



EUROPEAN CENTRAL BANK

BANKING SUPERVISION

RDARR as a Supervisory Priority

15 May 2025
DG-S/SUP conference

Francisco Garcia-Martin
Head of IT, Operational Risk & Resilience



Overview

1 Why Data quality and aggregation is important?

2 What was done until now?

3 Did it work?

4 What is coming next?

5 Conclusions

Why data quality and aggregation is important

- Many times, **RDAR is seen as a mere supervisory requirement** and the focus is many times on the quality of supervisory reporting, but
- Good data quality and data aggregation capabilities is actually a **competitive advantage for banks**:
 - ✓ Good data quality is paramount **for understanding the exposure to the different risks** a financial institution faces and to steer the entity;
 - ✓ Good aggregation capabilities provide flexibility to **understand the impact of unexpected shocks** and react to them
 - ✓ Good data quality is a **prerequisite for the implementation of new technologies**, like AI

1 Why Data quality and aggregation is important?

2 **What was done until now?**

3 Did it work?

4 What is coming next?

5 Conclusions

Work done so far

Lessons from the financial crisis:

Lack of risk information to make sound business decisions

→ **BCBS 239 Principles for effective risk data aggregation and risk reporting**

Deadline for full implementation in G-SIBs: **Jan'16**

2016

ECB Thematic review: 25 banks assessed. The outcome showed the implementation status of BCBS239 principles were **unsatisfactory**.

2013

2019

SSM letter to all significant institutions regarding **"Supervisory expectations on risk data aggregation capabilities and risk reporting practices"** which considers BCBS239 principles as a benchmark, **also for regulatory reporting**

2020

BCBS Progress report: As of the end of 2018, **none of the banks are fully compliant** with the BCBS 239 principles

2021

FSB Too-Big-To-Fail evaluation report stated that there is still scope for SIBs to **improve** their RDAR frameworks

2022

SSM Supervisory Priorities 2022 identified as a key vulnerability in management bodies' steering capabilities: **reliable data essential for decision-making**

2023

SSM Supervisory priorities 2023-2025: Key vulnerability
Deficiencies in risk data aggregation and reporting

New BCBS Progress report confirms weaknesses

2024

The publication of the ECB Guide on selected priority topics that are a precondition for effective RDAR

