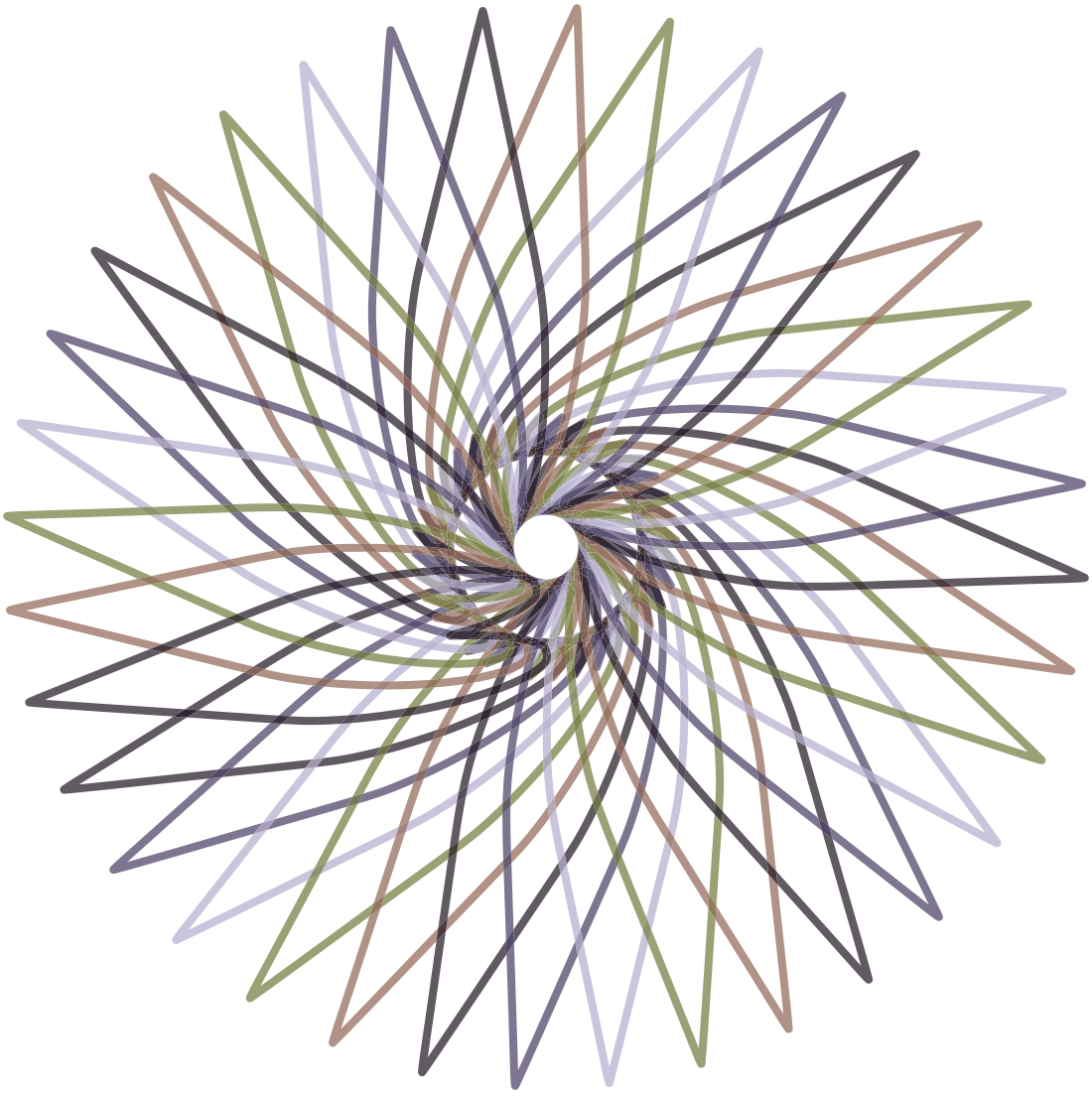
Deloitte.



How effectively are you complying with BCBS 239?

