sciendo

UDK: 336.71.078.3
DOI: 10.2478/jcbtp-2018-0023

Journal of Central Banking Theory and Practice, 2018, 3, pp. 57-72
Received: 10 November 2017; accepted: 27 December 2017

Joerg Orgeldinger *

* Ludwig Maximilians University of Munich, Munich, Germany

Email:
orgeldi1@yahoo.de

The Implementation of Basel Committee BCBS 239: Short analysis of the new rules for Data Management

Abstract: In January 2013, the Basel Committee on Banking Supervision issued 14 principles for effective risk data aggregation and risk reporting (BCBS 239) and outlined the paths to compliance for globally systemically important banks (G-SIBs) and domestic systemically important banks (D-SIBs).The Basel Committee devised BCBS 239 in order to ensure that banks and other financial institutions could monitor risks more effectively through superior data aggregation, enabling an overall more reliable and efficient risk management process. In a McKinsey report from June 2015 (Harreis et al, 2017) it is estimated that an average G-SIB would have to spend approximately 230 million USD and an average D-SIB 75 million USD to aggregate risk data that was previously dispersed over a wide variety of systems, geographic locations and banking groups. As the BCBS 239 for G-SIBs deadline was - at the time of writing – 10 months overdue, what approach towards compliance will prove to be more effective? In this article, the new principles according to BCBS 239 are described, criticized and one possible solution to meet the requirements is presented.

Keywords: BCBS 239 – Principles – Finrep - Chisholm's analysis – Risk data engine – financial stability

JEL Codes: C80, G18, N20

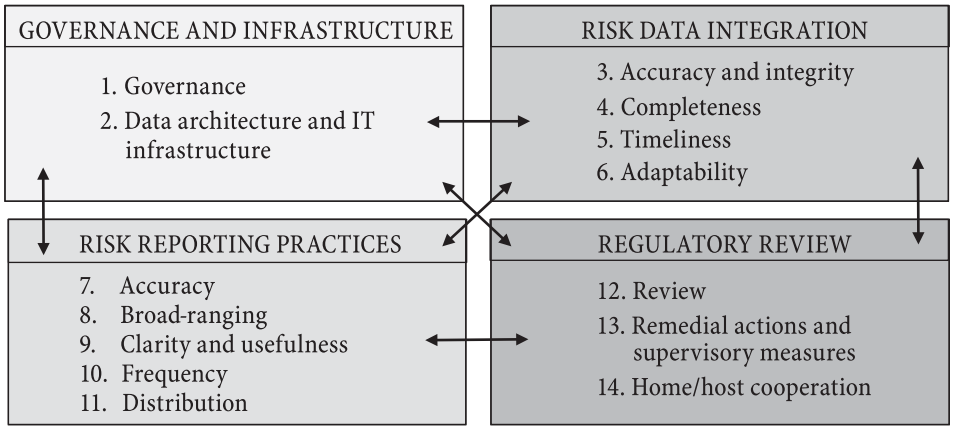
1. Introduction

"BCBS 239" is a common shorthand term for referring to the paper *Principles for effective risk data aggregation and risk reporting* published by the Basel Committee on Banking Supervision (BCBS) in January 2013 (BCBS 2013a). It is a global regulation that presents a challenge for globally systemically important banks and a wide range of other financial services companies to archive their data governance and data management practices to achieve bank compliance and financial stability in the next years (for financial stability please refer to Vlahovic in her 2014 essay on safeguarding financial stability). In this article, the response of the industry regarding the BCBS 239 is evaluated and one solution for adaptation of the new rules is presented. This paper seeks to identify the capabilities that the broad community of data management professionals and academics in financial information need to understand in order to plan for compliance. After a critical assessment of the new directive, one new approach to comply with the new regulation is presented.

2. Description of the rules and principles

Of 14 principles shown in Figure 1, eleven focus on responsibilities of the risk management function of banks. The remaining three are aimed at supervisory bodies.

