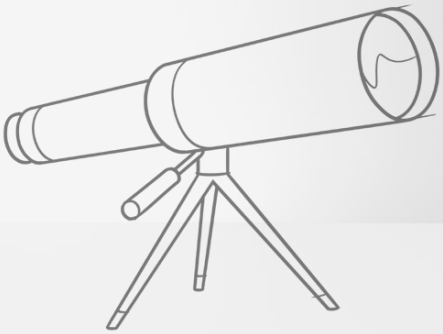
» REGULATORY TRENDS IN BANKING



Since the financial crisis reached its peak in 2008, 10 years of continuous work on regulatory and supervisory standards have passed. During this time, a multitude of new regulations and laws for banks – such as the CRD IV package – have been released.

To this day, policies are constantly amended, adapted or simply updated to reflect new findings. Thus, even after a decade of transformation in the banking sector, the "flood of regulations" does not cease.

This paper summarises current trends and developments in the areas of banking regulation and supervisory practice.

On the one hand, the BCBS Standard "Finalising Basel III" indicates that regulators are **turning away from** allowing banks to use **internal models** (Trend 1); on the other hand, the regulatory focus on **new risks** such as cyber risk (Trend 2) seems to increase. Furthermore, there is a tendency towards **reporting single data cubes** instead of aggregated reports (Trend 3) – one reason, why many banks are starting to concentrate on **standardising and consolidating their IT applications** at group level (Trend 4). In a nutshell, fulfilling regulatory requirements remains complex and demanding for banks.

» TREND 1
TURNING AWAY FROM INTERNAL MODELS

STATUS QUO

Currently, internal models play an important role in both **regulatory capital** calculation and internal **risk assessment**. Compared to standardised approaches, they allow for a more risk-sensitive RWA calculation and might thus lead to a reduction in capital adequacy requirements.

Yet, in context of the Supervisory Review and Evaluation Process (SREP), it was shown that the use of internal models implies a **heterogeneous risk assessment** – even if banks have similar risk profiles – and thus leads to **non-comparability** of capital adequacy requirements.

The supervisory authority reacted by introducing the Targeted Review of Internal Models (TRIM)[1], an audit of internal models used at systemically-important banks. The purpose was to confirm the adequacy of approved Pillar 1 models, ensure compliance with regulatory standards and harmonise supervisory practices under the Single Supervisory Mechanism (SSM).

In addition to revising the model approval process, there is an ongoing discussion on whether and – if so, in which scope – internal models should be allowed as tools to determine regulatory capital adequacy requirements.

TREND

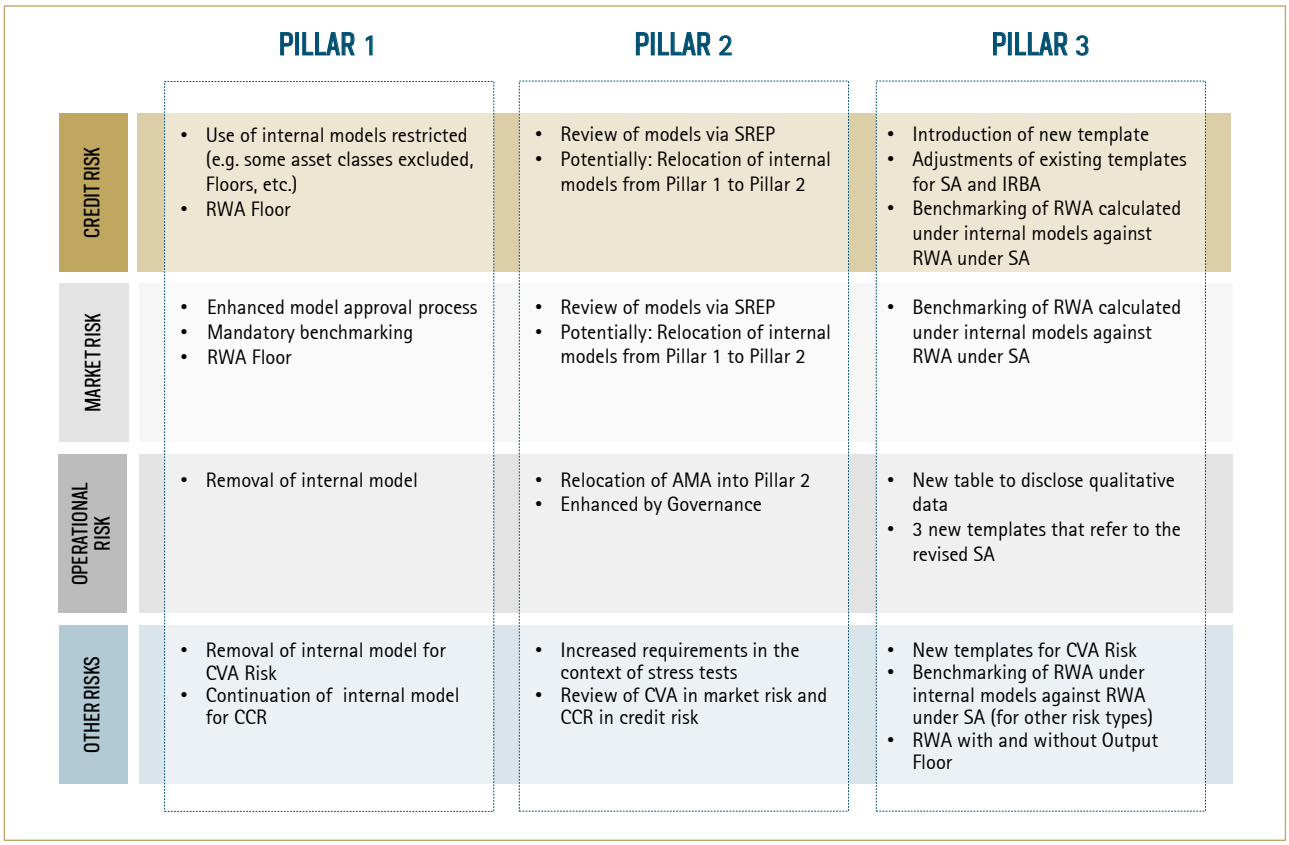
Supervisory authorities and regulators are increasingly turning away from internal models used by banks to determine risks and capital adequacy requirements. Instead, they focus on simple, risk-sensitive and standardised methods. These aim to enhance transparency and comparability, thereby facilitating the monitoring of financial system stability. Another reason for the authority's tendency to prefer standardised methods is to minimise the advantage bigger and more complex banks have over smaller ones, resulting from their superior resources.