A guide to assessing your risk data aggregation strategies

Deloitte Malta
Risk Advisory - Banking

Risk Advisory

The goal of this paper is to provide measurable parameters that banks can use to gauge their level of compliance, and determine what actions to take if improvement is required

Introduction: BCBS 239

There is no question that many banks need to address and further develop their Risk Data Aggregation and Risk Reporting (RDARR) capabilities. The recent global financial crisis demonstrated that many banks lacked the ability to efficiently and effectively provide senior management with a true picture of the risks the organisation faces. This inability poses a significant threat, not only to the well-being of individual financial institutions, but to the entire banking system and the global economy.

Aimed predominantly at G-SIBs (Globally Systemically Important Banks) and designed to set compliance expectations for different risk types, BCBS 239 is the Basel Committee's attempt to close existing gaps in RDARR. The regulation focuses on governance, infrastructure, risk data aggregation and reporting capabilities, as well as supervisory review, tools and cooperation. These are presented in the form of 14 principles—for example, "completeness", "timeliness" and "adaptability" – with which banks must comply.
Western banks have already started executing strategies around these principles. Indeed, G-SIBs had until early 2016 to implement the principles in full. For their part, Domestic-SIBs (D-SIBs) and Les Significant Institutions (LSIs) will also be required to adhere to these principles within three years after their designation as D-SIBs. BCBS has set expectations that any bank newly designated as a G-SIB or D-SIB must comply within three years of the designation.

The challenge is that BCBS 239 is a principle-based standard, so there are few clear predefined metrics that banks can use to monitor compliance. The goal of this paper is to provide measurable parameters that banks can use to accurately gauge their level of compliance and determine what actions to take if improvement is required.

We begin by considering the key challenges banks face in implementing BCBS 239, then take a closer look at some of the BCBS principles that can be more readily measured, addressing the key focus areas and providing criteria to help organisations report more effectively on their implementation progress.

Three key implementation challenges for BCBS 239

Challenge 1

Lack of infrastructure and quality data

In many organisations, data capture and aggregation processes are unwieldy and relatively unsophisticated. This necessitates data cleansing and manual reconciliation before the production of aggregated management reports. Moreover, difference risk types require data with varying degrees of granularity, complicating the issues of consistency and quality. Banks also need the ability to generate aggregated risk data across all critical risk types during a crisis, which can be especially challenging due to poor infrastructure and data quality.

Banks need to strike a balance between automation (to increase accuracy and timeliness), and flexibility (i.e. manual processes that allow them to fulfil ad-hoc requests). The challenge is significant, and unless banks improve their infrastructure to meet it, they will fall short of meeting the RDARR capability requirements. As well, they risk undermining the strategic decision-making process by regularly relying on incomplete, inaccurate or out-of-date data.

Challenge 2

Increasing demand created by new reporting requirements

Bank functions simply have more requirements today when it comes to meeting reporting demands. Regulators are asking for more information, increased transparency, and clear accountability. Management is looking for more information to develop data-driven strategic insights and plan strategy. This puts growing pressure on departments throughout the bank.

For most banks, the data aggregation process remains largely manual, with the responsibility for submitting risk reports falling to individual business lines and legal entities, often using different approaches. This creates siloed processes, duplicated data and more work and pressure than many departments can manage. These reports, often in spreadsheet form, must then be manually reconciled and the data manually validated. With such clearly inefficient and inevitably inaccurate processes, banks have not been able to effectively aggregate risk data in ways that consistently drive decision making and enable strong risk management.