Figure 1: The 14 principles of BCBS 239 (BCBS 2013a)



The principles require rigorous governance and thorough data management which should result in increased understanding of data, and risk exposure (credit

risk, market risk, liquidity risk, operational risk and other risks) as well as produce validated, accurate, comprehensive and useful reports in a timely manner. Robust governance arrangements must be in place. The following table gives an overview of the new principles:

Figure 2: The new principles according to BCBS 239 explained (BCBS 2013b)

Principle 1	Governance	A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Committee.
Principle 2	Data architecture and IT infrastructure	A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting the other Principles.
Principle 3	Accuracy and Integrity	A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors. (Annex 2).
Principle 4	Completeness	A bank should be able to capture and aggregate all risk data across the bank. Data should be available by business line, legal entity, asset type, industry, region and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations and emerging risks.
Principle 5	Timeliness	A bank should be able to generate aggregate and uptodate risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bankspecific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the bank.
Principle 6	Adaptability	A bank should be able to generate aggregate risk data to meet a broad range of ondemand, ad hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries.
Principle 7	Accuracy	Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.
Principle 8	Comprehensiveness	Risk management reports should cover all material risk areas within the organisation. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.
Principle 9	Clarity and usefulness	Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decisionmaking. Reports should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. Reports should include meaningful information tailored to the needs of the recipients.
Principle 10	Frequency	The board should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decisionmaking across the bank. The frequency of reports should be increased during times of stress/crisis.
Principle 11	Distribution	Risk management reports should be distributed to the relevant parties while ensuring confidentiality.

Principle 12	Review	Supervisors should periodically review and evaluate a bank's compliance with the eleven Principles
Principle 13	Remedial actions and supervisory measures	Supervisors should have and use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting practices. Supervisors should have the ability to use a range of tools, including Pillar 2.
Principle 14	Home/host cooperation	Supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the Principles, and the implementation of any remedial action if necessary.

Processes, controls, roles & responsibilities, data items, identifiers and reporting must be defined and documented. The lineage of risk data throughout the data lifecycle must be understood. Risk data and reports should be reconciled and subject to independent validation.

Group structure should not hinder aggregation capabilities within the organization. It must be possible to aggregate data at legal entity, geographical, industry, asset class and business line levels. Banks must implement flexible infrastructure and processes to produce timely ad hoc reports – under both stressed and normal conditions. Reports must be sent to the bank's board within 10 to 15 days after the end of month, in stress phases documentation about all relevant and critical credit, market and liquidity positions have to be submitted to the board within a short period of time (often daily or at once). The Board must be aware of and address any technical or legal limitations that compromise risk data aggregation. BCBS 239 requires automatization. Only in cases when business judgement is needed, manual processes are permitted. Banks must assess the impact of change on risk data aggregation and reporting capabilities, including regulation, products, process changes and IT initiatives. Enterprise-wide understanding of the data architecture and resilience mean that the approach to compliance must be sustainable. Myers provides a nice table which shows the different dimensions of data quality:

Figure 3: Different data dimensions (please refer to Myers 2013)

Reporting	Data management	Integration services Data quality Data lineage
	Internal and external reporting	Reporting capabilities and definition Impact on regulation
Data	Robustness and compliancy	Stress testing Audit
	Data strategy	Capability led planning Common information model

3. Former surveys and investigation

The BCBS analysed the progress in adopting the principles for effective risk data aggregation and risk reporting in two surveys, one in 2013 and one in 2014. The 2013 survey was analysed in more depth by Malcolm Chisholm (2014, p. 21).

