Monday, February 5, 2018

Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

After all these security issues with the Internet of Things, we have even more security issues with the Internet of Bio-Nano Things (IoBNT).

Scientists elaborate on the possibility to combine Internet-enabled devices with miniaturization and biological processes.

It is being envisaged that technology will provide “tools to control, reuse, modify, and reengineer the cells’ structure and function, and it is expected to enable engineers to effectively use the biological cells as programmable substrates”. In this context an implementation of Bio-Nano Things as biological embedded computing devices is being considered as a main enabler.

If seen together with developments in DNA research, biocomputing and advances in e-health and medicine, IoBNT opens up numerous avenues for technological breakthroughs where cyber becomes part of and controls vital human biological processes.

*It could be good, but what about cyber risks?*
Such a development will bring massive challenges to technology, including ethical, social, legal economic and political aspects, to mention the most imminent ones.

Though the effects of these developments are difficult to assess by now, technologist will need to be aware that a lot of work will be necessary in order to cope with such challenges.

Coverage of security issues in IoBNT will bring massive challenges for security and cyber-security: level of protection will be the highest possible, as the assets to be protected are the building blocks of life and health.

Moreover, trust in the functions and in the communication between all involved components will be of great importance.

Finally, requirements of identification, accountability, non-repudiation and integrity functions will be decisive for the development and deployment of IoBNT.

Read more at Number 2 below. Welcome to the Top 10 list.

Best Regards,

George Lekatis
President of the IARCP
General Manager, Compliance LLC
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828
Basel III - sense and sensitivity

Ms Sabine Lautenschläger, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the European Central Bank, at the Institute for Law and Finance Conference on Basel III, Frankfurt am Main.

It is done: Basel III has been finalised.

I admit that it was a long journey, but in my view, it was worth the wait: Basel III will help to make banking safer. It is crucial, though, that Basel III is properly implemented - in Europe and around the world. It must not be watered down.

Basel III marks the end of the post-crisis reforms; regulatory certainty has been restored. The banks know what awaits them; they can be confident about the regulatory framework, and can plan ahead and support the real economy.

Looking into the crystal ball

A report on emerging technologies and security challenges

The time has come for ENISA to take a look at the crystal ball of technology; In particular looking at what are considered to be emerging technologies and what might be their prospective usage scenarios.

Considering emerging technologies and applications is an important step in assessing future security needs.
Improving recognition of ICT security standards

Recommendations for the Member States for the conformance to NIS Directive

This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs.

This document provides the results of an assessment of the maturity of the implementation of the European Cyber Security Standardisation activities in the EU Member States with respect to the NIS Directive concerning measures for a high common level of security of network and information systems across the Union.

Basel III: Are we done now?

Keynote speech by Mr Stefan Ingves, Chairman of the Basel Committee on Banking Supervision, at the Institute for Law and Finance conference on "Basel III: Are we done now?", Goethe University, Frankfurt am Main.

The title of this conference is "Basel III: Are we done now?". Let me answer this question at the outset: yes, we are done, but that doesn't mean the work has ended. In some respects, it's only just beginning.
PSD2 - will it be a game-changer?

Job Swank, Executive Director of the Netherlands Bank, at ESB's Conversation with Regulators on Innovation in Payment Services, The Hague.

“Today's topic is PSD2. PSD2 is a European directive, to be implemented through national legislation. And PSD2 is about payments. To most people, these topics - legislation and payments - are extremely boring, a necessary evil. Probably not to you. Otherwise, you wouldn't be here, but you are certainly a minority.”

Ethics and trust in finance

François Villeroy de Galhau, Governor of the Bank of France, at the 6th "Ethics and Trust in Finance" Global Prize ceremony, Paris.

“The philosophers among you will have recognised in this divergence between rules and ethics the classic contrast between Kant’s "categorical imperative" and Aristotle's "practical wisdom". But I am thoroughly convinced that in practice, in the financial sector and in society in general,
we must respect the rules and behave ethically - even when we are respecting the rules.”

**Number 7 (Page 32)**

**Are banks opaque? Evidence from insider trading**

Fabrizio Spargoli and Christian Upper  
BIS Working Papers No 697, February 2018

We contribute to a long literature on whether banks are more opaque than other firms.

*By opaque we mean* that outsiders, such as investors or depositors, are less able to assess the soundness of a bank than that of another type of firm.

An answer to this question has important implications for regulation. For instance, bank opacity could undermine market discipline.

**Number 8 (Page 34)**

**Basel III - Are we done now?**

Statement by Dr Andreas Dombre, Member of the Executive Board of the Deutsche Bundesbank, at the Institute for Law and Finance Conference on Basel III, Frankfurt am Main.

Please let me start with a confession: I strongly support the Basel III finalisation package - in these times, a global minimum standard is a crucial (and noteworthy) success.
It contributes to stabilising the global financial system and prevents regulatory arbitrage.

When talking about Basel III, many banks or lobbyists may think: "Things are never as bad as they seem." Of course, they are hoping for of a less strict implementation of the Basel standards. But I have to say that I, in their stead, would not cherish these hopes.

Looking ahead, all Basel Committee member jurisdictions must do everything in their power to ensure full implementation.

**Number 9 (Page 37)**

**DARPA Seeks to Improve Military Communications with Digital Phased-Arrays at Millimeter Wave**

New program aims to create multi-beam, digital phased-array technology, operating at 18-50 GHz to enhance secure communications between military platforms.

There is increasing interest in making broader use of the millimeter wave frequency band for communications on small mobile platforms where narrow antenna beams from small radiating apertures provide enhanced communication security.

Today's millimeter wave systems, however, are not user friendly and are designed to be platform specific, lacking interoperability and are thus reserved for only the most complex platforms.