Challenge 3

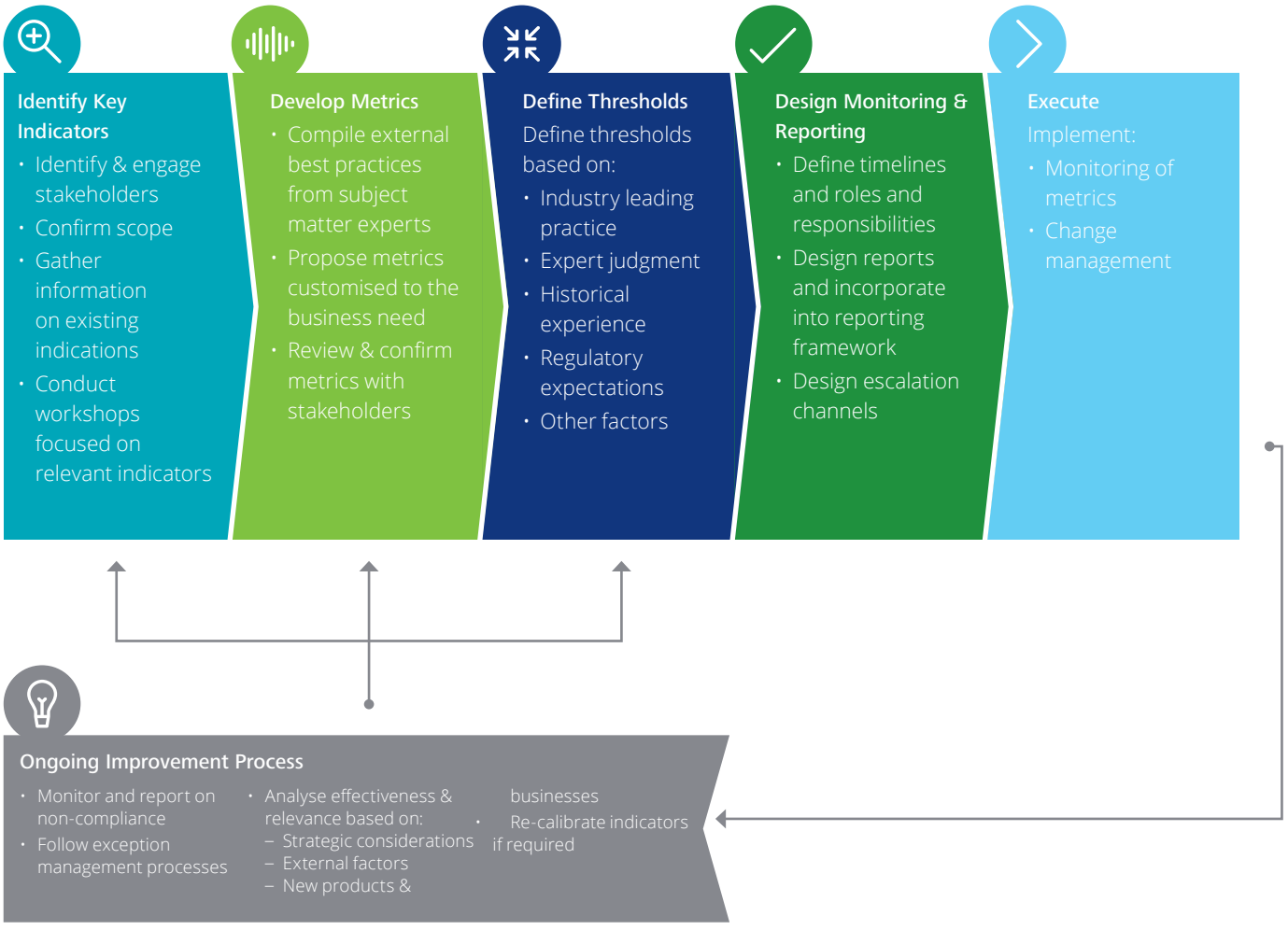
Measuring compliance against the regulations

The principle-based nature of BCBS 239 presents some additional challenges; banks must demonstrate their efforts to comply with the principles without associated compliance metrics. Adding to the challenge, principles focusing on qualities such as “completeness”, “timeliness”, “adaptability” and “accuracy” can have different meanings, and potentially different metrics, when applied to different risk types (e.g. credit, market, liquidity). However, this also presents an opportunity to interpret these principles in a manner that is both compliant and adds real business value.

It is therefore clear that, wherever possible, banks need specific criteria against which they can measure their RDARR activities – across different risk types – to determine how they are performing, where their capabilities sit, what they must do to change, and by how much they can improve over time.

