The Economist Intelligence Unit

A report by The Economist Intelligence Unit

DIGITAL FINANCE:
Meeting ethics and compliance challenges in financial services

Sponsored by:

MAZARS

CONTENTS

EXECUTIVE SUMMARY

The chaos unleashed on the global financial system in 2007-08—a toxic combination of the cavalier attitude of some participants and of obscured systemic risks—triggered a wave of financial regulation. Many of those regulations focus on the ethical behaviour of financial services providers themselves: the quality of their supervision of staff; their transparency with customers, shareholders and regulators; and their thoroughness and honesty in evaluating the risks they face as individual institutions and the risks they could pose to the broader economy.

Today, financial services companies are in the process of implementing the changes required by the new regulations. At the same time, they are responding to a surge of digitisation, in commerce in general and in financial services in particular. Some forward-looking financial services companies—either alone or in combination with financial technology providers—are seizing on the opportunities presented by both regulation and digitisation to upgrade their internal and customer-facing systems. Their aim is to improve risk assessment, increase transparency, and thereby begin to restore the public trust that was damaged by the financial meltdown.

This research considers how financial services companies are responding to both the wave of regulations and the surge in digitisation. It considers how adopting specialised digital technologies might help financial companies to improve their services, manage risks better, raise their standards of transparency and build trust. The research reaches the following main conclusions:

- The wave of regulation, particularly those involving data storage and handling, are causing major operational worries for financial services companies

- While complaining about the volume and scope of new ethics-oriented regulation, three-fourths of financial services companies surveyed also claim that they are raising their standard of ethical conduct beyond the requirements of the law, and are using digital technologies to do so

- In particular, financial companies say they rely most on advanced data analytics and cyber security technologies to raise their standard of ethical conduct, although the use of these technologies alone is not sufficient to foster a culture of ethical behaviour

- A majority of financial companies surveyed say they have tried to—and succeeded in—turning compliance with ethical standards into a competitive advantage; the biggest benefits cited were in enhancing companies' brand images

- On the other hand, three-fourths of companies surveyed say the use of data mining and/or enhanced data analytics carries potential ethical problems of its own, such as possibly compromising customer privacy; respondents point to the use of third-party analytics providers as particularly risky in this regard

- While focusing on complying with the new transparency and cyber security requirements, financial services companies surveyed admit they have made few changes to internal procedures or codes of conduct—suggesting that their focus is on narrow legal compliance rather than on changing corporate cultures to emphasise ethical conduct

ABOUT THIS RESEARCH

"*Digital finance: Meeting ethics and compliance challenges in financial services*" is a briefing paper written by the Economist Intelligence Unit and sponsored by Mazars. The report focuses on the financial services industry's use of digital tools and corresponding organisational changes both to comply with new regulatory requirements and to meet the challenges of competition from internet-based providers of financial services. The report is based on a combination of desk research, an online survey of 200 financial services companies worldwide, and in-depth interviews with six experts in the topic under study.

The Economist Intelligence Unit surveyed 201 executives of financial services industries in December 2015 and January 2016. Of these respondents, 50 were IT specialists, 51 risk/compliance specialists, and 100 represent a range of other functions. Half the respondents are C-level (CEO, CIO, etc) and above, and half represent companies with global annual revenues above US$500 million. The respondents are concentrated in three regions: 60 in Asia-Pacific, 60 in Europe, 61 in North America, and 20 from the rest of the world. The full survey results are provided in the Appendix to this report.

In addition, the EIU carried out in depth interviews with six experts in the field of study. The EIU would like to thank the following individuals (listed alphabetically by company name) for their time and insights:

- Dr Thomas Loesler, Global Chief Compliance Officer, Allianz
- Andrew White, CEO, FundApps (a regulation technology company)
- Ben Hammersley, Futurist and cybercrime expert
- James Kennedy, Applications Delivery Chief Technology Officer, UBS
- Giancarlo Bruno, head of financial services industries and member of the management committee, World Economic Forum
- R. Jesse McWaters, financial innovation lead, World Economic Forum

The Economist Intelligence Unit is solely responsible for the content of this report. The views expressed here may or may not be those of the sponsor. The author of the report is Anna Lawlor, and the editor is Aviva Freudmann.

I. A WAVE OF ETHICS REGULATION

In the wake of the financial crisis of 2008-09, regulators worldwide, but particularly in the United States and Europe, have sought to increase accountability and foster ethical behaviour in their financial services industries. Among the regulatory changes aimed at improving ethics are enhanced disclosure and reporting requirements, such as the transparency requirements in the United States' 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act.

In the European Union, the Markets in Financial Instruments Directive (MiFID) was updated in 2014 (MiFID II[1]) to prescribe new business conduct standards in the provision of investment products and services. These include curbing speculative investment in commodity markets, addressing conflicts of interest in the provision of financial advice, and bringing greater transparency to algorithmic trading (known as high-frequency trading). Firms engaged in algorithmic trading, under MiFID, now must divulge their trading strategies among other elements.

Other EU regulations relate more directly to customers, such as Anti-Money Laundering/ Know Your Customer[2] requirements. Moreover, the European Union's General Data Protection Regulation, which aims to protect EU citizens' data privacy wherever their data is stored, has considerable implications for how multinational financial services capture, store and transfer customer data.

Other countries have taken a variety of other approaches to ethics regulation in financial services. In France, for example, a 2015 law requires French institutional investors to disclose the carbon footprint of their portfolios, while in Switzerland a law taking effect in 2016 requires increased disclosure by insurers of their financial performance, governance structures, risk management systems and Board-level compensation, among other elements.

