
- Anticipate tomorrow's threats; don't be satisfied solving yesterday's problems
- Identify and protect your crown jewels
- Don't forget about risks from within your own organization and extended enterprise
- Accept the fact that breaches are inevitable and prepare your business to bounce back quickly
- Share insights and leverage expertise beyond your own organization

Cyber risk is growing exponentially, and no company is immune. However, armed with the right strategy and tools, this is a risk you can master. ●







The rise of advanced data analytics and cognitive technologies has led to an explosion in the use of algorithms across a range of purposes, industries, and business functions. Decisions that have a profound impact on individuals are being influenced by these algorithms—including what information individuals are exposed to, what jobs they're offered, whether their loan applications are approved, what medical treatment their doctors recommend, and even their treatment in the judicial system. At the same time, we're seeing a sharp rise in machine-to-machine interactions that are based in the Internet of Things (IoT) and powered by algorithms.

What's more, dramatically increasing complexity is fundamentally turning algorithms into inscrutable black boxes of decision-making. An aura of objectivity and infallibility may be ascribed to algorithms. However, these black boxes are vulnerable to risks, such as accidental or intentional biases, errors, and fraud, thus raising the question of how to "trust" algorithmic systems.

Embracing this complexity and establishing mechanisms to manage the associated risks will go a long way toward effectively harnessing the power of algorithms—and the upside is significant. Algorithms can be used to achieve desired business goals, accelerate long-term performance, and create differentiation in the marketplace. Organizations that adapt a risk-aware mindset will have an opportunity to use algorithms to lead in the marketplace, better navigate the regulatory environment, and disrupt their industries through innovation.


### When algorithms go wrong

From Silicon Valley to the industrial heartland, the use of data-driven insights powered by algorithms is skyrocketing. Growth in sensor-generated data and advancements in data analytics and cognitive technologies have been the biggest drivers of this change, enabling businesses to produce rich insights to guide strategic, operational, and financial decisions. Business spending on cognitive technologies has been growing rapidly, and it's expected to continue at a five-year compound annual growth rate of 55 percent to nearly US\$47 billion by 2020, paving the way for an even broader use of machine learning-based algorithms.<sup>1</sup> Going forward, these algorithms will be powering many of the IoT-based smart applications across sectors.

While such a change is transformative and impressive, cases of algorithms going wrong or being misused have also increased significantly. Some recent examples include:

- In the 2016 US elections, social media algorithms were cited for shaping and swaying public opinion by creating

opinion echo chambers and failing to clamp down on fake news.

- During the 2016 Brexit referendum, algorithms were blamed for the flash crash of the British pound by six percent in a matter of two minutes.<sup>2</sup>
- Investigations have found that the algorithm used by criminal justice systems across the United States to predict recidivism rates is biased against certain racial classes.<sup>3</sup>
- Researchers have found erroneous statistical assumptions and bugs in functional magnetic-resonance imaging (fMRI) technology, which raised questions about the validity of many brain studies.<sup>4</sup>
- In several instances, employees have manipulated algorithms to suppress negative results of product safety and quality testing.
- Users have manipulated some artificial intelligence-powered tools to make offensive and inflammatory comments.
- According to a recent study, online ads for high-paying jobs were shown more often to men than to women. 

1. "Worldwide Cognitive Systems and Artificial Intelligence Revenues Forecast to Surge Past \$47 Billion in 2020, According to New IDC Spending Guide," Press release, IDC Research, Inc., October 26, 2016, <http://www.idc.com/getdoc.jsp?containerId=prUS41878616>.

2. Netty Idayu Ismail and Lukanyo Mnyanda, "Flash Crash of the Pound Baffles Traders With Algorithms Being Blamed," Bloomberg, December 7, 2016, <https://www.bloomberg.com/news/articles/2016-10-06/pound-plunges-6-1-percent-in-biggest-drop-since-brexit-result>.

3. Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias," ProPublica, May 23, 2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

4. "When science goes wrong (I) Computer says: oops," The Economist, July 16, 2016, <http://www.economist.com/news/science-and-technology/21702166-two-studies-one-neuroscience-and-one-paleoclimatology-cast-doubt>.

Increasing complexity, lack of transparency around algorithm design, inappropriate use of algorithms, and weak governance are specific reasons why algorithms are subject to such risks as biases, errors, and malicious acts. These risks, in turn, make it difficult to trust algorithms' decision choices and create concerns around their accuracy.

Many traditional checks and balances are designed for managing "conventional risks" where algorithm-based decisions aren't significantly involved, but these checks and balances aren't sufficient for managing risks associated with today's algorithm-based decision-making systems. This is due to the complexity, unpredictability, and proprietary nature of algorithms, as well as the lack of standards in this space.

These risks have the potential to cascade across an organization and negatively affect its reputation, revenues, business operations, and even regulatory compliance. That's why it's important for organizations to understand and proactively manage the risks presented by algorithms to fully capture the algorithms' value and drive marketplace differentiation.

### What are algorithmic risks?

Algorithmic risks arise from the use of data analytics and cognitive technology-based software algorithms in various automated and semi-automated decision-making environments. Figure 1 provides a framework for understanding the different areas that are vulnerable to such risks and the underlying factors causing them.

- **Input data** is vulnerable to risks, such as biases in the data used for training; incomplete, outdated, or irrelevant data; insufficiently large and diverse sample size; inappropriate data collection techniques; and a mismatch between the data used for training the algorithm and the actual input data during operations.

- **Algorithm design** is vulnerable to risks, such as biased logic, flawed assumptions or judgments, inappropriate modeling techniques, coding errors, and identifying spurious patterns in the training data.
- **Output decisions** are vulnerable to risks, such as incorrect interpretation of the output, inappropriate use of the output, and disregard of the underlying assumptions.

These risks can be caused by several underlying factors:

**Human biases:** Cognitive biases of model developers or users can result in flawed output. In addition, lack of governance and misalignment between the organization's values and individual employees' behavior can yield unintended outcomes.

**Example:** Developers provide biased historical data to train an image recognition algorithm, resulting in the algorithm being unable to correctly recognize minorities.

**Technical flaws:** Lack of technical rigor or conceptual soundness in the development,

training, testing, or validation of the algorithm can lead to an incorrect output.  
**Example:** Bugs in trading algorithms drive erratic trading of shares and sudden fluctuations in prices, resulting in millions of dollars in losses in a matter of minutes.

**Usage flaws:** Flaws in the implementation of an algorithm, its integration with operations, or its use by end users can lead to inappropriate decision making.

**Example:** Drivers over-rely on driver assistance features in modern cars, believing them to be capable of completely autonomous operation, which can result in traffic accidents.

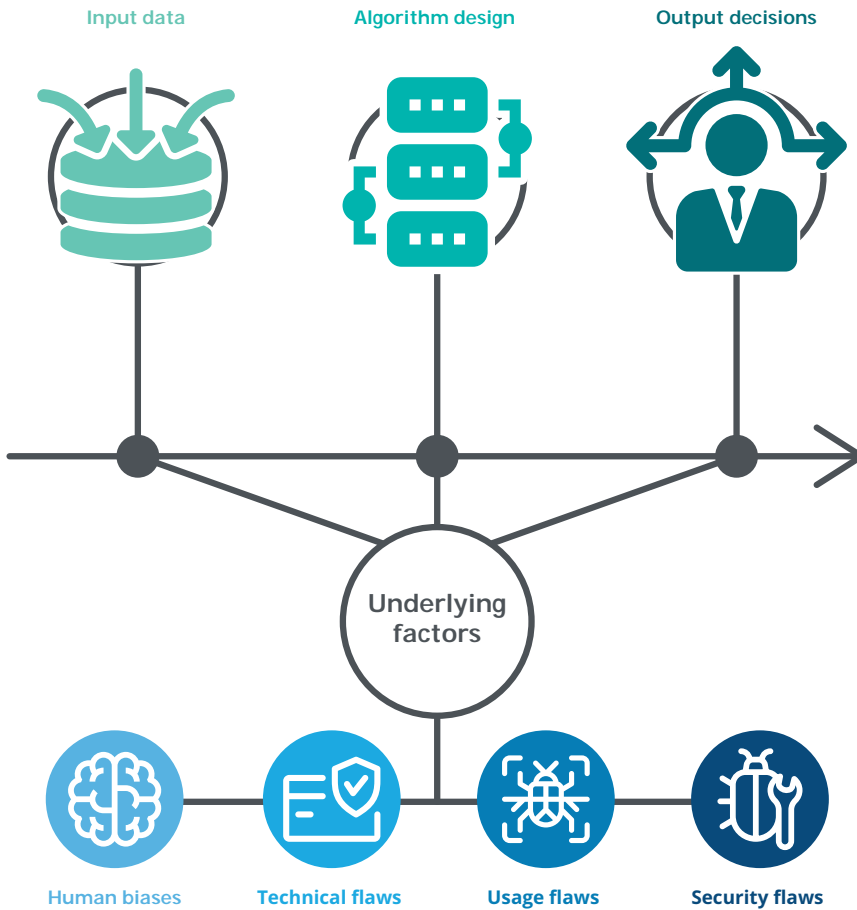
**Security flaws:** Internal or external threat actors can gain access to input data, algorithm design, or its output, and manipulate them to introduce deliberately flawed outcomes.

**Example:** By intentionally feeding incorrect data into a self-learning facial recognition algorithm, attackers are able to impersonate victims via biometric authentication systems.

It's important for organizations to understand and proactively manage the risks presented by algorithms.



Figure 1: Framework for understanding algorithmic risks



**Why are algorithmic risks gaining prominence today?**

While algorithms have been in use for many years, the need to critically evaluate them for biases, lack of technical rigor, usage flaws, and security vulnerabilities has grown significantly in recent times. This growing prominence of algorithmic risks can be attributed to the following factors:

**Algorithms are becoming pervasive**

With the increasing adoption of advanced data analytics and machine learning technology, algorithm use is becoming more prevalent and integral to business processes across industries and functions. It's also becoming a source of competitive advantage. One study predicts that 47 percent of jobs will be automated by 2033.<sup>5</sup> Figure 2 highlights some prominent business use cases of algorithms.

These use cases are expected to significantly expand in the near future, given the tremendous growth in IoT-enabled systems. These systems can lead to the development and proliferation of new algorithms for connecting IoT devices and enabling smart applications.

**Machine learning techniques are evolving**

Improvements in computational power coupled with the availability of large volumes of training data—data used to train algorithms—are driving advancements in machine learning. Neural networks are becoming an increasingly popular way of implementing machine learning. Techniques such as deep learning are being used for tasks like computer vision and speech recognition.

These advances in machine learning techniques are enabling the creation of algorithms that have better predictive capabilities but are significantly more complex.

**Algorithms are becoming more powerful**

Not only are algorithms becoming more pervasive, but the power and responsibility entrusted to them is increasing as well. Due to advancements in deep learning techniques, algorithms are becoming better at prediction and making complex decisions. Today, algorithms are being used to help make many important decisions, such as detecting crime and assigning punishment, deciding investment of millions of dollars, and saving the lives of patients. ➔

5 Carl Benedikt Frey and Michael Osborne, "The Future of Employment," Oxford Martin Programme on Technology and Employment, September 17, 2013, <http://www.oxfordmartin.ox.ac.uk/downloads/academic/future-of-employment.pdf>.

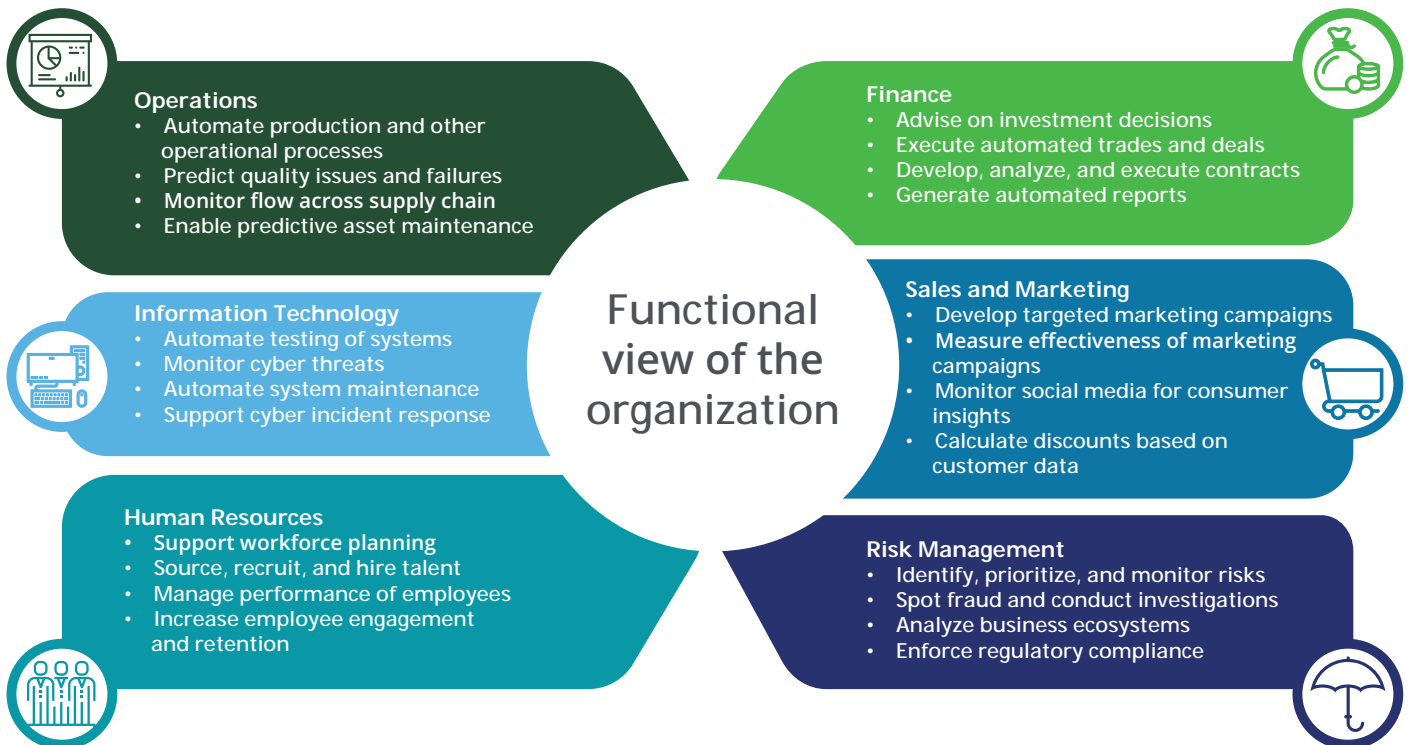
**Algorithms are becoming more opaque**

Algorithms run in the background and often function as black boxes. With their internal workings and functioning largely hidden from developers and end users, monitoring algorithms can be difficult. Many new machine learning techniques, such as deep learning, are so opaque that it's practically impossible to understand what they deduce from training data and how they reach their conclusions—thus making it hard to judge their correctness. This difficulty in understanding algorithmic decisions, coupled with the unpredictability and continuously evolving nature of algorithms, makes inspecting them a challenge.

**Algorithms are becoming targets of hacking**

Machine learning algorithms are exhibiting vulnerabilities that can be exploited by hackers. A common vulnerability is the data used to train algorithms. Manipulating that training data as it's presented to the algorithms results in skewed algorithms that produce erroneous output, which in turn leads to unintended actions and decisions. In addition, attackers are also tampering with the actual live data to which the algorithms are applied. A recent report revealed that cyber criminals are making close to US\$5 million per day by tricking ad purchasing algorithms with fraudulent ad click data, which is generated by bots rather than humans.<sup>6</sup>

Figure 2. Algorithm use across business functions



6. Thomas Fox-Brewster, "Biggest Ad Fraud Ever": Hackers Make \$5M A Day By Faking 300M Video Views," Forbes, December 20, 2016, <https://www.forbes.com/sites/thomasbrewster/2016/12/20/methbot-biggest-ad-fraud-busted/#4324f6c74899>.



### What do algorithmic risks mean for your organization?

As noted previously, data analytics and cognitive technology-based algorithms are increasingly becoming integral to many business processes, and organizations are investing heavily in them. Nevertheless, if the issues highlighted in this report aren't adequately managed, the investments may not yield the anticipated benefits. Worse yet, they may subject organizations to unanticipated risks.

