What are the main data regulations impacting organizations?

Regulatory-driven data management

Table of contents

Introduction

What are the major regulatory trends?

Articles

Introduction

How data are collected and used affects the course of business for almost all firms in the world. As the field of data collection matures and transforms the economy, its importance has not escaped the attention of European and national regulators. In this article we look at the regulatory trends and the ways your organization can implement data management tools that lead to reduced risk, better communications and ultimately a better environment for profitability.

Data have become an invaluable asset for organizations. They are the backbone of all critical business processes. This results in increased risks, which must be controlled and mitigated.

More and more, regulators request large datasets and complex reporting in order to better understand risks taken by financial institutions. Data quality and data governance are considered essential to ensuring these datasets and reporting present an accurate picture of the situation.

Therefore, most new on-site inspections and regulations include a section dedicated to data. Following an initial push by the Basel Committee with BCBS 239 principles, European and Belgian regulators have published several regulations, including data management chapters, which require financial institutions to make significant efforts to become compliant.

This article aims to provide you with an overview of key data regulations applicable to Belgian organizations. In addition to providing a summary of each regulation, we will provide an outline of major areas on which regulators are likely to focus.

What are the major regulatory trends?

Most regulations we have analyzed include common principles. We have grouped them in three categories and summarized the main trends.

1. Data Governance

Most regulations require the establishment of "strong data governance." However, they fail to precisely describe their expectations. Many of them mention the definition of roles and responsibilities, and a few of them refer to a business glossary. It takes knowledge of the market, an understanding of the regulator's expectations and a capacity to translate "strong data governance" into practice.

2. Processes

Most regulations require robust data and IT architecture. These technical resources must work even in times of stress or crisis. Therefore, the regulator expects financial institutions to be able to rapidly produce new ad-hoc reliable reports upon request or need.

In addition, many regulations require institutions to have appropriate tools for a timely detection and resolution of errors and inconsistencies in reports. Regulators also require that processes get documented end-to-end (i.e. from data sourcing to reporting, and reporting processes get automated to the greatest extent) in order to minimize risks.

When it is not possible to automate a part of the process, a few regulations mention explicitly that End-User Computings (EUCs) should be documented and that related risks should be managed. They mention as well that key controls should be documented. Finally, they indicate the frequency and recipients of the reports should be appropriate.

3. Data Quality

Most regulations include requirements regarding data quality. They mention different dimensions, including completeness, accuracy, validity, consistency and integrity of data. Other standards include the adaptability/flexibility of the reporting process and the timeliness of the reporting. They also require data to be traced and auditable (which is usually done via data lineage). Finally, many regulations mention confidentiality and security as data quality dimensions.

Regulations only describe the expected result ("…data should be of sufficient quality…"), not how institutions achieve this result.

How to benefit and create value for your organization?

Beyond regulatory compliance, there are numerous incentives for improving data management practices of your organization:

- Data governance increases responsibility and accountability of data by defining clear roles and responsibilities.
- A data quality management process improves the quality of the data; good data quality is a requirement for performing proper data analytics and reporting, as well as data monetization. The quality of the output is essential when corporate decisions are based on data.
- Metadata management improves the understanding of data and increases awareness of the quality of data. This results in fewer errors of interpretation, smoother collaboration within the organization and a decline in erroneous decisions.
- Data documentation and data governance reduce the time and costs needed to understand and use data, resulting in improved operational effectiveness.
- Data lineage facilitates an impact analysis in the context of change management and allows for the identification of the source of errors, duplicate or wrong data sources or the usage of wrong data for reporting/analytics. This study can ultimately lead to cost reduction.
- A data catalogue increases awareness of available data and authoritative sources, which makes finding relevant data easier.