BCBS 239 OSI Campaign

By end of 2024, ~30+% of SIs planned to be covered

RDAR HelpDesk

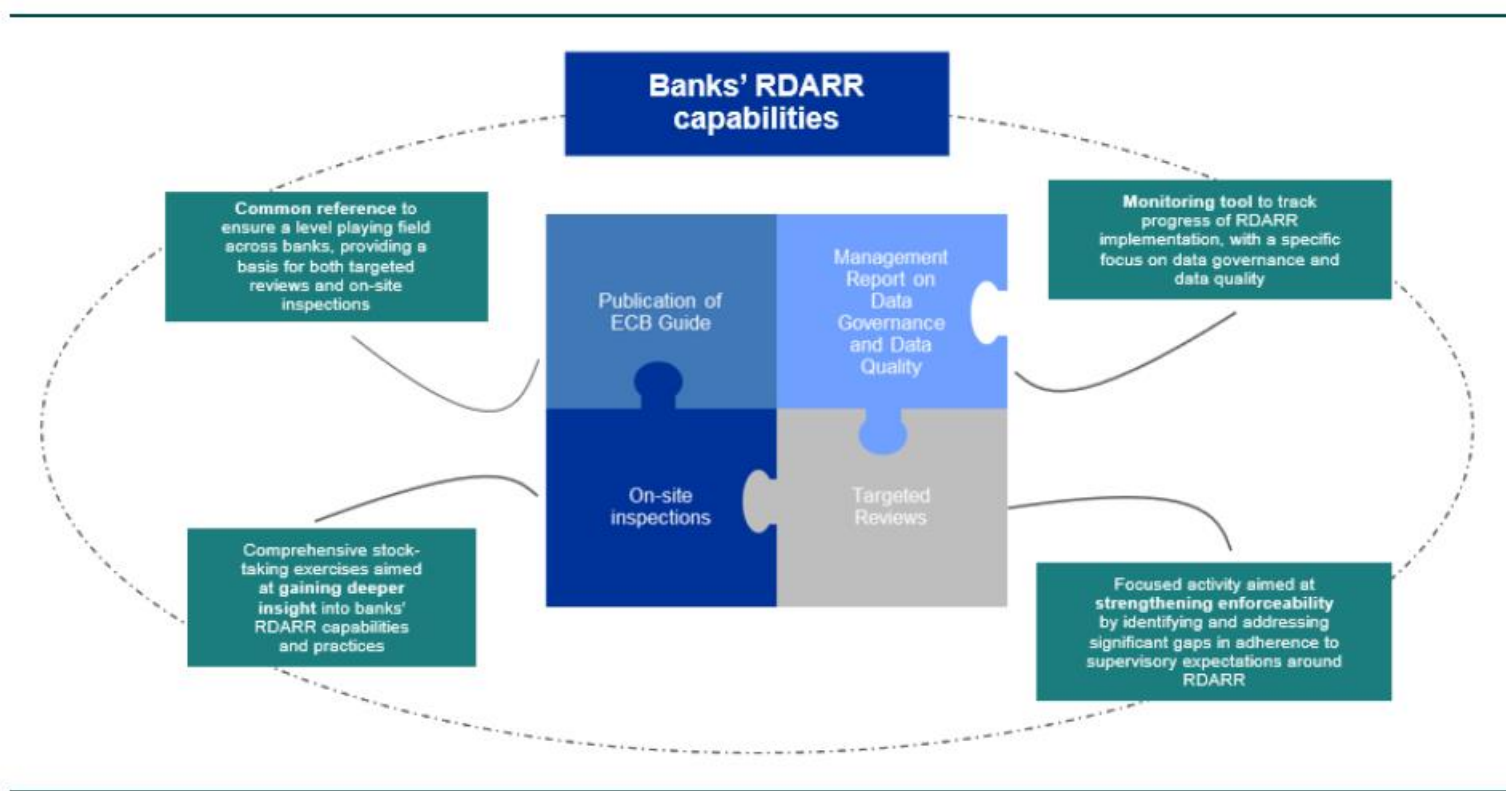
Regular ad hoc RDAR trainings

Management Report

RDAR TR

Focus areas translated into targeted supervisory activities

Comprehensive approach since 2022



The ECB Guide on RDAR

Make **transparent our minimum supervisory expectations on selected, priority topics** focussing on those **preconditions deemed essential to be in place** to facilitate progress in data aggregation capabilities, with focus on **how to achieve expected level** of RDAR capabilities

- ① **Full responsibility of Management Body**
- ② **Sufficient scope of application** of data governance frameworks in terms of risk types, reports and risk indicators, legal entities, business lines and risk, financial and supervisory reporting
- ③ **Effective group-wide data governance frameworks** incl. data owners, a data governance function, an independent validation function and regular validation by internal audit
- ④ **Integrated data architecture** with uniform data definitions and glossaries and data lineage back to the sources
- ⑤ **Group-wide data quality management and standards** incl. automated data quality (DQ) checks, reconciliations, measurement of data quality indicators (including tolerance levels) and an up-to-date and complete register of DQ issues
- ⑥ **Timeliness of internal risk reporting** should allow the banks to duly react in timely manner
- ⑦ **Effective implementation programs**

The ECB Guide on RDAR

Example: Full responsibility of Management Body (MB)

- MB should make RDAR a **key priority** for the institution and ensure the deployment of **adequate resources**.
- MB should **formulate, approve and review**:
 - ✓ Entity's **definition of BCBS239 compliance** and key RDAR **frameworks and policies**
 - ✓ concrete **requirements for data quality in terms of accuracy, completeness, timeliness and adaptability** in normal times and in times of stress
 - ✓ **KPIs** to monitor data quality
- MB should **oversee and monitor**:
 - ✓ key deliveries of **remediation programmes**
 - ✓ **adherence to BCS239 principles** as well as any potential **limitation that prevent full risk data aggregation**.
 - ✓ **Roll-out** of RDAR frameworks and policies **across the Group**
- MB members should have a **sufficient understanding, sufficient skills and experience** in the topic.

1 Why Data quality and aggregation is important?

2 What was done until now?

3 **Did it work?**

4 What is coming next?

5 Conclusions

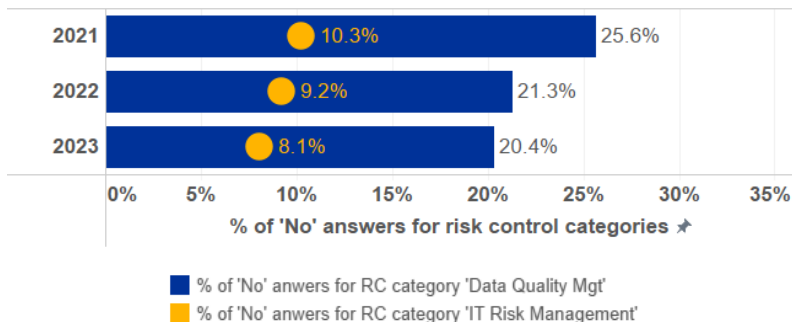
Did it work?