The immediate fallouts of these algorithmic risks can include inappropriate and potentially illegal decisions relating to:

- Finance, such as inaccurate financial reporting resulting in regulatory penalties and shareholder backlash, as well as taking on unanticipated market risks beyond the organization's risk appetite.
- Sales and marketing, such as discrimination against certain groups of customers in product pricing, product offerings, and ratings.
- Operations, such as credit offers, access to health care and education, and product safety and quality.
- Risk management, such as not detecting significant risks.

- Information technology, such as inadequate business continuity planning and undetected cyber threats.
- Human resources, such as discrimination in hiring and performance management practices.

Algorithms operate at faster speeds in fully automated environments, and they become increasingly volatile as algorithms interact with other algorithms or social media platforms. Therefore, algorithmic risks can quickly get out of hand.

Financial markets have already experienced significant instability because of algorithms. The most high-profile instance was the flash crash of 2010, which sent the Dow Jones Industrial Average on a 1,000-point slide.<sup>7</sup>

Algorithmic risks can also carry broader and long-term implications for an organization, such as:

- Reputational risks: The use of algorithms can significantly increase an organization's exposure to reputation risks. This is particularly true if the various stakeholders believe that the workings of the algorithm aren't aligned to the ethics and values of the organization, or

if the algorithms are designed to covertly manipulate consumers, regulators, or employees.

- Financial risks: Errors or vulnerabilities in algorithms, especially those used for financial and strategic decision-making, can result in significant revenue loss for organizations and negatively affect the integrity of their financial reporting.
- Operational risks: As algorithms are used to automate supply chain and other operational areas, errors can result in significant operational disruptions.
- Regulatory risks: Algorithms making decisions that violate the law, circumvent existing rules and regulations, or discriminate against certain groups of people can expose organizations to regulatory and legal actions.
- Technology risks: The wide-scale use of advanced algorithms can open up new points of vulnerability for IT infrastructure.
- Strategic risks: With algorithms being used increasingly as sources for strategic decision-making, errors or vulnerabilities within them can put an organization at a competitive disadvantage. ➤

7. Silla Brush, Tom Schoenberg, and Suzi Ring, "How a Mystery Trader With an Algorithm May Have Caused the Flash Crash," Bloomberg, April 22, 2015, <https://www.bloomberg.com/news/articles/2015-04-22/mystery-trader-armed-with-algorithms-rewrites-flash-crash-story>.

It's important for organizations to evaluate their use of algorithms in high-risk and high-impact situations.

#### **What's different about managing algorithmic risks?**

With the growing urgency of algorithmic risk management, it's important to note that conventional risk management approaches may not be effective for that purpose. Instead, organizations should rethink and reengineer some of their existing risk management processes due to the inherent nature of algorithms and how they're used within organizations. For example, algorithmic risk management can't be a periodic point-in-time exercise. It requires continuous monitoring of algorithms, perhaps through the use of other algorithms. Three factors differentiate algorithmic risk management from traditional risk management:

#### **Algorithms are proprietary**

Algorithms are typically based on proprietary data, models, and techniques. They're considered trade secrets and sources of competitive advantage. As a result, organizations are typically unwilling to share data, source code, or the internal workings of their algorithms. This makes it difficult for regulatory agencies and outside watchdog groups to monitor them.

#### **Algorithms are complex, unpredictable, and difficult to explain**

Even if organizations were to share their algorithm codes, understanding them may be difficult because of their inherent complexity. Many of today's algorithms are based on machine learning and other advanced technologies. They evolve over time based on input data. In many cases, even the teams that develop them might not be able to predict or explain their behaviors.

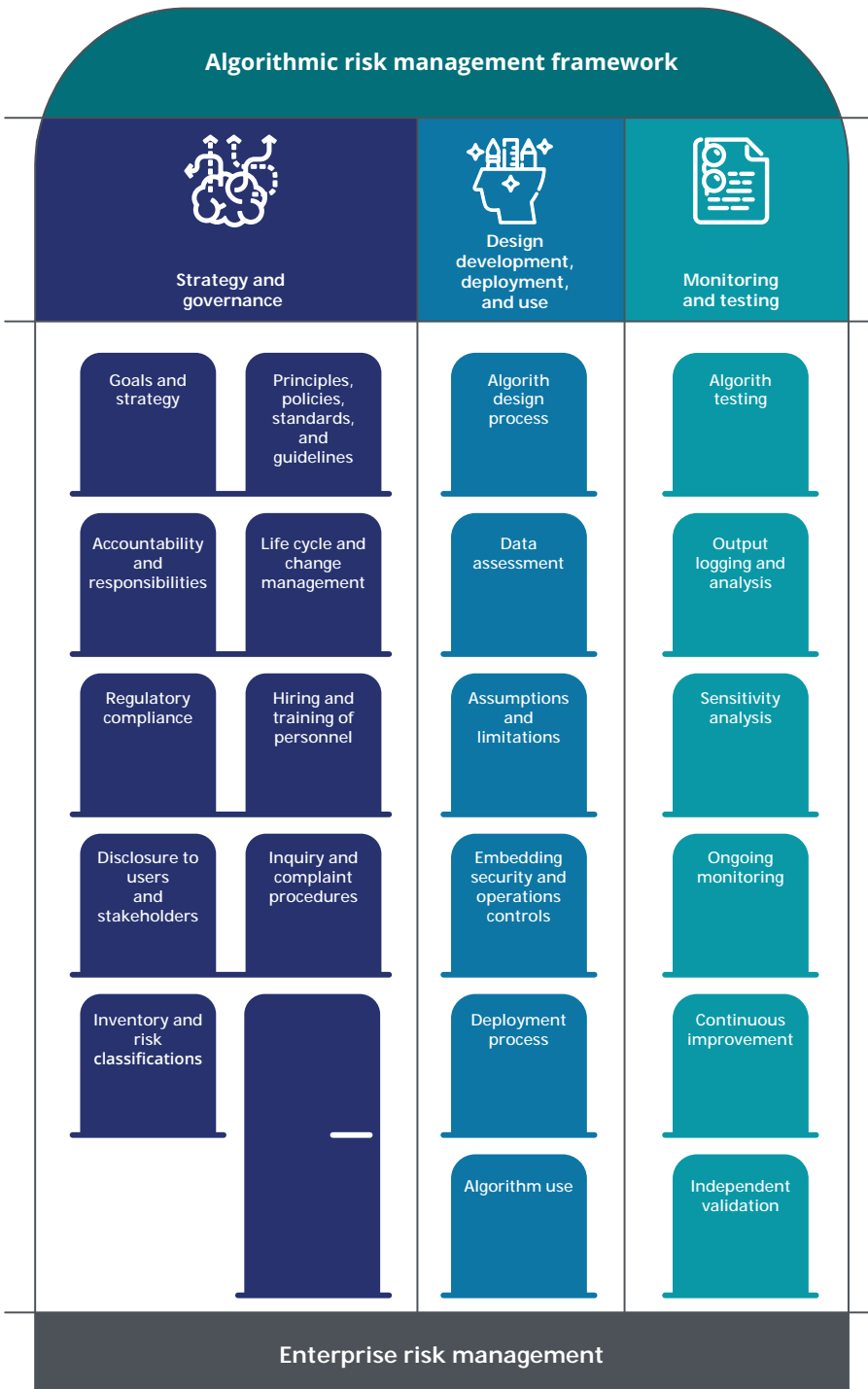
Machine learning algorithms can even develop their own languages to communicate with each other. This is an area with both tremendous potential and risk, given the anticipated growth in IoT and machine-to-machine communications.

#### **There's a lack of standards and regulations**

In financial services, model validation has become very important over the past few years, and there are widely accepted standards such as SR 11-7: Guidance on Model Risk Management. However, these standards have limitations when applied to complex machine learning techniques such as deep learning. Currently, no widely accepted cross-industry standards exist to govern many types of machine learning algorithms, including processes around data collection, training, and algorithm design. As a result, there's a lack of consistent business controls for development, implementation, and use of algorithms. Developers frequently use their experience and theoretical knowledge to make these decisions without management oversight, leading to variations in processes and the increased likelihood of errors.

In addition, regulations in this space are still evolving and apply to only a limited set of algorithms, such as those relating to capital management and stress testing in the banking sector. While there have been some attempts to broadly regulate the use of algorithms (especially in Europe), there's still a lack of clarity about, and many unanswered questions around, how these regulations will be implemented. This lack of standards and regulations makes it difficult to drive accountability and fairness in the use of algorithms.

Figure 3. A framework for algorithmic risk management



## Is your organization ready to manage algorithmic risks?

The rapid proliferation of powerful algorithms in many facets of business is in full swing and is likely to grow unabated for years to come. The use of intelligent algorithms offers a wide range of potential benefits to organizations, from innovative products to improved customer experience, to strategic planning, to operational efficiency, and even to risk management. Yet as this article has discussed, some of those benefits could be diminished by inherent risks associated with the design, implementation, and use of algorithms—risks that are also likely to increase unless organizations invest effectively in algorithmic risk management capabilities.

It's not a journey that organizations must take alone. The growing awareness of algorithmic risks among researchers, consumer advocacy groups, lawmakers, regulators, and other stakeholders should contribute to a growing body of knowledge about algorithmic risks and, over time, risk management standards. In the meantime, it's important for organizations to evaluate their use of algorithms in high-risk and high-impact situations and implement leading practices to manage those risks intelligently so algorithms can be harnessed for competitive advantage.





Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018h](http://www.deloitte.com/lu/InsideRisk2018h)



# Fight fire with fire

## Cyber response training through immersive simulation

**Dominic Cockram**

Partner  
Deloitte UK

Making sure you have an effective management response to cyber crises is a key requirement for any 21<sup>st</sup> century business. But how can you optimize your cyber response capability? Simulating a crisis is one way to see just how ready you are—or how far you have to go!

In this article, we consider the unique challenges presented by a cyber-related crisis, setting out the options for building up your cyber response capability and preparing your cyber response teams to perform optimally to protect the reputation of your business and minimize losses. [▶](#)



Effective cyber crisis management is dependent on having the right people in the right roles, with good, well-understood procedures and processes, supporting tools, and effective leadership.

A crisis, by definition, is a situation that poses a serious threat to an organization and requires decisive action at a strategic level to minimize the impact on the business and its stakeholders. The stakes are high, and all crises create a complex, stressful, and high-pressure environment for those involved. The "cyber factor" brings added nuances and an uncomfortable interface between the complex IT domain and strategic decision-makers. Add to that social media, journalistic and regulatory scrutiny, and public opprobrium and you have the perfect ingredients for a nightmare scenario.



## So, what characterizes a cyber crisis?



### Speed

They usually hit businesses fast and without warning. The very nature of technology means issues move and spread quickly.



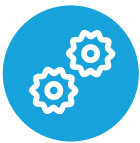
### Complexity

They are usually the result of an attack on you or your systems and, as with most planned assaults, they are designed to make matters opaque, confusing, and chaotic to enhance the attackers' opportunities to achieve their objectives.



### Uncertainty and lack of (or sometimes too much) information

Uncertainty is a characteristic of all crises but with a data breach or a ransomware attack, this is often magnified by an initial lack of understanding of what has happened. With floods and fires, the nature of the disaster is clear; with malware or breaches, you may never know what happened.



### Terminology and technical awareness

While awareness is growing, there is still a significant gap in understanding between the technical IT experts and the strategic decision-makers in a company.



### Victim versus villain

You may feel like the victim, but to many, the external perception may be that you are the villain. If customer data has been lost or systems paralyzed, people may begin to ask why you "allowed" this to happen.



### Media scrutiny and public outrage

To lose sensitive personal data hits right at the heart of customer trust and will attract intense media and public scrutiny.



### Timelines

To understand what has happened, why and just how bad the situation is takes time. However, time is not a luxury you have when it comes to communicating with your stakeholders.



### "Wicked" decisions

will you shut down key systems, shut customers out from websites or, as a last resort, disconnect from the internet? Plenty of difficult decisions will have to be made. ➔

### What makes good cyber crisis management?

Effective cyber crisis management is largely dependent on having the right people in the right roles, with good, well-understood procedures, supporting tools, and effective leadership. However, human behavior during a crisis response is also a key factor. We can be resilient, adaptive, and flexible, but our behavioral patterns can also be plagued by error, stubbornness, and inefficiency. Therefore, the executive team must have a repertoire of effective crisis management skills to function in situations involving high levels of stress, complexity, and time pressure. Maximizing those skills depends on the level of experience with and exposure to previous events.

### Readiness to respond to a cyber crisis

Building skills and widening experience would be easy if you could learn on the job and slowly build your expertise. However, crises do not happen every day, so cyber response capability must be developed, validated, and improved through an accelerated mechanism of frequent practice, training, and exercising of the people involved—particularly the leadership at each response level and the strategic executive group. Just like a football team, the more training and practice they do, the quicker they fall into their drills and patterns in a match, perform as a team, and score goals.

### The right training environment for every level

Crisis training provides the ideal training environment, building people's experience through exposure to different scenarios under various conditions. The aim is to develop their muscle-memory from lessons learned so that they can be applied to real events. Many different types of exercise exist; each approach builds different capabilities and is chosen to suit the maturity of participants.

- **Cyber workshop**—introducing teams to the issues around cyber response and crisis management using case studies, videos, and scenarios to raise understanding of the issues and challenges to be faced.
- **Cyber desktop (tabletop)**—take a scenario and bring together the key cyber response teams to “walk and talk” the response against a timeline. Useful for discussion and establishment of roles and responsibilities.
- **Red teaming**—an assault on your defenses in real time during a simulated “hack” or penetration test. Great for testing your defenses and validating your monitoring of alerts and notifications. Highly operationally focused but can, on occasion, be linked to strategic decisions.
- **Cyber incident team training**—exercising your technical “quick response” team (CSIRT, CIRT, etc.) and their ability to use their tools, assess and analyze the data, conduct a coherent and coordinated investigation and sleuth their way to the answers based on a real trail of simulated intrusion paths and clues using safe and tested methodologies playing out on your network in real time. How else can you check just how good they really are?
- **The “full” cyber simulation**—rehearsing the end-to-end response to a large-scale cyber crisis. Scenarios start with alerting and mobilizing the CIRT and the technical teams, while rehearsing the escalation up to the business/management level and then to the strategic team. Each level has to consider the issues and requirements of its remit, and the interplay of responsibilities upward and downward. Internal and external communications are also critical; bringing the media, public, investors, and other stakeholders into play, adding to the strategic challenge. The business impacts unfold, while the technical teams investigate the cause of the crisis.

For many businesses, immersive cyber simulation exercises are the most appropriate tool for building crisis response capability.



### Experiential, immersive simulations

For many businesses, immersive cyber simulation exercises are the most appropriate tool for building crisis response capability. Such exercises truly test the end-to-end response, taking the teams from alert through to the most senior executives and placing them all in the maelstrom of a cyber crisis.

### Perception versus reality

To rehearse a team's performance, simulations must have the ability to create the perceptions, emotions, and behaviors that occur in real crises. Therefore, any simulation should be engaging at its developmental center. For simulation exercises to be engaging they must be credible to the players. This is achieved by incorporating high levels of fidelity, complexity, dynamicity, and opaqueness in the cyber crisis scenarios used during the exercise.

### Generating immersive detail

Successful simulations are immersive, with players becoming fully involved and responding as if the scenario playing out in front of them were reality. Key to generating this environment is the scenario and the detail, facts, and storylines created behind the scenario. The scenario must have the ability to adapt during the exercise in response to the decisions and actions the teams have taken. This approach requires experience and depth of planning to ensure that there is sufficient background to make changes to the scenario during the exercise.

Immersive simulations are the only tools that truly test and validate the efficacy and coherence of your cyber response capability because they re-create the reality that is faced in the early stages of a cyber crisis. Being under the pressures and desires for more information, the reaching

for facts and certainty, and the wicked decision of whether to go public or not.

To play these critical points out in a simulated reality is to learn where the conflicts are, where policy fails to meet reality, and where reputation overrides logic and perception challenges fact. ➤



The Wannacry and NotPetya attacks have established a whole new paradigm of cyber challenges to be faced and managed.