3.1 Chisholm's analysis at Loughborough University

The 2013 survey broke down each principle into a total of 87 specific requirements for the first 11 principles (the ones that apply directly to banks). This breakdown was analysed in terms of capabilities needed. The capabilities were divided into 4 categories: Leadership, organization, methodology and technology. Each requirement for each principle was analysed to determine what aspects conformed with the four capability groups shown above. Each requirement has its corresponding capabilities in the 4 groups scored as follows:

0 = No to weak involvement
3 = Supporting role
5 = Required

Figure 4: Assessment of capabilities for BCBS 239[1] (adapted from Chisholm 2014, p. 21)

No.		Scores			
	Principle title	Leadership	Organization	Methodology	Technology
1	Governance	58	93	120	31
2	Data architecture	0	40	65	40
	Subtotal	58	133	185	71
3	Accuracy	5	60	75	53
4	Completeness	11	35	35	20
..	..	..	..	..	…
		127	406	505	275

The overall scores indicate that *leadership* is the category with the fewest number of capabilities needed. *Technology* with its lowest score is important, and vital for some areas, but technology ALONE is not a solution for BCBS 239 requirements. The next highest scoring group is *organization*, which means that many capabilities will need to be provided by staff working within a set of defined relationships and goals. The highest scoring category is *methodology*, meaning that organizations must have defined ways of working in areas of concern, within defined organizational structures using specific technology. This means employing uni-

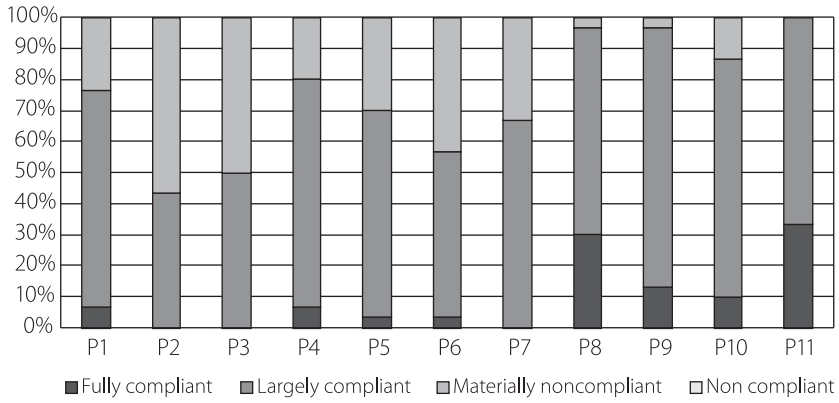
[1] Chisholm (2014), p. 21

form valuation models, definitions, data glossary and consistent input parameter investigations.

3.2 The 2014 survey by BCBS

The BCBS issued another self-assessment exercise to 31 G-SIBs in 2014. The results of these questionnaires (BCBS 2014) clearly showed banks must work hard to meet the January 1, 2016 deadline. Banks have not been fully compliant with the January 1 deadline. Progress has remained slow. As a result, the BCBS principles have increased the pressure to achieve these goals as soon as possible. This compliance-focused approach will not see the full operational and best practice benefits that BIS intended (see Chartis 2016). The research report focuses on the current implementation status of BCBS 239 by systemically important banks, and explores the potential reasons behind the current lack of progress. It also looks at the lack of feedback from the Basel Committee concerning the CBS 239, and reasons for banks to ensure they address the BCBS 239 principles.

Figure 5: Self-assessment ratings by principles (BCBS 2014)



P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11
2	0	0	2	1	1	0	9	4	3	10
21	13	15	22	20	16	20	20	25	23	20
7	17	15	6	9	13	10	1	1	4	0
0	0	0	0	0	0	0	0	0	0	0
Governance/Infrastructure		Risk data aggregation capabilities				Risk reporting practices				

Supervisors are aware of the challenges banks face and know many G-SIBs are still not sufficiently covering one or more principles ten months after the deadline. Banks generally assess reporting practices higher than infrastructure and

data-aggregation capabilities, which might lead regulators to ask critical questions about dependency on manual processes and sustainability of sound reporting capacities. Banks struggle most with Principle 2 (Data architecture/IT infrastructure), Principle 3 (Accuracy and Integrity) and Principle 6 (Adaptability). About a third of the G-SIB banks indicated they would not be compliant with these principles by the January 2016 deadline. In general, in the above study, banks assigned themselves higher ratings on the risk reporting principles than they did on the data aggregation principles. A few banks that rated fully compliant with principle 8 (comprehensiveness risk reporting) assessed themselves as being materially non-compliant with one or more data aggregation principles. The following table provides important regulatory initiatives with their implications on the BCBS 239:

Figure 6: Overview of the most important regulations influencing BCBS 239 (own table)

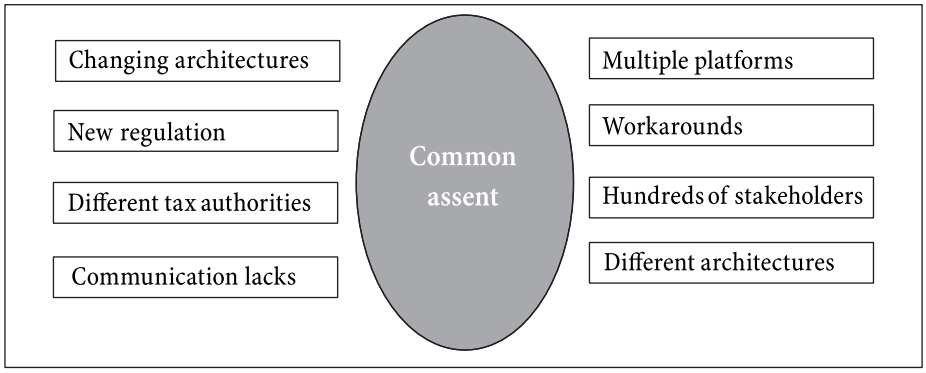
Initiative	Contents	Influence on BCBS 239	From when on
AnaCredit	AnaCredit is a project to set up a dataset containing detailed information on individual bank loans in the euro area, harmonized across all Member States. "AnaCredit" stands for analytical credit datasets.	Intensifying the data storage and additional integration of group data	01.01.2017
FRTB Fundamental review of the trading book	The Committee's goal is to improve trading book capital requirements and to promote consistent implementation of the rules so that they produce comparable levels of capital across jurisdictions.	Intensifying the data storage, adaption and improvement of calculations	End of consultative phase beginning 2016
SREP Supervisory Review and Evaluation Process	SREP shall ensure that institutions have adequate arrangements, strategies, processes and mechanisms as well as capital and liquidity to ensure a sound management and coverage of their risks, to which they are or might be exposed, including those revealed by stress testing and risks institution may pose to the financial system.	Intensifying the data storage, new processes and productions	First short-term exercise in March 2015
IFRS 9	IFRS 9 includes a logical model for classification and measurement, a single, forward-looking 'expected loss' impairment model and a substantially-reformed approach to hedge accounting (IFRS 2016)	New ratios and calculations	1.1.2018
BRRD/SAG Bank Recovery and Resolution Directive	This directive is designed to provide adequate tools at European Union level to effectively deal with unsound or failing credit institutions'. It aims to make sure a bank or an institution can be resolved speedily and with minimal risk to financial stability.	Intensifying the data storage, ad hoc reporting of failing credit institutions	1.1.2015 for the rescue scheme
FINREP Financial reporting	FINREP requires granular data relating to the income statement and balance sheet.	FINREP requires over 40 templates with around 3,500 data fields to be completed and submitted quarterly.	First complete FINREP documentation 2015 For IFRS obliged, 2017 local GAAP

4. Critical analysis of BCBS 239

Banks are challenged to combine the BCBS 239 principles, specific capability based requirements and their existing workload across different functional areas, lines of business and regions. This is often evidenced by a limited number of BCBS 239 initiatives, especially at divisional levels.

In many instances, data attributes have not been required for external reporting purposes or are not even stored electronically in the systems of the bank (e.g. cumulative recoveries since default). Especially in the latter situation, the bank must rapidly demonstrate its ability to source information to the national regulator to fulfil the new principles.

