Guidance Solvency II data quality management by insurers

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.

Guidance Solvency II data quality management by insurers

Guidance document of De Nederlandsche Bank N.V., dated 1 September 2017, with guidelines for Solvency II data quality management by insurers.

Related legislation and regulations

This guidance document relates to the following legislation and regulations:

- Solvency II Directive (2009/138/EC): Sections 42, 46, 82, 86f and 121
- Solvency II Commission Delegated Regulation: Sections 19, 219 and 265
- Financial Supervision Act (*Wet op het financieel toezicht – Wft*): Section 3.17
- Guidelines on the valuation of technical provisions: EIOPA-BoS-14/166

Contents

Introduction

We developed this guidance document in the context of our thematic examination into data quality management with respect to Solvency II reporting. Structural attention from the Management Board is essential to embed data quality and data governance into the organisation. Data and information are the key elements required for assessing insurable risks and translating these into fitting premiums with the help of modelling.

Data quality is determined by the demonstrable degree of accuracy, appropriateness and completeness of the data, and compliance with internal and external quality standards. Good data management not only ensures and improves the quality of data used for prudential accountability to the supervisory authority, but also improves the quality of management and governance information, control function reporting, financial reporting to stakeholders and information provision to policy holders.

This guidance document provides more clarity on the key elements and principles needed to ensure quality data in the context of Solvency II. The thematic examination outlined general shortcomings with respect to data quality management. This document will explain our expectations in this regard in more detail. We have also described the good practices we encountered in the course of our examination. The guidance document will help you achieve the required level of data quality management and implement adequate safeguards throughout the chain, from initial recording of data at the source to final reporting.

Are you looking for guidance on how to set up a data quality policy? Please see Part 1. Do you need information about data identification and risk assessment? Please refer to Part 2. Our expectations with respect to the control framework are described in Part 3, and you can find the principles for assessing data quality management in Part 4. The final Part (5) deals with our expectations regarding your IT landscape.

Principles

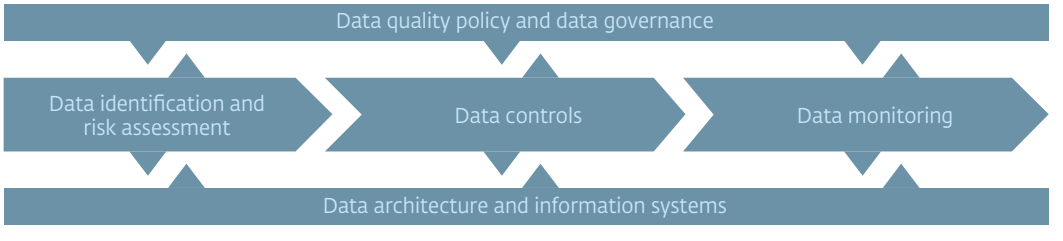
Pursuant to Section 3.17 of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), insurers must have sound and ethical operational management. This includes adequate management of operational processes and risks. In other words, we expect you to have processes in place to effectively identify, analyse, monitor and mitigate risks, and to effectively report on these risks. The same processes can also be applied to your data quality management. This document encompasses the principles on which our approach for examinations into data quality management is based.

The elements of the data quality management framework in the figure below may help you give structure to sound operational data quality management and be in control. A way to achieve this is by defining various aspects of data quality management within your organisation, such as data governance, data quality, data management and data architecture.

Continuous interaction between the framework elements will safeguard data quality and ensure structural improvements. Where possible, you can use existing (data) quality management standards, for example DAMA DMBOK[1], CMMI DMM[2], ISO8000[3].