## Building the right cyber challenges

### Scenarios versus training benefits

Scenarios are central to any cyber simulation, but some scenarios suit teams at certain levels better than others; for example by providing more scope for technical detail or focusing on media and other stakeholder issues.

While there is, often quite, rightly a desire to test the scenarios that are highest on the risk register, at times it is better to choose the right scenario to rehearse the response capability of the teams and to provide a longer, more thorough step through of the assessment, escalation, activation, response, communication, and recovery stages of the cyber response.

### Not enough hours in the day

In addition, a further challenge is that of time. There is only so much time available in the agendas of senior executives and thus exercise play is often squeezed into a single day—or even worse, a three-hour slot—which prevents certain key, longer-term decision points from being played out, such as notifying the regulator following a data breach (under GDPR within 72 hours). Such critical decision points can be neglected in a one-day exercise unless time jumps are introduced to allow the fast forwarding of events.

### Post-data-breach customer engagement considerations

Under the forthcoming GDPR rules, businesses in Europe will be under far more pressure to proactively notify customers of a breach and to conduct a full “breach notification and customer engagement” program. This in itself is beginning to provide a specific scenario worthy of exercising and validating. An organization’s ability to respond and manage the customer engagement with appropriate resources, messaging, and identity protection considerations are all critical considerations, as is the all-important insurance discussion.

## Train hard, fight easy

“Train hard, fight easy” is a great cry of the armed forces, but very true in all arenas surrounding crises. The better prepared the response, the better we are able to deal with the chaos of a crisis and deliver well-informed decisions in a timely fashion. This article has only touched on the edges cyber crisis preparedness, and there is much that can be done to build a real capability.

Most large organizations recognize that the question is “when,” not “if,” they will be beset by some form of cyber crisis. The Wannacry and NotPetya attacks have established a whole new paradigm of cyber challenges to be faced and managed.

At the same time, GDPR brings to Europe—and all those businesses with customers inside Europe—new and much tougher regulations, and preparedness is one of the many facets now in focus.

Against this backdrop, it is no longer acceptable for any business not to be well prepared and rehearsed. That ability to be able to show, post any form of crisis, that you were as well prepared as you could (and should) be is invaluable in the investigations that follow.

Most critical is that your teams are genuinely trained and have experiential awareness of the different types of cyber challenge built up. This must be through simulations of just what each crisis can present in terms of key decisions, challenges, and communication nuances.

Knowing that from top to bottom your business has played through the interaction of teams at every level is the only way to really know you are ready to go out and defend your business and its reputation at its most vulnerable time. ●



**Roland Bastin**

Partner  
Risk Advisory  
Deloitte Luxembourg

**Irina Hedeá**

Director  
Risk Advisory  
Deloitte Luxembourg

**Francesco Martini**

Manager  
Risk Advisory  
Deloitte Luxembourg

**Florent Normandin**

Consultant  
Risk Advisory  
Deloitte Luxembourg

Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018i](http://www.deloitte.com/lu/InsideRisk2018i)

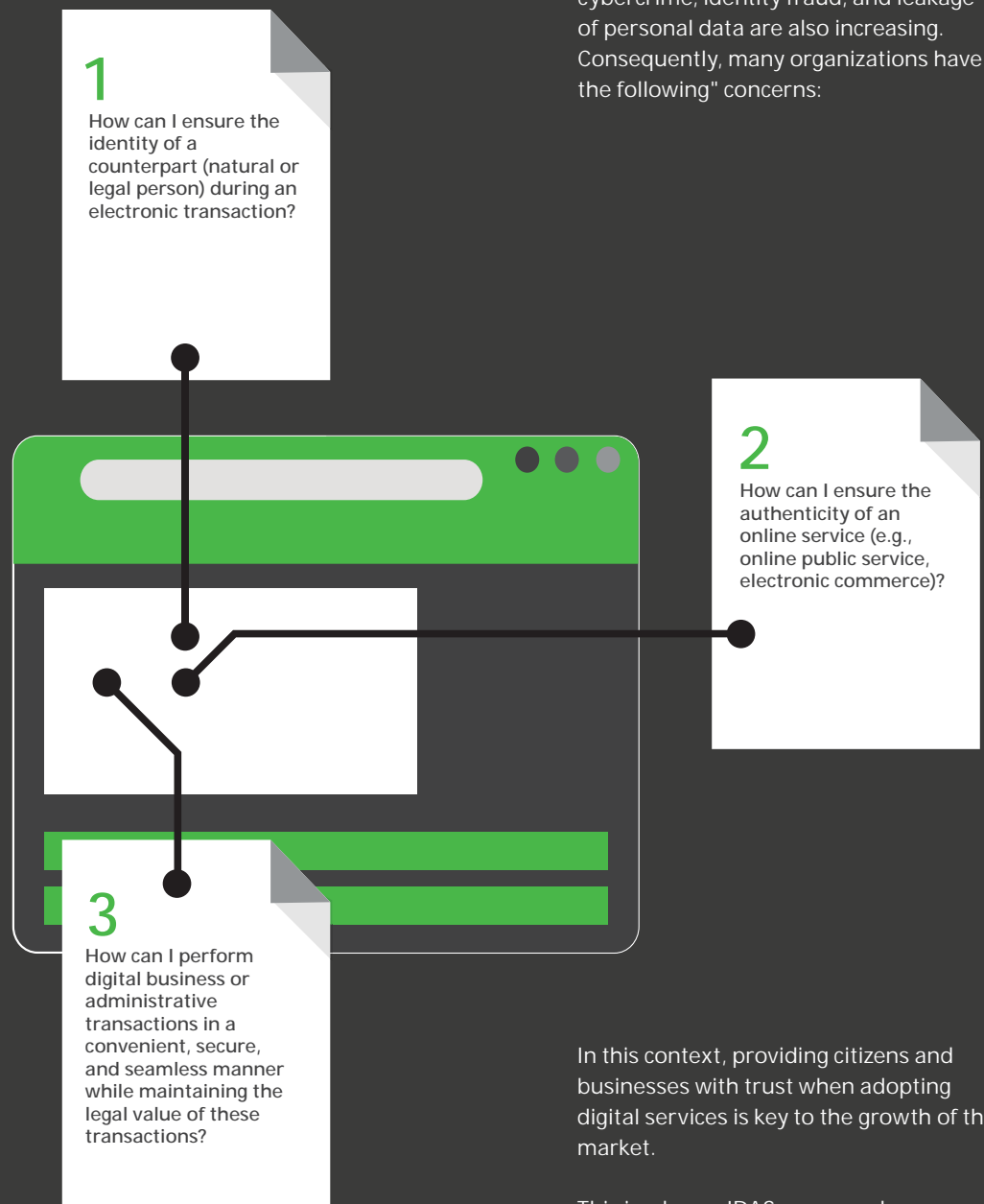


# eIDAS

The EU as a  
forerunner  
in boosting  
the digital  
economy >

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

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



In this context, providing citizens and businesses with trust when adopting digital services is key to the growth of this market.

This is where eIDAS comes as leverage for the European Digital Single Market, addressing these concerns and accelerating the development of the business in a trusted and secure environment.



## Electronic Identification

By 29 September 2018, a European citizen with an eID card, notified to the EU Commission according to eIDAS, will be able to access any online public service from any EU Member State and perform administrative procedures online with the same trust as if the person was physically present in the concerned administration.

Identifying a person without his or her physical presence will be possible through electronic identification, defined by eIDAS. As of today, several electronic identification means are deployed in the EU, either by the member states (e.g., electronic identity cards or eID cards) or by private actors (e.g., private smart cards, authentication tokens, or mobile applications). Without eIDAS, there is no mutual recognition of these eID means between member states, nor alignment on the level of assurance and trust offered by these eID means. For example, a Luxembourg citizen's eID card is not automatically recognized by other EU Member States for authentication for online services and electronic transactions.

This allows the development of cross-border digital administration services such as filling taxes, registering online to university programs, or accessing medical records online across the EU.

Nevertheless, the trust placed in eID means will depend on the level of assurance that they provide toward the identity of the physical or legal person behind them. The regulation defines three assurance levels—low, substantial, and high—that depend on different aspects, such as the applicant's identity verification process. The public sector bodies of each member state offering online services will define the assurance level required to access these services.

The recognition of the notified eID means by all EU Member States is mandatory as of 29 September 2018.

However, as of 29 September 2015, the Member States already had the option, on a voluntary basis, to notify their eID means to the European Commission, and to recognize the eID means defined by other Member States.<sup>3</sup>

# eIDAS brings an important change for the current European digital market, as the regulation defines a framework for cooperation between member states for a cross-border mutual recognition of eIDs.

eIDAS brings an important change for the current European digital market, as the regulation defines a framework for cooperation between member states for a cross-border mutual recognition of eIDs.

In practice, eIDAS gives EU Member States the opportunity to notify their eID means to the European Commission, and makes it mandatory for other member states to recognize the notified eID means on their online public services. As a concrete application of this provision, a European citizen with an eID card (among the list of notified eID means) will be able to access any online public service from any EU Member State and perform her administrative procedures online as if she was physically present in the concerned administration.

Mutual recognition of eID means will help break down the barriers related to electronic administrations within Europe. However, like for all electronic processes, the benefits also come with new risks and security matters. To address them, the regulation enforces the member states' accountability and responsibilities toward the eID means under their responsibility. Member states will be held liable for damages caused intentionally or negligently in a cross-border transaction due to a failure to comply with the regulation. In addition, in case of security breach affecting the reliability of the notified eID means, member states will have to suspend or revoke the cross-border authentication or the compromised parts and notify other member states and the European Commission. ➔

1. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>
2. DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=en>
3. "The first big step in eIDAS implementation accomplished" by Andrea Servida: <https://ec.europa.eu/digital-single-market/en/blog/first-big-step-eidas-implementation-accomplished>

“A qualified electronic signature shall have the equivalent legal effect of a handwritten signature”.

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

**Trust services**

“A qualified electronic signature shall have the equivalent legal effect of a handwritten signature”. Article 25(2) of the eIDAS regulation.

Since 1 July 2016, eIDAS created opportunities for banks to remotely open clients' accounts, sign electronic contractual documents, validate electronic transactions, and deploy other electronic services while ensuring a cross-border legal value of these documents and processes within the EU.

Before eIDAS, when the European Union adopted the Directive 1999/93/EC on electronic signatures, the objective was the promotion of electronic signatures,

the development of international electronic commerce, and cross-border activities. However, the main shortcoming of the previous framework was that, as a directive, it was transposed differently in national laws, thus leading to a lack of harmonization between member states regarding the technical standards.

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

**EIDAS new trust services**



**Electronic seals**

Trust service intended for legal persons to ensure the origin and integrity of data and documents



**Electronic time stamps**

Trust service aiming at ensuring the correctness of the time linked to data and documents



**Electronic registered delivery service**

Trust service aiming at transmitting data and documents between third parties and providing evidence relating to this transmission



**Website authentication**

Trust service that ensures visitors of a website of the identity of the legal person who owns the website



**Validation service**

for qualified electronic signatures, qualified electronic seals, certificates related to those services, and certificates for website authentication



**Preservation service**

for qualified electronic signatures, qualified electronic seals, and certificates related to those services

To address the risks related to the provision of these trust services and for ensuring an adequate level of security, the regulation defines security requirements for trust service providers in terms of risk management and security incident management.

Moreover, for each of the trust services, the regulation defines which are considered qualified trust service providers and qualified trust services. Even if all trust services benefit from the principle of non-discrimination as evidence in legal proceedings, only qualified trust services benefit from the presumption of reliability in legal proceedings (i.e., the presumption of integrity, correctness of origin, and accuracy) and cross-border recognition of qualified status in the EU Member States. In the specific case of qualified electronic signatures, the regulation goes even further by bestowing upon a qualified electronic signature to have the legal equivalent of a handwritten signature.

### International aspects

With eIDAS, the EU positions itself as a forerunner in electronic identification and trust services, given that the regulation applies at the European continental scale. Several countries have implemented national legislations covering the legal value of electronic signatures. For example, in the USA, the applicable laws are the Electronic Signatures in Global and National Commerce Act (ESIGN),<sup>4</sup> adopted by the federal government, and the Uniform Electronic Transactions Act (UETA),<sup>5</sup> used as a baseline for state regulations. According to both laws, a signature shall not be denied legal effect or enforceability solely because it is in electronic form (ESIGN Section Sec. 101 and UETA Section 7). However, in the USA or in other third countries, even when national legislation exists, it only covers electronic signatures, and not other trust services.

Europe is a precursor on electronic identification and trust services, as eIDAS defines a common ground for all EU Member States on key foundations of the digital economy such as the electronic identification and the trust services. The European Union has also understood the need to open the European Single Digital Market to non-EU citizens, businesses, and administrations across the world. This topic has a dedicated article in eIDAS, titled "International aspects," which allows for the mutual recognition of trust services between the European Union and third countries under specific conditions.<sup>6</sup>

## Conclusion

With the eIDAS Regulation, the European Union provided fertile ground for a trustworthy, secure, and convenient digital single market. In addition, as no similar regulation exists on the other continents, Europe positions itself as a forerunner and paves the way to remove the legal and regulatory barriers related to the cross-border digital transactions.

The eIDAS Regulation is a wonderful opportunity for the European Union to harmonize trust in digital services across the different member states. It is up now to European actors of the digital economy (citizens, businesses, and public authorities) to unlock the full potential of this regulation and to boost the growth of the digital economy. ●

4. <https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/html/PLAW-106publ229.htm>

5. [http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta\\_final\\_99.pdf](http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf)

6. Article 14. 1. "Trust services provided by trust service providers established in a third country shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union where the trust services originating from the third country are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU"



# Part 03

---

From a governance  
and compliance  
perspective ▶

# Risk, reward, and the realities of doing business right

## Insights from the Deloitte Risk Conference

**Dr. Martyn Davies**

Managing Director  
Emerging Markets &  
Africa  
Deloitte South Africa

**Hannah Edinger**

Associate Director  
Africa Services Group  
Deloitte South Africa

**Akiva Ehrlich**

Director  
Risk Advisory  
Deloitte South Africa

The Deloitte Risk Conference 2017, held in October last year in South Africa, brought together global thought leaders in the field of risk management under the theme of "Creating and sustaining value." With speakers including Nhlanhla Nene, Trevor Manuel, and Justice Malala, the conference was a must-attend event for South Africa's corporate elite. Making an unwelcome appearance at the conference was the ever-present shadow of the accounting profession's so-called "black swan," highlighting that irrespective of how thorough risk management is, black swan events can still be overlooked. ➤

Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018j](http://www.deloitte.com/lu/InsideRisk2018j)

Printed with permission of Deloitte South Africa







To ensure good corporate governance, the focus needs to be on the financial management decisions of a company.

On that note, the conference kicked off by discussing how business in South Africa is now perceived as being exploitative, self-interested, and a vehicle for corruption. This follows a series of scandals that have hit the country in recent years. The majority of businesses know that this is not a true representation; however, these perceptions tarnish the image of the majority of good corporate citizens. To have a credible voice on important issues, businesses must be willing to "clean house."

The auditing profession specifically has been affected. This is shown in the recently released World Economic Forum's Global Competitiveness Report. South Africa's rating for "Strength of auditing and reporting standards" slipped from the first to the thirtieth position out of the 137 economies included in the index worldwide.

South Africa's institutional strength has also been eroded. As reported in the Global Competitiveness Report, the strength of South Africa's institutions dropped from position 40 to position 76 in the last year. Although this is likely to be an overreaction based on recent events, it requires a concerted response from both government and business to restore trust in the country's institutions.

Keynote speaker and Old Mutual Chairman Trevor Manuel explained that good corporate governance should be a firm's first safeguard against both internal and external risks.

To ensure good corporate governance, the focus needs to be on the financial management decisions of a company. The failure of a system to address risk is





As reported in the Global Competitiveness Report, the strength of South Africa's institutions dropped from position

40

to position

76

in the last year.

the result of internal processes. In order to survive and mitigate risk, both companies and countries need to focus on the long-term view and internalize risk management to be effective.