**Number 10 (Page 40)**

**MI6, British Intelligence Explained**

---

International Association of Risk and Compliance Professionals (IARCP)
Number 1

Basel III - sense and sensitivity

Ms Sabine Lautenschläger, Member of the Executive Board of the European Central Bank and Vice-Chair of the Supervisory Board of the European Central Bank, at the Institute for Law and Finance Conference on Basel III, Frankfurt am Main.

It is done: Basel III has been finalised.

I admit that it was a long journey, but in my view, it was worth the wait: Basel III will help to make banking safer. It is crucial, though, that Basel III is properly implemented - in Europe and around the world. It must not be watered down.

Basel III marks the end of the post-crisis reforms; regulatory certainty has been restored. The banks know what awaits them; they can be confident about the regulatory framework, and can plan ahead and support the real economy.

But does Basel III deliver what was promised? Does it, on the one hand, create rules which are sufficiently risk-sensitive to set the right incentives for banks? And does it, on the other hand, create rules which are simple enough to decrease model risk?

Banks are not enchanted by Basel III. Many of them claim that it throws risk sensitivity overboard and penalises low risk exposures. Are these claims justified?

Well, we have not thrown risk sensitivity overboard. And why would we? Risk sensitivity helps align capital requirements with actual levels of risk and supports an efficient capital allocation. It prevents arbitrage and risk shifting. And risk-sensitive rules promote sound risk management.
But we all know how challenging it is to measure and model risks. Much depends on the quality of the models; much depends on the data and the assumptions that feed into those models; and much depends on supervisors' capacity to act.

If there are errors along the way, banks might end up undercapitalised and vulnerable. This, in turn, might lead markets to question the reliability of risk-based capital requirements in general, which would undermine trust in banks more generally.

Therefore we need to balance risk sensitivity with some safeguards. And this is exactly what we aim to do with Basel III. It preserves risk sensitivity. It retains internal models for most asset classes. And it enhances the risk sensitivity of the standardised approaches. But at the same time, Basel III adds a few safeguards.

First, I think we can all agree that it makes no sense to allow for more complex risk-sensitive capital requirements if risks cannot be measured and modelled. Basel III therefore aligns the degree of risk sensitivity with the extent to which it is possible to measure and model risks.

Second, there are some more conservative haircuts on collateral and some input floors. These input floors lie beneath the parameters for "probability of default" and "loss given default". And there will be floors beneath the "exposure at default" calculation as well. These floors work bottom-up; they will keep banks from feeding their internal models with excessively low inputs. This serves as a safeguard as it prevents capital requirements from being set too low.

And, yes, these input floors make the rules a bit less risk-sensitive. But we need to look at this in absolute terms - for residential mortgages, the input floor increases from three basis points to five basis points. Five basis points correspond to a once-in-2,000 years default rate! Is such a floor really too conservative? At global level, the bottom-up reforms see small increases in capital for exposures to other banks, large corporates and equity investments. This is somewhat offset by a reduction in risk weights for loans to small and medium-sized enterprises.

Third, there is the hotly debated output floor. It ensures that risk-weighted assets calculated with internal models do not fall too far below those calculated with standardised approaches. "Too far below" means they must reach at least 72.5%. Does that kill risk sensitivity? No, it does not. Obviously, there is still room for banks to apply individual risk weights and
to benefit from lower capital requirements for classic, low-risk banking business.

And more than that: the effective floor might even be lower than 72.5%. This is due to the fact that many banks apply the standardised approaches to at least some exposures. This implies that, depending on the share of assets still under the standardised approach, the effective floor for them could be lower than 72.5%.

At the same time, Basel III makes the standardised approaches themselves more risk-sensitive. Let me give you just one example: residential mortgages. Under Basel II, the standardised approach assigned the same risk weight to almost all such mortgages.

But in Basel III, the risk weights of residential mortgages depend on the loan-to-value ratios.

The output floor is thus set in relation to a benchmark, which itself has become more risk-sensitive.

And let us not forget that, in some cases, the standardised approaches have become less costly in terms of capital.

At global level, the capital requirements from standardised approaches have been reduced by about 2% on average. Mortgages and corporate lending make up the majority of these reductions.

So, Basel III does keep risk sensitivity on board. It acknowledges, though, that there are limits to internal models. It provides safeguards to restore trust in risk-based capital requirements.

Does this mean that Basel III is the perfect standard - the philosopher's stone of banking regulation?

Well, Basel III is a global standard, and across the world, financial sectors differ greatly. Just think of real estate financing and how differently it is treated in Europe compared with the United States.

Thus, a global standard cannot suit everyone perfectly. The key is to find an acceptable compromise; the alternative would be to have no global standard, and that would definitely be worse. The output floor in particular is one such compromise.
What impact will the final Basel III package have on banks - and on their business models and their capital?

The rules are not neutral. The bottom-up safeguards in Basel III, including the input floors, will impact on risk weights in some business areas. Certain retail credit card exposures are one example.

The top-down output floor affects overall capital requirements, depending on the overall portfolio composition of a bank.

For example, our analysis suggests that the difference between internal ratings-based and standardised risk weights tends to be relatively large in certain segments of real-estate markets where historical loss rates are exceptionally low.

The output floor tends to be more binding for banks which are heavily engaged in these markets.

Overall, it is hard to predict how business models will evolve. This depends not only on regulation, but also on many other factors, including the future path of profitability in different business areas, the pricing power of banks and, eventually, how banks will adapt their business models.

Now what about additional capital requirements? What about the banks' claim that the burden might be too heavy for them?

Well, there are two things to bear in mind.

First, there will be a long transition period. This is at the heart of the overall compromise which paved the way for finalising Basel III. This transition period runs right through to 2027.