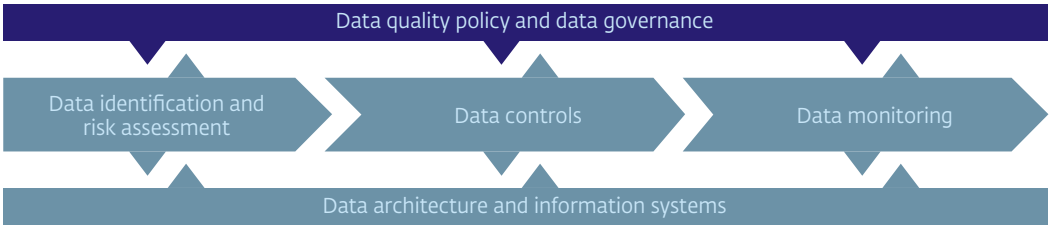
Responsibility for the quality (and data quality) of Solvency II reporting usually rests with the CFO, CFRO or a comparable function. However, the responsibility for data quality should lie with the organisation as a whole, given the fact that data initiation and processing usually take place in various units throughout the organisation, such as insurance policy administration systems. We based our thematic examination on the following general principles:

- Data quality is a regular item on the Management Board's agenda.
- Data quality receives ongoing priority attention within the organisation.
- Data quality management is a structural component of operational management.
- Data quality management is applied to the processes related to Solvency II reporting and also to the insurer's operational processes in general.



1 http://ww.dama.org - DAMA International Guide to Data Management Body of Knowledge (DAMA DMBOK®)
2 http://cmmiinstitute.com - Data Management Maturity Model V1.0
3 https://www.iso.org - ISO 8000-8:2015: Data quality - Part 8: Information and data quality: Concepts and measuring

1 Data quality policy and data governance



As an insurer, the law requires you to apply a policy-based approach in carrying out your core activities. This means you must have a risk management policy in place, laid down in a policy document with adequate safeguards to ensure sound and ethical operational management. The policy must be based on the mission, vision and strategy of your organisation and set out your organisation's framework conditions for managing data quality.

Data quality policy elements

We expect your data quality policy to include the following elements:

a. Your organisation's data quality objectives.
b. A detailed description of the scope of your organisation's data quality policy.
c. Definitions of data quality: interpretation of the Solvency II data quality requirements relating to accuracy, appropriateness and completeness.
d. Your organisation's risk appetite and related risk standards.
e. Your organisation's data quality management cycle: identification, assessment, control, monitoring and reporting.
f. Your organisation's approach to ensuring compliance with data quality standards and the distribution of responsibilities between business units, other group companies and external data suppliers.
g. Your organisation's incident management processes and approach to data recovery activities.
h. Your organisation's policies that govern or support the data quality policy, such as an outsourcing policy.

Proportionality

Achieving full compliance with the data quality requirements has proved to be a challenge for insurers. However, we expect insurers to make every effort to achieve this with respect to critical[4] data elements, including primary as well as derived data.

4 See Part 2, Scope and granularity section

If data is excluded based on your organisation's size, nature and complexity of risks and activities, you must be able to provide an adequate and transparent estimate of the impact of the excluded data on your financial reporting. You must also be able to provide documentary evidence substantiating your well-considered risk assessment and decision-making.

Data Governance

The quality of your data governance framework determines the quality of implementation of the data quality policy and ongoing data quality improvement. A clear distribution of tasks and duties is crucial, as is an adequate mandate and explicit anchoring of responsibility and commitment at management board level. These aspects must also be addressed throughout the data processing chain.
Data governance is made explicit by clearly formulated processes and procedures, including roles and responsibilities, giving all data quality management roles their place within the framework as a whole. Data governance has its own planning and control cycle, with adequate reporting lines.
Responsibilities and mandates are role-dependent, e.g. data owner, data user, data manager and data developer. The framework provides for consultative structures up to board level, where the various data roles (first line), compliance, risk management (second line) and the internal audit department (third line) meet.

We expect your data governance framework to address the following aspects:

a. Embedding of the data quality management function in your organisation, specifying the relevant procedures, roles and instruments.
b. Roles and responsibilities of the data owner with respect to data quality.
c. Roles and responsibilities of the roles responsible for executing the data quality policy, for example in the form of a RACI matrix.
d. Embedding of data governance in operational practice, addressing data (quality) incidents and data quality management information, in the presence of at least the data owner and the risk manager.
e. Periodical assessment and review of the data governance framework's effectiveness.