According to Manuel, South Africa's current environment and unpredictability have resulted in uncertain long-term consequences and made it very difficult for companies to make decisions.

Ian Stewart, Chief Economist at Deloitte UK, gave a wider, global view on risk and volatility, explaining how the global economy had entered the "new normal," with slower growth and greater volatility after the global financial crisis. [➔](#)



# Global growth is approximately only

# 75%

# of its pre-crisis level.

Global growth is approximately only 75 percent of its pre-crisis level. Slower growth leads to heightened volatility, and risks become more difficult to manage and mitigate. Corporates are exhibiting behavior that is more cautious and risk averse as perceptions of risk increase; risk appetite declines; investments, mergers, and acquisitions fall; and corporate cash balances increase.

Stewart shared the global economy's current top five risks, which are Brexit, imbalances in the Chinese economy, rising US protectionism, North Korea, and—possibly the most important—monetary tightening.

The effect of global politics was also discussed at the conference. Whether it is the inauguration of Donald Trump as President of the United States, Brexit in Europe, preparations underway for China's new leadership, or allegations of state capture and corruption in South Africa, uncertainty about trade and investment policy is rising for both international and South African businesses.

According to the speakers, for South African businesses, the biggest risk from the ongoing local political turmoil is a prolonged low growth environment, with growth expected to reach a mere 0.6 percent in 2017 and recover to just over 1 percent in the medium term. This lackluster growth will continue to place pressure on industries such as retail and financial services.

However, the situation is unlikely to worsen to the extent seen in, for example, its emerging market peer Brazil, where analysts expect the economy to continue shrinking, after contracting by 4 percent annually for the past two years. Political uncertainty is predicted to start waning past the ANC's December elective conference and this could mark the end of a downward cycle for South Africa, though the economic recovery thereafter will likely be slow.

Another risk to South Africa's political economy is the country's changing demographics. About 40 percent of South Africa's population is under the age of 20, and 75 percent of its people are under the age of 40. As young people seek employment opportunities, net migration within South Africa is toward the major business hubs in Gauteng. With more young people migrating into urban hubs, a greater proportion of the population is becoming interracial, intercultural, and more socially integrated. This is setting the stage for what could be an incredible political shift.

From an investment perspective, many companies have grown tired of South Africa's political risk, and are looking for other opportunities inside and outside of Africa. Accordingly, foreign direct investments to South Africa have fallen and portfolio investments, rather than bricks and mortar, make up the bulk investment flows into the country. ➔

Despite the high level of political uncertainty in South Africa, when compared to the sentiments of investors about Brexit, for instance, and political turmoil in other emerging countries such as Brazil, South African bond issues are still oversubscribed by foreign funds to a surprising extent. This continued confidence from international investors highlights the independence and strength of domestic institutions such as the South African Reserve Bank, and points toward brighter prospects for the economy.

One conference topic with very little positive sentiment to boast of was that of cyber risk. According to the 2017 World Economic Forum's Global Risk Report, cybercrime ranked sixth among the top 10 risk concerns for executives across the world. With the recent surge in major cyber-attacks, organizations that fail to pay significantly more attention to cyber security do so at their own peril. The nature of cybercrime has changed drastically over the past decade with even nation states and multinationals actively perpetrating attacks through various organized cybercrime networks.

Besides the rise in orchestration of cybercrimes by well-resourced organizations, the form of attacks is rapidly expanding with new major business threats presented through Internet-of-Things innovations. As perpetrators such as nation states are better resourced and have better technological capabilities, businesses can barely keep up with cybersecurity innovations and defend themselves against constantly evolving forms of attack.

Looking in more detail at the South African context, the Ponemon Institute's 2017 Cost of Data Breach Study found that South African organizations are the most vulnerable to cyber-attacks compared to organizations in other countries. A major reason for this is poor capacity. Though cyber security skills programs in the country are oversubscribed, there is still a shortage of skills in the sector. As a result, businesses lack the necessary human capital to manage cyber-related risks.

The topic of regulatory compliance also received its time in the limelight at this year's event and, as demonstrated, for good reason. Thomson Reuters tracks about 750 different regulators globally. Between them, these regulators produce a regulatory update every seven minutes. This statistic marks how challenging complying with regulation and legislation has become in the last few years.

In South Africa, regulation is currently incredibly costly and can stifle business growth. According to the World Bank, it takes up to 56 days to register a business in South Africa compared to less than 10 days in Rwanda.

**South African  
bond issues  
are still  
oversubscribed by  
foreign funds to a  
surprising extent.**

As many analysts point to insufficient regulation as the major cause for the 2008 global financial crisis, regulation in the financial sector has become an increasingly serious issue. In South Africa's context, increasing regulation has largely had a negative impact on the financial sector from a financial inclusion perspective. On a global scale, analysts forecast that banks will have paid over US\$400 billion in fines between now and 2020 due to failure to comply with a rapidly changing regulatory environment.

Although regulation is burdensome for corporate South Africa, companies must not view compliance as the avoidance of penalties, but rather as an opportunity for proactive risk management. Regulation always has unintended consequences, but from a risk management point of view it is critical to mitigating various economic and business risks. ➤

Though cyber security skills programs in the country are oversubscribed, there is still a shortage of skills in the sector. As a result, businesses lack the necessary human capital to manage related risks.





Possibly the most important economic risk facing decision-makers in South Africa are the implications of the outcome of the ANC national elective conference in December 2017.

Possibly the most important economic risk facing decision-makers in South Africa are the implications of the outcome of the ANC national elective conference in December 2017. According to political analyst Justice Malala, however, the question was whether the elective conference would even take place.

As Malala explained, if the faction supporting President Jacob Zuma thought that there was a possibility that they may lose, they would disrupt the proceedings, delay the appointment of a leadership team, and finally install a compliant team of their own choosing.

There were concerns that KwaZulu-Natal (and possibly the Eastern Cape) would not be able to resolve their leadership disputes in time, and hence be excluded. If they had been excluded, Zuma's faction could have argued that the conference lacked credibility as two of the largest provinces were not represented and therefore the conference could not have gone ahead. Although Cyril Ramaphosa and Dr. Zweli Mkhize's supporters would have pushed for the conference to go ahead, there was approximately only a 60 percent probability of the conference happening.



There were three contenders in the ANC leadership race: Dr. Nkosazana Dlamini-Zuma, Cyril Ramaphosa and Dr. Zweli Mkhize. Ramaphosa, who emerged victorious from the conference, chose to keep quiet through numerous scandals involving President Zuma, allowing the status quo to continue and alienating many that had goodwill and faith in his leadership abilities. In 2017, Ramaphosa finally found his voice and began to speak out against the corruption he previously tacitly supported. In terms of policy, he supports the implementation of the National Development Plan. In the run-up to the conference, Ramaphosa was seen as the most business- and reform-friendly candidate.

Dlamini-Zuma's policy stance was centered on radical economic transformation and the expropriation of land without compensation. This also related to the question of ownership of the South African Reserve Bank. Dlamini-Zuma's policy stance closely mirrored what President Zuma articulated in the State of the Nation Address in February last year. Her greatest drawback was the support shown to her by the ANC Youth League and the Umkhonto we Sizwe Military Veterans Association

as this associated her campaign with the Zuma-Gupta faction.

Mkhize had been running a low-level campaign. However, he had delivered more speeches than any other candidate had. Although his campaign had been less forceful than Dlamini-Zuma and Ramaphosa's, it had been very thorough, astute, and professional. His policy stance was very closely aligned with that of Ramaphosa's.

Although Dlamini-Zuma's campaign seemed to be dead in the water in the weeks prior to the conference, there was the risk that her camp would use gatekeeping, corruption, cash bribery, and the forging of memberships to sway the election in her favor. If she had won, the status quo would have continued. Her victory would have increased the risk of the ANC as a party to split and actors such as Ramaphosa, Makhosi Khoza, and Pravin Gordhan to form a new party, resulting in the legal ANC and a new party claiming to be the "true" ANC.

Malala predicts the national election in 2019 will likely be a standoff between establishment and anti-establishment

politics. Had Dlamini-Zuma become the leader of the ANC, a coalition government after 2019 would have been very likely and would have resulted in horse-trading between parties. Ramaphosa's victory, however, makes the outcomes of 2019 much more difficult to predict.

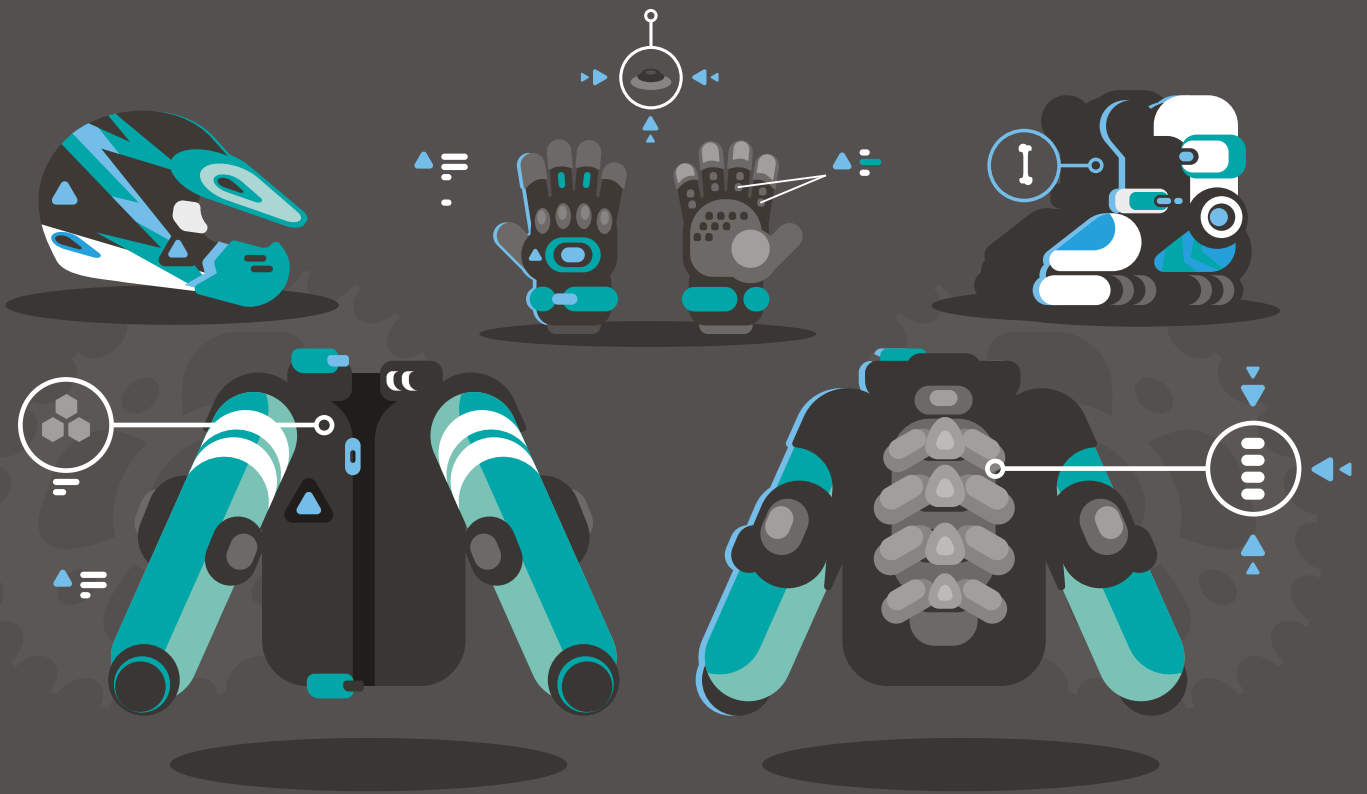
Despite the uncertainty currently facing the economy, one consistent message emerged from the Deloitte Risk Conference 2017—companies need to move away from short-termism and aspire to the long-term view. The importance of risk management should now be built into company strategies as lower growth and higher volatility further compound existing risks. Although mitigation of risks is costly, it provides companies with the opportunity to understand both their business and clients better and, hopefully, thrive for years to come. ●

# Global Risk Management Survey

**Edward Hida**

Partner  
Global Risk & Capital  
Management Leader  
Deloitte US

We are pleased to share with you a selection of key insights explored in Deloitte's Global Risk Management Survey, 10<sup>th</sup> edition. In this feature, we focus on the evolution of risk management, the role of the CRO, and board risk committees for discussion.



Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018k](http://www.deloitte.com/lu/InsideRisk2018k)

Printed with permission of Deloitte US



The years since the global financial crisis have seen a wave of regulatory change that increased both the scope and the stringency of regulatory requirements, and financial institutions have now had more time to understand the practical implications of these new regulations and what is required to comply.

Today, risk management is becoming increasingly important; financial institutions confront a variety of trends that have introduced greater uncertainty than before as regards the future direction of the business and regulatory environment. Economic conditions in many countries continue to be weak, with historically low interest rates.

The continual increase in regulatory requirements may abate or even be reversed in the near term as President Trump, the US Congress, and others have questioned whether regulatory oversight has gone too far. Strategic risk is increasing as entrepreneurial FinTech players are competing with traditional firms in many sectors. The rapidly changing environment suggests that risk management programs may need to increase their ability to anticipate and respond flexibly to new regulatory and business developments and to emerging risks, for example, by employing predictive analytics tools.

Deloitte's Global Risk Management Survey assesses the industry's risk management practices and the challenges it faces in this turbulent period. The 10<sup>th</sup> survey was conducted in the second half of 2016—after the Brexit vote in the United Kingdom but before the US presidential election—and includes responses from 77 financial services institutions around the world that conduct business in a range of financial sections and have aggregate assets of US\$13.6 trillion.

**The evolution of Risk Management**

Over the 20 years that Deloitte has been conducting its global risk management survey series, the financial services industry has become more complex, with the evolution of financial sectors, the increased size of financial institutions, the global interconnectedness of firms, and the introduction of new products and services. At the same time, regulatory requirements and expectations for risk management have broadened to cover a wider range of issues and also become more stringent, especially in the years since the global financial crisis. Deloitte's survey series has assessed how institutions have responded to these developments, the substantial progress that has occurred in the maturity of risk management programs, and their challenges. In general, over this period, risk management programs have become almost universally adopted, and now programs have expanded capabilities. Boards of directors are more involved in risk management and more institutions employ someone in a senior-level CRO position. The following are some of the key areas where the survey series has documented increasing maturity in risk management programs.

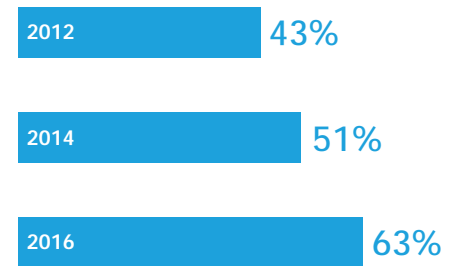
• **More active board oversight**

In 2016, 93 percent of respondents said their board of directors reviews and approves the overall risk management policy or ERM framework, an increase from 81 percent in 2012.

• **More use of board risk committees**

It is a regulatory expectation that boards of directors establish a risk committee with primary responsibility for risk oversight. The use of a board risk committee has become more widespread, although there is clearly room for further adoption (Figure 1). ➔

**Figure 1: Percentage of institutions placing primary responsibility for risk management at the level of the board of directors with a board risk committee**



Source: GMRS survey 10<sup>th</sup> edition

The rapidly changing environment suggests that risk management programs may need to increase their ability to anticipate and respond flexibly to new regulatory and business developments and to emerging risks, for example, by employing predictive analytics tools.

**• Increased adoption of a CRO position**

Over the years, there has been a continual increase in the percentage of institutions with a CRO position or equivalent. As of 2016, the position has become almost universal (Figure 2). At the same time, the CRO is now a more senior-level position reporting to higher levels of the organization. Similarly, the CRO more often directly reports to the board of directors—at 52 percent of institutions in 2016, up from 32 percent in 2002. Furthermore, 77 percent of institutions reported that the CRO is a member of the executive management committee, an increase from 58 percent in 2010.