Approach

Deloitte proposes a multi-step approach for development of metrics for compliance against BCBS 239. The approach engages stakeholders to customize RDARR requirements to their business needs and continuously adapt to changes in the business environment.



Principles and suggested compliance metrics

For each principle, banks should define clear measures (e.g. customer risk rating), which are a function of two or more measures (e.g. correct customer risk ratings, as a percentage of total customers); and thresholds (e.g. 98% - green). A bank can demonstrate compliance with BCBS 239 principles by ensuring that key metrics are maintained within established thresholds.

This paper summarises the BCBS 239 principles, which were originally imposed on G-SIBs however are now expected to become applicable to D-SIBs and LSIs.

Data- Governance

A bank's board and senior management should promote the identification, assessment and management of data quality risks as part of its overall risk management framework, and should review and approve the bank's group risk data aggregation and risk reporting framework and ensure that adequate resources are deployed.

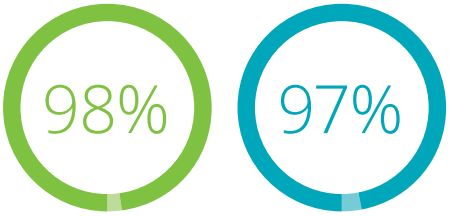
Data architecture & IT infrastructure

Principle 1 is concerned with banks' ability to design, build and maintain data architecture and IT infrastructure that fully supports their RDARR capabilities, in both normal times and during times of stress. One critical success factor for this principle, and for galvanising change, is gaining the support of senior leadership for a target data and IT infrastructure that aligns to industry leading practices.

Focus area examples	Metrics considerations
Business continuity planning and impact analysis capabilities	• Data availability (e.g. 99% uptime) • Disaster recovery metrics (e.g. time to restore) • Backup and restore capacity
Integrated data taxonomies and architecture	• Consistency of common data elements and architecture components • A common enterprise architecture and a set of common principles
Ownership and quality of risk data and information	• Assigned roles and responsibilities for both business and IT functions • Adequate controls throughout the lifecycle of the data for all aspects of the technology infrastructure • Risk data aggregation capabilities and risk reporting practices aligned with firm policies

For example, indicators for Data Accuracy could be the Customer Risk Rating and Customer ID, measured against the number of records and outstanding amounts on portfolios, expressed as a percentage of the total. The thresholds could be defined as green (≥98%), cyan (<98% - 96%) and blue (<96%) as depicted in the figure below.

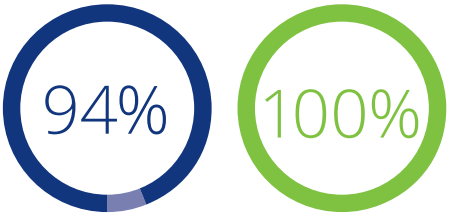
Customer Risk Rating



Accurate records (% of total)

Outstanding records (% of total)