Documenting policy

You are responsible for documenting policy information in the manner that best fits your organisation. Some insurers choose to draw up a separate data quality policy document. Others choose to link their data quality policy to other policy documents and monitor uniform implementation and execution throughout their organisation.

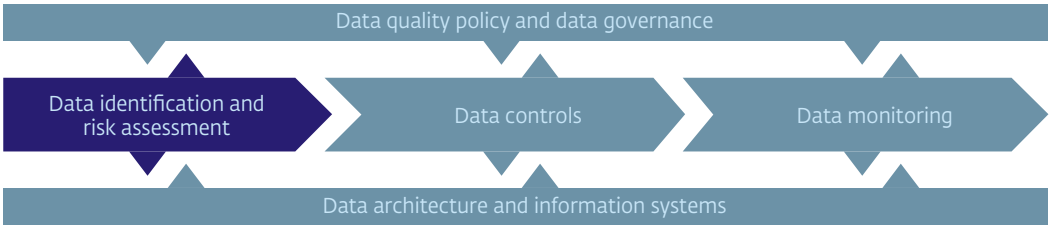
Implementing policy in operational and administrative procedures

You should work out the data quality policy in operational and administrative procedures. This includes internal procedures as well as procedures for external data-providing parties, e.g. your asset manager or authorised agent. You should ensure that the expectations you issue to internal or external data suppliers are in line with your data quality policy, to prevent unintentional or unexpected risks arising from the execution of such expectations by the data supplier. In other words, the principles underlying your data quality policy must be reflected in the conditions of the data delivery agreement. You must also have measures in place for both the supplying and receiving party to assess whether the data delivered is of adequate quality.

We have observed the following good practices with respect to drawing up and implementing data quality policy and data governance structures:

- Data quality management is an integrated part of operational management and is embedded as a formal function within the organisation.
- Existing data quality management standards are used as a basis for structuring the data quality policy. Examples (non-exhaustive) include DAMA DM BOK, CMMI DMM and ISO8000.
- Data governance is embedded in the organisation and is addressed at all hierarchical levels of the organisation. The roles and responsibilities of all parties involved in data management are clearly and uniformly described.
- There is a data governance board at management board level, safeguarding the connections between the various domains within the organisational chain and the effective execution of data management function activities.
- For each data domain a data steward has been appointed who takes on a coordinating role, is responsible for risk analyses and recommendations for improvement and assists in defining data and KPIs. The data steward is also actively involved in improving data quality awareness within the organisation.
- With each external data supplier a data delivery agreement is in place as part of the service delivery agreement, specifying at data element level which data is to be received, how compliance with data quality requirements is ensured and which steps the delivering and recipient party should take in the event that the quality requirements cannot be met.
- There is explicit attention to data or data quality incidents, which is reflected in the data governance structure.
- The specific characteristics of all relevant data elements, such as primary data in source systems, data cleansing applied and migration results, are recorded at the central level.

2 Data Identification and Risk assessment



In the context of Solvency II reporting, data is made accessible, transformed and enriched to create useful data sets for management and actuarial purposes and the quantitative reporting templates (QRTs). Data quality objectives can only be achieved if insurers translate their data quality management into a clear approach for the entire chain, from source system to QRTs, and are prepared to implement it. This includes identification and risk assessment of the data required under Solvency II and a thorough understanding of the data flows and data processes through the entire chain.

Data identification and risk assessment

Your data identification and risk assessment (and any derived model points) should include at least the following aspects:

a. Define and identify the data elements required under Solvency II, i.e. the data required for the QRTs.
b. Provide insight into how data flows through the entire chain at data element/data set level.
c. Create process flows that make clear at the data element/data set level how the data flows through the chain and what process steps this involves, including the relevant supporting systems and interfaces.
d. Compile a data directory showing at the data element/data set level for which purposes (QRT) the data is used, the data source and the data characteristics.
e. Carry out a risk analysis resulting in the definition of key risks that have an impact on data quality.
f. Define Key Risk Indicators (KRIs) and Key Performance Indicators (KPIs) linked to the data quality objectives.