**• Wider set of responsibilities for the CRO**

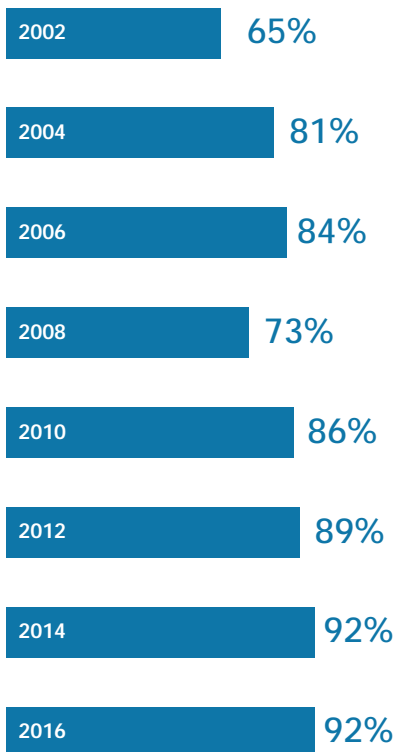
Over time, the CRO and the independent risk management program have been given a wider set of responsibilities at many institutions. For example, in 2016, 92 percent of respondents said that one of the responsibilities of the CRO was to assist in developing and documenting the enterprise-level risk appetite statement, compared with 72 percent in 2008. Similarly, 76 percent said that the CRO was responsible for assessing capital adequacy, while this was the case at 54 percent of the institutions in 2006.

**• Widespread adoption of an ERM program**

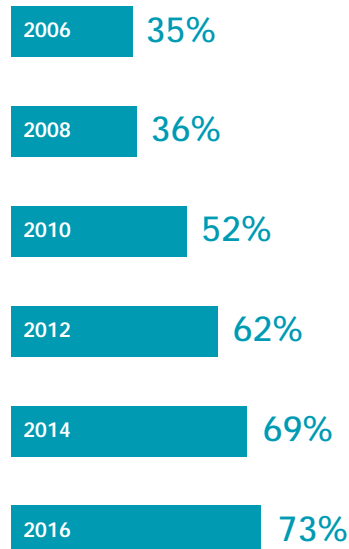
The adoption of ERM programs has more than doubled, from 35 percent in 2006 to 73 percent in 2016 (Figure 3). The implementation of ERM programs moved upward in 2010, which was likely in response to the post-financial crisis focus on enhancing risk management.

While there has been considerable progress in the continued development and maturation of risk management programs, there remains considerable work to do.

**Figure 2: Percentage of institutions with a CRO or equivalent**



**Figure 3: Percentage of institutions with an ERM program in place**



The survey found that the trend toward independent directors on board risk committees has become pronounced.

Source: GMRS survey 10<sup>th</sup> edition

### Board Risk Committees

Placing oversight responsibility for risk management with a board risk committee is a general regulatory expectation and has come to be seen as a leading practice. The Basel Committee issued guidance in 2010 that stressed the importance of a board-level risk committee, especially for large banks and internationally active banks, and revised guidance in 2015 specifying the appropriate role of the risk committee<sup>1</sup> Similarly, the enhanced prudential standards (EPS) issued by the Federal Reserve establish certain requirements for US banks to have a risk committee of the board of directors, with some requirements phased in based on the size of the institution.

Sixty-three percent of institutions reported that they have a risk committee of the board of directors with primary responsibility for risk oversight, up from 51 percent in 2014. As a result of the ascendance of the board risk committee, only 16 percent said the full board has primary responsibility, down from 23 percent in the prior survey.

Placing primary responsibility in a board risk committee is much more common in the United States and Canada (89 percent) than in Europe (65 percent), Asia Pacific (52 percent), or Latin America (63 percent). This may be a response to the requirements of the Federal Reserve's EPS and the Office of the Comptroller of the Currency's (OCC) heightened standards regarding board risk committees.

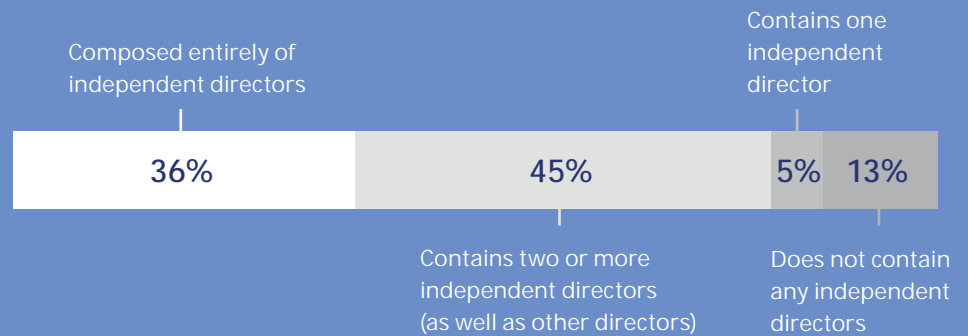
A prominent role for board risk committees is more common at banks (74 percent compared to 56 percent in 2014), although it also rose at investment management firms (65 percent up from 44 percent) and insurers (61 percent up from 49 percent).

As noted, there has been a trend for regulators to require that financial institutions include independent directors on their board risk committees. The Federal Reserve's EPS requires that the risk committee include at least one

independent director, while the US OCC regulations increased the required number to two independent directors.

The survey found that the trend toward independent directors on board risk committees has become pronounced. Forty-five percent of institutions reported that their board risk committee includes two or more independent directors (as well as other directors), while 36 percent said it is composed entirely of independent directors (Figure 4). ➔

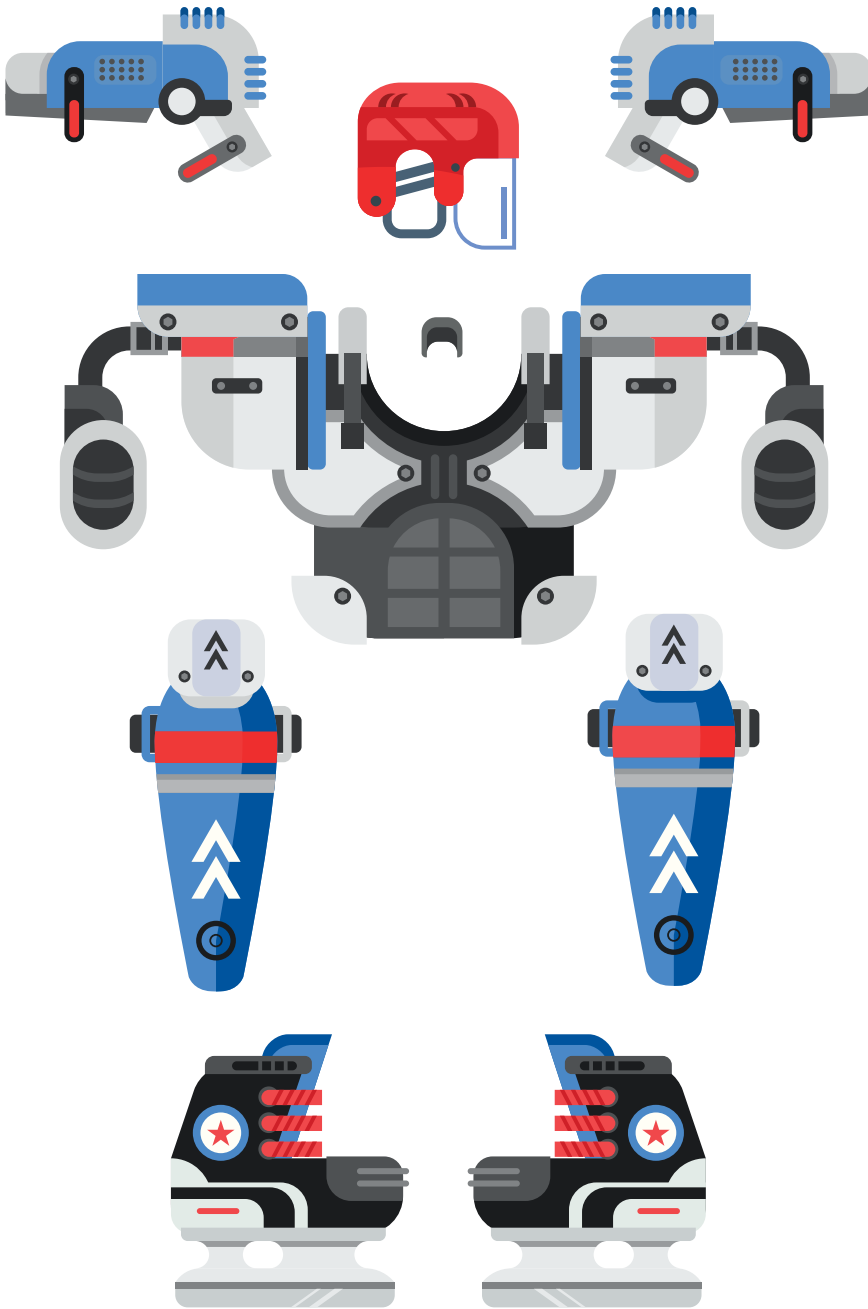
**Figure 4: Which one of the following accurately describes the membership of independent directors on your board risk committee or the equivalent committee(s) responsible for overseeing risk management?**



Note: Percentages may not total due to rounding  
Source: GMRS survey 10th edition



1. Basel Committee on Banking Supervision, Principles for enhancing corporate governance, October 2010, <http://www.bis.org/publ/bcbs176.pdf>; Basel Committee on Banking Supervision, Guidelines: Corporate governance principles for banks, July 2015.



Having the risk committee chaired by an independent director and having the participation of a risk management expert are becoming regulatory expectations for larger institutions. Many institutions find that in practice it is easier to have independent directors as members of their risk committee, or even for their risk committee to be chaired by an independent director, than to secure the participation of an identified risk management expert. Seventy-two percent of institutions reported that their board risk committee is chaired by an independent director, while 67 percent have a risk management expert on their committee.

Having an identified risk management expert is most common in the United States and Canada (78 percent), Asia Pacific (72 percent), and Latin America (86 percent), whereas it is less common in Europe (52 percent). One reason for the lower prevalence in Europe is that European regulations contain a more general requirement that risk committee members "...shall have appropriate knowledge, skills, and expertise to fully understand and monitor the risk strategy and the risk appetite of the institution."<sup>2</sup>

### Role of the CRO

Having an independent risk management function headed by a CRO is a regulatory expectation. The Basel Committee guidance on governance recommends that large banks and internationally active banks have a risk management function and a CRO position with "sufficient authority, stature, independence, resources, and access to the board."<sup>3</sup>

Adoption of a CRO position is almost universal, with 92 percent of institutions reporting that they have a CRO or equivalent position. The CRO position is more common at institutions in the United States/Canada (89 percent) and Europe (92 percent) than in Asia Pacific (73 percent) or Latin America (63 percent).

2. Official journal of the European Union, "Directive 2013/36/EU of the European Parliament and of the Council, Article 76," 26 June 2013, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:EN:PDF>.

3. Basel Committee on Banking Supervision, Principles for enhancing corporate governance.

There are significant benefits, and a general regulatory expectation, for the CRO to report directly to the board of directors as well as to the CEO, but this is not the case at many institutions. The CRO reports to the board of directors at 52 percent of the institutions surveyed, up slightly from 48 percent in 2014. Further, the CRO reports to the CEO at 75 percent of institutions, meaning that at one quarter of the institutions the CRO does not report to the most senior management executive in the organization. It appears that many institutions have more work to do to improve the reporting structure for their CRO.

At 90 percent of surveyed institutions, the CRO regularly meets with the board of directors or board committees responsible for risk management, although fewer (53 percent) reported that their CRO meets in executive sessions with the board. Affording the CRO the opportunity to meet with the board of directors or the board risk committee without the CEO or other members of senior management present can provide the board with an opportunity to receive a frank assessment of the state of the risk management program and the specific challenges the institution faces.

It is a leading practice for the CRO to be the most senior management position responsible for the risk management program, but the CRO does not universally have this role. Only 48 percent of institutions reported that the CRO or equivalent is the highest level of management responsible for the risk management program, similar to the percentage in 2014. Other common responses were the CEO (27 percent), the executive-level risk committee (16 percent), or the CFO (4 percent). Assigning primary responsibility for risk management to the CRO is more common among institutions in the United States and Canada (78 percent) than in Europe (50 percent), Asia Pacific (38 percent), or Latin America (25 percent).

Institutions assign a broad range of responsibilities to the firm-wide, independent risk management group headed by the CRO. Many oversight

Many institutions find that in practice it is easier to have independent directors as members of their risk committee, or even for their risk committee to be chaired by an independent director, than to secure the participation of an identified risk management expert.

activities were nearly universal, including developing and implementing the risk management framework, methodologies, standards, policies, and limits (94 percent), identifying new and emerging risks (94 percent), and developing risk information reporting mechanisms (94 percent).

However, a number of other important oversight activities are in place at no more than two-thirds of institutions, including providing input on business strategy development and the periodic assessment of the plan (65 percent) and participating in day-to-day business decisions that affect the risk profile (63 percent). Risk management considerations need to be infused into both strategy and business decisions so that risk implications can be assessed, and more progress still needs to be made in these areas.

Another area that a relatively low percentage of respondents said was a responsibility of the risk management program was approving new business or products (58 percent). This may be partly explained by the fact that relatively few new products are being introduced in the current economic and regulatory environment.

Finally, regulators and industry leaders have devoted considerable attention to the role that incentive compensation and culture play in risk management, yet the activity of reviewing the compensation plan to assess its impact on the risk appetite and culture was identified as a responsibility by just 54 percent of respondents. This was more often a risk management responsibility at institutions in the United States and Canada (75 percent) and Europe (62 percent) than in Asia Pacific (38 percent) and Latin America (43 percent).

## Conclusion

With the future direction of risk management more uncertain than it has been for years, perhaps the most important lesson is that many risk management programs should become nimbler. In the coming years, risk management programs should focus not only on being effective and efficient, but equally on acquiring the agility to respond flexibly to a new set of demands on risk management. ●


# The future of risk in financial services

**Edward Hida**  
Partner  
Global Risk & Capital  
Management Leader  
Deloitte US

**Julian Leake**  
Partner  
Risk Advisory  
Deloitte UK

Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018](http://www.deloitte.com/lu/InsideRisk2018)

Printed with permission of Deloitte US, UK

A digital network dome, composed of glowing white nodes and connecting lines, arches over a silhouette of a mountain range. The background is a sunset sky with warm orange and red tones. The dome's structure is semi-transparent, allowing the sun and mountains to be seen through it.

**The future of risk management will likely look dramatically different than the current risk capabilities many are familiar with. Business units will have clear ownership of the risks that they take. Conduct and culture management will be pervasive throughout the organization. The role of the risk management function will also be clear, consisting of oversight and challenge. The risk function itself will be streamlined and much slimmer with a rationalized risk infrastructure. It will use location and delivery models for cost optimization and leverage the power of digital tools for both efficiency and effectiveness.**

The digital tools will include cognitive agents scanning a wide range of signals in the internal and external environment to identify new risks, emerging threats, and potential bad actors. These digital tools could not only strengthen the risk function but also provide the business and strategic execution with additional insight. Big data analytics will be used to provide deeper insight into the interactions of risks and causal factors. Robotics and process optimization will restructure and automate processes; it will dramatically reduce operational risk and improve risk management quality, including the review of conduct and culture risks.

Automated risk triage will continuously take place to elevate the risk analysis for assessment and treatment in the event of more significant risk issues. Insofar as reports are needed to summarize the risk activity, natural language generation techniques will be applied to prepare draft reports, with risk analysts only required to perform reviews and selected input tasks. >



### Developments in risk management

Over the past two decades, risk management has gone through several distinct phases:



Yet risk management has now reached an inflection point, presenting financial institutions with a fresh set of demands.



### Risk management enters a new era

Today's environment presents risk management with a unique set of demands. Slower economic growth and declining margins have placed a premium on increasing the efficiency and reducing the cost of risk management. These developments are all characterized by a heightened level of volatility and uncertainty in the business, geopolitical, and regulatory environment. The responsibilities of the business and risk management are not clearly defined. A legacy risk technology infrastructure and the difficulty in gaining access to timely, accurate, and aggregated risk data create complexity and additional costs. Institutions will need to make sure risk management plays an active part in setting strategy; they need to leverage the new technologies available to substantially reduce costs by automating repetitive manual activities, while simultaneously improving monitoring and response.