These are just a few examples of a barrage of new regulations aimed at financial services companies. The impact is already being felt as increased demand on companies' operational resources, according to an online survey carried out for this research. Nearly half (47%) of respondents say the volume of regulatory changes affecting the financial sector causes the greatest worry for their companies. Similarly, 45% say the scope of regulations affecting financial services is causing the greatest worry (See Chart 1).

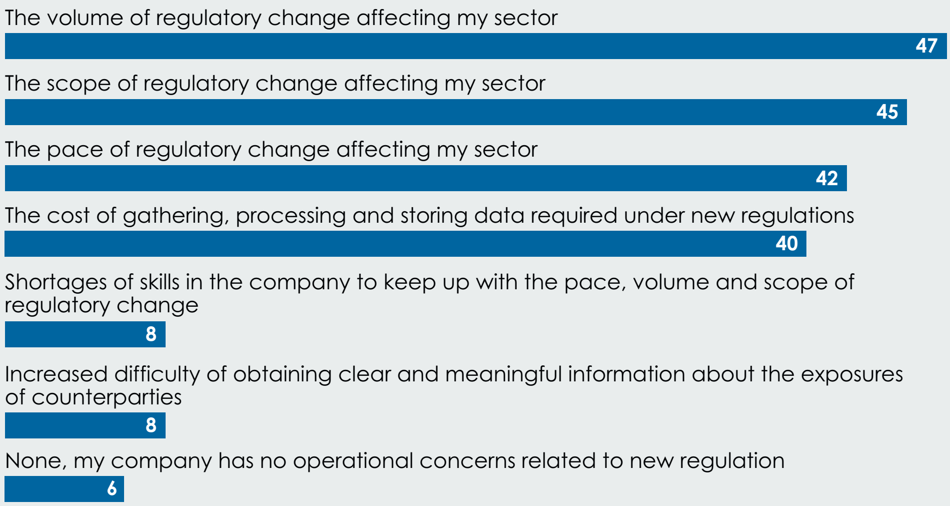
The aspects of regulation currently causing the greatest headaches among financial services respondents are those dealing with safe storage and handling of data, such as data of depositors, borrowers or investees; well over half (58%) of survey respondents cite data storage and handling as a major concern. More than half (52%) also say that ensuring acceptable risk-management and/or governance structures of corporate borrowers or investees is a major cause of concern (See Chart 2).

[1] https://www.cfainstitute.org/ethics/Documents/MiFID%20II%20Policy%20Brief.pdf

[2] Know Your Customer is a global anti-money laundering process in which a business must verify the identity of its customers. These procedures are being used globally to prevent identity theft, financial fraud, money laundering and terrorist financing

Chart 1

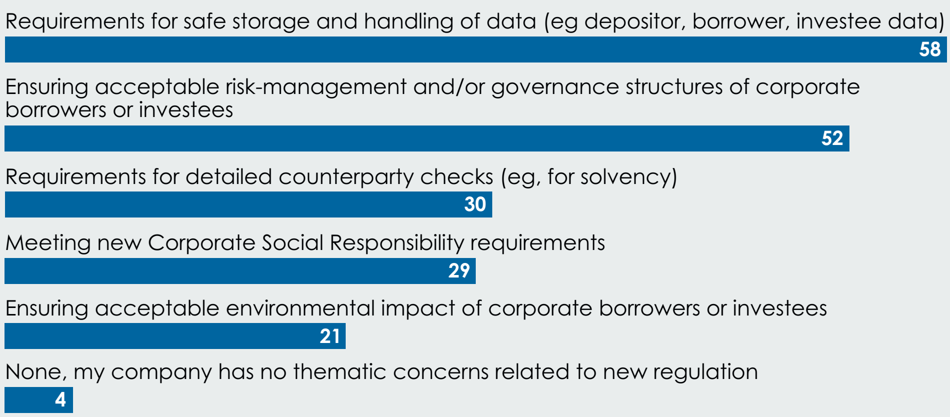
Thinking about the operational requirements imposed by the new regulations, which of the following aspects of regulation, if any, causes the greatest worry for your company? Please select the top two.
(% respondents)



Source: The Economist Intelligence Unit.

Chart 2

Thinking about the wave of new financial services regulations over the past seven years, which of the following regulatory themes, if any, causes the greatest worry for your company? Please select the top two.
(% respondents)



Source: The Economist Intelligence Unit.

James Kennedy, Applications Delivery Chief Technology Officer of UBS, says that the cumulative nature of the regulations from different jurisdictions poses its own type of challenge. He also points to "inconsistencies in the specific requirements of individual regulators", which adds to the complexity and cost facing financial companies.

Yet for all the worries over the scope, pace and content of regulations aimed at promoting transparency and ethical conduct, financial services companies are making progress in implementing the required changes. Survey results show a great deal of activity under way to improve transparency and/or ethical conduct: 57% say their companies have introduced new information gathering and reporting requirements in recent years; 45% say their companies have introduced new internal procedures and/or business practices aimed at enhancing ethics; and 43% say their companies have introduced new corporate policies or codes of conduct (See Chart 3).

Chart 3

Beyond the use of enhanced digital tools, which additional measures or corporate practices, if any, has your company introduced in recent years to improve transparency and/or ethical conduct?
Please select all that apply
(% respondents)

Source: The Economist Intelligence Unit.

Interestingly, in each of these three areas smaller companies (those with global annual revenues below $500 million) nosed ahead of larger financial services in introducing these changes (by 3%-5%). Also, Asian firms were the most likely to introduce new internal procedures and/or business processes (52%, at least 10% more than European and North American firms). Asian firms were also most likely to introduce new corporate policies or codes of conduct (50% compared with 44% for North America and 38% for

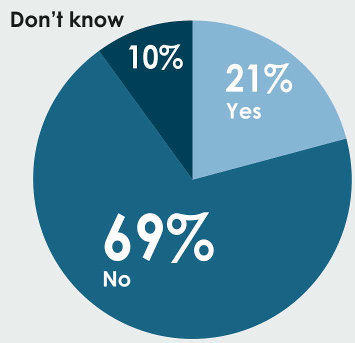
Europe), despite the fact that most of the regulatory changes originated in Europe and North America.