Scope en granularity

Data quality management applies to all data steps throughout the entire chain, from policy administration systems to reporting. External parties such as asset managers or authorised agents also qualify as data sources. We expect you to have adequate management measures in place to safeguard data quality.

The QRTs comprise a large number of data elements, and we expect you to take appropriate measures to ensure compliance with the relevant data quality standards for all of these elements.

If your organisation chooses to safeguard data quality by focusing on critical data elements (CDEs), we expect you to apply a selection process based on an appropriate risk analysis and to clearly describe which data elements are considered critical, and why. The risk management function is responsible for assessing both the selection process and the final set of CDEs.

Missing data and data restrictions

The risk assessment may reveal that required data is missing, for example as a result of structural data loss in transfers between systems, or because of a lack of (sufficient) historical data. We expect you to estimate the impact on your Solvency II reporting of any data that appears to be missing based on your risk analysis. We also expect you to have a consideration and decision-making process in place for addressing the risks related to missing data. You must document your decisions, substantiating your reasons, and you must be able to demonstrate that the measures proposed (or the decision not to take any measures) match your organisation's risk appetite.

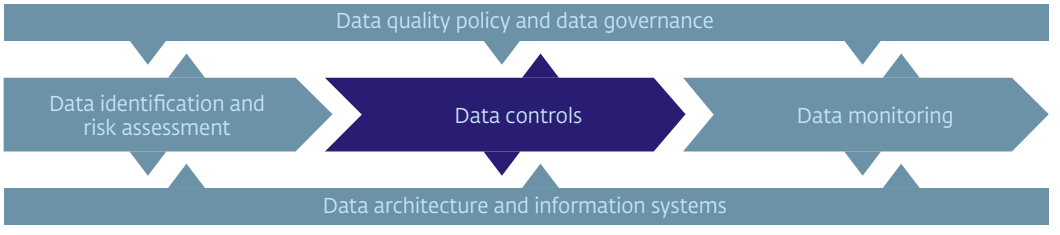
Data identification and risk assessment

You are responsible for recording data flows, process flows and the data directory in the format and level of detail that best fits your organisation. We expect you to describe the data and process flows of the entire reporting chain. A well-defined approach for the execution of data identification and risk assessment will benefit your organisation and contribute to controlled execution.

We have observed the following good practices with respect to data identification and risk assessment:

- Data flows are structured as process flows at different levels, each with an increasing level of detail. This approach fits in with the different information needs of the various stakeholders, such as users and developers.
- Assumptions and derivations of data are specified as such in the data and process flows.
- Business flows combining several elements such as systems, processes, data users, data owners and key controls.
- A data directory in which the data business definition, data characteristics, source and target data files, data owner and reference to the relevant QRT are recorded.
- A control process for the data directory, the data flows and supportive documentation has been defined, creating an audit trail and enabling the organisation to reconstruct data processes.
- Key controls for critical processing points have been defined, based on the data flows.
- Some insurers have anchored this in the form of data flow management, which ensures that all relevant data elements are identified. This is done in cooperation with the data's primary users, e.g. the actuary and the individual(s) responsible for the QRTs.

3 Data controls



Based on the risk assessment and the established KRIs and KPIs, appropriate controls must be in place to manage and mitigate the identified risks.

Automated and manual controls

We expect your controls to address the following aspects:

a. The control objectives linked to the data quality standards.
b. The method (automated or manual) and frequency of execution of the controls.
c. The type of controls, e.g. reconciliation controls, input controls, (EIOPA[5]) validation controls, plausibility controls, interface controls.
d. Identification of key controls throughout the chain to safeguard quality (based on a comprehensive risk analysis).
e. Safeguarding of audit trails and logging of the entire chain, from source system to QRT.
f. Structural data analysis of the entire reporting chain based on predefined business rules, such as business logic.

End user computing

We expect insurers who use end user computing (EUC), to describe up to the critical data element level how data is processed and whether adequate control measures are in place. We also expect insurers to have control measures in place to manage EUCs, such as access management, change management and version management.