Figure 7: Existing problems in the banks arise from…



The lion's share of the information required for the risk reports and submissions to the regulator exists in banks' data warehouses. Banks need to assess if the data is granular enough to meet the requirements of BCBS 239 and whether the content is coherent i.e. if the data quality is sufficient (CEIOPS 2009). Banks will be required to review the data for errors from a technical perspective (based on a check error process) and from the financial perspective (based on a general ledger reconciliation process). The following methodology is recommended: First define different Key Performance Indicators (KPIs) and business rules. If they cannot be fulfilled, there is an error. Later, an error rate must be calculated, which is the ratio of unfulfilled business rules to total business rules. With the help of a lean six sigma system bandwidth can be defined, which allows the classification of the data quality as very good, good, satisfying, sufficient and inadequate. The achieved quality level can be visualized with a traffic light approach and integrated in data management dashboards.

The requirements of BCBS 239 will force banks to critically review their current *reporting architecture and regulatory reporting processes*. Are the current systems capable of dealing with the increased amount of data owing to the low reporting threshold? Do the systems possess strong data aggregation functionalities that can aggregate data from different sources within the bank (e.g. risk management and finance)? Can the current reporting solutions submit more reports at more frequent intervals? Must the bank rely on manual workarounds for its regulatory reporting and how can they be reduced? Is data governance strong enough to maintain consistency and quality data reporting?

Many banks are struggling with the new rules. They rely too heavily on existing purpose built infrastructure and reporting capabilities. Banks rate their own compliance with the risk reporting principles higher than their compliance with the governance, infrastructure and data aggregation principles. Banks must fulfil the BCBS 239 principles group wide. Often banks appear compliant at group level or at the level of a specific legal entity – but lack the same capability at different aggregation levels. They do not meet the adaptability requirement. Many banks have limited resources. The data landscape is constantly changing, creating a lack of embedded enterprise wide understanding of the data and the business context in which it operates.

Two large consequences arise if data and IT platforms for these programs are not properly addressed. First, there is massive regulatory risk and a reputational risk if a bank fails to comply. Aside from possible specific supervisory sanctions, deficiencies reported in early assessments of BCBS 239 often result in "breakup the banks" arguments. Second, the bank might incur excessive but not fully productive investment.

The principles of BCBS 239 are somewhat vague and, unfortunately, there are only a few definitions supplied in the regulation. "Governance" e.g. would seem to need to include "Data Governance", but neither "Governance" nor "Data Governance" is defined. There is no exact definition of "risk data". Banks are likely to be unable to address the compliance with BCBS 239 simply by purchasing and implementing technology.

Additionally, the BCBS merely provides principles. There is a lack of specific guidance on specific methods on how to implement and enforce. Although the principles are sound these rules of the Basel committee show the biggest gap between theory and practice. Inconsistent terminology across the industry has been one of the bigger challenges for banks in sharing information and learning from the practices of peers (as is recommended in the December 2013 BCBS 239

progress update). Data lineage ensures at least technical metadata involving data points and its various transformations. Full data lineage is time consuming and resource intensive. However, it is essential if banks are to fully identify and remediate the root causes of underlying data quality issues.

In many cases, international banks have underestimated the level of effort required to develop a standardized set of documentation. First, the underlying reality of monolithic systems needs to be addressed and transformed. The technological response of the institution must be appropriate and clearly depends on the size and complexity of the institution. Large banks can handle these requirements better than smaller ones.