It gives banks and legislators time to implement all the changes introduced by Basel III.

Second, the European Banking Authority estimates that, for EU banks, the final Basel III package will lead to an aggregate Tier 1 capital shortfall of €34.4 billion.

Is that a lot? In 2016, the largest banks in the euro area earned €50 billion - net, after taxes, and in a difficult environment.
Also, the capital shortfall refers to the end of the transition period, which is nine years away. Most banks should be able to earn their way out of potential shortfalls.

To sum up, Basel III preserves risk sensitivity in a sensible way. At the same time, banks will be able to handle its impact and, in the long run, they too will benefit from a more stable banking system.

Thank you for your attention.
Looking into the crystal ball
A report on emerging technologies and security challenges

The time has come for ENISA to take a look at the crystal ball of technology; In particular looking at what are considered to be emerging technologies and what might be their prospective usage scenarios.

Considering emerging technologies and applications is an important step in assessing future security needs.

ENISA has performed this effort in collaboration with external experts from academia and industry.

Starting with a small number of individuals, it is planned to expand this assessment by engaging additional experts, both within and outside ENISA committees and bodies.

For the time being, the initial sight to emerging technologies has shown that currently top technological challenges are:

- The Internet of Things,
- Autonomous systems,
- Next generation virtualized infrastructures (including SDN and 5G),
- Upcoming societal challenges,
- Virtual and Augmented reality,
- The Internet of Bio-Nano Things,
- AI and Robotics.

Knowing that the above list is not exhaustive, ENISA will continue the dialogue with experts to complement it.

For the above emerging technology areas both technological and cyber-security challenges are presented in this report.

By taking into account the emerging security challenges, the most important cyber security areas have been identified by means of “emerging security related areas”.
These are:

- Elaboration on Certification,
- Coordination of actions in cyber space,
- Development of trustworthiness,
- Coverage of complete lifecycle,
- The future of cryptography,
- Future Identification technologies,
- Use of Artificial Intelligence and Machine Learning in cyber security,
- Increasing end-user involvement.

ENISA believes that these cyber security areas will present challenges to the cyber security community in the years to come and hopes that they will be extensively discussed within its stakeholder communities.

Last but not least, in this work input that has been received by the ENISA Permanent Stakeholder Group (PSG) is being mentioned.

In a similar manner, input will be integrated through an interaction with the new PSG that will have its kick-off end of October 2017. In this manner, both previous and new contributions from PSG will be put in the context of the areas presented in this report, widening thus significantly the number of contributors.

To read more:
https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball
Improving recognition of ICT security standards

Recommendations for the Member States for the conformance to NIS Directive

This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs.

This document provides the results of an assessment of the maturity of the implementation of the European Cyber Security Standardisation activities in the EU Member States with respect to the NIS Directive concerning measures for a high common level of security of network and information systems across the Union.

The main assertions this report makes include the following:

• Standardisation for compliance with the NIS Directive is essential;

• Recognition of standardisation in policy is low;

• Utilisation of standards give value to Member States and their infrastructure;

• Utilisation of standards raises Cyber Security levels;

• Utilisation of standards provides sustainability and interoperability at European level.

The current market research has clearly shown that the information security/cyber security standard development ecosystem is healthy and fast moving.

Few gaps actually exist and to implement the NIS Directive choosing the rights ones and implementing them is of paramount importance.
In the scope of this survey a questionnaire was sent to the Member States representatives and used as the basis of data gathering either in the form of interviews, or by directly completing it and sending responses to the authors.

A summary of the responses given have been collated and summarised.

The content of these responses does not allow to identify whether Member States perceive the existence of a gap in current available standardisation.

However, the content, and general limitations in the cohesion amongst Member States suggests that there is insufficient guidance from the specialists in the field (e.g. national normalization institutes, European institutions etc.), on which of the many standards available are to be used.

It is reasonably straightforward and it follows on the current rate on transposition, to suggest that all Member States are aware of the NIS Directive and their responsibilities in implementing it.

What is less clear is the role that standards have in the NIS Directive implementation.

There is insufficient information with regard to the responses to conclude that a lack of knowledge of standards exists.

This suggests however that if an appropriate standard is available, it will be adopted.

For example, even though the ISO27000 series of standards are in the form of broad guidance, there is a well established eco-system that addresses their implementation.

A major concern is that the NIS Directive domain, and compliance with the NIS Directive requirements, is often perceived as a purely national prerogative.

Where international, cross-border, information sharing is required, this has been perceived as in the domain of existing CSIRT relationships used for reporting security incidents and not directly as an element of NIS Directive compliance.
At the operational level there is very little specified for standards-based NIS Directive compliance and this is one area where ETSI, for example, has made some contributions.
However, there are no mandates at either national or European level to guide this activity at the implementation level.

In light of the above, the following solutions are recommended to mitigate the lack of overall awareness and trainings on the role of standards in NIS Directive compliance and to encourage wide deployment of common security platforms in the OES and PDS entities:

- Training initiatives by the European Commission and ENISA through workshops for Member States’ relevant agencies

- Promotion of new work items in the European SDOs for some areas (e.g. criteria for defining OES / DSP) or the adoption of appropriate standards in Europe where existing (for example information exchange, where several mature efforts already are in place, like STIX )

- Repeat the information gathering as performed within the elaboration of this study after an adequate interval of time

Basel III: Are we done now?

Keynote speech by Mr Stefan Ingves, Chairman of the Basel Committee on Banking Supervision, at the Institute for Law and Finance conference on "Basel III: Are we done now?", Goethe University, Frankfurt am Main.

Introduction

Good morning, and thank you for inviting me to deliver the keynote speech. The title of this conference is "Basel III: Are we done now?". Let me answer this question at the outset: yes, we are done, but that doesn't mean the work has ended. In some respects, it's only just beginning.