Customer ID



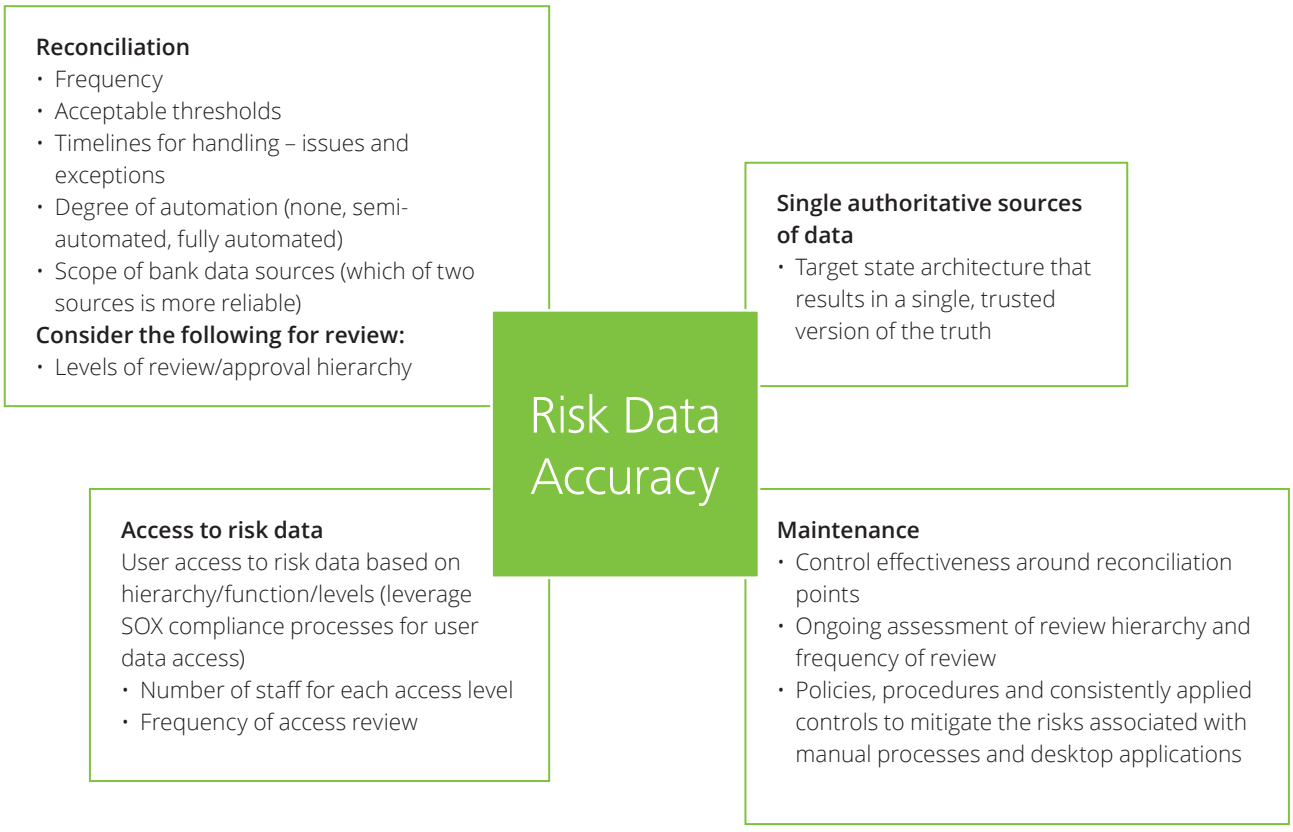
Accurate records (% of total)

Outstanding records (% of total)

Accuracy and Integrity

Clearly, accurate data is critical to both effective risk management and strong decision making—two core issues the BCBS addresses with regulation 239. The Committee requires a bank to be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements, and to minimise errors – largely by automating data aggregation and reconciliation.

Focus area examples	Metrics considerations
Risk data accuracy	Definition of "accurate" and "reliable" from two perspectives: • Normal vs. stress/crisis situations • Critical vs. non-critical data elements (CDEs)



Principles and suggested compliance metrics (cont.)

Accuracy and Integrity *(cont.)*

Focus area examples	Metrics considerations
Data dictionary	Existence of a data dictionary that is usable from both the business and technology perspectives, as well as a clear definition of: • Update frequency (including levels of review and approval for new data dictionary items)
Degree of risk related to automation and manual data aggregation	• Number of processes that do not need professional judgment • Criticality of risk data (higher levels of automation are desired for more critical data) • Impact of manual process on timely production of data for reporting and decision making
Documenting risk data aggregation processes	Existence of process documentation for all types (e.g. automated, semi-automated and manual): • Frequency of reviewing and updating process documentation, particularly for manual processes, when a process changes
Measuring and monitoring	Existence of practices or data profiling and Data Quality Analysis (DQA) that occurs on a regular basis. Metrics may include: • Dashboarding/monitoring of data quality • Frequency of DQA • Thresholds for exception reporting and remediation • Timelines for handling issues and exceptions • Degree of automation • Number of data sources considered for a comprehensive DQA

Completeness

Without access to complete information, banks are at risk of making uninformed decisions. As a result, the ability of decision-makers to access the full range of relevant risk data is critical. According to BCBS 239, completeness is defined by a bank's ability to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and other groupings – as relevant for the risk in question – that support efforts to identify and report exposures, concentrators and emerging risks.