While sophisticated data-storage and cyber-security technologies are helping financial companies meet the new requirements, the availability of new tools is not—in and of itself—prompting most financial companies to use them for this purpose. The main impetus for changes seems to come from the regulatory imperatives; the technologies are brought in as a way to comply. So, for example, technology is enabling firms to automate processes to respond to multi-jurisdiction regulations, and to monitor electronic communications to protect against leakage of confidential data or intellectual property.

That said, internal procedures and codes of conduct—which lie closer to the heart of compliance—have been slow to change. More than two-thirds (69%) of survey respondents say that their companies have not changed any internal procedures or codes of conduct in response to the availability of new digital tools, such as those for protecting sensitive data (See Chart 4).

Chart 4

Has your company changed any of its internal procedures or codes of conduct in response to the availability of new digital tools?
(% respondents)



Source: The Economist Intelligence Unit.

Yet changes in internal procedures and codes of conduct are a necessary component for raising the standard of ethical behaviour. The Association of Chartered Certified Accountants (ACCA), the global body for professional accountants, concluded in its report '*Culture vs regulation: what is needed to improve ethics in finance?*[3]: "Regulation can ultimately only be a backstop; it can make rules for behaviour up to a point, but the regulator is not in the room with the customer".

[3] http://www.accaglobal.com/content/dam/acca/global/PDF-technical/corporate-governance/pol-tp-cvr.pdf

II. USING DIGITAL TECHNOLOGY TO RAISE ETHICAL STANDARDS

Clearly, advanced cyber-protection, data gathering and data analysis technologies are a necessary—albeit not sufficient—condition for meeting regulatory requirements for ethical behaviour in financial firms. The ACCA Global report suggests: "Ethical situations need to be tested out, placing people in scenarios so that they truly consider the opportunity cost of acting unethically, noting that embedding ethics cannot be achieved merely by passing a test but must involve understanding what it means to act and behave ethically." So far, only a few financial firms have adopted this recommendation. (See Box: "Ethics deliberations at Allianz")

ETHICS DELIBERATIONS AT ALLIANZ

Some financial companies are already using digital technologies, such as internal social media platforms, to raise the bar on ethical practice One of them is German insurance and asset management giant Allianz. Its global chief compliance officer, Dr Thomas Loesler, says his company uses an internal social media platform – Allianz Connect – that shifts compliance training from "boring…legalese" to a more open, collaborative approach based on "dilemma situations".

The social media hub at Allianz hosts an array of real-life cases that are not "clear-cut compliance cases" but "are difficult to deal with and the obvious solution doesn't present itself easily", Dr Loesler says. The aim is to encourage staff members to post comments and questions, and to challenge each other on how to respond to the scenario. This can only occur in a non-judgemental learning environment; a video of Allianz's CEO discussing his take on some "dilemma situations" has been posted to Allianz Connect, targeting a culture of transparency and open dialogue about compliance.

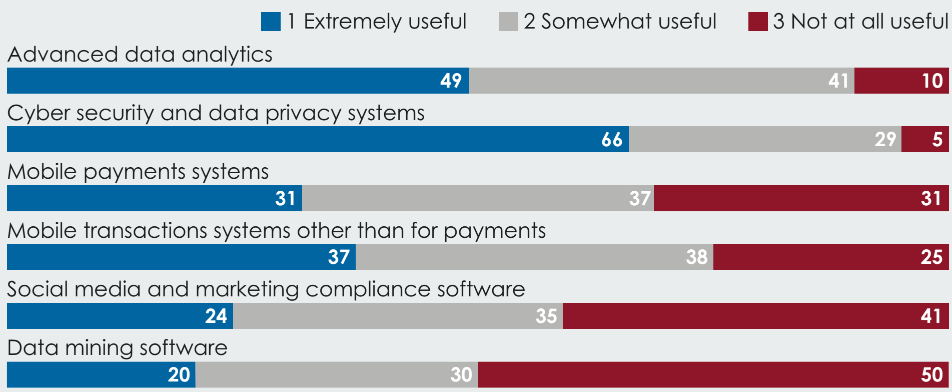
Dr Loesler says the greatest risk of non-compliance in financial services comes from employees cutting corners because of personal/professional pressures, not because they set out to break the law. The danger is that such shortcuts can become culturally entrenched if they occur frequently. Open, accessible dialogue about making decisions with integrity, involving all levels of the company, could not be achieved without digital media tools, he adds.

Dr Loesler emphasises that "the IT is not the most important thing here." However, the discussion hub has reached a broad range of employees, more frequently and more directly than could be achieved via classroom or web-based training programs. The hub puts ethical judgements at the forefront of conversations about compliance. "Compliance is not just a control function to us, it's an advisory function, which is equally important," he says.

The digital technologies most likely to help financial companies to comply with new regulations are those focusing on data privacy and data analytics. Nearly half (49%) of respondents say advanced data analytics technologies have been extremely useful in meeting new requirements. Two-thirds (66%) say cyber security and data privacy systems have been extremely useful. As for technologies enabling mobile transaction systems other than for payments, three-fourths (75%) of respondents say these technologies are either extremely useful or somewhat useful (See Chart 5).

Chart 5

On a scale of 1-3, with 1=extremely useful and 3=not at all useful, please indicate how useful each of the following technologies has proven in meeting new regulatory requirements for enhanced transparency and ethical conduct.
(% respondents)



Source: The Economist Intelligence Unit.