These objectives are particularly reflected in the **finalised Basel III reform**[2], published in December 2017. In this paper, more risk-sensitive standardised approaches for Credit Risk, Credit Valuation Adjustment Risk (CVA Risk) and Operational Risk (OpRisk) are introduced. For Credit Risk, this implies amongst others the existence of new asset classes (such as subordinated debt and covered bonds), the adjustment of required risk weights as well as the obligation to perform due diligence. The standardised approach for OpRisk is recalibrated, i.e. large institutes must include own loss data, the volume-oriented "Business Indicator" serves as reference value and events with a loss value of less than €20,000 may be excluded.

Furthermore, the reform excludes internal models for CVA Risk and OpRisk from Pillar 1 and considerably restricts the scope of the internal model for Credit Risk. For instance, using the advanced IRB-Approach for risk exposures towards large and medium-sized companies, banks or other financial institutions will not be allowed in future, as the robust and conservative modelling of credit risk is not possible for these asset classes. So, in a first step, the supervisory authorities are **turning away from allowing banks to use internal models**.

[1] See also: https://www.bankingsupervision.europa.eu/about/ssmexplained/html/trim.en.html

[2] Standard BCBS 424 (Basel III: Finalising Post-Crisis Reform)



Reference: ifb group

In a second step, the supervisory authority is concentrating on avoiding the **disproportional reduction of capital adequacy requirements** for those institutions that are allowed to use the IRB Approach for Credit Risk. For example, to reduce RWA variability, the use of fixed values for Loss Given Default (LGD) and Exposure At Default (EAD) in the Foundation Approach is made mandatory. Additionally, Input Floors are introduced into both the Foundation and Advanced IRB Approaches, which define minimum thresholds for the Probability of Default (PD) as well as for LGD and EAD (only in Advanced IRB Approach). At the same time, haircuts used for collaterals increase while LGD parameters decrease.

However, the most fundamental change is the introduction of **a minimum threshold for aggregated RWAs**, the Output Floor: From now on, the value of total RWAs under the IRB Approach may only be as low as 72.5 % of the corresponding value that would be applicable under the standardised approaches.

To take account of these Basel III Framework changes within existing **disclosure policies**, a new consultative document updating the Pillar 3 requirements[3] was published in February 2018. Besides adjusting the existing disclosure requirements for Credit Risk, OpRisk and CVA Risk, the Basel Committee also aims at introducing an entirely new one: The **Benchmarking of RWAs** under internal models against RWAs under standardised approaches. More precisely, the RWAs for each risk type, calculated by applying internal models, must be compared to the RWAs that would be applicable if standardised approaches were used. This way, transparency is enhanced and comparability between different banks improved.

[3] Standard BCBS 400 (Pillar 3 disclosure requirements – consolidated and enhanced framework, Consultative Version)

EFFECT

IN THE SHORT RUN, the new regulatory rules imply higher costs for banks: They will have to adjust existing IT systems, calculation and reporting processes and prepare for potentially higher capital adequacy requirements. Both the introduction of the Output Floor and the obligation to use standardised approaches for CVA Risk and OpRisk, might increase the RWA values and lead to higher capital requirements in the medium term. Complying with regulatory standards might thus be more expensive in the future and even force institutions – in extreme cases – to reduce their distribution of dividends.

IN THE LONG RUN, however, the standardisation of risk models offers chances, too. It facilitates stakeholders' comparison of institutions' accepted risks and available capital buffers. And banks can also profit: As internal models are complex, expensive to implement, depend on a rich data history and are difficult to get approved, the removal of these from Pillar 1 offers huge cost reduction opportunities – risk model governance will necessarily become cheaper and more streamlined through, for example, "off-the-shelf" risk models, which are devised and managed by external providers. Such outsourcing is conceivable for the risk assessment of both Credit and Market Risk for regulatory, perhaps even internal management, purposes.