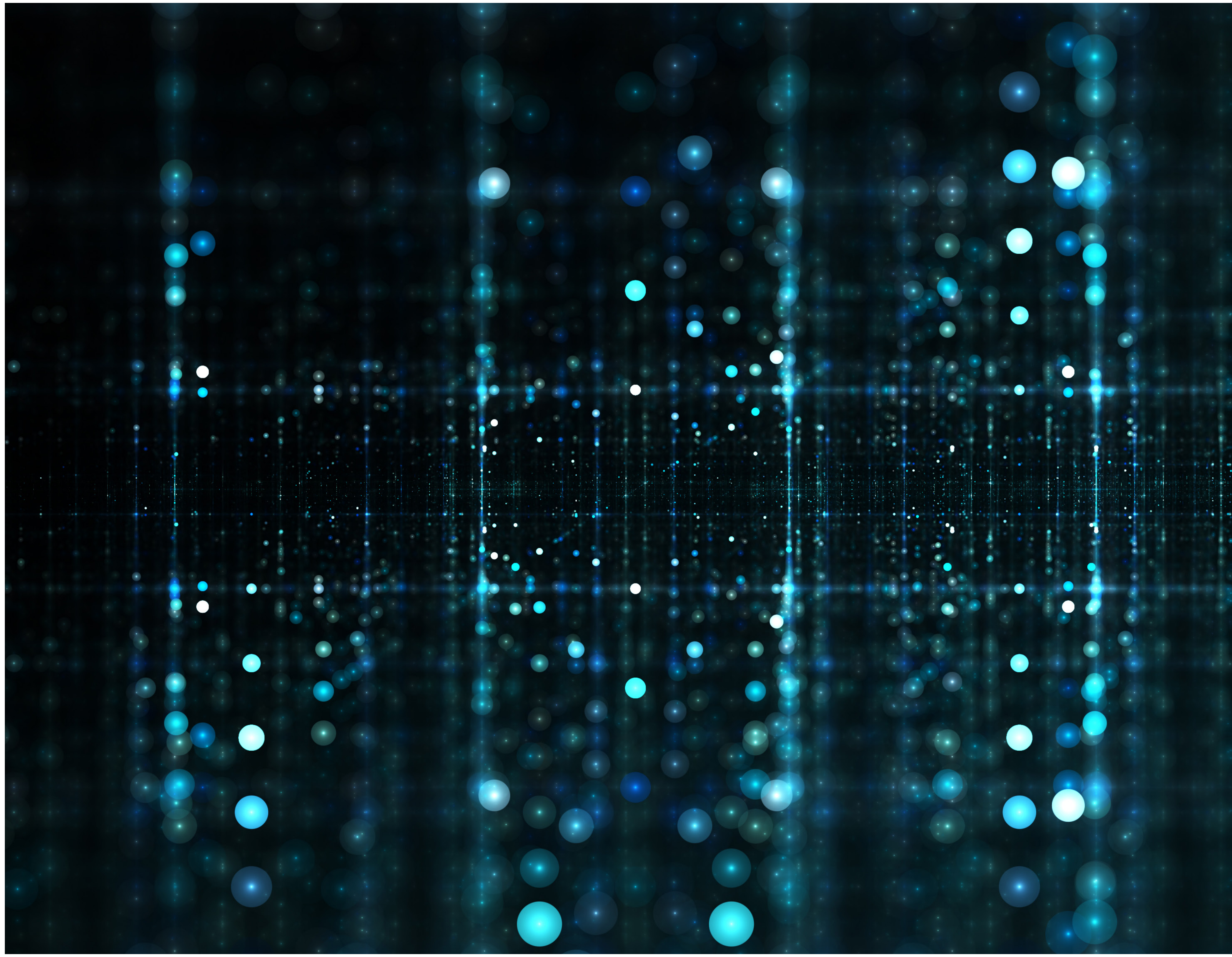
- Data classification improves the security and privacy of data, allowing for a better management of access rights and the avoidance of data breaches. It also helps identifying key data elements.
- Data access and security management are improved when you know who creates and uses the data.
- A better knowledge of the data landscape and improved data consistency result in an easier integration of data from different systems.
- Defining and measuring KPIs helps management make informed decisions on data.

How KPMG can help?

Leveraging our experience and track record across many industries, KPMG can assist you in complying with regulations and overcoming challenges in your data transformation. Thanks to our multidisciplinary approach (combining regulatory and data experts with sector knowledge), we adapt our proven methods and tools to specifically help you comply with various regulations and reap the benefits of trustworthy data assets.