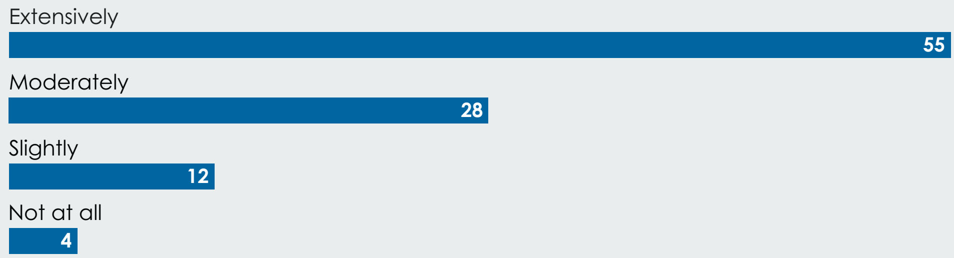
Advanced data analytics technologies, in particular, have proven useful to financial companies in complying with transparency and risk management requirements. More than four-fifths (83%) of respondents say their companies have relied on advanced data analytics either extensively or moderately in improving transparency and risk management (See Chart 6).

Advanced data analytics and data privacy technologies also help companies to "raise their game" in ethical behaviour beyond the strict requirements of the law. More than three-fourths (76%) of respondents say their companies rely on advanced data analytics or data privacy technologies to raise ethical standards beyond simple compliance (See Chart 7).

Respondents say there are good business reasons for going beyond mere compliance. A large proportion say they try to turn compliance with ethical standards into a competitive advantage. Four-fifths (80%) report having improved their brand image as a result of setting and maintaining higher ethical and/or transparency standards, while 51% said their financial results have improved (See Chart 8).

Chart 6

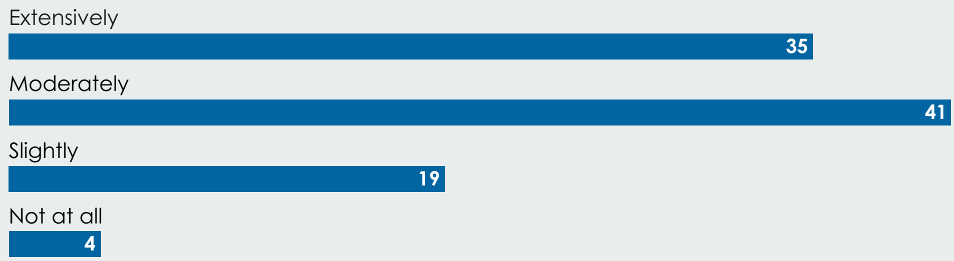
To what extent does your company rely on advanced data analytics to comply with enhanced requirements for transparency and risk management?
(% respondents)



Source: The Economist Intelligence Unit.

Chart 7

To what extent does your company rely on advanced data analytics and/or data privacy technologies to raise its standard of ethical conduct, beyond simple compliance?
(% respondents)



Source: The Economist Intelligence Unit.

Among survey respondents, Europeans (58%) were most likely to say they boost financial results by turning compliance with ethical standards into a competitive advantage; North American firms were the least likely (41%) to say so. Interestingly, more small companies[4] report reaping financial benefits of this approach (52% compared with 49.5% for larger firms), while larger firms[5] are more likely to say they benefit from an improved brand image as a result of having – and communicating – their higher ethical standards (82% compared with 78% for smaller firms).

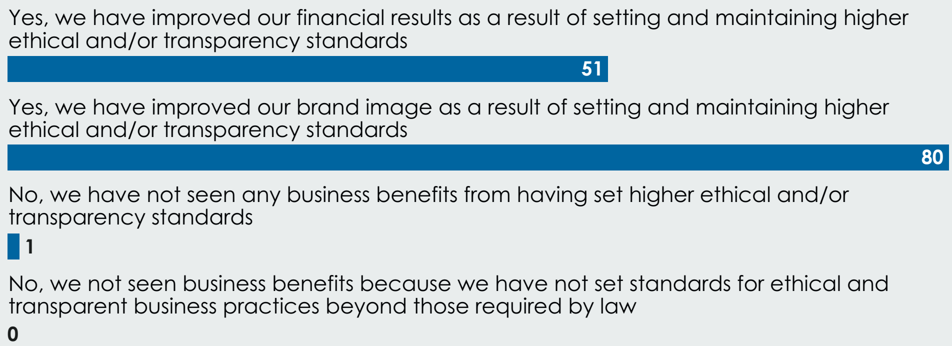
[4] Global annual revenues less than $500m

[5] Global annual revenues more than $500m

Chart 8

Has your company tried to turn compliance with ethical standards into a competitive advantage? Select up to two.

(% respondents)



Source: The Economist Intelligence Unit.

III. NEW TECHNOLOGIES, NEW RISKS AND OPPORTUNITIES

For all the positive news about compliance efforts and business benefits, the use of new technologies to comply with ethics rules carries risks. One such risk was alluded to above: a focus on the tools alone, to the exclusion of the broader ethical eco-system within a company that aims to ensure ethical and transparent practice.

Ben Hammersley, futurist and cyber-crime expert, says there are limits to what software alone can achieve with regards to changing ethical behaviour. He explains: "I think an awful lot of that is good in theory and doesn't really work in practice. If you think about what an insurance firm is trying to do, for example, it is to measure risk. This is the same with regulatory compliance. In order to do that you have to think carefully about what that risk is, and how that risk could be mitigated. Do we install some software, or do we just train our employees better, or do we just not employ idiots? [For] large incumbents, [use of these technologies] is not being innovative, it's just being law-abiding."