IN SHORT

Currently, the supervisory authorities are increasingly turning away from internal models, which manifests itself, on the one hand, in far-reaching restrictions to their application in Pillar 1 and, on the other hand, in increased model approval requirements. Hence, banks should reduce their focus on internal models to save costs; at the same time, they must be aware of potentially higher capital adequacy requirements in the future.

» TREND 2

FUTURE OF PILLAR 2 – INTEGRATING NEW RISKS & GOVERNANCE

Today STATUS QUO

The **traditional risk types** Credit, Market and Liquidity Risk have reached a **high degree of maturity** from both a regulatory and economic standpoint – calculation and steering of these risks are mostly standardised due to regulatory requirements in Pillar 1 and highly mature internal bank processes governed in Pillar 2.

Meanwhile, supervisory authorities and regulators are becoming aware of **new risk types** such as Cyber and **Model Risk**, which are considered to be sub-categories of Operational Risk (OpRisk).

However, the Standardised Approach for OpRisk in Pillar 1 is a rather vague indicator whose main purpose is to homogenise and increase the comparability of the calculation of capital requirements between institutions. There is no explicit distinction between single risk sub-types – such considerations are to be found for the time being in **Pillar 2**.

TREND

Just recently, the Basel Committee (BCBS) developed a new standardised approach for OpRisk in **Pillar 1** (Standardised Measurement Approach, **SMA**). Because the idea to introduce an internal model (Advanced Measurement Approach, AMA) has had no success so far, this standardised approach will now be extended to include a **historical loss component**, reflecting the idiosyncratic nature of operational risks.

In **Pillar 2**, the supervisory management of operational risks is increasingly achieved via **explicit Governance requirements**, e.g. in the context of SREP. Here, "**new**" and previously unregulated **risk types**, or those only regulated to a small extent, are considered.

Risk managers regard operational risks, which are difficult to quantify and likely to involve – should they be incurred – enormous losses, as particularly important in 2018.[4] Among these are Cyber, Model and Geopolitical Risk. Due to their low probability of occurrence, these risk types have been typically not / only to a minor extent observed and / or managed; yet, due to current global developments the likelihood of their occurrence is steadily increasing. Therefore, particularly the new risk types that have gained relevance over the last few years are managed via Governance requirements.

In its "**Pillar 2 Roadmap**"[5] (published in April 2017), the EBA confirmed this focus. It considers Internal Governance to be one of the sections in the SREP Guidelines that needs to be updated, and emphasises its intention to increasingly take Governance into account in future.

In its Consultation Paper on the revision of SREP[6], published at the end of 2017, the EBA therefore adds the requirement that national supervisory authorities should not only determine the banks' individual risk score by solely evaluating inherent risks, but should also include considerations with regard to risk management and controls.

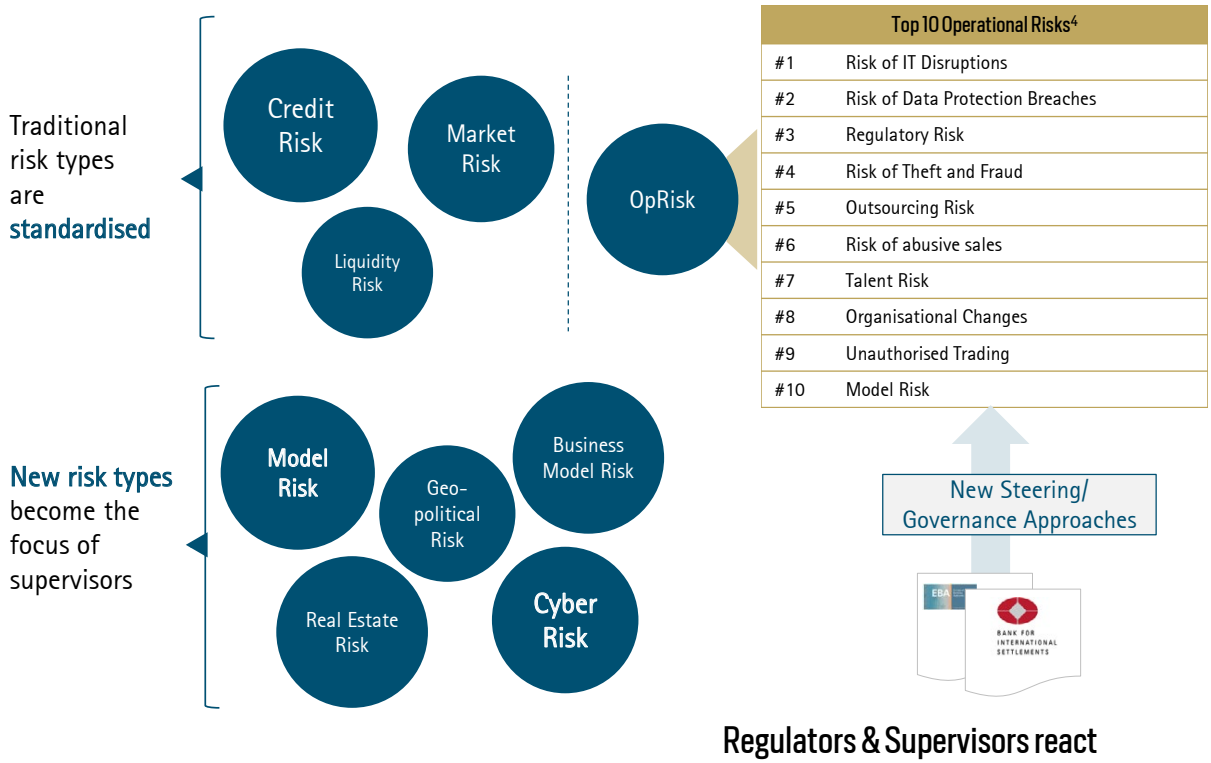
Nevertheless, the regulatory requirements regarding new risk types such as Cyber or Model Risk are **rather general** so far and not yet mature. Guidelines for calculation methods, e.g. concerning stress testing or scenario analyses, are currently missing.