While finalising Basel III was an important milestone, work remains to

(i) implement Basel III nationally in a full, timely and consistent manner;

(ii) evaluate its effectiveness in reducing the excessive variability of risk-weighted assets (RWAs); and

(iii) continue to monitor and assess emerging risks. My remarks this morning will focus on these three topics.

Basel III: from 2010 to 2017

But let me start with a brief review of the Basel III framework, which has been ten years in the making.

As you know, the Basel III framework is a central element of the Basel Committee’s response to the global financial crisis. The initial phase of Basel III reforms, published in 2010 (BCBS 2010(a)), focused on
addressing some of the main shortcomings of the pre-crisis regulatory framework, including:

- improving the quality of bank regulatory capital by placing a greater focus on going-concern loss-absorbing capital in the form of Common Equity Tier 1 (CET1) capital;

- increasing capital requirements to ensure that banks can withstand losses in times of stress;

- enhancing risk capture by revising areas of the risk-weighted capital framework that proved to be acutely miscalibrated, including the global standards for market risk, counterparty credit risk and securitisation;

- adding macroprudential elements to the regulatory framework, by: (i) introducing capital buffers that are built up in good times and can be drawn down in times of stress to limit procyclicality; (ii) establishing a large exposures regime that mitigates systemic risks arising from interlinkages across financial institutions and concentrated exposures; and (iii) putting in place a capital buffer to address the externalities created by systemically important banks;

- specifying a minimum leverage ratio requirement to constrain excess leverage in the banking system and complement the risk-weighted capital requirements; and

- introducing an international framework for mitigating excessive liquidity risk and maturity transformation, through the Liquidity Coverage Ratio and Net Stable Funding Ratio.

These reforms have demonstrably helped to strengthen the global banking system. Since 2011, the Tier 1 leverage ratio of major internationally active banks has increased by over 65% (from 3.5% to 5.8%), while their CET1 risk-weighted ratio has increased by over 70% (from 7.2% to 12.3%).

The bulk of this change was achieved by an increase in banks' CET1 capital resources (from €2.1 trillion to €3.7 trillion). There has also been a corresponding reinforcement of banks' liquidity: holdings of liquid assets have increased by 30% (from €9.2 trillion to €11.6 trillion).

There are also clear social benefits from these reforms. During the global financial crisis, the weaknesses in the banking sector were transmitted to the rest of the financial system and the real economy, resulting in
substantial costs. Ten years after the start of the crisis, the global economy is still recovering from its effects. These costs include much higher public debt, increased unemployment and substantial output losses.

To give just one example, a recent study estimates that the cumulative output loss resulting from financial crises is in the order of 100% of GDP in net present value terms.

This output loss would probably have been much larger without the massive public sector interventions. The increase in banks' capital and liquidity resources will help mitigate both the probability and impact of future banking crises.

But a major faultline remained in the regulatory framework, namely, the way in which RWAs were calculated. At the peak of the global financial crisis, a wide range of stakeholders lost faith in banks' internally modelled risk-weighted capital ratios.

The complexity and opacity of internal models, the degree of discretion provided to banks in modelling risk parameters, and the use of national discretions all contributed to an excessive degree of RWA variation.

A growing number of studies by authorities, academics and the private sector pointed to a worryingly large variation in banks' estimated RWAs (BCBS (2013a,b)).

For example, one study found that banks' reported capital ratios could vary by 50% for the same hypothetical portfolio.2 The loss in the public's confidence in banks' reported capital ratios clearly highlighted the need for tighter limits to the way in which RWAs are calculated and greater transparency.

The recently finalised Basel III reforms seek to restore the credibility of RWA calculations, and as a result the public's confidence in the banking system, by:

- enhancing the robustness and risk sensitivity of the standardised approaches for credit risk and operational risk, which will make banks' capital ratios more comparable;

- constraining the use of internally modelled approaches, including by removing the use of the most advanced modelled approaches for certain credit risk asset classes and for calculating operational risk; and
- complementing the risk-weighted capital ratio with a finalised leverage ratio and a revised and robust output floor.

Collectively, the set of Basel III reforms addresses a number of shortcomings in the pre-crisis regulatory framework and provides a foundation for a resilient banking system that will help mitigate the impact of future banking crises and the build-up of systemic vulnerabilities.

The post-crisis framework will also help the banking system support the real economy and contribute to economic growth.

**Full, timely and consistent implementation: more than just words**

But are these reforms enough, or does more need to be done? The answer depends in part on the extent to which the reforms are implemented in a full, timely and consistent manner across jurisdictions. To borrow the words of Goethe (1829): "willing is not enough, we must do".

The Basel Committee's standards are global minimum standards. The Committee has no supranational authority, its decisions carry no legal force, and it cannot impose fines or sanctions.

Rather, once the Committee agrees on a standard, its member jurisdictions are responsible for converting this standard into law or regulation.

So internationally agreed standards that are not properly implemented will ultimately have no impact in practice.

It is therefore imperative that the Basel standards are effectively implemented by all the Committee's jurisdictions.

To this end, the Committee's flagship Regulatory Consistency Assessment Programme (RCAP) monitors the timely adoption of Basel standards across jurisdictions and reviews whether standards are completely and consistently adopted by member jurisdictions.

They also highlight any deviations from the Basel framework. As a result of the RCAPs, over 1,200 deviations were identified as part of the peer reviews focusing on the initial Basel III capital reforms. Two thirds of Basel Committee members have risk-weighted capital rules that are considered compliant or largely compliant with the Basel standards.
Looking forward, the RCAP will continue to play a key role in ensuring that the recently finalised Basel III reforms are implemented as agreed by the Committee. But let me stress three points.