In the context of such a regulatory-driven data transformation, we can assist you by:

- Assessing your organization against regulatory requirements
- Designing your Data Strategy and guiding the implementation of your transformation plan
- Guiding you through the identification and prioritization of remediation actions (on data governance, metadata management, data quality, data lineage, etc.)
- Evaluating the best tools to support your progression and assist in their integration



Title	Date of publication	Publisher	Purpose
BCBS 239	January 2013	Basel Committee on Banking Supervision	Improve risk data aggregation capabilities and risk reporting practices
NBB Data Quality Circular	October 2017	National Bank of Belgium	wider reference framework for monitoring and improving the quality of the internal reporting process and prudential data
Loan origination and monitoring guidelines	June 2020	European Banking Authority	Improve data quality and information symmetry between institutions and investors in the NPL secondary markets in Europe
Internal models guidelines	October 2019	European Central Bank	Guidelines for use of internal models to determine regulatory capital requirements
Resolution (SRB valuation)	April 2020	Single Resolution Board (delegated to National Resolution Authorities)	Guidelines to demonstrate that banks are resolvable and prepared for crisis management
GDPR	April 2016	European Parliament & Council of the European Union	Harmonize data privacy laws across all of EU members states as well as providing greater protection and rights to individuals
AI Act	April 2021	European Commission	Risk-based approach that prohibits specific unacceptable uses of AI, heavily regulates some other uses classified as high risks, and encourages the adoption of codes of conduct on uses that are of limited risk or no risk at all
DORA	September 2020	European Commission	Enhance and strengthen the digital operational resilience of the EU financial sector
Solvency II	November 2009	European Parliament, Council of the European Union	Unify the insurance market and set minimum standards regarding risk management practices
ESG disclosures	June 2022	European Banking Authority (under the CRR Article 434a mandate)	Harmonize the ESG reporting practices by putting forward comparable disclosures templates, standardized definitions and KPIs

BCBS 239

Basel Committee on Banking Supervision' standard number 239

Publisher	Basel Committee on Banking Supervision
Key dates	Published in January 2013 Enforced on 1/01/2016 (or 3 years after the institution got designated as a G-SIB or D-SIB)
Purpose	Following the global financial crisis of 2007-2008, the banks' IT and data architectures were deemed inadequate to support the broad management of financial risks, in particular regarding the ability to aggregate risk exposures and identify concentrations quickly and accurately at bank group level, across business lines and between legal entities. The Basel Committee issued this regulation in order for banks to improve their risk data aggregation capabilities and risk reporting practices.
Audience	— Global Systematically Important Banks (G-SIBs) — Domestic Systematically Important Banks (D-SIBs) — Significant institutions (ECB designation)

Overview of Main Principles

Risk data aggregation capabilities and risk reporting practices should

- Be subject to strong governance
- Be supported by a data architecture and IT infrastructure not only in normal times but also during times of stress or crisis
- Allow to generate accurate and reliable aggregated risk data on a largely automated basis, including in times of stress/crisis
- Allow to capture and aggregate all material risk data
- Allow to generate aggregated and up-to-date risk data in a timely manner
- Allow to meet a broad range of on-demand, ad hoc risk management reporting requests
- Allow to accurately and precisely convey aggregated risk data
- Allow to cover all material risk areas within the organization
- Allow to communicate information in a clear and concise manner
- Allow for an appropriate frequency of risk reporting
- Allow for the distribution of risk management reports to relevant parties while ensuring confidentiality

NBB Data Quality Circular

NBB Circular 2017_27 on Data quality

Publisher

National Bank of Belgium

Key dates

Published in October 2017
Initial self-assessment to be performed by June 2018

Purpose

The aim of this circular is to draw the attention of the financial institutions concerned to the high importance given by the supervisory authorities to the quality of the prudential and financial data submitted to supervisors by the institutions under supervision. It is also intended to raise awareness to the various quality tests which the institutions concerned are required to comply with for the data they submit.
It subsequently proposes a wider reference framework for monitoring and improving the quality of the internal reporting process and prudential data.