[4] See also: https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018

[5] See also: https://www.eba.europa.eu/-/eba-outlines-roadmap-of-its-plan-to-update-2017-2018-srep

[6] EBA/CP/2017/18: Consultation Paper on Draft Guidelines on the revised common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing

The presence of new risk types in the recent public and supervisory discourse, though, indicates that this might change. From a bank's perspective, an early assessment of the topic is thus vital; particularly because whether/how risk controlling of new risks is conducted will be monitored in the course of SREP as early as 2018.



Reference: ifb group

FOR THE FOLLOWING RISK TYPES, POSSIBLE SUPERVISORY ACTION CAN ALREADY BE PREDICTED:

CYBER RISK

In a report prepared for the G20 Summit 2017 in Hamburg[7], the Financial Stability Board (FSB) mentioned the treatment of cyber risks as one of the top three priorities for international collaboration in the areas of supervision and regulation.

The Bank for International Settlements (BIS) has also focused extensively on the topic of cyber risks. According to a paper[8] on current regulatory approaches towards the treatment of cyber risks, **two contradictory opinions** exist in international comparison:

[7] See also: www.fsb.org/2017/06/fsb-issues-a-report-on-the-financial-stability-implications-from-fintech/

[8] Crisanto, J. C., & Prenio, J. (2017). Regulatory approaches to enhance banks' cyber-security frameworks. *FSI Insights on policy implementation No 2.*

1. The majority of bank supervisory authorities is of the opinion that there is no need to account for cyber risks as a stand-alone risk type so far. Instead, cyber risks are covered by current regulations as part of Op- or TechRisk.
2. A few single jurisdictions (amongst those Hong Kong, Singapore, UK and the US), however, do not share this opinion. From their point of view, an **explicit regulation of Cyber Risk** is necessary. Thereby, some favour the use of a principles-oriented approach, whereas other favour the application of precise rules.

The few existing regulatory requirements regarding cyber risks might serve as examples for other jurisdictions in the future – should the explicit consideration of cyber risks be established as standard in the international regulatory landscape.

Since 1st January 2018, European supervisory authorities must adhere to a specific guideline dealing with the treatment of Cyber Risk – or more precisely, of the "**Information and Communication Technology (ICT) Risk**" – as a component of OpRisk under SREP. In this guideline, published in May 2017[9], the EBA defines not only the emergence of (new) cyber risks in the sense of attacks on the bank's IT landscape, but also the increased dependence on outsourced ICT services and products from third-party providers as cyber risks. In their bank audit process, national supervisory authorities should explicitly address whether and how these cyber risks are covered in the context of Internal Governance as well as in the bank's internal risk assessment.

How exactly the regulatory and supervisory treatment of Cyber Risk will develop in future remains to be seen. However, it is anticipated that regulators will increase their focus on qualitative requirements such as Governance to ensure a conscious risk management by banks.

MODEL RISK

In 2011, the Federal Reserve Board, one of the United States' three bank supervisory authorities, introduced with its Guideline SR-11-7[10] a principles-based approach to supervise and assess the **aggregated Model Risk**.

In Europe, Model Risk must be considered, too: It is assessed as **part of the OpRisk** in the context of SREP. Besides the risk of underestimating capital adequacy requirements when applying internal models, losses resulting from the development, implementation or inadequate use of internal models also count as model risks. The supervision is based on questions concerning Governance and risk awareness of the institute – quantitative requirements have not yet been legally established.

In other words: European regulators are increasingly following the US example and focus on **Model Governance**. Hereby, they mainly concentrate on the first sub-risk, the potential underestimation of capital adequacy requirements. For example, the purpose of defining minimum PDs / LGDs and an Output Floor is to prevent strong deviations between the results of standardised approaches and internal models. Additionally, TRIM (Targeted Review of Internal Models) was introduced to ensure an annual review of the applied models.

