We manifest change.

Interview

# *Piecing Together the Puzzle: Critical Data Elements & BCBS 239*

An interview with Monocle's BCBS 239 SME:

## Catherine Horne

MONOCLE

We sat down with **Catherine Horne, Partner at Monocle and BCBS 239 subject matter expert**, to discuss the complex compliance task of identifying and managing critical data elements (CDEs).

As banks in the United Kingdom and Europe increasingly focus on complying with the principles of BCBS 239 and building robust data management and governance capabilities, many institutions are finding it challenging not only to define what a CDE is, but also to practically approach the process of identifying and managing them within their organisations.

We asked Catherine to shed some light on the basics of CDEs and to provide insights into the processes, systems, and approaches that can help sort through the pieces of this data "puzzle."

# Piecing together the Puzzle of CDEs

## How would you **define CDEs** in the context of BCBS 239 and what criteria should data meet to be considered critical?

CDEs are defined as individual data elements that are either part of a calculation or are stored in a table, whether at an aggregate or at a granular level. A key aspect of a CDE is their criticality – if you removed a CDE, the accuracy, integrity, and functionality of the calculation or process relying on that data would be compromised.

## How would you determine the **level of granularity** required for CDEs?

Determining the granularity of CDEs isn't about defining all detailed data as critical but about identifying which specific elements are essential to your calculations. Not every data element should be a CDE because not every data element materially impacts calculations. There's a balancing act between regulatory expectations, business needs, and practical feasibility. Furthermore, the required level of granularity for each critical data element should be defined to ensure meaningful aggregation and traceability.

Take, for example, the *Group Credit Exposure Report* - a key report used by risk and finance teams. It provides daily exposure values by counterparty, product, and region. As part of this report, the *counterparty ID* must be captured at the legal entity level to enable risk exposure analysis per counterparty and across groups. The exposure amount should reflect the net position after accounting for collateral and netting, reported in the appropriate currency. *Product type* should be specified at a granular level, such as "Interest Rate Swap" or "Term Loan," rather than broader categories like "Derivatives."

A similar level of assessment must be applied to other data elements, including *region, collateral type, booking entity* and *maturity date*. This example illustrates the challenge of setting granularity: over-engineering adds complexity and cost, while under-engineering undermines risk insight and regulatory compliance.

## What role do CDEs play in meeting **BCBS 239 compliance**?

Defining CDEs is foundational to achieving BCBS 239 compliance, but it is only the first step. It is essential that each CDE has clearly assigned ownership, well-documented metadata and business definitions, robust data quality controls and technical data lineage traced at the level of the individual CDE.

## Is there a **standard process or framework** that banks can follow to determine whether a data element should be classified as critical?

While there is no universal standard as the nature and size of institutions are different and expert judgement plays a role in determining criticality of CDEs in an institution, a common approach involves defining the scope to which BCBS 239 compliance is being applied – such as a specific risk report or regulatory metric. From there, banks can then define the data elements that are critical to the calculation and identify which of them have a material impact on the accuracy and integrity of the output. From there, a structured approach should be followed.

> *"Over-engineering adds complexity and cost, while under-engineering undermines risk insight and regulatory compliance."*

Different areas within a bank may have different types of CDEs, depending on their specific business functions and reporting needs. What is considered a critical data element in one area may not be critical in another. Working alongside executives in each of the risk areas to determine the metrics used for key decision making will help identify the in-scope reports and metrics and aid in defining the data elements critical to each area.

## How are **data sources, data lineage and controls validated** as part of the definition process?

Once CDEs have been defined, the next step is to trace their data lineage back to their originating data source. This is akin to assembling a puzzle, where each piece – data sources, transformations, data quality checks, metadata, ownership, and service level agreements – must fit together to form a complete and accurate picture of the entire data flow. By connecting data from source to target, banks can overlay each of the BCBS 239 principles and progressively fill in the gaps to meet compliance. This end-to-end lineage helps ensure that each CDE is supported by a well-governed and compliant data ecosystem.