First, in developing its standards, the Committee actively seeks the views of all stakeholders, public and private.

For example, in finalising Basel III, the Committee consulted extensively with academics, analysts, banks, finance ministries, parliamentarians, market participants and trade associations as well as the general public.

These views were duly considered by the Committee in finalising its standards. So there are plenty of opportunities for all stakeholders to express their views before the standards are finalised. The focus then should be on full, timely and consistent implementation.

Second, in endorsing the finalised Basel III reforms, the Group of Governors and Heads of Supervision (GHOS) has unanimously reaffirmed that they expect full, timely and consistent implementation "of all elements" of the Basel III package (BCBS (2017a)). So I take comfort that all of the Committee's members keep this aim in the forefront of their minds during the implementation phase.

Third, the move to national implementation should not be read as an invitation to reopen policy issues and debates at a domestic level.

While the varying legislative and procedural arrangements used to implement Basel standards across the Committee's membership must be fully respected, it is concerning to see ongoing lobbying efforts by some banks and other stakeholders to undo or dilute aspects of the agreed Basel standards in some jurisdictions.

The unsound expedient of adopting standards that fall below the Basel Committee's minimums can only lead to regulatory fragmentation, and in a bad scenario a potential race to the bottom.

Just getting up close, as we like to say in Sweden, isn't enough to shoot the hare.

Reducing excessive RWA variability: mission accomplished?

Assuming that the Basel reforms are properly implemented, will they reduce excessive RWA variability and restore the credibility of the
risk-weighted capital framework? While I am confident that the Basel III reforms are an important step in that direction, the honest answer is that only time will tell.

To that end, the Committee has initiated a rigorous evaluation of its post-crisis reforms, including those that relate to reducing excessive RWA variability.

As the reforms will only start to be implemented from 2022 onwards, this exercise will take several years.

But I believe that the Committee should remain open to the possibility of considering whether additional measures, or revisions to existing measures, are warranted to reduce excessive RWA variability.

In a similar vein, the Committee is also further evaluating the interactions and coherence of its post-crisis reforms. The findings will provide an important input for future deliberations by the Committee about the robustness and effectiveness of its post-crisis framework.

I will not prejudge the outcomes of these evaluations, but let me make three observations.

**First**, the purpose of these evaluations is not to reopen already agreed standards.

**Second**, the Basel Committee is a member-led and consensus-based body. Accordingly, the Basel III reforms are a compromise that reflects the different views of its members.

**Third**, as the Basel reforms are minimum standards, jurisdictions are welcome to apply more conservative requirements should they wish to do so. This could include faster transitional arrangements and/or more conservative steady-state requirements.

**Enhancing financial stability: an ongoing journey**

If the Basel reforms do reduce excessive RWA variability, is the job then done? Probably far from it. Banking crises are inevitable. So, while the Basel standards cannot prevent all future crises, they can seek to mitigate their likelihood and impact.
This, in turn, requires the Basel Committee to remain vigilant for emerging conjunctural and structural risks. It also needs to monitor how banks are responding to its post-crisis reforms.

All this highlights the importance of supervision as a complementary tool to regulation. Let me say a few remarks about both these issues.

Emerging risks

An example of a topical risk of direct relevance for the Basel Committee is cyber-risk. The banking system is increasingly reliant on information technology, which exposes it to a growing and evolving set of operational risks.

Banks with operationally resilient systems, staff, processes and technology can better adapt to evolving shocks and maintain the provision of critical financial services.

The Committee is reviewing its existing cyber-risk measures and will consider whether additional measures are needed to enhance banks' operational resilience.

Behavioural responses to post-crisis reforms

With the Committee's post-crisis reforms now finalised, and with only minor technical issues remaining, the Basel Committee will carefully monitor banks' responses to its reforms.

It will continuously assess banks' behavioural responses, and the potential emergence of any optimisation or arbitrage techniques that may not meet the letter or spirit of the Basel standards. In this case, it will consider whether any measures are needed to address such issues.

Supervision

The Committee's response to the global financial crisis included much more than just regulation. It also encompassed a range of measures to support strong supervision.

These include principles and guidance on corporate governance, risk data aggregation, the prudential treatment of assets, the treatment of weak banks and an updated set of core principles for effective banking
supervision. The Committee will step up its efforts to promote improvements in banking supervision practices and principles.

**Conclusion**

In summary, the finalisation of Basel III in December 2017 represents an important milestone for the Basel Committee’s response to the global financial crisis. The full set of Basel III reforms will help enhance the resilience of the banking system.

But we cannot rest on our laurels. Whether it relates to the proper implementation of these reforms, their evaluation, or the assessment of emerging risks, the Basel Committee will continue to exercise its mandate to strengthen the regulation, supervision and practices of banks worldwide.

The agenda changes, but the purpose is constant - to safeguard and enhance financial stability.
PSD2 - will it be a game-changer?

Job Swank, Executive Director of the Netherlands Bank, at ESB's Conversation with Regulators on Innovation in Payment Services, The Hague.

Ladies and gentlemen, I'm grateful to the organizers of this conference for inviting me here. This Conversation with Regulators is the last in a series of events on innovation in payment services, organized by ESB. For those of you who can read Dutch, I highly recommend the dossier Innovatie in Betalen, issued by ESB in September. It has much more to offer than you will hear from me today.

Today's topic is PSD2. PSD2 is a European directive, to be implemented through national legislation. And PSD2 is about payments. To most people, these topics - legislation and payments - are extremely boring, a necessary evil. Probably not to you. Otherwise, you wouldn't be here, but you are certainly a minority.