Another risk is misuse of digital tools in ways that intrude on individual privacy. For example data mining—the use of customer data to develop insights for marketing and other purposes—has acquired a bad reputation in some quarters, as it has raised concerns about compromising consumer privacy with intrusive, individually tailored advertising. Yet another type of risk arises in potentially compromising data security when using the wrong third-party data analytics or data security provider. New trading platforms for computer-generated "bitcoins" have raised the stakes for cyber-hackers. Mobile applications for financial transactions have also increased concerns about the potential for compromising users' data.

Survey respondents worry about such cyber-security breaches, particularly when third-party service providers are involved. A large majority (87%) say the use of digital technologies (for example, for data analytics) by third-party suppliers poses either major or minor ethical or compliance problems for their companies (See Chart 9).

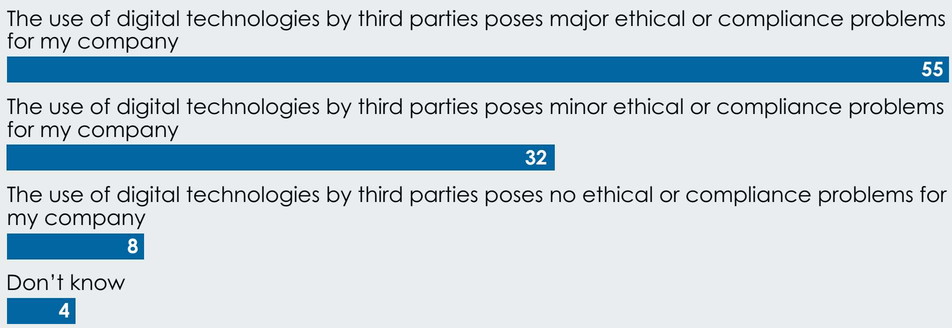
Jesse McWaters, Financial Innovation Lead at the World Economic Forum, believes that third-party IT providers represent "a fundamentally different type of risk". "It's an operational risk; as we see operational risk centralised, that comes with risks to systemic stability that has not traditionally been the primary focus of regulators," he says. He adds that one result may be that regulators increase their supervision of third party IT service providers to financial companies.

On the other hand, an array of new digital technologies that streamline information gathering and data analysis are also helping financial companies to improve on their existing strengths in risk assessment, provision of liquidity, moving money between payers and payees, providing tailored customer advisory services, and implement customers' investment strategies. To an increasing extent, such services are now being offered via online and physical networks that are meshed together through digitisation.

Chart 9

To what extent does the use of enhanced digital technologies — such as advanced data analytics and data mining — by third parties (eg, suppliers or counterparties) create potential ethical or compliance problems for your company?

(% respondents)



Source: The Economist Intelligence Unit.

Financial firms, either alone or in combination with specialised technology providers, aim to use digitisation to build upon their existing strengths in protecting customer data and providing money-related services. For example, French banking giant BNP Paribas has established an innovation hub for financial technology companies. The idea is to provide start-up firms with tailored banking solutions, drawing on the financial expertise of specialist BNP Paribas bankers and the digital strengths of financial technology firms.

Some specialised financial technology providers believe that digitisation of financial services will improve the sector's data security. Andrew White is founder of FundApps, which organises regulatory information and delivers a cloud-based managed-service to automate shareholding disclosure and monitor investment restrictions across 100 regulatory regimes on a daily basis. He says: "One of the most crucial advantages of the cloud (if done right) is the "strength in numbers" aspect. For example every one of FundApps' rules has been reviewed and approved by each of our 20 clients—ranging from smallish hedge funds to large asset managers. Compare this to a typical compliance department where a single incorrect Excel formula created by one employee can possibly cost the company millions and incur reputational damage."

Mr White adds that the regulatory technology market is growing—with about a dozen start-ups globally– and that the UK, the U.S. and Ireland are leading in adoption. "Continental countries such as Germany and Switzerland are still lagging and Asia is probably further behind still," he says.

Help in improving transparency in financial services may come from another quarter as well. Advanced technologies such as Blockchain, a shared public ledger that documents transactions, could also help financial services companies demonstrate transparency to regulators. Since transactions are recorded simultaneously on multiple ledgers and cannot be altered, the technology provides financial services with transparent provenance for trading and any other forms of information or value exchange. Moreover, the information on Blockchain is 'live', not collected retrospectively; this could shift the focus of governance for some types of business from retrospective reporting to agreeing on what information to include in the Blockchain.

That said, in all solutions aimed at improving transparency and ethical dealing, the quality of people implementing and using the technologies is decisive, Indeed, the quality of the entire corporate culture surrounding the use of digital tools is key; without a general orientation toward strict data privacy, seamless integration of online and physical communication channels, transparent operations and accurate risk assessments, digitisation is unlikely to enhance performance, and could in fact increase rather than reduce exposure.

Michael Luca, Assistant Professor of Business Administration at Harvard Business School, in a co-authored recent article for *Harvard Business Review*[6], highlights the importance of the broader eco-system surrounding the new digital tools. He warns that computer software understands only what it is explicitly told about risks and other factors, and lacks the ability to apply an ethical lens to decision-making. Of crucial importance is a human oversight function that queries whether the technical processes aid or hinder fair and honest dealing.

[6] *Algorithms Need Managers Too*, Harvard Business Review, Jan-Feb 2016, page 97

IV. FUTURE PRIORITIES: PROTECTING AND ANALYSING DATA

One clear outcome of the regulatory response to the financial crisis of 2008-09 is that regulators have raised the stakes for financial firms when things go wrong, Regulators are imposing record fines on financial companies for hiding risks, misleading customers, or failing to exercise proper caution in protecting sensitive data.