To move forward, institutions should ask themselves the following questions:

#### Is risk management doing the right things?

- Is there a clear definition of the activities and services it should perform according to its core mandate and regulatory requirements vs those performed by the lines of business?
- Is the function able to plan, assess, and manage increased demands from regulators and the business?
- Should other additional activities and services be performed?
- Is there an appetite to provide increased transparency for the function?

#### How should risk management be organized to deliver effectively?

- What is the optimal organizational structure for risk management?
- Is the resourcing structure optimized between the lines of defense and business units?

- Are there efficiencies that can be achieved through shared services of centers of excellence for some risk capabilities?
- Should lower cost locations or outsourcing be considered for some capabilities?

#### How can transformation be made through digitization and ecosystems?

- Application of robotics to reduce manual processes, human resource requirements, and improve central environment
- Application of cognitive intelligence to provide better automated decision support and data filtering (e.g., credit underwriting, surveillance)
- Increase use of Big Data, advanced analytics, and visualization for better data management and decision support
- Partner with external ecosystems (collaboration of different firms working together) to transform, innovate, and provide core CRO services

Today, risk management is at a crossroads. Financial institutions need to decide whether they will continue with business as usual or fundamentally rethink their approach to risk management.

The new environment provides strong incentives for financial institutions to transform how they manage risk to become substantially more effective and efficient. This will require institutions to seize opportunities related to strategy, people, technology, and the three lines of defense model in a coordinated way. Institutions will need to embrace emerging technologies—such as robotic process automation, artificial/cognitive intelligence, natural language processing, and machine learning—that can reduce costs, while also offering foresight into emerging risk issues. ➤

Institutions will need to make sure risk management plays an active part in setting strategy; they need to leverage the new technologies available to substantially reduce costs by automating repetitive manual activities, while simultaneously improving monitoring and response.

## Six imperatives



### Increase focus on strategic risk

Strategic risk will demand more attention from senior executives, supported by an improved ability to identify strategic risks and analyze their potential impact on the organization. These improved capabilities can not only help the institution manage strategic risk, but they will also provide insights to help the institution achieve its strategic goals and objectives.



### Rethink the three lines of defense and risk alignment

Institutions should consider restructuring and eliminating overlapping responsibilities across the three lines of defense. In particular, they should ensure that business units take full ownership of the risks in their area, while the risk management function focuses on its risk control role through oversight and challenge.



### Do more with less

In addition to traditional process reengineering, substantial efficiency improvements can be achieved by leveraging RegTech solutions. Deeper and more sustainable cost efficiency and improved return-on-investment performance can be realized by leveraging new capabilities, such as using business decision modeling to assess the cost of change, cost mutualization, and cloud-based services, such as Platform-as-a-Service.



### Establish a formal conduct and culture program

Recent instances of inappropriate behavior by employees at financial institutions have led to an increased focus by senior management and regulatory authorities on the importance of instilling a risk-aware culture and encouraging ethical behavior.



### Enhance risk management capabilities

Institutions will need to integrate their siloed responses to the many regulatory requirements that have been introduced in recent years. At the same time, they will need to leverage the power of RegTech solutions to increase their agility in responding quickly to new developments, while providing the analytics that support more effective risk management.



### Strategically manage capital and liquidity

Recent regulatory requirements have significantly increased capital and liquidity requirements; institutions will need to carefully consider the impacts of their business strategy on capital and liquidity so they can improve their returns on equity by optimizing the use of these scarce resources.

Institutions should address these six imperatives in a coordinated program so that they do not work at cross-purposes on individual initiatives. An integrated risk and regulatory change portfolio management approach will be required to advance simplification and modernization efforts, while making sure that underlying capabilities are not compromised.

The six imperatives for risk management previously outlined affect almost every part of an institution. The drive to transform and modernize risk management will need to be based on the following four foundational areas.

**Levers to drive change**



**Infuse risk management into strategy**

Risk management should play an active part in setting the institution's business objectives and strategic plan, and assessing the impact of new products and markets on the organization's risk profile and on its capital and liquidity position.



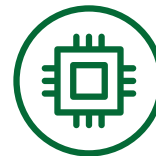
**Focus on people**

Institutions should work to ensure they have sufficient specialists with subject matter expertise on high-risk and complex activities and provide adequate training to continually upgrade skills. Risk practitioners across all three lines of defense need to work more closely with senior leadership to drive cultural changes across the organization that encourage constructive challenge, ethical decision-making, appropriate incentives, openness, and transparency.



**Enhance the three lines of defense**

Institutions should clearly define the risk management responsibilities of each line of defense, streamline the governance structure by eliminating overlapping responsibilities, and ensure that business units take full ownership of the risks in their areas.



**Leverage emerging technologies**

The latest technologies have the potential to fundamentally transform risk management. In addition to substantially reducing operating costs, these and other technologies can provide risk management with new capabilities, including building controls directly into processes, prioritizing areas for testing and monitoring, deploying automated monitoring of limits with defined escalation, addressing issues in real-time to improve the enterprise-wide view of risk, and providing decision support.

These levers should not be addressed in isolation, but instead need to be pulled in a coordinated way. For example, the business strategy established will have significant implications for the potential for conduct risk, while the responsibilities assigned to business units will determine the types of risk management skills they require. An overall risk management approach needs to be developed that harmonizes the steps taken to address each of the four levers and considers their interaction. >

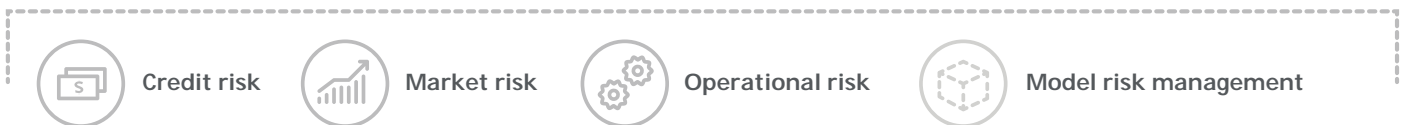
**Firms can get started by identifying key processes in their risk lifecycle for assessing the impact of the future of risk change levers**



**Risk management lifecycle**



**Illustrative risk stripes**



**Example automation opportunities**

1. Risk identification
2. Credit rating/scoring
3. Product pricing
4. Product P&L attribution
5. Limit setting & review
6. Vendor risk management
7. Counterparty/Product/Position risk exposure
8. Limit management
9. Collateral management
10. Automated risk monitoring
11. Compliance testing
12. Loan review
13. Model validation documentation
14. Risk reporting
15. Model governance and reporting

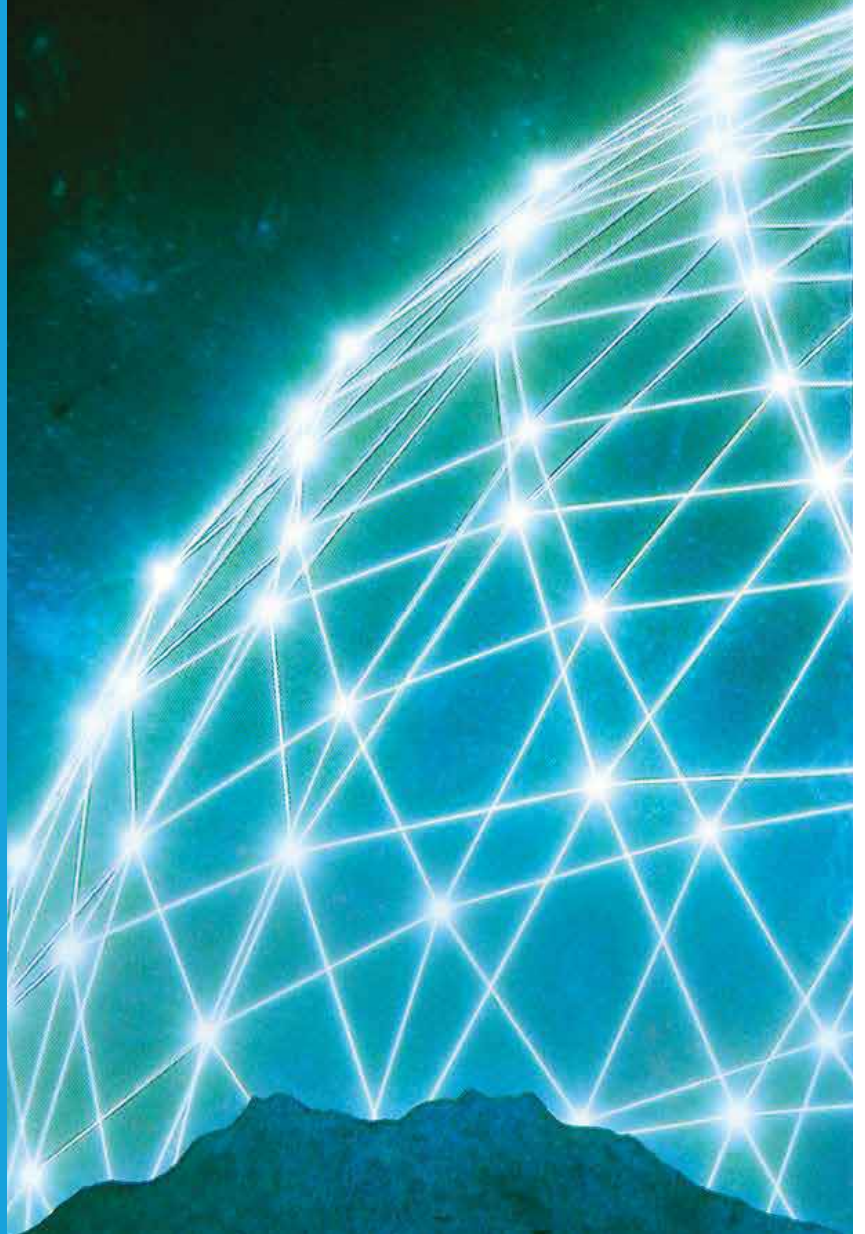
## Conclusion

In today's environment of volatility and uncertainty, risk management is at an inflection point. Will financial institutions continue with their traditional methods or instead fundamentally rethink how risk is managed? Institutions content with their existing approach will suffer from inefficient processes, will lack the capability to proactively identify and manage risks, and will struggle to gain a holistic view of the risks facing the organization.

Institutions that instead fundamentally transform how they manage risk can become more dynamic and capable of responding quickly to new developments. In the new era, the risk management function will need to:

- Play a greater role in the organization's strategic decision-making
- Expand risk management capabilities through all three lines of defense
- Secure talent with the right risk management skills and business experience to effectively manage risk
- Be agile to react quickly to the unexpected developments inevitably arising in today's uncertain environment
- Leverage emerging technologies to create a new digital environment able to substantially reduce costs while simultaneously improving the ability to proactively identify and manage risks, and do so at a lower cost

Each institution will need to decide whether to continue with business as usual, thereby running the risk of being unprepared for new risks, trailing their peers, and falling short of regulatory expectations, or to seize the opportunity to take risk management to an entirely new level that truly provides the capabilities to support the organization's strategic plan. ●



# You and I were meant to fly

# The rise of managed services

## Hugo Morris

Partner  
Managed Risk Services  
Deloitte UK

## Mark Whitehead

Director  
UK Risk Advisory  
Deloitte UK

## Kseniia Jones

Senior Manager  
Global Risk Advisory  
Deloitte UK

## Ian Chance

Senior Manager  
Global Financial  
Services Industry  
Deloitte UK

As financial institutions navigate today's unpredictable economic and regulatory landscape, the pressure on risk and compliance operating models has never been greater. Adoption of managed services is rising as firms seek a more strategic response in order to better organize, operate, and safeguard their business. Given that the adoption of managed services entails the transfer of a higher degree of control to a third party, determining when and how to adopt them is key. Get it right, and the potential rewards are significant. ➔

Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018m](http://www.deloitte.com/lu/InsideRisk2018m)

Printed with permission of Deloitte UK



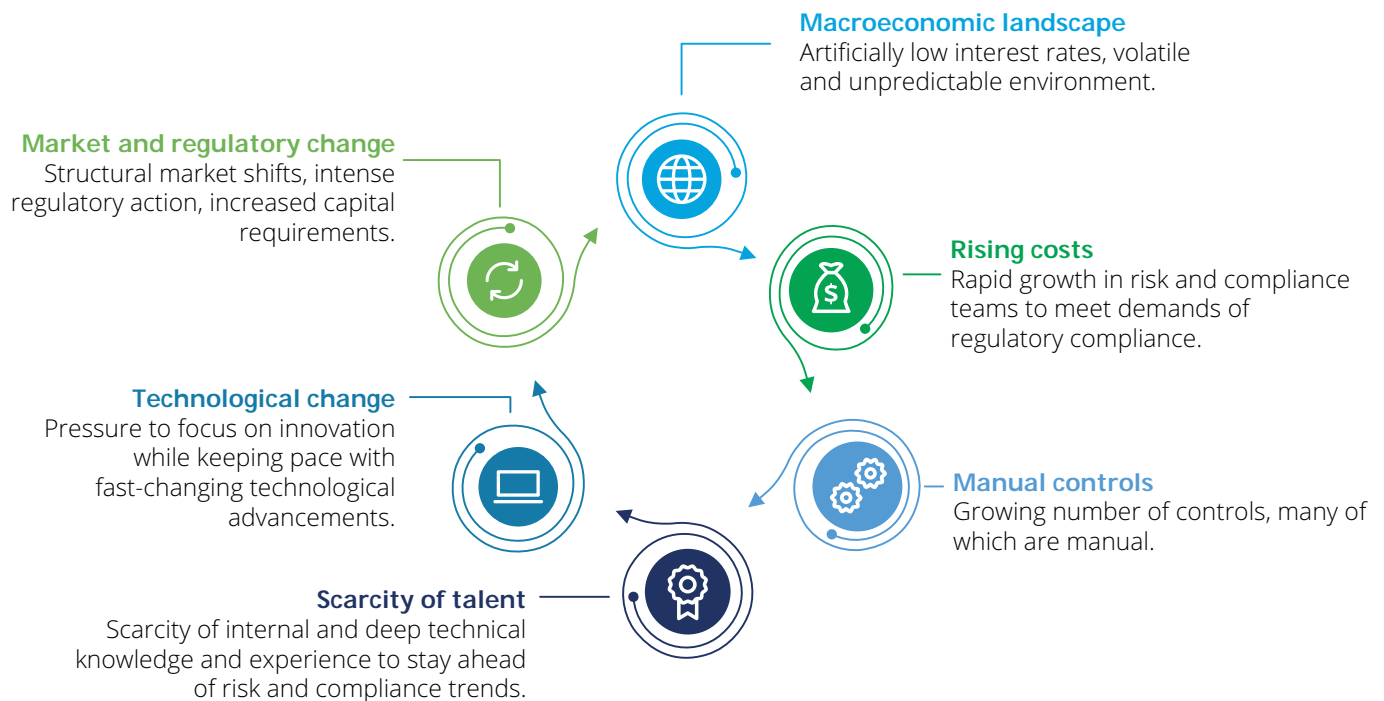


Since the financial crash of 2007-2008, business models have faced extreme pressure from market, regulatory, and macroeconomic forces. As firms have felt the burn on revenue, cost, and capital, the focus on operational efficiency and effectiveness has sharpened.

Risk and compliance functions are by no means immune given soaring costs to meet the demands of regulatory compliance. According to Citigroup, the cost is US\$270 billion annually—10 percent of the operating cost—across the banking industry.<sup>1</sup> Much of this is due to a doubling of the size of compliance and regulatory teams in many of the biggest global banks,<sup>2</sup> a trend replicated across financial services.

These resources are often tied up managing manual internal control processes, thus limiting their availability to address pressing risk and compliance trends. Many processes are supported by legacy systems beset by under-investment as firms move to a “one-system” strategy. Although new technologies such as automation and artificial intelligence could transform services, building in-house capabilities can be slow and commercially unviable. Finding people with the necessary skills and experience is just as hard.