To read more:
https://www.bis.org/review/r180130c.pdf
Ladies and Gentlemen,

It is with great pleasure that I welcome you all to the auditorium of the Banque de France for the 6th "Ethics and Trust in Finance" Global Prize ceremony. I would particularly like to welcome Angel Gurria, Secretary-General of the OECD, and Professor Paul Dembinski, the Co-chair of the prize.

The venue that you have been invited to today sends a message in itself: as the Autorité de contrôle prudentiel et de résolution is backed by the Banque de France, some might have a tendency to think that the bank and insurance supervisor, as the "guardian of the temple", would only be concerned with compliance with prudential rules, which are collective and compulsory.

They might also think that the supervisor would consider that an ethical approach is too poorly defined to be inspected, as each financial institution - and even each professional - has their own perspective on it, and would also consider that an ethical approach leaves them free to look after the interests of their clients.

The philosophers among you will have recognised in this divergence between rules and ethics the classic contrast between Kant’s "categorical imperative" and Aristotle’s "practical wisdom". But I am thoroughly convinced that in practice, in the financial sector and in society in general, we must respect the rules and behave ethically - even when we are respecting the rules. A number of cases that have recently made the headlines have also shown that citizens and customers alike are becoming
increasingly demanding in this regard. Adopting the same reasoning, Paul Dembinski likes to quote Ricoeur's broader definition of ethics as "a wish for a fulfilled life - with and for others - in just institutions".

1. From this perspective, what is at stake is more than a simple contrast, but the sound balance and dynamic tension between compulsory rules and enduring, freely adopted ethics.

There can be no doubt that the financial sector needs rules. This is not just a question of an activity that involves intermediation between different parties - each of which must be convinced that the rules are being properly applied - but it is also a question of managing risks, while protecting the interests of customers and policyholders. Financial instability also has substantial externalities on the economy, and on social cohesion through unemployment. The recent financial crises have brought the failings of the financial system into focus, not forgetting the impact of new technologies, such as high frequency trading, FinTechs, or crypto-assets.

But rules have their limitations. An ethical approach is needed if we are to respect the spirit of the rules - and not just the letter of the law - and if we are to make informed decisions when clear rules are not available. In addition to financial institutions’ in-house ethical practices, the financial sector must now also consider how society - NGOs, the media, fellow citizens included - perceive its activities from an ethical standpoint.

Clearly, the 2007-09 crisis was partly created by an imbalance: too much trust had been placed in ethics, while the rules were insufficient. The weaknesses in the corporate culture of financial institutions were thrust into the spotlight; incentives to take risks were too powerful and governance was inappropriate.

Certain Anglo-Saxon expressions perfectly illustrate the period: "too big to fail" created a widespread moral hazard, "tick the box" encouraged overly lax self-regulation through a purely formal compliance with the rules... and in so doing, the "light touch" of the British FSA at the time clearly showed its limitations.

Since then, I am happy to say that we have significantly tightened up the rules. With the CRD IV Capital Requirements Directive and Basel III for banks and, at least in Europe, Solvency II for insurers, quantitative requirements have been reinforced to ensure greater resilience, governance of financial institutions has been improved and compensation policies for bankers have been reined in a little.
International regulation is our common good. It strengthens a sound financial system. But as we strengthen international regulation, we must not lower our guard in terms of ethics. Ten years later, this would generate the opposite imbalance to that of 2007-08. In other words, there’s a risk that the pendulum could swing back the other way.

2. **Ethics must permeate the day-to-day practices and culture of financial institutions.**

Over and above the good intentions, declarations and codes of conduct, which did nothing to prevent the excesses that caused the 2008 crisis, the challenge now is for all actors from the bottom to the top of these organisations to adopt an ethical approach.

As the "Banking Conduct and Culture" report of the Group of Thirty, which brought together private and central bankers and academics, asserted, the "tone from the top" must have an "echo from the bottom".

This begins with the Boards of Directors and the management teams, who must always be exemplary, and who need to realise that their behaviour is scrutinised at all times for indications of what is acceptable and what is not, irrespective of their declarations of intent. Actions speak louder than words.

It then requires employees to be trained and informed on ethical standards on a regular basis and not only on their first day on the job. Situations change; new developments can be an opportunity to reconsider existing practices; stakeholder expectations evolve.

Ethics - just like technical issues - must be subject to constant communication and ongoing training. And this is no easy task. As ORSE's report on corporate ethics, responsibility and strategy1 quite rightly reminds us, "Corporate ethics is not built on obedience, but on engagement and discernment". Employees must be able to identify ethical "grey areas" even when their manager or clear rules are not available.

If ethics are to permeate corporate practices, they must form an integral part of HR policies and structures. For example, during selection procedures for external recruitment or internal promotion, particularly for management positions, the integrity of candidates during their career should be seriously assessed and taken into account.
Ethics in themselves have value. Good performances can neither excuse nor compensate for questionable ethical behaviour. Results obtained at the expense of ethical standards should not be rewarded.

On the contrary, they should be penalised in order to send the right message with regards to expected behaviour, including from the managers of the employees concerned.

Diversity within teams, and particularly management teams, should be encouraged. Experience shows that diversity - in terms of gender, social background, education, thinking - is a factor in risk prevention.

An overly homogeneous group does not debate, loses critical thinking and as a result takes more risky decisions.

At a time when technical processes and compliance procedures are becoming increasingly complex and favour dialogue between human and machine, direct human contact should once more be given the importance it deserves.

Employees must be able to approach managers with their questions on ethics in just the same way as they can ask technical questions; with the same ease, the same freedom, the same legitimacy.

No-one should be afraid of raising ethical questions, being concerned about certain practices, or raising ethical concerns, which is now protected by law since the introduction in France of the Sapin II Act.

Alongside the approach offered by human resources, the permeation of ethics into corporate practices and cultures is achieved through their integration into business strategy, and their monitoring and supervision by the three lines of defence - first, management; second, ethics and compliance officers; and third, audit.