Expert judgements

Expert judgements can be used as a subjective component in the data quality assessment control framework. We expect you to clearly explain and document the assumptions underlying the expert judgements and that risk management is taken into account. We also expect you to make the use of expert judgements explicit in your data and process flows and ensure that they are periodically included in internal audit assessments.

5 https://eiopa.europa.eu/regulation-supervision/insurance/reporting-format: Solvency II Taxonomy.

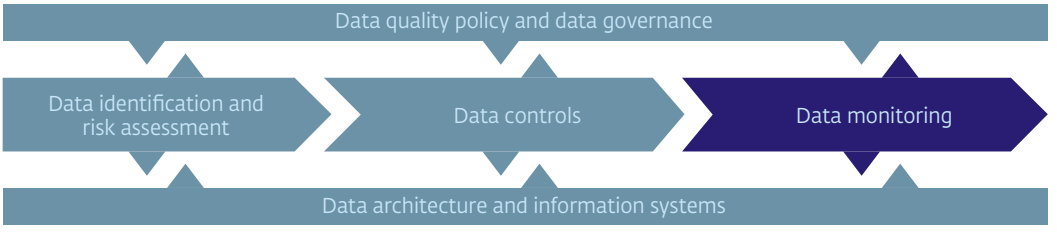
Data incidents

Data incidents may occur if a control measure is ineffective, or if information is unavailable or not properly documented. This may impact the reliability of your Solvency II reports. We therefore expect you to have a data incident process in place to resolve any data incidents in a structural manner and prevent them from occurring again. We also expect you to have an escalation procedure to address any issues at the appropriate management level. Last but not least, you should have a detailed strategy for ontrolled execution of recovery activities.

We have observed the following good practices with respect to effective data quality control measures:

- Minimise the use of EUCs.
- The use of expert judgements is laid down in a policy document, specifying when expert judgements are used, how the impact on the data is made clear and how the substantiation of expert judgements is recorded.
- The use and approval of expert judgements is validated at management level.
- Control measures to safeguard data quality are part of the internal control framework, and the responsible first-line representative must sign off the control measures.

4 Data monitoring



You must monitor your data quality to assess whether your organisation complies with the relevant data quality standards. Monitoring provides your organisation with the necessary management information to improve specific business processes or to make adjustments to the data quality policy and/or the data governance framework. Such actions are essential for ensuring structural improvement of data quality.

We expect your data quality management information to address the following aspects:

a. Reports of continuous monitoring of the entire reporting chain based on predefined business rules such as business logic, e.g. on the basis of data analysis or continuous process monitoring.
b. Dashboards with current information on KRIs and KPIs, providing insight into the effective functioning of control measures and key controls.
c. Data quality reports from data suppliers, including service level management reports. These must include explicit accountability on the control and quality of the data delivered.
d. Periodical reports on data quality, including data incidents.

Actuarial function

The actuarial function is a second-line function which plays an important role in the assessment of technical provision calculations. It is responsible for assessing the completeness and quality of the data used in these calculations. We expect the actuarial function to have a policy as well as a working programme in place on which to base their assessments.
We expect the assessments to include the following elements:

a. The relevant data and possibly modelling points.
b. The homogeneous risk groups identified.
c. The risks and control measures in place.
d. Monitoring of compliance with control measures.
e. Data-oriented checks.

We also expect any shortcomings or deficiencies to be evaluated with respect to the effectiveness of technical provisions and to be reported in the actuarial function report (AFR).