5. Advantages of the new BCBS 239 for the banks

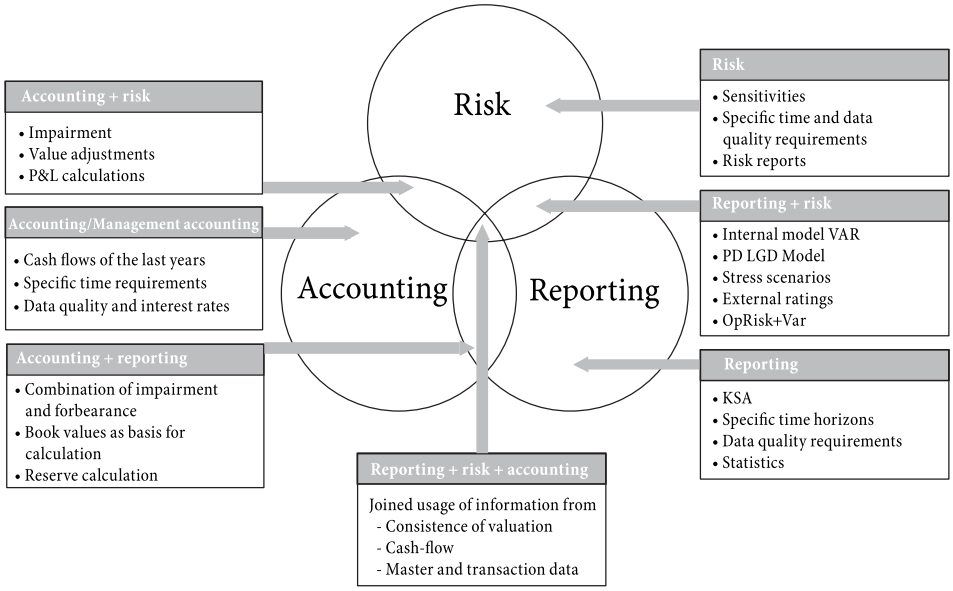
The BCBS 239 requirements address what supervisors see as the major weakness that carried banks into the 2008 financial crisis: Inability to efficiently comprehend and communicate overall exposures, as well as other key risk metrics influencing crucial institutional decisions.

Because of the BCBS 239, large capital investments in data reporting will pay for themselves through lower losses, lower capital needs, lower operational risk costs and lower operational costs.

The competitive advantage of excellent risk data aggregation can positively affect a bank's bottom line and allow for better judgement through more accurate risk analysis. Moreover, by aggregating information across the business, banks will be more convincing to customers and cross-sell through existing relationships, whilst providing more comprehensive support and services to existing customers.

There should be a single authoritative source for risk data per type of risk. This data must be reconciled with accounting data (where appropriate) to ensure the risk data is accurate. Ideally, these two datasets should be stored in the same system, which makes these reconciliation efforts redundant. The data architecture requirements are what most G-SIBs are struggling with. BCBS 239 increases pressure on banks to invest in data quality and a solid data architecture (Thun 2015). The benefits of this "single source of truth", that contains both risk, accounting, controlling and reporting data, are numerous: clear data lineage, less reconciliation, the ability to use the same data for multiple purposes are only the tip of the iceberg in terms of benefits.

Figure 8: Interrelation between risk, accounting and finance (own table)



Many other regulatory pressures (MaRisk AT 4.3.4, MaRisk AT 7.2, SREP, AnaCredit, IFRS 9) in addition to the BCBS 239, will reinforce these requirements as will the need to meet the requirements of expected-credit-loss provisioning under international and the US accounting requirements consistently with the BCBS's pending guidance on expected credit losses. Accounting debit is no longer a reliable proxy for exposure, mutate by derivatives. Risk data aggregation and reporting can then follow predefined aggregation paths, for example, by legal entity, line of business, risk type, customer, product and geography.