Financial companies are not always quick to make changes, even after a major breach. For example, the United States' second-biggest insurer, Anthem, was fined $1.7m after a 2010 computer breach that resulted in the disclosure of personal information of approximately 612,000 people. Other cyber hacking victims have included America's JPMorgan Chase and Fidelity Investments; the UK's HSBC, Barclays Bank and travel insurer Staysure; and Switzerland's Banque Cantonale de Geneve. Some of these hack attacks allegedly originated in China, Vietnam, Ukraine and Russia, targeting the U.S., UK, Australia, Canada and Hong Kong, and indicating the global challenge posed by this issue.

In December 2015, the Bank of England warned of the "serious and growing threat" to system stability posed by a cyber-attack at the heart of the UK financial system. U.S. financial regulators warned that hackers are trying to extort banks and credit unions with increasing "frequency and severity" and urged the industry to protect its networks from unauthorised access. The European Central Bank itself received one such hacker's ransom demand in July 2015.

Research by IT security firm Kaspersky Labs has found that financial services is the sector most targeted by hackers, particularly investment funds, banks, and stock and currency exchanges[7]. Mr Hammersley is unsurprised; "The dirty secret, especially in high-street banking, is that [financial services companies'] technical infrastructure [can be] incredibly out-of-date. It's very difficult for these banks to innovate because they're too busy trying to keep their current system from falling over."

Mr McWaters says he has heard some financial institutions say "there is a literally unlimited budget for cyber security", due to the massive loss of trust resulting from the financial crisis. "There is a lack of public trust in financial institutions to act in their interest," he says. "If you have that combined with a lack of public trust in the ability of financial institutions to fundamentally, operationally execute on their promises, that would be deeply damaging to the financial system."

The message concerning the importance of cyber security has not been lost on the financial industry. As noted above, 66% of respondents rated cyber security and data privacy systems as "extremely useful" in meeting new regulatory requirements for enhanced transparency and ethical conduct. Asia Pacific respondents were the most adamant (75%) about cyber security technology being "extremely useful", compared

[7] Research by Kaspersky Lab quoted in Corporate Hacks Doubled in 2015, City AM: http://www.cityam.com/231476/

with 67% for Europe and 57% for North America. The lower numbers in Europe and North America are a bit surprising, given the high profile hacking cases in those regions to date, and the preparations for a wide-ranging European Data Protection directive.

Moreover, as noted above, 49% of respondents pointed to advanced data analytics as "extremely useful" in meeting regulatory requirements, suggesting a focus on upgrading data analytics systems in future. The strongest proponents of this view were in the banking (58%) and private equity (56.5%) sectors. Insurers, who are often cited as key beneficiaries of data analytic business intelligence, tend (50%) to say data analytics is only "somewhat useful" in achieving regulatory compliance. Securities trading firms (56%), investment banks (49%) and asset managers (48%) find advanced data analytics technologies only "somewhat useful".

CONCLUSION

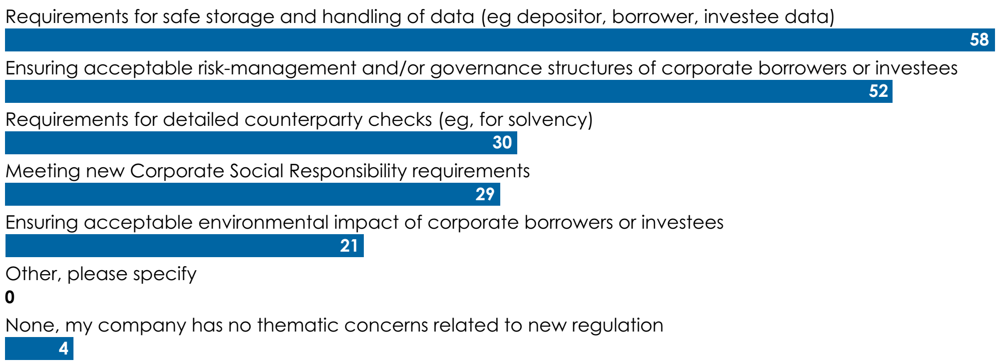
This research suggests the financial services industry is responding to the wave of new ethics-oriented regulation despite its worries about operational impacts. The industry is devoting most of its compliance attention to information technologies that promote transparency and effective risk management. The response is in its early stages, and financial companies still have many improvements to make in their data security, data analysis and data handling systems. But the groundwork has been laid, and a new crop of third-party providers is springing up to aid financial firms in this process.

Less encouraging is the progress on the management practices front—that is, in changing corporate procedures and codes of conduct to ensure compliance with the spirit as well as the letter of the new regulations. Our survey shows a relatively sluggish response on this aspect of promoting ethical behaviour—even though it is widely acknowledged that a strictly technological fix is insufficient to ensuring safe and fair conduct. The human element of risk-management and transparent dealing may yet be added in future, as respondents say their companies have already reaped financial and corporate-image benefits from making known their compliance with new ethical standards.