In 2018, the second sub-risk, losses arising from the use of internal models, could increase in relevance – particularly because precise rules on how to measure and manage Model Risk are still missing. This topic has gained importance, since banks are increasingly using new methods such as **Machine Learning** to select and validate their models.

This is not necessarily within the regulators' interest, as shown by a statement of the Federal Reserve: In its opinion, using Machine Learning to validate models leads to systemic model risk and, additionally, to a decrease in transparency.

The treatment of Machine Learning and other advanced validation methods thus presents a considerable challenge for regulators: Supervising such "Black-Box Models" is difficult, in some cases even impossible, and complex methods used to estimate model risk across risk types themselves constitute a new model risk to the bank. From this perspective, the increasing focus on standardised models is understandable.

Despite the increasing move away from internal models, it should be noted that Model Risk is gaining importance from a regulatory perspective and is increasingly supervised in the context of Pillar 2.

[9] EBA/GL/2017/05: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)
[10] See also: https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf

EFFECT

IN THE SHORT RUN, banks must expect documentation efforts and costs for Internal Governance as well as for compliance with Pillar 2 regulations to increase.

IN THE LONG RUN, the move away from internal models could facilitate the quantification of model risks and reduce the importance of this risk type. Cyber risks, however, will gain further relevance and should be managed via adequate approaches and strategies.

SUMMING UP

Including new risk types in supervisory practices and regulatory requirements as well as focusing increasingly on the Internal Governance of banks are discernible trends in the current financial environment. Especially cyber and model risks are intensely discussed and could become part of new supervisory publications to be released in the upcoming year.

To react effectively and efficiently to such new regulations, it is necessary to critically assess the relevant topics from an early stage. Approaches of other regulatory bodies such as the Federal Reserve can help with the preparation.

» TREND 3

FROM AGGREGATED REPORTS TOWARDS SINGLE DATA CUBES

STATUS QUO

Since the financial crisis, regulatory reporting requirements for banks are continuously increasing. To better prevent future systemic crises, supervisory authorities and central banks increasingly favour internally-led analyses such as stress tests and ad-hoc reporting over traditional reporting tools. For this reason, they need **more granular data** than before.

The currently valid reporting requirements are **heterogeneous**: They require banks, on the one hand, to deliver a variety of predefined forms with aggregated data to supervisory authorities; on the other hand, first reports (e.g. Statistics on Holdings of Securities, SHS) necessitate explicitly the delivery of granular data.

In addition, the reporting requirements are regulated **at different levels**:

Due to this development, many credit institutions are confronted with multiple reporting forms that each prescribe a different **level of aggregation** and reporting frequency. The result is a complex system that is less and less transparent for outsiders, but also for internal stakeholders.

Moreover, it leads in part to the generation and transmission of redundant information, as similar data sets must be reported in slightly different structures. Additionally, banks face the challenge of validating the content of their single reports and to ensure data consistency between those. Like this, the **costs** linked to reporting requirements increase significantly.

TREND

As a long-term strategical project, the European System of Central Banks (ESCB) is planning to largely harmonise and facilitate the reporting system across Europe.

To achieve this goal, the regulator is focusing on upgrading the "**European Reporting Frameworks" (ERF)** (also "Primary Reporting" or "Output Layer")[11]. Within the scope of this reporting framework, data will be raised uniformly throughout Europe to serve, in a first step, statistical and, in a second step, supervisory purposes. Focus is placed on the transmission of single data points and the general reduction in the level of aggregation. In doing so, content-related overlapping in currently required reporting sets will be lowered.