Audience

- Credit institutions under Belgian law (including branches)
- Insurance companies under Belgian law
- Payment / Electronic money / Settlement institutions under Belgian law
- Stockbroking firms under Belgian law
- Financial holding companies

Overview of Main Principles

Governance

- Necessary roles and responsibilities for prudential reporting are identified and documented; this is regularly reviewed
- There are enough capable employees at each stage of the reporting process to report properly, even in times of crisis

Technical capacities

- The data and IT infrastructures are adequate to produce and verify the prudential reporting, even in times of stress or crisis
- The institution has appropriate tools for timely detection and resolution of errors and inconsistencies
- Reporting processes are sufficiently automated and integrated; EUC is documented and risks are under control

Process

- The End-to-End reporting process is properly documented and reviewed regularly. In addition, the institution has a business glossary, a list of interpretations and assumptions, and records of all reconciliations
- Per table, divisions involved in all preparation steps are documented
- Key controls are integrated and documented

Loan origination and monitoring guidelines

Loan origination and monitoring guidelines

Publisher	European Banking Authority
Key dates	— June 2020: publication of the guidelines — June 2021: application of the guidelines to newly originated loans — June 2022: application of the guidelines to existing loans that have been renegotiated — June 2024: application of full monitoring requirements to the stock of existing loans
Purpose	The guidelines introduce requirements for assessing the borrowers' creditworthiness, together with the handling of information and data for the purposes of such assessments. They aim to improve data quality and information symmetry between institutions and investors in the NPL secondary markets in Europe.
Audience	— Banking institutions, as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013 — Creditors, as defined in Directive 2014/17/EU (the Mortgage Credit Directive, MCD) or in Directive 2008/48/EC (the Consumer Credit Directive, CCD)

Overview of Main Principles

Data quality

- When using technology-enabled innovation for credit-granting purposes, institutions should understand and ensure the quality of underlying data, as well as their confidentiality, integrity and availability. They should ensure the traceability, auditability, robustness and resilience of the inputs and outputs of related models.
- Credit risk data requirements include depth, breadth, accuracy, integrity, reliability, timeliness, consistency and traceability.

Data infrastructure and processes

- Institutions should have an appropriate data infrastructure to support the credit-granting process as well as the monitoring of the credit facilities throughout their lifecycle. It should ensure the continuity, integrity and security of related information.
- Institutions should have adequate IT processes, systems, capabilities and sufficient and accurate data for the purposes of any statistical model-based or index-based (re)valuation.
- The data infrastructure should provide the capability to gather and automatically compile data regarding credit risk without undue delay and with little reliance on manual processes.
- The data infrastructure should allow the generation of granular risk data meeting the regulator's requirements for regular prudential and statistical reporting, as well as supervisory stress testing and crisis management purposes.

Internal models guidelines

ECB guide to internal models

Publisher	European Central Bank
Key dates	Specific chapters published in February 2017, March 2018, September 2018, November 2018 and July 2019. Publication of the consolidated version of the guide on 1/10/2019
Purpose	In the wake of the financial crisis the use of internal models to determine regulatory capital requirements came under heightened regulatory and supervisory scrutiny. The reasons for this were twofold. Firstly, internal models are becoming more and more complex due to detailed regulatory requirements, making them hard to monitor and maintain. Secondly, the outcome of numerous studies indicated potential irregularities and high variability in the calculation of capital requirements using internal models between banks with similar portfolios. To counter these issues, the ECB published these guidelines.
Audience	Banking institutions, as defined in point 3 of Article 4(1) of Regulation (EU) No 575/2013

Overview of Main Principles

These guidelines set out principles regarding following elements for the management of IRB data:

— IT systems: infrastructure and implementation testing

— The bank should have a sound and robust IT infrastructure

— The bank should have documentation of the End-to-End data flows, the IT architecture, the functional and technical specifications of IT systems and databases used by models

— The bank should have a comprehensive IT testing process

Policies, roles and responsibilities in data processing and data quality management

— All data transformations should be traceable and controlled; rules should be formalised with regard to manual interventions

— All data transfers should be formally agreed upon (via e.g. SLA) to ensure timeliness and accountability

— Business owners should ensure (i) data are correctly entered, kept up-to-date and aligned with data definitions; (ii) data aggregation capabilities and reporting practices are consistent with policies.