Focus area examples	Metrics considerations
Risk data aggregation capabilities	• Consistent materiality levels across the organisation • Identification of the specific approach used to aggregate risk exposures • Impact on the bank's ability to effectively manage risks where data is not entirely complete
Reporting approach to risk data aggregation	• Completeness thresholds for CDE's and non-CDEs for credit risk, for example: – Total number of records – Percentage of outstanding loan balances – Percentage of authorised balances • Effectiveness controls at key data transfer points • Frequency of completeness tests • Timelines for handling issues and exceptions • Degree of automation (none, semi-automated, fully automated) Quantified impact by risk type, business line, industry, region (e.g. number of accounts, customers and loans, as well as total exposure amount that is impacted as a result of incomplete data)

Principles and suggested compliance metrics (cont.)

Timeliness and adaptability

Timely access to data, in today's digital environment, is a critical aspect of risk management and risk-based decision making. Managing shifting market risk, for example, is particularly dependent on having data on hand immediately, although the precise timing will depend on the nature and potential volatility of the risk being measured, in addition to its criticality to the bank's overall risk profile. BCBS 239 suggests that a bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy, integrity, completeness and adaptability. Although timeliness can be variably defined, banks need risk systems capable of rapidly producing aggregated risk data during times of crisis for all critical risks. See Table 1 on page 12 for examples of these risks and measures to define and identify them.

Focus area examples	Metrics considerations
Frequency of aggregation and reporting	• Reporting requirements and thresholds • Compliance measured against defined thresholds
Timely data availability in stress/crisis situation	Extent to which compliance is defined and monitored against defined thresholds for critical data elements in stress/crisis situation
Review of bank - specific frequency	See "Frequency of aggregation and reporting" above requirements

Table 1 – Examples of critical risks

Examples of critical risks include but are not limited to	Measure to define and identify critical risk type
The aggregated credit exposure to a large corporate borrower (by comparison, groups of retail exposures may not change as critically in a short period of time but may still include significant concentrations)	• Credit exposure for large clients • Define thresholds for what clients are considered "large" (e.g. based on outstanding loan amount exposure, number of loans, corporate size, etc.)
Counterparty credit risk exposures, including, for example, derivatives	• Counterparty exposure • Counterparty rating by credible rating agencies • Composition of portfolio
Trading exposures, positions, operating limits and market concentrations by sector and region data	• Position exposure • Portfolio exposure • Maximum allowed exposure • Value at risk • Concentration • Volatility • Sector • Region
Liquidity risk indicators such as cash flows/ settlements and funding	**Liquidity ratios:** • Liquidity coverage ratio • Net cumulative cash flow • Net stable funding ratio
Operational risk indicators that are time-critical (e.g. systems availability, unauthorised access)	• Risk control self-assessment results and coverage • Operational loss distribution and thresholds • Business environment and internal control factors such as RCSA, Internal audit results, etc.

Principles and suggested compliance metrics (cont.)

Reporting – Accuracy

Reporting accuracy has become more important than ever; executives, shareholders and boards rely heavily on risk management reports to drive strategies, control risk exposure and drive innovation. BCBS 239 requires that these reports accurately and precisely convey aggregated risk data and that reports must be reconciled and validated.