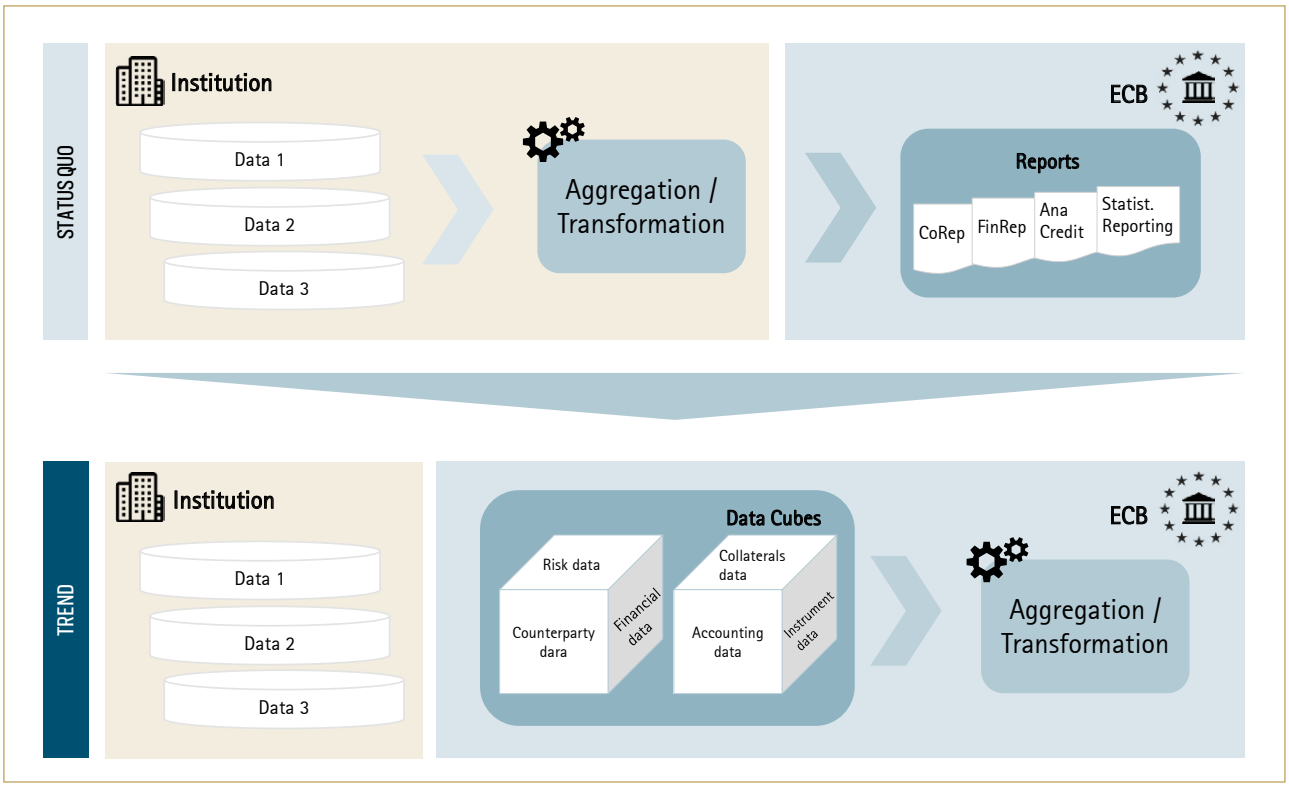
The Austrian reporting system, established in 2013, serves as an example for the planned unified system.

[11] European Reporting Framework (ERF): Key facts and information

It is set up as follows: The Austrian National Bank (OeNB) defines a standardised, complete data model at granular level, the so-called **Basic Cubes**, which banks use to deliver micro data of their individual transactions. Through aggregation and transformation, these Basic Cubes become so-called Smart Cubes, which are transferred to the OeNB and evaluated by the central bank. To implement the data path between Basic Cubes and Smart Cubes, the reporting platform "AuRep – Austrian Reporting Services GmbH"[12] was founded. This platform functions as a sort of buffer, where the data of Austrian banks can be retrieved upon request (ad hoc or regularly) and provided to the supervisory agency; service and regulatory maintenance are hereby centralised.

The first new regulatory requirement designed to establish a unified system based on the Austrian system by creating a European credit register is **AnaCredit**[13] (Analytical Credit Datasets), which will enter into force in September 2018.

To facilitate the harmonisation of Europe's reporting framework and the use of data cubes, the supervisory authority has launched the initiative "**BIRD – Bank's Integrated Reporting Dictionary**"[14] . This dictionary contains a pan-European harmonised data model as well as specific transformation rules that can be used to comply with current regulatory reporting requirements. It is made available as a "public good", at no costs to banks. The use of the BIRD specifications is, however, on a voluntary basis.



Reference: ifb group

[12] AuRep is a joint venture that was founded by eight banking groups at the suggestion of the OeNB

[13] Finale AnaCredit-Verordnung: EZB-VO (EU) 2016/867

[14] See also: www.banks-integrated-reporting-dictionary.eu/

EFFECT

IN THE SHORT RUN, financial institutions must expect high costs and an increase in efforts to implement the new reporting requirements, especially in relation to the setup of Data Cubes. There will be a long transition period, during which data retrieval will continue to be redundant, so that initially the number of required reports will increase. Additionally, investments in new hard- and software are necessary, and new know-how on the constantly changing reporting requirements, but also on data budget and IT systems, must be acquired.

IN THE LONG RUN, a uniform European reporting system benefits both the supervisory authority and the credit institutions. Thanks to the new system, the supervisory authority can optimise the monitoring of financial stability: On the one hand, banks can be more easily compared and thus more efficiently supervised. On the other hand, risks within the European financial system can be detected at an early stage. For institutions, the reporting efforts are likely to decrease: In future, optimised reporting processes will ensure that relevant data at micro-granular level will only be transmitted to the supervisory authority once; further data transformation will then be performed by the supervisory authorities or the ECB. This way, the production depth that lies in the responsibility of banks – and thereby costs and efforts – will decrease over time. In addition, the new regulations force banks to promote automation, which in turn will counteract the increase in costs for IT and data retrieval.

ALL IN ALL

A uniform and granular European reporting system holds long-term cost-savings potential for banks and thus promises to increase efficiency. To what extent these positive forecasts will become true, however, remains to be seen. Crucial for a successful harmonisation of the reporting systems are enhanced automation of reporting processes and the guarantee of sufficient data quality. For now, banks face a "mountain of work" and significant investments.