**External and internal forces driving firms to consider new operating models**





### Refocusing attention where it counts

Banks and other financial institutions are increasingly turning to managed services to address these challenges and to enable them to refocus their time and skills on activities of the most value to their business.<sup>3</sup> Market analysis indicates the global managed services market is expected to grow to US\$229 billion by 2020.<sup>4</sup> Risk and Compliance are on a similar trajectory, as we see more Chief Risk and Compliance Officers turn to managed services to proactively limit enterprise risk and strengthen compliance.

### What is a managed service?

In a managed services model, a strategic partner takes on, transforms, and runs business operations and processes to improve operational quality and efficiency on a long-term basis. It works particularly well for processes, people, and locations that are increasingly expensive to maintain and are not competitive differentiators. Within Risk and Compliance, the areas gaining most value from the managed service model range from third-party risk management and software asset management, to a range of cyber services, model risk management, and regulatory reporting.

### More than a cost reduction exercise

The long-term, tightly integrated nature of a managed services partnership offers substantial strategic benefit in addition to cost reduction. In our experience, risk and compliance leaders are looking to transform business critical risk processes, taking advantage of scalable, innovative technology and expertise too expensive and time-consuming to build in-house, while also benefiting from predictable, outcome-based pricing, and reduced exposure to financial risk. ➔



1. Martin Arnold, "Banks' AI plans threaten thousands of jobs," Financial Times, 25 January 2017
2. Ibid
3. Deloitte University Press, "Managed Services: a catalyst for transformation in banking"
4. Statista.com, "Managed Services market size worldwide 2014-2020"

## Benefits of managed services



Accessing a scalable, global third-party delivery infrastructure on a pay-per-use basis enables the bank to increase domicile and investment country coverage and increase volume without additional investment.



### Growing adoption across Risk and Compliance

We are seeing institutions across financial services explore how they can realize these benefits within the Risk and Compliance functions. In one recent case study, a global bank deployed a managed services solution to reduce the cost of client tax reclaims and tax reporting while also improving service coverage and scalability. Given the nature of the service, it was critical for the bank to remain the “face” of the service to their clients, maintaining client data confidentiality, and a high level of service quality. The managed service achieves all these aims. Both running costs and annual maintenance costs are significantly reduced, by more than 30 percent and 100 percent respectively. Accessing a scalable, global third-party delivery infrastructure on a pay-per-use basis enables the bank to increase domicile and investment country coverage

and increase volume without additional investment. As the white-labelled service meets rigorous compliance and quality assurance standards, it also ensures the bank continues to deliver a seamless, high-quality service to its clients.

Another recent example saw a US bank needing a more effective way to address new lease accounting and reporting standards, ASC842 and IFRS16, which require all lease transactions and financial disclosures to be captured on the balance sheet by January 2019. Like many other companies, the bank relied on mostly manual processes to manage this data, and initially focused on software solutions such as SAP ERP to achieve compliance. However, after realizing technology alone could not support the adherence and compliance requirements, the bank turned to a managed services solution designed to both meet the regulatory priority and

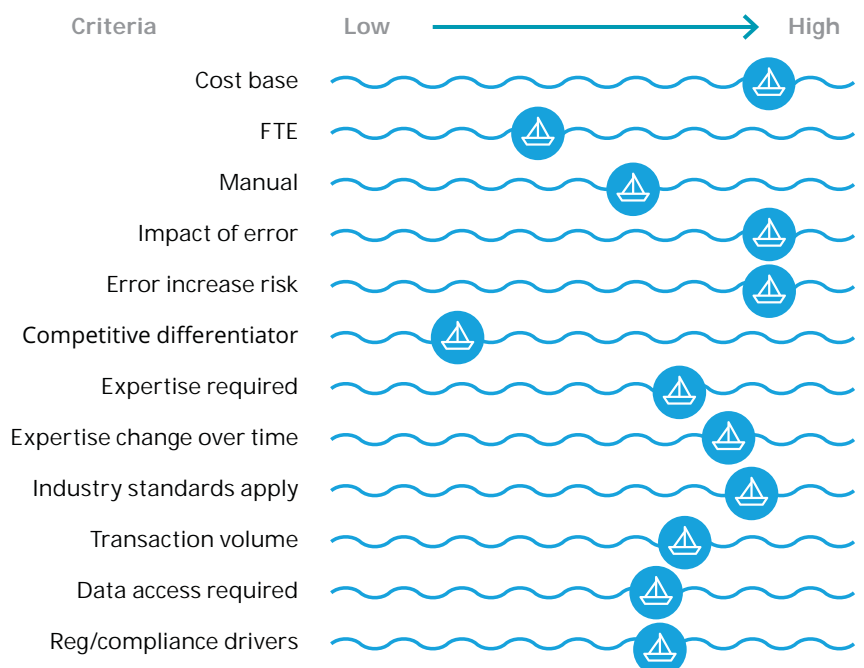
deliver wider long-term benefits. With the solution in place, the bank benefits from a re-engineered lease accounting and reporting model driving faster, more accurate processes, and improved confidence in compliance through access to trained staff, ongoing support, and high-quality, audit-ready monthly reporting packages. The total cost of ownership is also lower, and outcome-based pricing gives the bank the flexibility to scale up or down to meet current and future reporting commitments, as well as compliance mandates. ➔



Determining the best fit sourcing model  
 With the variety of sourcing models on the table, how firms determine which fits a particular operation or process is critical. We believe the interplay of 12 criteria determines the suitability of a particular process for insourcing, outsourcing, or a managed service.

Typically, a managed service is most applicable when failure poses a high enterprise risk, when the need for expertise is urgent, specialized, and evolving quickly, and when competitive differentiation is low. In these scenarios, the costs and challenges of building a cutting-edge function in-house may not pay off through market differentiation, while the transactional, shorter-term nature of traditional outsourcing models represents too high a risk.

**Profiling a process or operation suitable for managed services**



Let's consider the example of model risk management.

The number of models relied on by banks and other large institutions is rising fast—by 10-25 percent annually according to McKinsey.<sup>5</sup> These models support ever-expanding areas of decision-making with increasing sophistication, enabled by technology developments, such as automation and Big Data analytics. Global regulation is also increasing, as the US SR11/7 standard becomes the “de-facto” benchmark for model risk management functions on both sides of the Atlantic. These factors mean managing the risk of defective or misused models is increasingly important, complex, and expensive. In addition, workload peaks and troughs are putting more pressure on specialized skills that can be hard to source and maintain in line with the latest intelligence. While risk models can certainly provide competitive differentiation for a firm, a standardized model validation process does not. Therefore, model risk management fits the profile for managed services—increasing cost, high enterprise risk, low competitive differentiation, and scarce talent.

By leveraging a strategic partner's specialist, multi-faceted technology, processes, and expertise to run all or part of the function, a firm can deliver the complexity and volume of firm-wide modelling more efficiently. This frees up the in-house workforce to focus on the higher value tasks of decision-making and independent challenge through monitoring, reporting, validation, and governance. In addition, the partner's knowledge of industry-leading practices and regulatory expectations improves confidence in production models by normalizing them against best practice and global regulations. Operational costs also benefit from the scale efficiencies of a global “around-the-clock” utility service, and from more predictable pricing based on outcomes.

### Implementing managed services successfully

Clearly, the transfer of more business critical operations to a third party requires careful management under the watchful eye of regulators. Four aspects are particularly key to successful implementation:

#### Choice of managed service provider

Although cost inevitably plays a role when choosing a teammate, to realize the long-term innovation, talent, and quality benefits of managed services requires a stronger focus on strategic fit, and on a provider's level of investment, global consistency, and domain and regulatory maturity.

#### Transition approach

Given that managed services may move control of a process externally for the first time, the right approach to transition—whether it be parallel runs, staggered transitions, or piloting—is critical to ensuring adequate safeguards and oversight are maintained through the process.

#### Vendor management

Introducing a long-term partnership model will require enhanced governance procedures for many vendor management functions. New procedures will ensure partners have the capability to meet required outcomes, both at the point of selection and throughout the subsequent delivery of services. Clear dispute resolution mechanisms and decision-making accountability will further aid robust vendor risk management.

#### Stakeholder management

As one would expect when adopting a new operating model that transfers a greater degree of control to a third party, how the concerns of stakeholders such as regulators, investors, and employees are managed will be critical to a smooth and timely implementation, and to realization of the desired benefits.

### A path forward through an uncertain future

Looking ahead, the forces driving institutions to adopt the next evolution of outsourcing are unlikely to weaken their pull. Risk and compliance leaders will continue to feel pressure to cut costs and improve the effectiveness of processes from cybersecurity to reporting, remediation, and legal advice, all while responding to regulatory expectations and delivering against core business priorities. For the firms responding by adopting a managed services model, the potential rewards are significant. In addition to cost efficiency, scalable access to the latest technologies, expertise, and knowledge is already improving outcomes across a wide spectrum of critical risk, regulatory, cyber, legal, and compliance operations. As confidence in the model grows, we believe adoption will widen further, enabling firms across financial services to focus their precious resources and skills where it matters most—on driving growth and competitive advantage. ●

5. McKinsey & Company, “The Evolution of Model Risk Management,” February 2017

## What's next for bank board risk governance?

# Recalibrating to tackle new risk oversight expectations



**Scott Baret**

Partner  
Vice Chairman  
US Banking & Securities  
Leader  
Deloitte US

**Edward Hida**

Partner  
Global Risk & Capital  
Management Leader  
Deloitte US

Help us choose our Top 10 Topics for 2018  
[www.deloitte.com/lu/InsideRisk2018n](http://www.deloitte.com/lu/InsideRisk2018n)

Printed with permission of US

We are pleased to share key insights from the Deloitte Center for Financial Services (DCFS)'s fourth-in-a-series study on board risk governance. In this edition, we focused on how bank board risk committees are documenting their risk management governance<sup>1</sup> mandates in light of their evolving roles in managing information flow, holding senior management accountable, and ensuring that the risk management function maintains sufficient independence, among other key priorities. ➤



1. To view the full 22-page report, please visit our Deloitte Insights page at [dupress.deloitte.com/dup-us-en/industry/financial-services/bank-board-risk-governance-study.html](https://dupress.deloitte.com/dup-us-en/industry/financial-services/bank-board-risk-governance-study.html)

Ironically, the demand for more rigorous risk management protocols has emerged at a time when the pace at which new regulations are produced has slowed after a decade of continuous escalation, and when most banks appear to have mastered the large, post-crisis regulatory compliance items such as the US Federal Reserve (the Fed) Comprehensive Capital Analysis and Review process<sup>2</sup>.

In August 2017, the Fed proposed revisiting supervisory expectations of bank boards "to establish principles regarding effective boards of directors focused on the performance of a board's core responsibilities." The Fed's proposal delineates board member oversight responsibilities and management's obligations in new board effectiveness (BE) guidance, and follows the US Department of the Treasury's June 2017 recommendation of an interagency review of requirements imposed on banks' boards<sup>3</sup>.

In this context, the DCFS study is a timely addition to the current discussion around the role of boards at large banks. The renewed focus on the role of the board risk committee comes at a time when board members frequently find themselves being drawn "into the weeds" of risk management issues, and left with inadequate time to guide and challenge management on broader strategic issues.

### A sea change beckons

Since late 2014, when we last analyzed banks' board risk committee charters, many institutions have substantially expanded their compliance documentation procedures in response to expectations from the Federal Reserve's Enhanced Prudential Standards (EPS), the Office of the Comptroller of the Currency's (OCC) Heightened Standards, and the Basel Committee for Banking Supervision's (BCBS) guidelines on bank corporate governance.

However, despite significant progress, our analysis demonstrates that there is clearly much work to be done. Given a more complex and interconnected operating environment, boards must evaluate the interplay of risks resulting from the management's business strategies in order to probe risks to the bank management's business strategies.

Essentially, our study entails analyzing board risk committee charters. While these charters are a useful yardstick to measure the level and quality of risk management oversight of a board's risk committee, we acknowledge their limitations. That said, we see great value in our methodology as transparent, public, and comprehensive documentation is an essential first step to a board risk committee demonstrating its oversight accountability and intent.

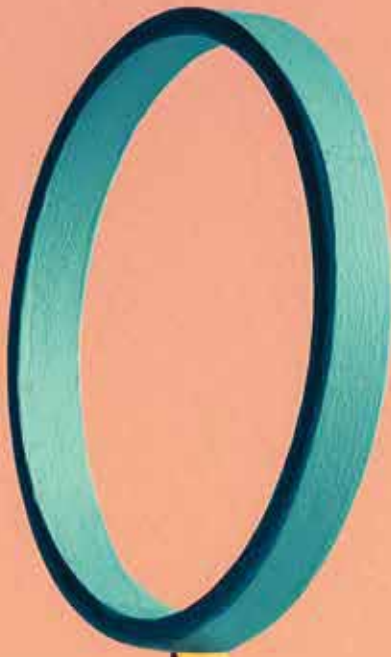
An effective board assesses whether the firm's significant policies, programs, and plans are consistent with the firm's strategy, risk tolerance, and risk management capacity.

2. "Federal Reserve releases results of Comprehensive Capital Analysis and Review (CCAR)," Board of Governors of the Federal Reserve System, 28 June 2017.

3. US Department of the Treasury, "A financial system that creates economic opportunities: Banks and credit unions," June 2017.







### **Analysis of 2016–2017 charters, and comparison to progress made since late 2014**

Because the Fed's August 2017 proposal for Board Effectiveness (BE) guidance coincided with our study, we decided to frame our results in relation to the five clear supervisory expectations that the proposal outlines<sup>4</sup>.

#### **01. Setting risk policies, overseeing the risk management and governance framework, and risk strategy and tolerance**

The Fed's first supervisory expectation outlines that "...the firm's strategy should clearly articulate objectives consistent with the firm's risk tolerance, and the risk tolerance should clearly specify the aggregate level and types of risks the board is willing to assume to achieve the firm's strategic objectives."<sup>5</sup> In terms of overseeing a firm's risk management framework, the Fed stipulates that "An effective board assesses whether the firm's significant policies, programs, and plans are consistent with the firm's strategy, risk tolerance, and risk management capacity prior to approving them."<sup>6</sup>

Our charter analysis revealed that compared to our charter analysis three years ago, boards have significantly improved their documentation on this front. Yet, this improvement was also expected given that the EPS had established these expectations shortly after our analysis of 2014 charters. And, in fact, in light of this US regulatory focus, the significant progress that non-US G-SIBs have made in mandating these fundamental policy issues is probably even more notable.

#### **02. Actively managing information flow, resources, capabilities, and committee discussions**

The Fed proposal noted that "...boards of large financial institutions face significant information flow challenges. Although boards have oversight responsibilities over senior management, they are inherently disadvantaged given their dependence on senior management for the quality and availability of information."<sup>7</sup>

Hence, it was encouraging to discover that most board risk committee charters mandate that committee members have unfettered access to resources, including access to internal executives and information, and the ability to obtain external legal or expert advice. However, managing information flow between the risk and compensation committees is still not commonly stated in charters. Also, we found it alarming that not one US bank risk committee charter mandated training for committee members. Interestingly, non-US G-SIBs are ahead of the game on this front, with nearly one in three charters mentioning training for committee members.



4. The Fed's proposed BE guidance describes effective boards as those which: (1) set clear, aligned, and consistent direction regarding the firm's strategy and risk tolerance; (2) actively manage information flow and board discussions; (3) hold senior management accountable; (4) support the independence and stature of independent risk management and internal audit; and (5) maintain an effective board composition and governance structure; "Supervisory expectations for the board of directors," Board of Governors of the Federal Reserve System.
5. "Supervisory expectations for the board of directors," Board of Governors of the Federal Reserve System.
6. Ibid.
7. Ibid.

### 03. Holding senior management accountable for overall risk management, and for specific emerging risk issues

The Fed's BE guidance is specific about the board ensuring that management is held accountable for its actions, and that it keep abreast of emerging risks: "An effective board engages in robust and active inquiry into, among other things, drivers, indicators, and trends related to current and emerging risks."<sup>8</sup>

Our analysis showed that committees appear to have increased the qualitative heft associated with such language in charters. Although not up to US standards yet, non-US G-SIBs have made notable improvements on both of these documented language criteria. However, there is still progress to be made as regards identifying emerging risks and risk management deficiencies, and oversight of management's remedial actions. Also, despite a significant increase from a low base, while half of US banks' board risk committee charters mentioned oversight of model risk, discussions of third-party and conduct risk (both issues that have led to billions in fines for many large banks across the world)<sup>9</sup> were surprisingly limited.