— IT functions are responsible for supporting data operations

Data quality management framework

— The framework should cover the completeness, accuracy, consistency, timeliness, uniqueness, validity, availability and traceability of data. It should cover the whole data life cycle from data entry to reporting

— Data quality should be measured in an integrated and systematic way

— Data quality issues should be identified, reported and remediated

Resolution (SRB valuation)

Resolution

Publisher	Single Resolution Board (delegated to National Resolution Authorities)
Key dates	2014: Adoption of the Bank Recovery and Resolution Directive (BRRD) 1/04/2020: Publication resolution guidelines for banks following consultations that took place in 2019 and will be phased in gradually until 2023.
Purpose	Banks should demonstrate that they are resolvable and prepared for crisis management. An entity shall be deemed to be resolvable, if it is feasible and credible to either liquidate it under normal insolvency proceedings or to resolve it with its resolution tools and powers while avoiding, to the maximum extent possible, any significant adverse consequences for financial systems, the economy and financial stability of the Member State in which the entity is situated, or other Member States, or the Union and with a view to ensuring the continuity of critical functions carried out by the entity
Audience	Institutions and groups - where the SRB is involved as home or host resolution authority - directly supervised by ECB or have entities in participating Member states. National translations will be done for institutions supervised by National Resolution Authorities.

Overview of Main Principles

Institutions should have Management Information System capabilities to produce necessary information for Resolution.

For the effective application of resolution actions, they need to:

- demonstrate that their governance arrangements adequately address the processes for consistent data collection and aggregation, and for their timely delivery
- establish a process for keeping this information up-to-date and of high quality
- ensure swift access to necessary data for all relevant stakeholders
- show ability to simultaneously produce multiple data under time pressure or financial stress conditions defined by the SRB

For the execution of a fair, prudent and realistic valuation, they need to:

- provide proof of the availability of data and their data aggregation capabilities during the resolution planning phase
- explain and clearly justify the underlying data sources, assumptions and methodologies of each of their internal valuation models. They must also show the flexibility and sensitivity of these models

For the preparation and update of resolution plans, they need to:

- demonstrate that they have quality assurance arrangements in place
- Show that they have a service catalog and repository of relevant service catalogs in place that are searchable, updated and comprehensive to support information gathering during and post resolution

GDPR

General Data Protection Regulation

Publisher	European Parliament & Council of the European Union
Key dates	27/04/2016: The GDPR was adopted. 25/05/2018: The General Data Protection Regulation become enforceable from this day on.
Purpose	The GDPR was designed to harmonize data privacy laws across all of EU members states as well as providing greater protection and rights to individuals (e.g. right to be forgotten and right to launch a complaint). GDPR was also created to impose rules and limits to how businesses and other organizations can use and process personal information (e.g. how it is collected, stored, used, disclosed and disposed of). GDPR replaces the 1995 Data Protection Directive which was adopted at a time when the internet was in its infancy.
Audience	The GDPR applies to all businesses and organizations when they process personal data if — they are based or established in the EU; — if they handle data of individuals located in the any of the EU member states (regardless of where the data is processed — If they are offering goods/services (paid or for free) or are monitoring the behaviour of individuals in the EU.

Overview of Main Principles

Lawfulness, Fairness, and Transparency (Article 5(1)(a)):
Organisations must meet the requirements described in the GDPR when processing the personal data of EU citizens, and should provide all necessary information to the individuals in a transparent way.

Purpose limitation (Article 5(1)(b)):
Organisations should only collect personal data for a specific purpose, clearly state what that purpose is and process the personal data reasonably and proportionately to the purpose.