- Despite this increased supervisory scrutiny, it has been concluded that the **progress made by Significant Institutions** to date has been generally **insufficient**.
- Based on the recent OSI campaigns and horizontal projects (e.g. Targeted Review and Helpdesk support), the slow remediation of RDAR deficiencies are the result of multiple root causes, in particular:
 1. Governance framework shortcomings
 2. Fragmented IT infrastructure and a large amount of manual aggregation processes
 3. Remediation of RDAR deficiencies is often costly, entails high risks and takes time

Did it work? – According to the ITRQ

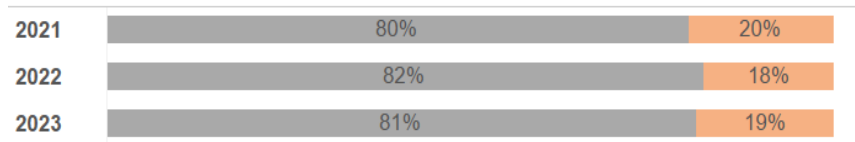
According to the ITRQ, **IT Data quality management is the least mature** of all IT Risk domains.

Average percentages of "No" answers for the "Data Quality Management" Risk Control category

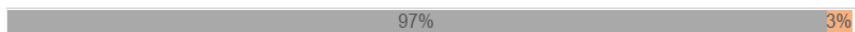


■ No
 ■ Yes

The supervised entity has defined and documented its data architecture, data models, data flows, golden (authoritative) sources, a data dictionary, and validated them with relevant business and IT stakeholders (% of SIs, by reference year)



Documented and enforced data classification in place



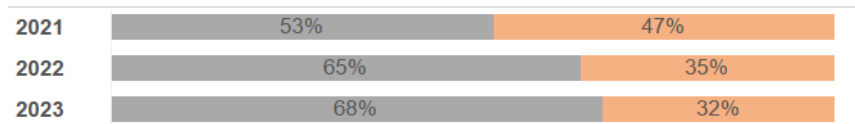
Data owners are defined



Criticality and sensibility of the information are defined



Data quality management procedures also apply to End User Computing (EUC) (% of SIs, by reference year)



Did it work? – According to the OSI campaign

Area	Main findings
Internal governance	<ul style="list-style-type: none">• Insufficient attention to RDAR from management board• Too narrow scope of application• Incomplete governance arrangements
Data infrastructure and IT architecture	<ul style="list-style-type: none">• Data infrastructure and IT architecture not fit for purpose• Insufficient data lineage and data taxonomies• Data ownership inappropriately assigned
Accuracy and integrity	<ul style="list-style-type: none">• Recurrent manual data corrections due to issues with data quality controls• Weakly controls of manual workarounds

Did it work? – According to the Targeted Review

- TR identified **significant gaps across sampled banks in meeting the expectations** outlined in the ECB Guide on RDAR.
- The table below shows **clusters of findings against the main aspects of the supervisory expectations** in the ECB Guide
- **Implementation programmes show the highest number of severe findings**, followed by data governance frameworks, responsibility of the management body and scope of application (details of the main deficiencies can be found in the annex)

Module	Sub-category (clusters of findings)	Bank 1	Bank 2	Bank 3	Bank 4	Bank 5	Bank 6	Bank 7	Bank 8	Bank 9	Bank 10	Bank 11	Bank 12	Bank 13	Bank 14	Bank 15
Module 1	Responsibilities of the management body	Low severity (F1/2)	Low severity (F1/2)	High severity (F3/4)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Low severity (F1/2)	Low severity (F1/2)	Low severity (F1/2)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	High severity (F3/4)	High severity (F3/4)
	Effective implementation programmes	Low severity (F1/2)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	High severity (F3/4)	High severity (F3/4)	High severity (F3/4)	High severity (F3/4)
Module 2	Sufficient scope of application	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Low severity (F1/2)	Low severity (F1/2)	Low severity (F1/2)	Low severity (F1/2)	High severity (F3/4)	Low severity (F1/2)	High severity (F3/4)	Low severity (F1/2)	High severity (F3/4)	High severity (F3/4)
	Effective data governance framework	Low severity (F1/2)	Low severity (F1/2)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Low severity (F1/2)	Low severity (F1/2)	High severity (F3/4)	High severity (F3/4)	High severity (F3/4)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)
	Integrated data architecture	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	High severity (F3/4)	High severity (F3/4)	Low severity (F1/2)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)
	Group-wide data quality management and standards	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Low severity (F1/2)	High severity (F3/4)	Low severity (F1/2)
	Internal risk reporting	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Low severity (F1/2)	Low severity (F1/2)	High severity (F3/4)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)	Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)



Low severity (F1/2)



High severity (F3/4)



Module not assessed by the JST (e.g., due to previous OSI findings or ongoing supervisory activities)

1 Why Data quality and aggregation is important?

2 What was done until now?

3 Did it work?

4 **What is coming next?**

5 Conclusions

RDAR as an SSM Supervisory Priority

Supervisory priorities for 2025-27, addressing identified vulnerabilities in banks