» TREND 4
STANDARDISING AND CONSOLIDATING IT APPLICATIONS AT GROUP LEVEL

STATUS QUO

On the one hand, banks are exposed to an **increasing margin pressure** resulting from the low-interest environment, a weak profit situation and higher capital costs. On the other hand, the number of **regulatory requirements** such as BCBS 239, AnaCredit and IFRS 9 is constantly growing.

To meet these challenges, banks must engage in profound changes. An enormous investment backlog and huge optimisation potential lies especially in banks' IT system and process landscapes.

The reason for this is the fact that banks often possess historically grown, silo-like structures in their IT system landscape – not only subsidiaries and headquarters, often even bank-internal departments work with different software applications or access separate data bases. This can result in **inconsistencies** and **additional expenses** for coordination. Yet, usually the executive committee tends to shy away from fundamental IT projects, as these involve high costs and mostly have no immediate, directly visible impact on the profit situation of a bank.

New regulatory requirements such as BCBS 239 aim at integrating the fragmented IT system landscapes of banks regarding finance and risk data. But independently of whether BCBS 239 has to be applied or not, all banks should develop an idea of how they will optimise their IT system and process landscape to sustain in the future.

TREND

Current developments in the banking industry show that banks focus more and more on **standardising and consolidating their IT applications** at single-institution as well as group level.

Included are, amongst others, the introduction of a group-wide IT target concept, the use of a uniform core banking system and further applications (existing systems, reporting tools, BI solutions) as well as the creation of an integrated data warehouse combined with a group-wide uniform data model.

To fully reap the benefits of an integrated data warehouse, building a comprehensive Data Governance Framework and conducting an effective data quality management become increasingly important.

In addition, the interaction between parent company and subsidiaries plays more and more a leading role in the standardisation and consolidation processes of IT applications.

INTEGRATED DATA WAREHOUSE (IDW)

The definition of a well-thought out **Integrated Data Warehouse (IDW)** is indispensable. It serves as a "golden source" for risk management and any other financial, supervisory or management-related reporting processes. Pre-condition for the creation of such an IDW is the successful interplay of the following three factors:

- Organisation (with regard to targets and change management)
- Departments (with regard to processes and data requirements)
- IT (with regard to IT systems and architecture)

When creating the IDW, a structured approach is crucial: First, a **uniform target concept** of the desired system landscape must be determined and promoted within the organisation. This requires, on the one hand, a high reconciliation level of the "needs" of the different departments within the bank and, on the other hand, the provision of adequate financial and personnel resources.

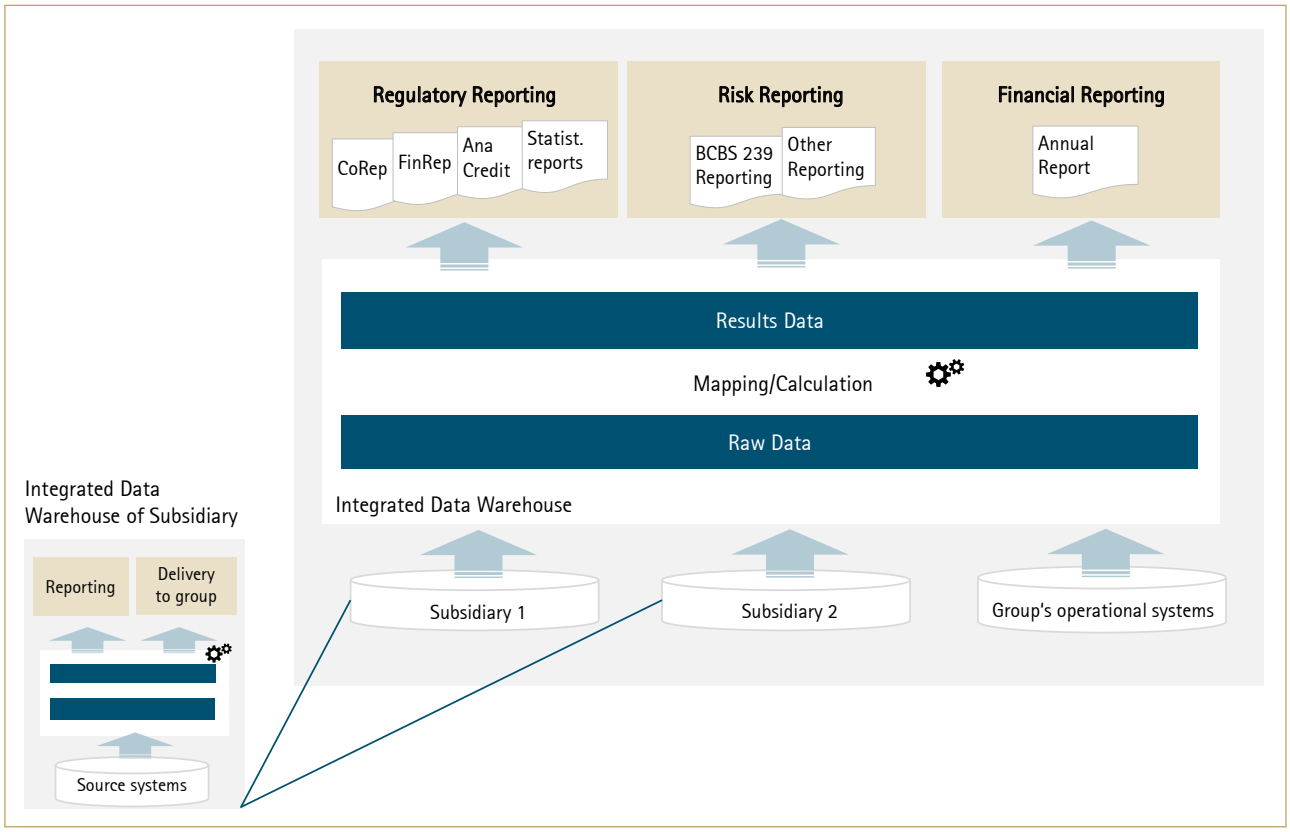
Next, a complete **technical data model**, which reflects the data requirements of the single reports, should be developed. This data model must be enhanced by meta data definitions and taxonomies, so that a group-wide uniform comprehension of the required features and key figures exists. To guarantee transparency and consistency within the group, documentation should take place in a glossary. In large corporations, a **top-down approach** is recommended, i.e. based on the final reports and key figures it is defined which data from the sourcing systems and single subsidiaries will be needed. The resulting data model is then to be transferred to all single subsidiaries, thereby enabling them to adequately deliver the data required to fill internal risk and external supervisory reports. As soon as the initial data model is implemented, it can gradually be extended by additional data requirements, such as profit centres.