By adapting the control and reporting frameworks that already exist in accounting and general ledger systems, risk accounting can potentially provide a viable solution to BCBS 239 at a fraction of the time and cost of reconfiguring entire IT and data infrastructures (for the application of risk accounting please refer to Hughes, Grody and Toms S. (2010) and Grody and Hughes (2015). The ultimate goal of creating a risk reporting framework with effective aggregation of risk data as demanded by the Basel Committee is only possible if there is a common measurement framework applied to cross-enterprise exposures to risk. We concluded that *Risk Accounting* could offer an elegant solution for the BCBS 239. It is innovative and requires accepting the introduction of a new risk measurement metric based on already trusted accounting data, thereby removing, in the short term,

the need for heavy investment in retooling risk data architectures (Harreis et al, 2017)

6. A possible solution risk data engine

New technological development allows the use of sophisticated programming tools (please refer to technological change in the article of Popovic, 2017), which can help to follow the principles by building up a *risk data engine*. The first two principles address frameworks for proper data governance, data and IT architecture. The proposed risk data risk engine must comply with the BCBS 239 principles that translate into data quality, standardization, auditability, robustness and reconcilability. It is generally accepted that software solutions – like those of SAP and SAS – can help to achieve these goals in a bank's overall IT landscape.

If the risk exposure calculation is based on sub ledger accounting data at the transaction level, the main important parts of principles 3,4,5, and 6 about robust controls and reconciliation with accounting data will be met. A common risk metric provides a timely and complete aggregation methodology – adaptable across all risk types.

The risk reporting framework governed by the principles 7, 8, and 9 addresses an area that comprises data accuracy, comprehensiveness, and clarity. The new data warehouse provides a complete and compliant data reporting environment and ad hoc reporting, both in normal and stress situations.

The BCBS 239 principles 10 and 11 of frequency and distribution are fulfilled by the risk data engine through its flexibility to acquire, store and aggregate data in the frequency with which data is made available to the bank. Data could be presented in aggregated form in physical reports and dashboards, visualization and heat maps. In addition, it should be made available in standardized common form. The risk data engine uses finance data from different source systems into a single, common system of record.

Figure 9: Key metrics of a bank in a dashboard (BCBS 2016, p. 7)

Purpose: The dashboard provides an overview of a bank's prudential regulatory situation.
Scope of application: The template is mandatory for all banks.
Content: Regulatory key metrics. Banks are required to disclose each metric's value using the corresponding standard's specifications for the reporting period-end (designated by T in the template below) as well as the four previous quarter-end figures (T-1 to T-4).
Frequency: Quarterly
Format: Fixed. If banks wish to add rows to provide additional regulatory or financial metrics, they must provide definitions for these metrics and a full explanation of how the metrics are calculated (including the scope of consolidation and the regulatory capital used if relevant). The additional metrics must not replace the metrics in this disclosure requirement.
Accompanying narrative: Banks are expected to supplement the template with a narrative commentary to explain any significant change in each metric's value compared with previous quarters, including the key drivers of such changes (eg whether the changes are due to evolutions in the regulatory framework, group structure or business model).

		a	b	c	d	e
		T	T-1	T-2	T-3	T-4
	Available capital (amounts)					
1	Common Equity Tier 1 (CET1)					
2	Tier 1					
3	Total capital					
	Risk-weighted assets (amounts)					
4	Total risc-weighted assets (RWA)					
	Risk-based capital ratios as a percentage of RWA					
5	Common Equity Tier 1 ratio (%)					
6	Tier 1 ratio (%)					
7	Total capital ratio (%)					
	Additional CET1 buffers requirements as a percentage of RWA					
8	Capital conservation buffer requirement (2.5% from 2019) (%)					

This approach enables the bank to break down the silos between risk, controlling, finance, accounting, and compliance. Ideally, these datasets should be stored in the same system as the single-point-of-truth, which makes these reconciliation efforts redundant. Existing reporting silos make group-wide convertibility and reconciliation between risk and accounting data laborious. The benefits of a single source of truth, that contains both risk and accounting data, are numerous: clear data lineage, less reconciliation, the ability to use the same data for multiple purposes are only the tip of the iceberg in terms of benefits.