Financial institutions must consider corporate culture as a key strategic element rather than a specific field only intended to provide a short-term response to regulatory requirements.

Personally, I am also convinced that in the long term, ethics pays, even if it does not always immediately pay in "cold, hard cash", as the Anglo-Saxons say.
It is only by promoting ethics as a desirable value in themselves that we will obtain the right mix between ethical standards and the regulations necessary for a sound financial system.

And that is why the Prize being awarded today is no stranger to the Banque de France and the ACPR. I hope you all enjoy the ceremony.
**Number 7**

Are banks opaque? Evidence from insider trading

Fabrizio Spargoli and Christian Upper
BIS Working Papers No 697, February 2018

Summary

Focus

We contribute to a long literature on whether banks are more opaque than other firms.

By opaque we mean that outsiders, such as investors or depositors, are less able to assess the soundness of a bank than that of another type of firm.

An answer to this question has important implications for regulation. For instance, bank opacity could undermine market discipline.

Contribution

We test whether banks are more opaque than other firms by looking at how equity prices respond to trades by bank or firm insiders.

These are purchases or sales by senior company officials, who presumably have better information on the future performance of their institutions than outside investors.

If companies are opaque, then insider purchases should be followed by increases in equity prices and insider sales by drops, at least on average.

We believe that price responses to insider trades provide a better measure of opacity than the variables used in previous studies, such as bid-ask spreads, which are also affected by a range of other factors.

Findings

Our results do not support the conventional wisdom that banks are more opaque than other firms.
Yes, purchases by bank insiders are followed by positive stock returns, indicating that banks are opaque.

But banks are not special as we find the same effect for other firms. Where banks are special is when bad news arrive.

We find that sales by bank insiders are not followed by negative stock returns.

This suggests that bank insiders do not receive bad news earlier than outsiders. By contrast, insider sales at non-banks tend to be followed by a decline in stock prices.

Abstract

We use trades by US corporate insiders to investigate bank opacity, both in absolute terms and relative to other firms. On average, bank insider sales do not earn an abnormal return and do not predict stock returns.

By contrast, bank insider purchases do, even though less than other firms. Our within-banking sector and over-time analyses also fail to provide evidence of greater opacity of banks vis-à-vis other firms.

These results challenge conventional wisdom and suggest that, to assess bank opacity, the type of benchmark (transparency vs. other firms) and transaction/information (purchase/positive vs. sale/negative) are crucial.

To read the paper: https://www.bis.org/publ/work697.pdf
**Number 8**

**Basel III - Are we done now?**

Statement by Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the Institute for Law and Finance Conference on Basel III, Frankfurt am Main.

Thanks Nicolas, it’s a great pleasure to contribute to this panel. And, on behalf of the Bundesbank, I am happy to see that so many outstanding experts accepted our invitation.

Please let me start with a confession: I strongly support the Basel III finalisation package - in these times, a global minimum standard is a crucial (and noteworthy) success.

It contributes to stabilising the global financial system and prevents regulatory arbitrage.

When talking about Basel III, many banks or lobbyists may think: "Things are never as bad as they seem." Of course, they are hoping for of a less strict implementation of the Basel standards. But I have to say that I, in their stead, would not cherish these hopes.

Looking ahead, all Basel Committee member jurisdictions must do everything in their power to ensure full implementation.

But as important as Basel III is, we should not forget what it was made for - and what not.

The Basel III standards are, first, minimum standards for, second, internationally active banks.
Let me say a few words about the first point: Since Basel standards are minimum standards, a country may decide to set stricter requirements.

The second qualification of the Basel III standard is that it is for internationally active banks. As such, jurisdictions are free to apply a different set of rules to smaller, only nationally active banks that pose no threat to international financial stability.

In sum, then, we should focus on truly global aspects, like regulating globally active banks, while leaving it to nation states to carry out those tasks that they are better suited to take care of, for example the regulation of locally active banks.

In this sense, let's not forget the former governor of the Bank of England, Mervyn King, who said: "Banks are global in life, but national in death."

To make one thing quite clear: There is no alternative to global standards, but within their implementation, we must not forget that a "one size fits all" approach does not always reflect national different banking systems.

So, in sum: Yes, we are done with Basel, but we should lose no time and start implementing it.

And one point is of crucial importance in my mind: After having implemented Basel III, we need a regulatory break - because, yes there is regulatory fatigue; but do not get me wrong - this is no ticket for regulatory capture and deregulation.

As tired as banks are of new regulation, as tired are we regulators of their (often unsolicited) lobbying efforts.

In that sense, I clearly expect from the industry to adapt their business models to those new rules.

The comparable positive reaction the stocks markets showed in face of the Basel compromise is in my view a sign for the value of regulatory certainty - so let's go for it.

Therefore, let me recall the objective of Basel III, which is to reduce RWA variability, and not to raise regulator capital on average. We still strive for that objective in the implementation period that will follow. So, the answer to our leading question is: Yes, we are done now with Basel III.
Therefore, all discussions about the outcome - or the desired outcome - are a waste of time. What we need to discuss is **how to implement** Basel III in a way that is as close to the agreed standards as possible, but, at the same time, also reflects national particularities.

And when this is done, we can have our regulatory break to see how all the reforms interact with each other and whether they all work as they should.

In the meantime, let's stop complaining about a one or two percent higher output floor, but let's start talking about the real stuff that may endanger our financial system. **Cyber crime** is only one catchword amongst many challenges that lie ahead.
DARPA Seeks to Improve Military Communications with Digital Phased-Arrays at Millimeter Wave

New program aims to create multi-beam, digital phased-array technology, operating at 18-50 GHz to enhance secure communications between military platforms.