The group-wide IDW is filled **with granular data** (i.e. at the level of individual transactions) from the existing operative systems and IDWs of the subsidiaries. This requires connecting all existing systems with the IDW – including connecting systems that are used internally within departments to process data and create reports. In addition, the **transfer of relevant Individual Data Processing (IDP) into Automated Data Processing (ADP)** as well as connecting these with the IDW of the parent company/single subsidiaries should be targeted. Hereby, a reduction of manual efforts to provide data and an increased frequency of data deliveries might be achievable.

SPECIFIC REQUIREMENTS FOR SUBSIDIARIES

To facilitate consolidation and standardisation, the data and IT architecture of subsidiaries should be integrated into the target concept of the group.

More precisely: To guarantee the transferability of data, the group's technical data model and calculation methods for relevant risk ratios should be applied by the subsidiaries. Thus, the system landscape of single subsidiaries must be oriented towards the group's. Ideally, single, independent IDWs at the level of the subsidiary are created and based on the group's technical requirements. Then, these IDWs are connected to the group-wide IDW and provide it with the subsidiaries' data.



Reference: ifb group

GROUP-WIDE DATA GOVERNANCE

Using an integrated data warehouse also requires that guidelines concerning data management and uniform data quality standards exist. This means that **Data Governance** must happen at group level, which can be facilitated by Data Lineage. Data Lineage refers to the possibility of tracing aggregated data back to its source, i.e. to the original single data points from which the data was derived, and of determining dependability between these data points. The thereby achieved transparency of the data flow is a precondition for a group-wide Data Governance Framework.

Furthermore, the implementation of a group-wide data model should be accompanied by the introduction of a complete, multi-step **Data Quality Management (DQM) Framework**. Besides defining data quality requirements, such a rulebook would allow for triggering corrective processes. Lastly, it must be ensured that data corrections can only be made within the operative systems (in exceptional cases also within the IDW).

EFFECT

IN THE SHORT RUN, banks should not delude themselves: Even if pioneer institutions can generate a competitive advantage by implementing the mentioned measures early on, initially they will face high costs and additional efforts as a result of the required IT investments. Yet, increasing data granularity to comply with regulatory requirements is necessary and would be supported by a standardisation and consolidation of the IT system landscape.

IN THE LONG RUN, though, the impact of standardisation and consolidation is promising: Less duplication of work and a closer collaboration between parent company and subsidiaries allows for higher efficiency (e.g. with regard to testing efforts). Redundancies (such as unnecessary interfaces) might be avoided and costs can be reduced, as less coordination efforts are needed. Further, the consistency of data should become easier to achieve, which might lead to an improvement in comparability and reconcilability of risk, accounting and supervisory data – implying faster, more transparent and flexible reporting processes. By having a uniform technical data model and DQM Framework, both completeness and validity of data can be achieved, providing a significant increase in data quality.

THUS

The current challenges and changes in the banking sector offer banks the unique opportunity to start optimising and overhauling their often strongly fragmented IT landscape. Thereby, important efficiency improvements and cost reductions can be realised in the long run. However, to do so, high investment expenses are needed in the short run. Nevertheless, banks should act strategically and develop a holistic, sustainable earnings-oriented concept – so-called "patchwork" will not be of great help.

Your contact person:

Juliana Müller
Director
M: +49 178 2448636
juliana.mueller@ifb-group.com

Authors:

Philipp Enzinger
Senior Consultant

Marcel Knodt
Senior Consultant

Juliana Müller
Director

ifb AG
Schloßstraße 23
82031 Grünwald
GERMANY
Tel. +49 89 69989437-0
info@ifb-group.com