Please consult our Open Book on Supervision website for more detailed information about our expectations regarding the actuarial function (in Dutch only).[6]

Internal audit

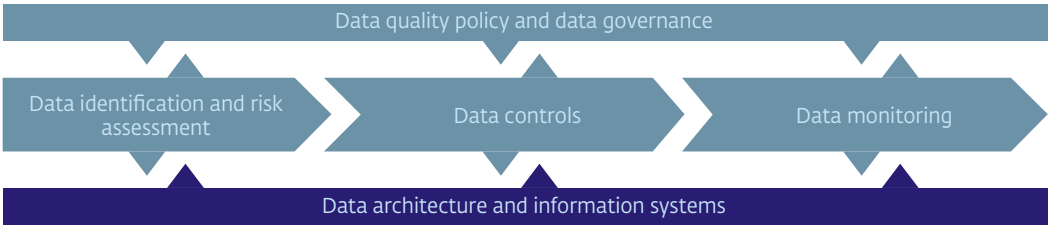
Internal audit is responsible for periodically assessing the effectiveness of policy and control measures with the aim of ensuring sound operational management. This also applies to the management of your data quality. We expect your internal audit department to periodically assess the design, existence and operating effectiveness of your data quality policy and control measures. The results form the basis for your evaluation of the data quality management framework.

We have observed the following good practices with respect to effective data quality control measures:

- Systematic recording of monitoring activities.
- Periodical comprehensive cross-data domain reports and dashboards.
- Periodical correctness checks
- Data quality is validated and improved at the source where possible. Quality indicators are translated into business rules integrated into the data flows at different levels within the organisation.
- Data quality is monitored continuously, preferably at the source systems.
- Data quality requirements and indicators are assessed and adjusted periodically.
- Data and data quality incidents are dealt with via a structured and standardised route, preferably by/at the source.
- Data stewards define the quality requirements for relevant data in consultation with data users. Data stewards continuously monitor the quality of relevant data based on quality indicators, and initiate follow-up actions for the various stakeholders in the event of deviations.

6 https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-verzekeren/nieuwsbrief-verzekeren-januari-2017/dnb351773.jsp

5 Data Architecture and Information Systems



A mature data quality management environment provides insight into all relevant data management aspects and allows the organisation to be in control. In practice, this often translates into a data architecture function. We consider the data architecture function as an important basis for the implementation of a data quality management system.
The data architecture function supports the organisation in determining the current and desired situation of data organisation as well as platform aspects such as data warehouses, data models, ETL processes, data dictionaries and metadata repositories.

With respect to managing your IT landscape relevant for the Solvency II reporting chain we expect you to address the following subjects:

a. An overview of the applications and related infrastructural IT components that are in scope for Solvency II, including their risk classification.
b. An overview of any outsourced IT services, applications and related infrastructural IT components that are in scope for Solvency II.
c. Insight into the controls for IT processes: access management, continuity management, change management and version management for the applications and related infrastructural IT components that are in scope for Solvency II.

Information systems

Control of your IT landscape and the identified general IT controls is an important condition for managing your data quality. We expect you to be able to provide insight into the actual design of the IT landscape, which includes the entire reporting chain from source system to QRTs as well as the outsourced IT landscape in case this supports the Solvency II chain. This involves applications, infrastructure, operating systems and databases.

Effectiveness of general IT controls

We expect you to periodically assess the design, existence and operating effectiveness of general IT controls at the level of applications, infrastructure, operating systems and databases. You should make clear whether the Solvency II reporting chain is fully or partially in scope of the general IT controls. We expect you to take appropriate additional control measures for any parts outside the scope.

18 We also expect the reporting chain, including information systems, infrastructure, operating systems, databases and EUCs, to comply with the relevant data security requirements. You can consult these on our Open Book on Supervision website[7].

7 http://www.toezicht.dnb.nl/3/50-203304.jsp

Disclaimer
This guidance document provides non-binding recommendations for the application of Solvency II rules and regulations regarding data quality requirements by insurers.

It sets out our expectations regarding observed or envisaged behaviour in policy practice that reflects an appropriate application of the rules and regulations to which this guidance pertains.

We encourage insurers to take our expectations into account in their considerations and decision-making, without them being obliged to do so. The guidance document is only indicative in nature and therefore does not exclude that some insurers may be subject to different, possibly stricter application of the underlying regulations. It is the insurer's responsibility to take this into account.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
P.O. Box 98, 1000 AB Amsterdam
The Netherlands
+31(0)20 524 91 11
dnb.nl