### 04. Supporting the independence and stature of the CRO, and risk management and compliance functions

There appears to be significant room for improvement regarding the board's role in elevating the stature and independence of the CRO, which the Fed's proposal also explicitly endorses: "An effective risk committee supports the stature and independence of the independent risk management function, including compliance, by communicating directly with the CRO on material risk management issues."<sup>10</sup> Although the charters of US bank risk committees generally mandated appointing and dismissing the CRO and ensuring that the CRO reports to both the committee and the CEO, only a few charters noted the committee's distinct role in terms of emphasizing the CRO's stature and authority within the institution. And only a little more than four in ten US bank charters include

language ensuring the independence of the risk management function overall. Furthermore, the committee's role in integrating controls with management goals and the compensation structure, another EPS mandate, was rarely mentioned explicitly. Hence, it was no surprise that few charters mirrored BCBS guidance that encouraged the risk committee to report on the state of risk culture at the bank.

### 05. Maintaining an effective board risk committee composition and structure

As the Fed's BE guidance notes, "An effective board has a composition, governance structure, and established practices that support governing the firm in light of its asset size, complexity, scope of operations, risk profile, and other changes that occur over time... An effective board is composed of directors with a diversity of skills, knowledge, experience, and perspectives."<sup>11</sup>

Eight years since we began these charter analyses, almost every bank now has a dedicated risk committee, and most also have detailed charters or the equivalent. Of course, regulatory requirements and guidance played a defining role in this transition. However, what has also developed during this period is a wider gulf between the documented compositions of the risk committees of US banks versus those of non-US G-SIBs, which seem to rarely require the inclusion of a risk expert. And while the majority of US banks now insist that a majority (or, in some cases, all) of the members of the risk committee be independent, this is still not the case for non-US G-SIBs. ➔

8. Ibid.

9. Gavin Finch, "World's biggest banks fined \$321 billion since financial crisis," Bloomberg, 2 March 2017.

10. "Supervisory expectations for the board of directors," Board of Governors of the Federal Reserve System.

11. Ibid.





An effective risk committee supports the stature and independence of the independent risk management function, including compliance, by communicating directly with the CRO on material risk management issues.

## Raising governance standards to navigate choppy seas

Now that we have analyzed our results in relation to the five supervisory expectations of the recent Fed BE proposal, we follow with analysis of how the risk committee mandates mesh with the six priorities of risk management in financial services firms as they look forward to 2018 and beyond.<sup>12</sup>

### 01. Present an effective challenge to the focus on strategic risk

Many institutions have established strategic risk working groups or centers of excellence that are owned by the CRO or the chief strategy officer (CSO) to proactively prepare for strategic threats.<sup>13</sup> The Fed, in addressing the governance side of the coin, notes that effective bank boards “set clear, aligned, and consistent direction regarding the firm’s strategy and risk tolerance.”<sup>14</sup> As we noted earlier, committees should look beyond metrics to evaluate why a strategy is working, probe what a failure would look like, and apply their analysis to the type and amount of enterprise risk appetite and risk management policies the institution should assume.

### 02. Oversee the rethinking of the three lines of defense

The delineation of risk control intended by the three lines of defense model—with business units owning and managing their specific risks, risk

management providing independent oversight and challenges, and internal audit reviewing the effectiveness of the overall risk control framework—has been difficult for banks to achieve in practice.<sup>15</sup> The committee can help the stature and authority of risk managers through a strong control environment that includes empowering senior risk management executives with the authority to escalate emerging risk issues in a timely fashion to the board. Group risk committees should also ensure that local boards effectively challenge local business heads on risk and strategic issues that pertain to the soundness of country-level entities, whether branches or subsidiaries.

### 03. Stay vigilant as management tries to “do more with less”

Advances in automation, machine learning, natural language processing, and Big Data techniques could help banks meet demands to optimize their internal risk and regulatory compliance footprint. Committee members should be dedicated to understanding and challenging the effective capabilities of new technology solutions—even in stress scenarios. Risk committees should also assess information flow in an automated risk reporting and control environment; these IT structures directly affect the bank’s ability to identify and respond to emerging risks.

### 04. Strengthen formal conduct and culture programs

In the five-year period to ending in 2016, the world’s biggest banks paid large sums in conduct-related charges, including fines, legal bills, and the cost of compensating mistreated customers.<sup>16</sup> Many banks have created conduct risk and culture programs, and regulatory focus on the issue of conduct has been more intense.<sup>17</sup> The first, likely obvious, step for risk committees is to clearly acknowledge oversight of conduct risk and risk culture in the language of their charters. Second, risk committee oversight of culture and conduct risk programs should look particularly at decision-making processes around product and service design, with a focus on senior management accountability.

### 05. Focus on the interconnectedness of risk

Many risks not only span the purview of specific business units, but of specialized committees outside and within the board of directors. Accordingly, board risk committees should work with other committees at board level (for example, technology, audit, remuneration, and operations) and with management risk committees embedded in businesses to identify and understand risk in a holistic way. And boards should also seek members

12. Edward Hida and Julian Leake, “The future of risk in financial services,” Deloitte Touche Tohmatsu Limited, 2017.

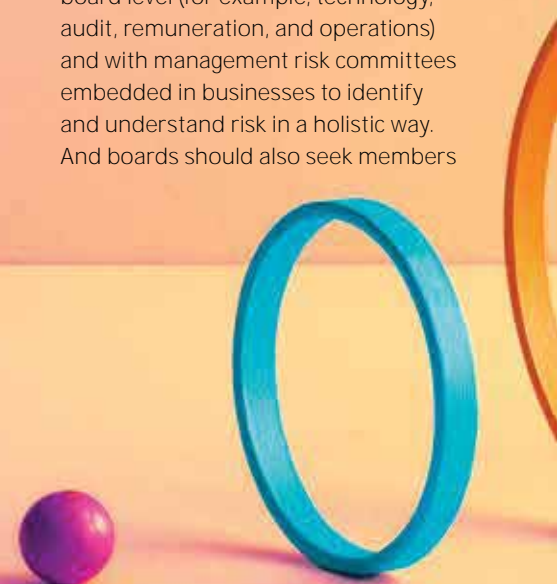
13. Anna Mok and Ronnie Saha, “Strategic risk management in banking,” Inside magazine, 2017 edition.

14. “Supervisory expectations for the board of directors,” Board of Governors of the Federal Reserve System.

15. Hida and Leake, “The future of risk in financial services.”

16. Jill Treanor, “World’s biggest banks face £264 billion bill for poor conduct,” The Guardian, 14 August 2017.

17. Deloitte, “Senior managers regime: Individual accountability and reasonable steps.”



with new talent profiles, such as technology expertise.<sup>18</sup> Another way to approach interconnectedness is, of course, to prioritize training for risk committee members.

#### **06. Oversee the strategic management of capital and liquidity**

Of all the risk management capabilities that most banks have built since the financial crisis, capital and liquidity stress testing at an enterprise-wide level may have arguably matured the most. As our results demonstrate, risk committee and board attention to stress-testing programs seems to have likewise increased substantially. Risk committees should also ensure that robust enterprise-level analytics are applied at the subsidiary, function, and regional levels.

#### **Orienting the compass to meet renewed expectations**

In conclusion, as late as 2011, having a dedicated risk committee on the board was viewed as a leading practice, whereas it is now ubiquitous. However, as Fed Governor Daniel Tarullo remarked in 2014, it was becoming apparent that the increasing operational burdens placed on bank boards were drawing director attention away from strategy and risk-related oversight.<sup>19</sup> Hence, it would be a mistake to view the Fed's new guidance delineating board and management roles as an

easing of expectations. As Fed Governor Jerome Powell remarked at the Large Bank Directors conference in Chicago earlier this year, "We do not intend that these reforms will lower the bar for boards or lighten the loads of directors."<sup>20</sup>

To meet and exceed expectations, board members should focus on creating robust information flow structures (especially around emerging risks), actively empowering the independent risk management function, and keeping pace with growing complexity in the risk environment. ●



18. John Reosti, "Cyber threats prompt run on tech experts for bank boards," *American Banker*, 17 May 2016.

19. Governor Daniel K. Tarullo, "Corporate governance and prudential regulation," Speech at the Association of American Law Schools 2014 Midyear Meeting, Washington, DC, 9 June 2014.

20. Governor Jerome H. Powell, "The role of boards at large financial firms."

# Contacts

## Argentina



**Martin Carmuega**  
Partner  
+54 11 432 027 00  
mcarhuega@deloitte.com

## Australia



**David Boyd**  
Partner  
+61 3 9671 7077  
davidjboyd@deloitte.com.au

## Austria



**Kurt Blecha**  
Partner  
+43 153 700 5800  
kblecha@deloitte.at



**Dominik Damm**  
Partner  
+43 153 700 5400  
ddamm@deloitte.at



**Alexander Ruzicka**  
Partner  
+43 153 700 7950  
aruzicka@deloitte.at

## Belgium



**Arno De Groote**  
Partner  
+32 2 800 24 73  
adegroote@deloitte.com



**Caroline Veris**  
Partner  
+32 2 800 23 06  
cveris@deloitte.com

## Brazil



**Luiz Dias**  
Partner  
+55 115 186 6206  
luizdias@deloitte.com

## Canada



**Bruno Melo**  
Partner  
+1 416 601 5926  
brmelo@deloitte.ca

## Caribbean Bermuda Countries



**Lawrence Lewis**  
Partner  
+1 242 302 4898  
llewis@deloitte.com

## Central Europe



**Andras Fulop**  
Partner  
+36 1 428 6937  
afulop@deloitteCE.com



**Jakub Bojanowski**  
Partner  
+48 22 511 0953  
jbojanowski@deloitteCE.com

## Colombia



**Roa Mauricio**  
Partner  
+57 1 4262098  
mroa@deloitte.com

## Cyprus



**Panicos Papamichael**  
Partner  
+357 223 608 05  
ppapamichael@deloitte.com

## Denmark



**Thomas Brun**  
Partner  
+45 30 93 6571  
tbrun@deloitte.dk



**Susanne Gildberg**  
Director  
+45 20 93 1187  
sgildberg@deloitte.dk

## Finland



**Lasse Ingström**  
Partner  
+358 207 555 389  
lasse.ingstrom@deloitte.fi

## France



**Laurence Dubois**  
Partner  
+33 1 40 88 28 25  
ladubois@deloitte.fr

## Germany



**Jörg Engels**  
Partner  
+49 211 877 223 76  
jengels@deloitte.de



**Andreas Knaebchen**  
Partner  
+49 152 090 076 00  
aknaebchen@deloitte.de



**Christian Haas**  
Partner  
+49 697 569 565 07  
chaas@deloitte.de



**Markus Salchegger**  
Partner  
+49 892 903 685 85  
msalchegger@deloitte.de

## Greece



**Alithia Diakatos**  
Partner  
+30 210 678 1100  
adiakatos@deloitte.gr

## Hong Kong & China



**Tony Wood**  
Partner  
+852 285 266 02  
tonywood@deloitte.com.hk

## Iceland



**Sif Einarsdottir**  
Partner  
+354 580 3009  
sif.einarsdottir@deloitte.is



**Bjorn Ingi Victorsson**  
Partner  
+354 580 3318  
bjorn.victorsson@deloitte.is

## India



**Muzammil Patel**  
Senior Director  
+91 22 6185 5490  
muzammilpatel@deloitte.com

## Ireland



**David Kinsella**  
Partner  
+353 141 725 29  
davkinsella@deloitte.ie

## Israel



**Linur Dloomy**  
Partner  
+972 3 608 5423  
ldloomy@deloitte.co.il

## Italy



**Mariano dal Monte**  
Partner  
+39 063 674 9293  
mdalmonate@deloitte.it

## Japan



**Masayuki Tanabe**  
Partner  
+81 908 349 3699  
masayuki.tanabe@tohatsu.co.jp

## Korea



**Young Sam Kim**  
Partner  
+82 266 761 522  
youngskim@deloitte.com

## Luxembourg



**Laurent Berliner**  
Partner  
+352 451 452 328  
lberliner@deloitte.lu

## Malta



**Steve Paris**  
Partner  
+356 234 324 00  
stparis@deloitte.com.mt

## Mauritius



**Peter Manju**  
Partner  
+230 403 5818  
mpeter@deloitte.com

## Mexico



**Carlos Perez**  
Partner  
+52 55 5080 6444  
caperez@deloittemx.com

## Middle East



**Aejaz Ahmed**  
Partner  
+966 1 282 8400  
aeahmed@deloitte.com



**Hani Khoury**  
Partner  
+966 1 128 285 00  
hakhoury@deloitte.com

## Morocco



**Fawzi Britel**  
Partner  
+212 661 154 586  
fbritel@deloitte.com

## Netherlands



**Harmen Meijnen**  
Partner  
+31 882 884 258  
HMeijnen@deloitte.nl

## New Zealand



**Rodger Murphy**  
Partner  
+64 930 307 58  
rodgermurphy@deloitte.co.nz

## Norway



**Sverre Danielsen**  
Partner  
+47 232 798 43  
sdanielsen@deloitte.no

## Portugal



**Sandra Carla Martins**  
Associate Partner  
+351 21 042 7506  
smartins@deloitte.pt

## CIS



**Natalya Kaprizina**  
Partner  
+749 578 706 00  
nakaprizina@deloitte.ru

## Singapore



**Tse Gan Thio**  
Partner  
+65 6216 3158  
tgthio@deloitte.com



**Serena Yong**  
Partner  
seyong@deloitte.com

## South Africa



**Akiva Ehrlich**  
Director  
+271 180 661 75  
akehrlich@deloitte.co.za

## Spain



**Alfonso Mur**  
Partner  
+34 914 432 103  
amur@deloitte.es



**Mercedes Gutierrez**  
Partner  
+34 914432620  
megutierrez@deloitte.es

## Sweden



**Elisabeth Werneman**  
Partner  
+46 752 462 486  
ewerneman@deloitte.se

## Switzerland



**Andrew Winters**  
Partner  
+41 58 279 7179  
ajwinters@deloitte.ch

## Taiwan



**Thomas Wan**  
Partner  
+866 225 459 988  
thomaswan@deloitte.com.tw

## Thailand



**Somkrit Krishnamra**  
Partner  
+66 2676 5700  
somkrishnamra@deloitte.com

## Turkey



**Cüneyt Kırlar**  
Partner  
+90 212 366 604 8  
ckirlar@deloitte.com

## United Kingdom



**Julian Leake**  
Partner  
+44 207 007 1223  
jleake@deloitte.co.uk

## United States



**Scott Baret**  
Partner  
+1 212 436 5456  
sbaret@deloitte.com



**Alok Sinha**  
Principal  
+1 415 783 5203  
asinha@deloitte.com

## West and Central Africa



**Anthony Olukoju**  
Partner  
+234 190 417 39  
aolukoju@deloitte.com

# Contacts



**J. H. Caldwell**

Partner  
Deloitte US  
Global Risk Advisory Leader  
Financial Services  
+1 704 227 1444  
jacaldwell@deloitte.com

Our knowledgeable authors, who are brimming with excitement about these disruptive topics, have written articles to help decision-makers to apprehend the new paradigms—if not to understand them all.



**Laurent Berliner**

Partner  
Deloitte Luxembourg  
EMEA Risk Advisory Leader  
Financial Services  
+352 451 452 328  
lberliner@deloitte.lu

## Deloitte.

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

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

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

For the convenience of the reader, a member firm of DTTL in a particular country is identified in the body of this report by the word "Deloitte" coupled with a country name (e.g., Deloitte Greece), in lieu of using the actual legal name of the member firm of DTTL in that country. In many countries, services may be provided by the actual member firms but could also be provided in addition by—or solely by—subsidiaries or affiliates of the DTTL member firm in that country, which are often organized as separate legal entities.

Specifically, in the United States, Deloitte USA LLP and Deloitte LLP are member firms of DTTL, and as used in this document, "Deloitte US" means one or more of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte USA LLP, Deloitte LLP and their respective subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.