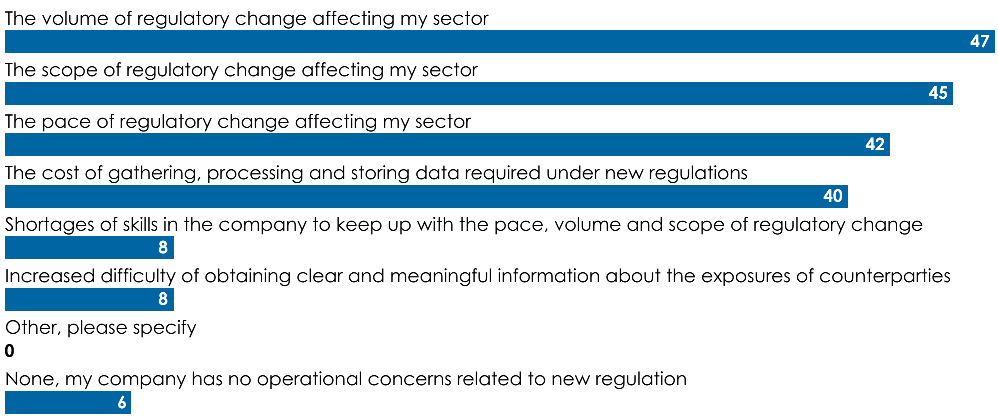
The industry's response to the wave of regulation may be an example of making the best of the inevitable, as the increased disclosure and risk-management requirements are by now a fact of life. Indeed, the severity of the financial risks encountered in the crisis mean that "light touch" regulation is a thing of the past. For financial companies—but even more so for society at large—the silver lining in the cloud that was the financial crisis may be the rules now sparking innovations in risk management, data gathering, and data analytics in financial firms. These digital innovations may be lending themselves to "box ticking" compliance at the moment; but they may also lead to a broader awareness in financial companies of the risks they need to manage, and of the wide range of technical and non-technical measures they will need to take to manage those risks.

APPENDIX

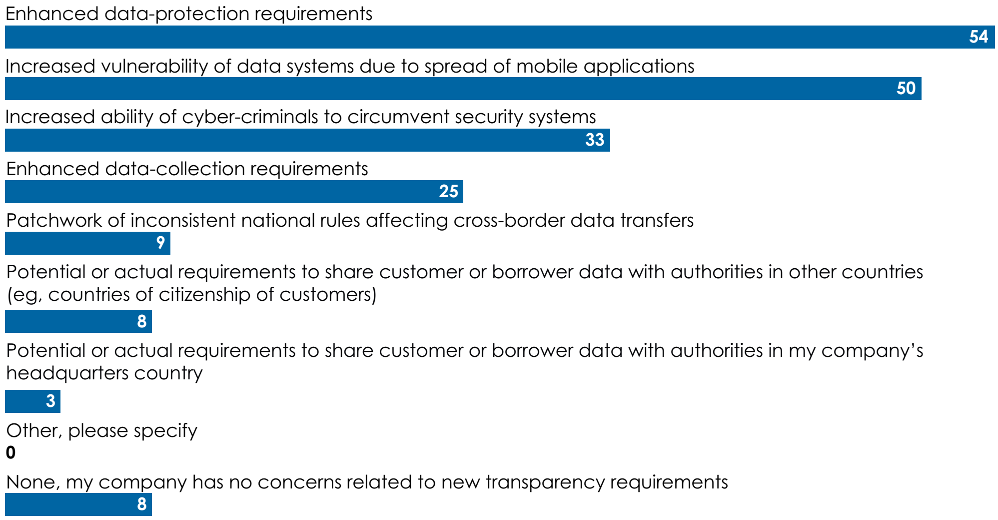
Thinking about the wave of new financial services regulations over the past seven years, which of the following regulatory themes, if any, causes the greatest worry for your company? Please select the top two.
(% respondents)



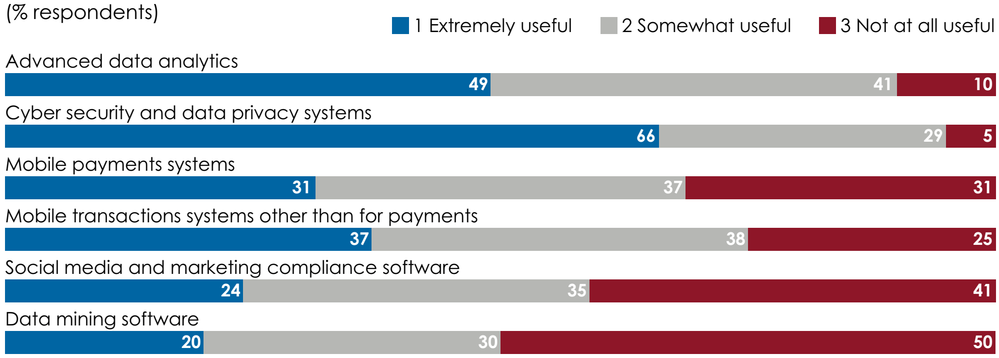
Thinking about the operational requirements imposed by the new regulations, which of the following aspects of regulation, if any, causes the greatest worry for your company? Please select the top two.
(% respondents)



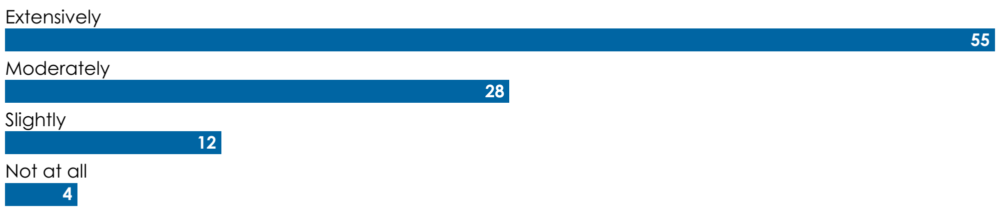
Thinking about regulations governing transparency, which of the following compliance aspects, if any, causes the greatest concern to your company? Please select the top two.
(% respondents)



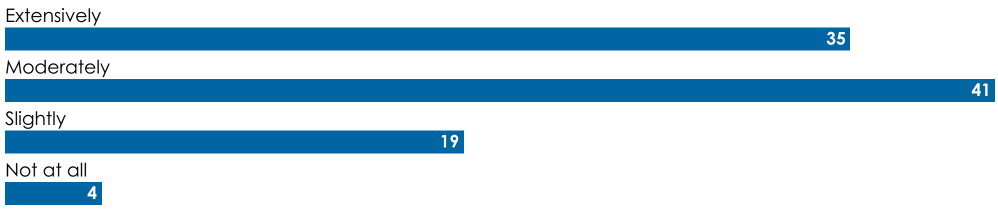
On a scale of 1-3, with 1=extremely useful and 3=not at all useful, please indicate how useful each of the following technologies has proven in meeting new regulatory requirements for enhanced transparency and ethical conduct.
(% respondents)