Priority 1: Banks should strengthen their ability to withstand immediate macro-financial threats and severe geopolitical shocks

Address deficiencies in **credit risk management frameworks**



Credit risk

Address deficiencies in **operational resilience frameworks** as regards IT outsourcing and IT security/cyber risks



Operational risk

Special focus: Incorporating the management of geopolitical risks in supervisory priorities



Multiple risk categories

Priority 2: Banks should remedy persistent material shortcomings in an effective and timely manner

Address deficiencies in business strategies and risk management as regards **climate-related and environmental risks**



Climate-related and environmental risks

Address deficiencies in **risk data aggregation and reporting**



Governance

Priority 3: Banks should strengthen their digitalisation strategies and tackle emerging challenges stemming from the use of new technologies

Address deficiencies in **digital transformation strategies**



Business model

We classify all banks in different buckets

Bucket 1

Banks without significant issues

- A previous assessment has been performed
- Good RDAR capabilities and no significant issue has been identified/no hints that there are DQ issues
- This is reflected for instance with a low SREP score in this area ($< 3+$)*

Bucket 2

Banks with identified issues

- Assessed in previous supervisory activities (e.g., via OSI or TR)
- There is a good understanding of the main deficiencies in the bank to ensure adequate RDAR capabilities
- In some cases, there can be an action plan in place with specific actions and deadlines/some work is in progress

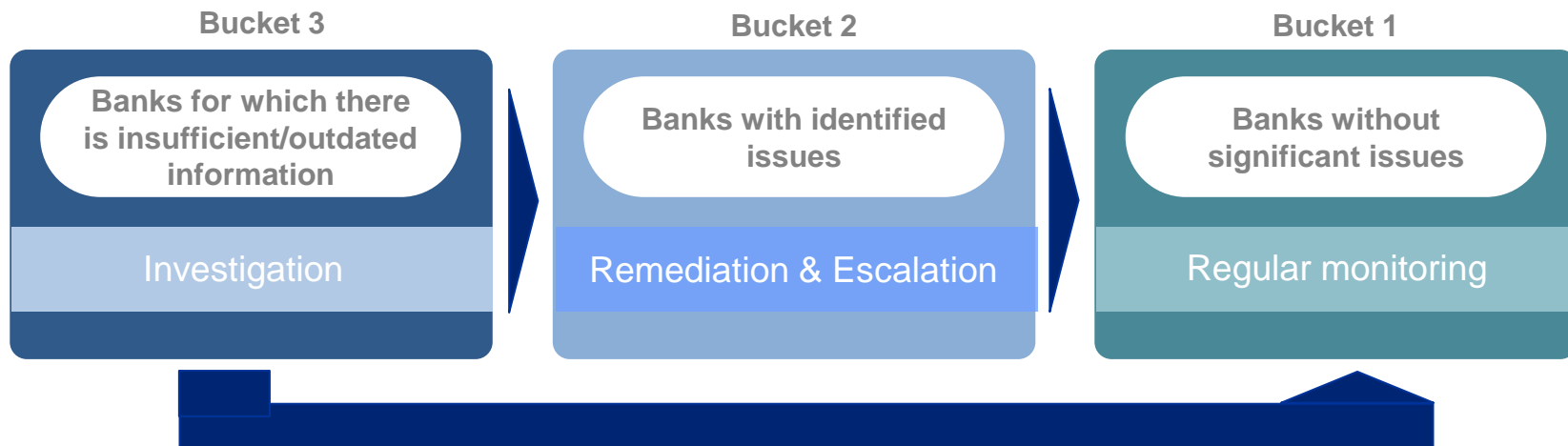
Bucket 3

Banks for which there is insufficient/outdated information

- Not thoroughly assessed in previous supervisory activities
- Hints that there are DQ issues
- In some cases, there might be some previous findings and measures, but they would be only partial and/or not well articulated

And we apply a different strategy in each of the buckets

The final objective is **to move as many banks as possible to bucket 1**. To do so, each bucket will be subject to a different supervisory strategy



Overview

1 Why Data quality and aggregation is important?

2 What was done until now?

3 Did it work?

4 What is coming next?

5 **Conclusions**

Conclusions

- RDAR, cannot be seen only as a supervisory compliance item. Good Data quality and aggregation capabilities provide evident benefits to credit institutions
- Despite the effort spent by regulators and supervisors for many year, progress made by supervised institution is deemed insufficient
- RDAR will continue being a supervisory priority. All Significant institutions will be classified in 3 different buckets and a different supervisory strategy will be applied to each bucket
 - ✓ For banks without any significant issue in this area, regular monitoring
 - ✓ For banks with significant issues already identified, follow up and escalation
 - ✓ For banks for which there is insufficient analysis, investigation