Data minimization (Article 5(1)(c)):
Organisations should only collect personal data adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy (Article 5(1)(d)):
The personal data that organisations process must be accurate.

Storage limitation (Article 5(1)(e)):
Personal data may not be kept longer than necessary.

Integrity and confidentiality (Article 5(1)(f)):
Organisations must ensure appropriate security of personal data.

Accountability (Article 5(2)):
Organisations are responsible of compliance with GDPR and must ensure policies.

AI Act

EU Artificial Intelligence Act*

Publisher	European Commission
Key dates	21/04/2021: The European Commission published the first-ever legal framework on artificial intelligence (AI). *The Act is now working its way through the European Parliament after which it will be subject to a two-year implementation period.
Purpose	The AI Act adopts a risk-based approach that prohibits specific unacceptable uses of AI (social scoring, facial recognition, dark-pattern AI,...), heavily regulates some other uses classified as high risks (education, employment, justice,…), and encourages the adoption of codes of conduct on uses that are of limited risk (chat bots, deep fakes, emotion recognition,…) or no risk at all (spam filters, video games,…). High-risk AI systems will need to meet certain technical and regulatory requirements before they can be brought to market.
Audience	The AIA applies to all businesses and organizations providing AI services or products reaching the EU market. This includes operators outside the EU if the output of the AI system impacts natural persons located in the EU.

Overview of Main Principles

High-risk AI systems must meet certain requirements before getting a CE mark, required for entering the European market. These requirements can be categorized under five key principles:

— **Data and Data Governance:** High-risk AI systems must be developed using high-quality datasets.

— **Transparency for Users:** Providers of high-risk AI systems must disclose information on the characteristics, capabilities, limitations and intended purpose.

— **Human Oversight:** High-risk AI systems must be designed to be overseen by humans. The overseer should understand the main limitations of AI systems and have the ability to identify shortcomings in a particular system.

— **Accuracy, Robustness and Cybersecurity:** High-risk AI systems must achieve a level of accuracy, robustness and cybersecurity corresponding to their intended purpose.

— **Traceability and Auditability:** Providers of high-risk AI systems must establish technical documentation containing information necessary to assess their compliance with the other requirements mentioned above.

DORA

Digital Operational Resilience Act for the financial sector

Publisher	European Commission
Key dates	Published on 24/09/2020 as a draft text – official regulation soon to be published which will apply after 24 months from the entry into force (except Article 23 and 24)
Purpose	The objective of DORA, part of the so-called Digital finance package, is to enhance and strengthen the digital operational resilience of the EU financial sector by harmonizing and upgrading the existing rules and introducing requirements (where gaps exist) on Information and Communications Technology (ICT) and security risk management. All participants of the financial system will be subject to a common set of standards to mitigate ICT risks for their operations.
Audience	Entities providing services through their own ICT systems and/or when they use, and rely on, ICT third-party providers. The financial entities are (among others): credit institutions; payment institutions; investment firms; Crypto-asset service providers (CASPs); central counterparties (CCPs); trading venues; insurance intermediaries; insurance and reinsurance undertakings; credit rating agencies; statutory auditors and audit firms.

Overview of Main Principles

The DORA proposal mentions below principles impacting 3 key data topics:

Data (process and scope) documentation

- Develop a backup policy specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the sensitiveness of the data;
- Identify and document all processes that are dependent on ICT third-party service providers, and any interconnections with ICT third party service providers.

Data classification, access and protection

- Implement policies that limit the physical and virtual access to ICT system resources and data;
- Draft protocols for strong authentication mechanisms with proper approved data classification and risk assessment processes

Data quality reporting

- Provide indication of full service level descriptions accompanied by quantitative and qualitative performance targets within agreed service levels to allow an effective monitoring by the financial entity.