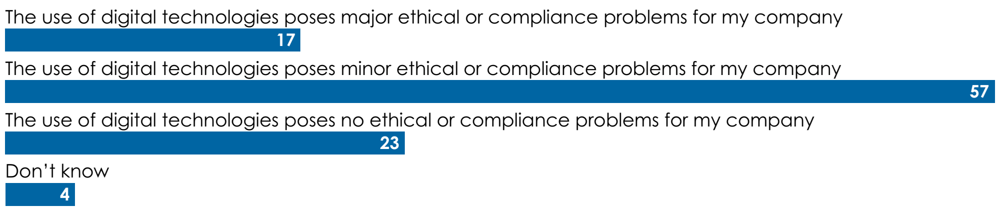
To what extent does your company rely on advanced data analytics to comply with enhanced requirements for transparency and risk management? Please select one.
(% respondents)



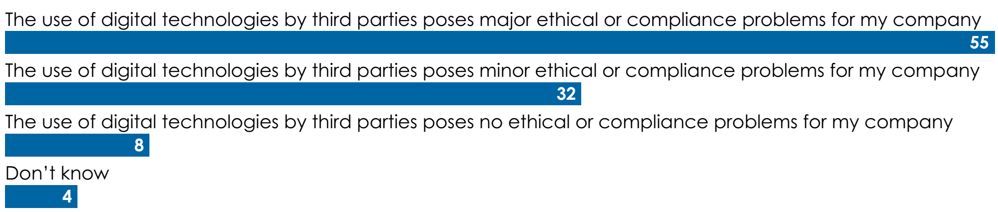
To what extent does your company rely on advanced data analytics and/or data privacy technologies to raise its standard of ethical conduct, beyond simple compliance? Please select one.
(% respondents)



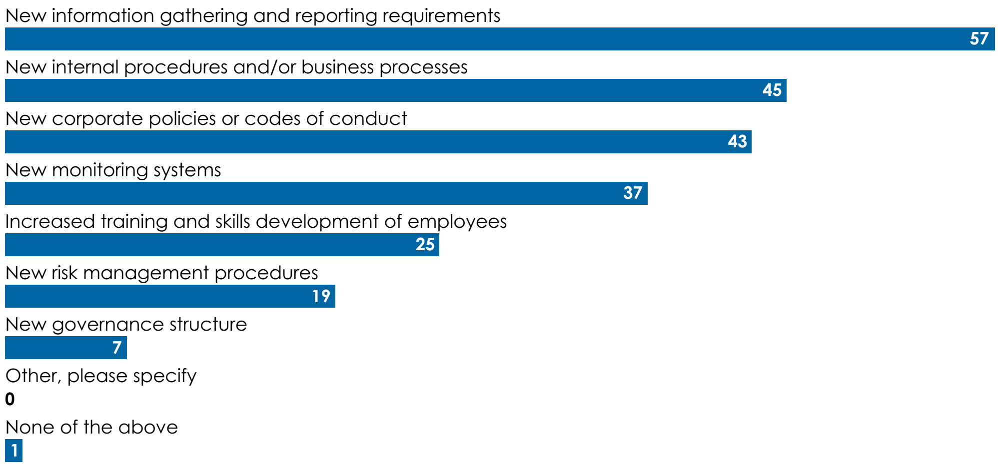
To what extent does your company's use of enhanced digital technologies — such as advanced data analytics and data mining — itself create potential ethical or compliance problems for your company, for example in the area of ensuring customer privacy? Please select one.
(% respondents)



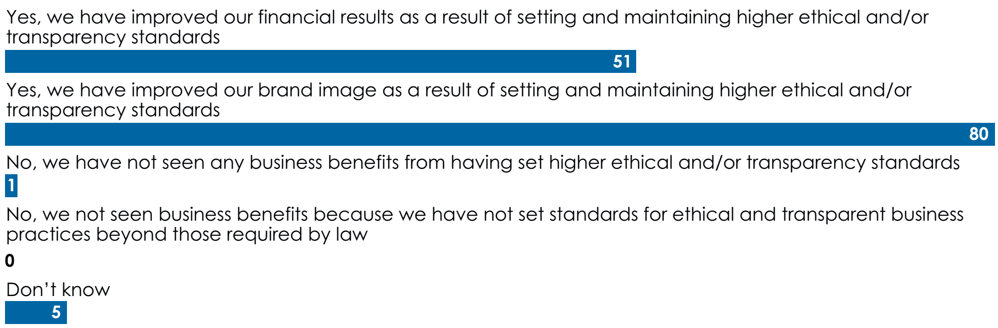
To what extent does the use of enhanced digital technologies — such as advanced data analytics and data mining — by third parties (eg, suppliers or counterparties) create potential ethical or compliance problems for your company? Please select one.
(% respondents)



Beyond the use of enhanced digital tools, which additional measures or corporate practices, if any, has your company introduced in recent years to improve transparency and/or ethical conduct? Please select all that apply.
(% respondents)



Has your company tried to turn compliance with ethical standards into a competitive advantage? Please select up to two.
(% respondents)



Has your company changed any of its internal procedures or codes of conduct in response to the availability of new digital tools?
(% respondents)

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: americas@eiu.com

HONG KONG
1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: asia@eiu.com

GENEVA
Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com