Focus area examples	Metrics considerations
Reporting procedures	• Materiality level based on business line, legal entity, risk type, asset type, industry, region and financial impact To ensure the accuracy of reports, a bank should maintain, at a minimum, the following: **Reconciliation of reports** **Report validation and validation procedure** • Variance analysis and range validation • Frequency with which reviews and inventory or mathematical validation procedures are conducted **Reporting data errors and weaknesses** Exception monitoring based on: • Thresholds • Frequency of exceptions • Timelines for handing exceptions
Approximation	• Frequency and timeline for reviews • Frequency of updating and approval of the assumptions for approximations • Back testing against historical risk data
Accuracy and precision requirements based on criticality	See "Principle 2"
Factors affecting accuracy and precision requirements	• Materiality level for different risk factors • Frequency of updates to documentation of assumptions and rationale for accuracy requirements

Comprehensiveness

An organisation should have a comprehensive view of the risks it faces. As banks become increasingly integrated, so do their risks. BCBS 239 requires that risk management reports 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.

Focus area examples	Metrics considerations
Reporting requirements (risk areas, risk components)	Whether exposure information by risk area and components of risk area is consistently used in reports and aligns with the organisation's risk taxonomy
Reporting components	• Frequency for each risk type • Thresholds for each risk
Forward-looking assessment of risk	• Frequency of defining the required forecasted range/duration • Appropriate confidence level for forecast

Reporting – Frequency

The board and senior management (and other stakeholders who rely on risk management reports) should set the frequency of report production and distribution. A report is of little value if recipients don't have time to examine it and apply it to their area of responsibility. 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, report frequency should be increased during times of stress/crisis.
The frequency of risk reports will vary according to the type of risk, purpose and recipients involved. A bank should periodically assess the purpose of each report and set requirements for how quickly the reports need to be produced in both normal and stress/crisis situations. A bank should routinely test its ability to produce accurate reports within established timeframes, particularly in stress/crisis situations which many, in some cases, require a bank to produce intraday position or exposure information.

Reporting – Distribution, clarity and usefulness

Though perhaps overlooked, reporting distribution is critical to getting risk information securely into the right hands. BCBS has mandated that risk management reports should be rapidly distributed to the relevant parties while ensuring confidentiality is maintained.

Focus area examples	Metrics considerations
Report and distribution procedures	• Frequency of review and update of distribution list • What constitutes timely dissemination? • Timelines for report distribution
Clarity and usefulness	• Content tailored to recipients requirements • Discussion of contents • Feedback from users

Bridging the gap between expectation and capability

While the principles outlined in BCBS 239 concentrate on risk data, the end goal is to help banks make timely, defensible, informed decisions. Although all the stakeholders understand the reasons behind and need for this regulation, implementing these principles will challenge banks on many levels. The timeframe for full compliance is relatively short and detailed self-assessments and remediation plans are required this year.

As a result, banks have a very difficult task in the short term, having to essentially determine whether their own compliance efforts are sufficient without access to practical metrics or benchmarks. It is critical that they find some way to measure their efforts both to satisfy the regulators and to stay on top of the changing compliance landscape. It is our hope that this paper will provide relevant guidance to banks and help them understand key questions around the principles.

Development of metrics and thresholds will be key to achieving compliance as well as realising the benefits of effective RDARR. The approach proposed here provides a solid foundation and suggests a range of leading practices and principle-specific metrics. By adopting these metrics as a tentative framework, banks will be ahead of the game when it comes to compliance and to leveraging their data to improve risk aggregation, reporting, management and oversight across the organisation.

Assessing your RDARR posture

- Are you prepared to report on your ongoing implementation of BCBS 239?
- How are your measuring your compliance performance?
- Are your RDARR capabilities adequate to meet the requirements of the BCBS 239 principles?
- Are you getting real business value from your RDARR activities?
- Do you have an action plan in place to define your specific compliance needs?
- Will you be ready to complete full BCBS 239 implementation when necessary?

For further information contact:

Mark Micallef
Risk Advisory - Banking Leader
mmicallef@deloitte.com.mt
+356 23432000

Berik Satpayev
Risk Advisory - Senior Manager
bestapayev@deloitte.com.mt
+356 23432000

Peter Galea
Risk Advisory - Assistant Manager
pgalea@deloitte.com.mt
+356 23432000

www.deloitte.com/mt
info@deloitte.com.mt
+356 23432000

Deloitte.