There is increasing interest in making broader use of the millimeter wave frequency band for communications on small mobile platforms where narrow antenna beams from small radiating apertures provide enhanced communication security.

Today’s millimeter wave systems, however, are not user friendly and are designed to be platform specific, lacking interoperability and are thus reserved for only the most complex platforms.

To expand the use of millimeter wave phased-arrays and make them broadly applicable across DoD systems, many technical challenges must be addressed, including wideband frequency coverage, precision beam pointing, user discover and mesh networking.

The use of multi-beam phased arrays as well as advances in digital radio and millimeter wave technology have propelled technology to the current state, and now there is a paradigm shift on the horizon as millimeter wave phased-arrays are poised to change communication and networked mobile platforms.

Phased-arrays operating at millimeter wave—or very high frequencies—are already an active area of research by the emerging 5G cellular market. Commercial applications are primarily solving the “last mile” problem, where consumers are demanding more bandwidth for high-throughput applications over relatively short ranges at predetermined frequencies and with minimal obstacles to user discovery.

DoD platforms on the other hand create far more complex communications environments. Often separated by tens or even hundreds of nautical miles, today’s military platforms are moving in three dimensions with unknown
orientations. This environment is creating unique beamforming challenges that can’t easily be solved by applying current communications approaches.

“Imagine two aircraft both traveling at high speed and moving relative to one another,” said DARPA program manager Timothy Hancock. “They have to find each other in space to communicate with directional antenna beams, creating a very difficult challenge that can’t be solved with the phased-array solutions emerging in the commercial marketplace.”

To address these challenges, DARPA is launching the Millimeter-Wave Digital Arrays (MIDAS) program. Announced today, the program aims to develop element-level digital phased-array technology that will enable next generation DoD millimeter wave systems.

To help solve the adaptive beamforming problem and ensure wide application of the resulting solutions, MIDAS seeks to create a common digital array tile that will enable multi-beam directional communications.

Research efforts will focus on reducing the size and power of digital millimeter wave transceivers, enabling phased-array technology for mobile platforms and elevating mobile communications to the less crowded millimeter wave frequencies.

Advances in element-level digital beamforming in phased-array designs is enabling new multi-beam communications schemes—or the use of several beams receiving and transmitting in multiple directions simultaneously—to help significantly reduce node discovery time and improve network throughput. “While critical to the next generation of phased-arrays, today’s digital beamforming is limited to lower frequencies, making the resulting arrays too large for use on small mobile platforms,” said Hancock.

To reduce the size of the arrays, advances in millimeter wave technology will help push the frequency of operation to higher bands, bringing the capabilities of directional antennas to small mobile platforms. “Through MIDAS, we are seeking proposals that combine advances in millimeter wave and digital beamforming technologies to create radios that will deliver secure communications for our military,” said Hancock.

To accomplish its goals, MIDAS is focused on two key technical areas. The first is the development of the silicon chips to form the core transceiver for the array tile.
The second area is focused on the development of wide-band antennas, transmit/receive (T/R) components, and the overall integration of the system that will enable the technology to be used across multiple applications, including line-of-sight communications between tactical platforms as well as current and emerging satellite communications.

Hancock envisions the four-year program being administered in three phases.

A full program description can be found in the Broad Agency Announcement that was issued on January 23: https://www.fbo.gov/index?s=opportunity&mode=form&id=d8c414aaf7c707bc4f7ac896a7b68b29&tab=core&cview=0
MI6, British Intelligence Explained

A very interesting page.

You may visit:
https://www.sis.gov.uk/intelligence-explained.html#section-01
Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;
- should not be relied on in the context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of an interpretative document;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.
The International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:

1. **Membership** – Become a standard, premium or lifetime member.

   You may visit:  
   www.risk-compliance-association.com/How_to_become_member.htm

   Become a lifetime member of the association, and to continue your journey without interruption and without renewal worries. You will get a lifetime of benefits as well.

   You can check the benefits at:  
   www.risk-compliance-association.com/Lifetime_Membership.htm

2. **Weekly Updates** - Subscribe to receive every Monday, the Top 10 risk and compliance management related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next:  
   http://forms.aweber.com/form/02/1254213302.htm

3. **Training and Certification** - The Certified Risk and Compliance Management Professional (CRCMP) training and certification program has become one of the most recognized programs in risk management and compliance.

   There are CRCMPs in 32 countries around the world. Companies and organizations like Accenture, American Express, USAA etc. consider the CRCMP a preferred certificate.

   You can find more about the demand for CRCMPs at:  

   For the **distance learning** programs, you may visit:  
   www.risk-compliance-association.com/Distance_Learning_and_Certification.htm
For instructor-led training, you may contact us. We can tailor all programs to meet specific requirements. We tailor presentations, awareness and training programs for supervisors, boards of directors, service providers and consultants.

4. IARCP Authorized Certified Trainer (IARCP-ACT) Program - Become a Certified Risk and Compliance Management Professional Trainer (CRCMPT) or Certified Information Systems Risk and Compliance Professional Trainer (CISRCPT).

This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

To learn more, you may visit: www.risk-compliance-association.com/IARCP_ACT.html

5. Approved Training and Certification Centers (IARCP-ATCCs) - In response to the increasing demand for CRCMP training, the International Association of Risk and Compliance Professionals is developing a world-wide network of Approved Training and Certification Centers (IARCP-ATCCs).

This will give the opportunity to risk and compliance managers, officers, and consultants to have access to instructor-led CRCMP and CISRCP training at convenient locations that meet international standards.

ATCCs use IARCP approved course materials and have access to IARCP Authorized Certified Trainers (IARCP-ACTs).

To learn more: www.risk-compliance-association.com/Approved_Centers.html