> *"Tracing data lineage is akin to assembling a puzzle, where each piece – data sources, transformations, data quality checks, metadata, ownership, and service level agreements – must fit together to form a complete and accurate picture."*

## How would a bank leverage **data management platforms or technologies** to track or manage their CDEs?

Banks should be using data management platforms – either developed in house or commercially purchased – to manage CDEs effectively. These technologies support a range of capabilities, including capturing metadata, assigning data ownership, implementing business rules for automated data quality checks as well as logging incidents.

The role of these technologies is to move away from manual tools such as spreadsheets and provide a centralised platform that ensures a more controlled, auditable environment. These data management platforms enable users to visualise upstream and downstream impacts, manage data lineage and ensure consistent application of BCBS 239 principles. Crucially, users can be trained on these platforms to ensure consistent data management practices across the bank, which strengthens long term data governance.

Additionally, advanced technologies like AI and machine learning can be leveraged to detect data anomalies and variances. These tools also allow banks to track progress towards compliance, for example by monitoring the reduction in CDEs without metadata over time, changes in data quality variances as well as providing measurable indicators of progress/improvement.

## How would a bank ensure **consistency and standardisation** of CDEs across different business areas?

To ensure consistency and standardisation of Critical Data Elements (CDEs) across business areas, banks typically implement a centralised data governance framework. This involves establishing enterprise-wide data definitions, naming conventions, and quality rules maintained in a central business glossary and metadata repository.

A dedicated data governance function—such as a Data Office or Governance Council—oversees the process, supported by data owners and stewards who ensure alignment between central standards and business unit implementations. Consistent metadata, lineage tracking, and common data quality rules help prevent discrepancies in how CDEs are defined, sourced, and used across the organisation.

Additionally, banks embed CDE standards into system architecture, reporting processes, and change management frameworks. Any changes to CDEs are subject to impact assessments and must go through formal governance channels. Automated data quality monitoring ensures that issues are detected and addressed promptly, while integration of CDE definitions into project delivery and system design ensures ongoing adherence to standards. This structured approach enables banks to maintain a unified view of their critical data, which is essential for accurate risk data aggregation and reporting under BCBS 239.

## How Monocle Can Assist

Principles must be converted into practice. With over ten years of implementation experience, BCBS 239 has been a significant aspect of Monocle's consulting expertise since the principles were published in 2013. At Monocle, we perform a variety of functions, including project management, business and technical analysis, and facilitation with regulators.

Our prior engagements include remediation of regulatory reporting deficiencies and participating in the end-to-end BCBS 239 implementation journey, from establishing robust programme oversight and governance frameworks to implementing comprehensive controls and effective data management strategies. We have also supported risk aggregation processes, enhanced risk reporting capabilities, and developed IT and data architectures, ensuring alignment with BCBS 239 requirements at every step.

**Leverage Monocle's expertise and view our latest insights on our website:**


**BCBS 239 Embedment**
Case Study


**The Continual Challenges (and Opportunities) of BCBS 239 Compliance**
Podcast


**3 Key Considerations for BCBS 239 Compliance Embedment**
Insights Paper

---


### Johannesburg

8th Floor, The MARC Tower 1
129 Rivonia Road, Sandton,
Johannesburg, 2196

*info.za@monoclesolutions.com*

+27 (0) 11 263 5600

### Cape Town

301 New Cumberland
163 Beach Rd Mouille Point
Cape Town, 8005

*info.za@monoclesolutions.com*

+27 (0) 82 952 1415

### London

1 Royal Exchange
EC3V 3DG
London, England

*info.uk@monoclesolutions.com*

+44 (0) 2030 022 514

### Amsterdam

Office 136, Gustav Mahlerplein 2,
1082 MA, Amsterdam,
Netherlands

*info.nl@monoclesolutions.com*

+31 (0) 2 02 256 182

www.monoclesolutions.com