Solvency II

Directive on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)

Publisher	European Parliament, Council of the European Union
Key dates	Published on 25/11/2009 Fully came into effect on 1/01/2016
Purpose	The Solvency II regime introduces a harmonized and robust prudential framework for insurance firms in the EU. It is based on the risk profile of each individual insurance company in order to promote comparability, transparency and competitiveness. The objective of this directive is to unify the insurance market and set minimum standards regarding risk management practices, including for capital requirements.
Audience	Insurance and reinsurance firms operating in the EU

Overview of Main Principles

- Data used for the calculation of the Minimum Capital Requirement should be accessible and auditable, even if this activity is outsourced.
- The Actual Function should assess the sufficiency and quality of the data used in the calculation of technical provisions. These data should be consistent with information provided by financial markets.
- Institutions shall have internal processes to ensure the appropriateness, completeness and accuracy of the data used in the calculation of their technical provisions.
- Data used for internal models shall be accurate, complete and appropriate. Institutions shall update the data sets used in the calculation of the probability distribution forecast at least annually.
- The model validation process shall include an assessment of the accuracy, completeness and appropriateness of the data used by the internal model.

ESG disclosures (1/2)

ITS on Pillar 3 disclosures on ESG (Environmental, Social and Governance) risk EBA/CP/2021/06

Publisher	European Banking Authority (under the CRR Article 434a mandate)
Key dates	Applicable as from June 2022 - EBA will follow a sequential approach (proportionality used considering current data gaps and need to develop methodologies)
Purpose	Disclosure of information on ESG risks is critical to promote market discipline, allowing stakeholders to assess banks' ESG related risks and sustainable finance strategy. The objective of the ITS is to harmonize the ESG reporting practices by putting forward comparable disclosures templates, standardized definitions and KPIs (incl. "green asset ratio"), as a tool to evaluate the actions taken by banks to integrate sustainability in their activities.
Audience	Large institutions with traded securities in EU official market

Overview of Main Principles

Under the (draft) ITS, institutions would need to disclosure both qualitative and quantitative information about their ESG risks.

Qualitative information

- Description on how banks incorporate ESG in their governance structure, business model/ strategy and risk management framework
- Quantitative data submitted must be accompanied with information on the source of data, proxies used and measures taken to address data gaps / improve data quality and accuracy.

Quantitative information

- Standardized templates in which banks have to disclose their exposures to transition and physical risks, as well as mitigating actions taken
- Specific template in which banks have to disclose their Green Asset Ratio(s).
- The templates cover a large spectrum of banking activities (banking and trading book, collateral held, alignment metrics)

The standard must be read in conjunction with other work conducted in the field of ESG reporting (e.g. EU Taxonomy regulation used to calculate the green asset ratio).

ESG disclosures (2/2)

ITS on Pillar 3 disclosures on ESG (Environmental, Social and Governance) risk EBA/CP/2021/06

Publisher	European Banking Authority (under the CRR Article 434a mandate)
Key dates	Applicable as from June 2022 - EBA will follow a sequential approach (proportionality used considering current data gaps and need to develop methodologies)
Purpose	Disclosure of information on ESG risks is critical to promote market discipline, allowing stakeholders to assess banks' ESG related risks and sustainable finance strategy. The objective of the ITS is to harmonize the ESG reporting practices by putting forward comparable disclosures templates, standardized definitions and KPIs (incl. "green asset ratio"), as a tool to evaluate the actions taken by banks to integrate sustainability in their activities.
Audience	Large institutions with traded securities in EU official market

Overview of Main Principles

Under the (draft) ITS, institutions would need to disclosure both qualitative and quantitative information about their ESG risks with some principles:

Data availability

Given the challenges in terms of availability of data for institutions to make the disclosures proposed in these templates, the EBA is proposing a phased-in approach, with a transitional period, for those disclosures for which they need data from their counterparties (e.g. proxies of missing data).

Data documentation

Institutions shall complement quantitative data with their metadata information as providing explanations of the data sources used and of the methodology in the templates.

Data quality

The disclosures also mention the measures taken by the institutions in order to close data gaps and to improve data quality and accuracy.

Contact

Koen De Loose
Partner, Head of Risk & Regulatory
KPMG in Belgium

E: kdeloose@kpmg.com

Nicolas Dubois
Director KPMG Lighthouse
KPMG in Belgium

E: ndubois@kpmg.com

home.kpmg/be