7. Conclusion

The BCBS 239 paper goes into extensive detail of the guiding principles for data management. According to Vucinic (2016), a good risk management also provides financial stability. There needs to be a clear understanding of which data is used and where, for what purpose, for what frequency, and by whom. The entire risk data cycle should be transparent, detailed, and well documented. The 14 Principles present an important opportunity for banks to improve and streamline their approach to risk data management. Benefits from unifying risk data sourcing and processing go far beyond regulatory compliance. Simply stated, the implementation of a single, transparent, and auditable BCBS 239 framework will create a common language that encourages unprecedented alignment between risk and finance and helps organizations realize the multitude of benefits from this important but still elusive goal to date.

References:

1. BCBS (January 2013a). *Principles for effective risk data aggregation and risk reporting.* Committee for Banking Supervision. Retrieved from http://www.bis.org/publ/bcbs239.pdf
2. BCBS (December 2013b). *Progress in adopting the principles for effective risk data aggregation and risk reporting.* Retrieved from http://www.bis.org/publ/bcbs268.htm.
3. BCBS (December 2014). *Fundamental review of the trading book. Committee for Banking Supervision.* Retrieved from http://www.bis.org/bcbs/publ/d305.pdf.
4. BCBS (December 2016). *Consultative Document Pillar 3 disclosure requirements – consolidated and enhanced framework.* Retrieved from http://www.bis.org/bcbs/publ/d356.pdf.
5. CEIOPS Committee of European insurance and occupational pensions supervisors (2009). *CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Technical Provisions – Article 86 f Standards for Data Quality (former CP 43).* Retrieved from https://eiopa.europa.eu/CEIOPS-Archive/Documents/Advices/CEIOPS-L2-Final-Advice-on-TP-Standard-for-data-quality.pdf
6. Chartis Research (2016). *Spotlight on BCBS 239 - It was never going to happen on time*. Research Report.
7. Chisholm, M. (2014). *The Implementation of Basel Committee BCBS 239: An Industry-Wide Challenge for International Data Management, Proceedings of the 2nd International Data and Information Management Conference (IDIMC),* Loughborough, UK.
8. Grody, A.D and P. Hughes (2015). *The Global Risk Regime – New Roles for Auditors.* Working paper Financial InterGroup (UK) Ltd.
9. Harreis, H.; Tavakoli, A.; Ho, T. ; Machado, J. ; Rowshankish, K. ; Merrath, P. (2017). *Living with BCBS 239*, retrieved from http://www.mckinsey.com/business-functions/risk/our-insights/living-with-bcbs-239.
10. Hughes P., Grody A.D., Toms S. (2010). *'Risk accounting - a next generation risk management system for financial institutions',* The Capco Institute Journal of Financial Transformation, 29 (1): 43-56.
11. IFRS (2016). *Financial instruments. International financial reporting standard.* Retrieved from: http://www.ifrs.org/current-projects/iasb-projects/financial-instruments-a-replacement-of-ias-39-financial-instruments-recognitio/Pages/Financial-Instruments-Replacement-of-IAS-39.aspx.

12. Myers, D. (2013). *Dimensions of Data Quality Under the Microscope.* Information Management Magazine. Retrieved from: http://www.information-management.com/news/news/dimensions-of-data-quality-under-the-microscope-10024529-1.html
13. Popovic, M. (2018). *Technological Progress, Globalization, and Secular Stagnation*, Journal of Central Banking Theory and Practice, 2018, 1, pp. 79-100.
14. Thun, C. (2015). *Moodys Analytics: AnaCredit Gives Banks an Opportunity to Improve Data Management, but Challenges Remain*, Enterprise Risk Solutions.
15. Vlahovic, A. (2014). *Challenges to the Implementation of a New Framework for Safeguarding Financial Stability*, Journal of Central Banking Theory and Practice, 2014, 3, pp.19-52.
16. Vucinic, M. (2016). *Importance of Macroprudential Policy Implementation for Safeguarding Financial Stability*, Journal of Central Banking Theory and Practice, 2016, 3, pp. 79-98.