Good Practice

Outsourcing Insurers

DeNederlandscheBank

EUROSYSTEEM

This brochure is published by De Nederlandsche Bank.
Pension Supervision and Insurance Supervision Divisions,
Expert Centre on Operational & IT Risks

Westeinde 1
1017 ZN Amsterdam, Telephone: +31 20 524 9111
Website: https://www.toezicht.dnb.nl/en/2/51-237170.jsp
Email: info@dnb.nl

Contents

Introduction

Many insurers are outsourcing IT, asset management, pensions and policy administration, accounting systems and other critical operational processes to external service providers. This allows them to benefit from these providers' expertise and size, and consequently reduce costs or focus more on their core competencies. At the same time, outsourcing activities and functions exposes insurers to risks. For example, an insurer's operations may be jeopardised by breaches of contract or financial problems on the part of the service provider, improper handling of confidential data or if the quality agreed does not match the quality delivered. This Good Practices document will help insurers to manage these and other risks related to outsourcing.

Relevant laws and regulations

The Good Practices document offers guidance on the following laws and regulations that are relevant for insurers when outsourcing activities:

- Financial Supervision Act (*Wet op het financieel toezicht – Wft*)
  - Section 1:1 - Definitions
  - Section 3:17 - Sound and ethical business operations
  - Section 3:18 - Outsourcing
- Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*)
  - Sections 27-32 - Outsourcing
- Solvency II Directive (2009/138/EC)
  - Article 13.28 - Definition of outsourcing
  - Article 38 - Supervision of outsourced functions and activities
  - Article 41 - General governance requirements
  - Article 49 - Outsourcing
- Solvency II Regulation (2015/35/EU)
  - Article 258 - General governance requirements
  - Article 274 - Outsourcing
- EIOPA Guidelines on the system of governance
  - Guidelines 60-64 in Section 11 on outsourcing (not applicable to Basic insurers)

Definities

Section 1(1) of the *Wft* defines outsourcing as a financial enterprise commissioning a third party to carry out on its behalf:

- activities that are part of or ensue from its operations as a financial enterprise or the provision of financial services; or
- activities that are part of the critical processes supporting its operations as a financial enterprise or the provision of financial services.

Article 13(28) of the Solvency II Directive (2009/138/EC) defines outsourcing as an arrangement of any form between an insurer or reinsurer and a service provider, whether a supervised entity or not, by which that service provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurer or reinsurer itself.

Stages in the outsourcing process

The Good Practices document describes the following five stages in the outsourcing process:

1. **Designing the outsourcing policy:** defining the considerations underlying the decision to outsource and the preconditions that apply. The outsourcing policy sets out how the insurer organises the outsourcing of activities and how it manages the associated outsourcing risks.

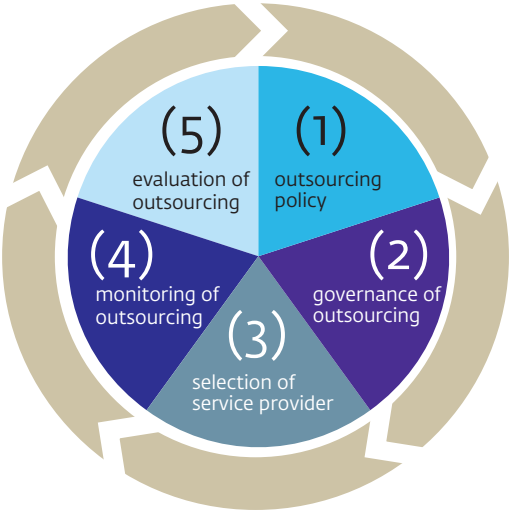
2. **Organising governance and drafting the outsourcing agreement:** the outsourcing policy provides direction and functions as a framework for drafting the outsourcing agreement. The resulting outsourcing agreement meets all statutory requirements as well as the insurer's own requirements and preferences.

3. **Selecting the service provider:** the service provider selection process.

4. **Monitoring the outsourced activities:** the insurer monitors whether the service provider complies with the outsourcing agreement provisions and meets the performance and results targets.

5. **Evaluation of outsourcing:** the insurer regularly evaluates the performance of its service providers as well as its own policy and processes in all stages of the outsourcing process; if necessary, the insurer takes appropriate measures, replaces poorly performing service providers or adjusts its outsourcing policy.

Figure 1 Five stages of outsourcing



Sound and ethical operational management comprises the entire process of planning, directing, monitoring and steering of objectives, processes and risks. This Plan, Do, Check, Act cycle can also be applied to the outsourcing process, translated into five stages.

The following five sections reflect the five stages in the outsourcing process and describe the good practices we found for each stage. Each section begins with a brief introduction of the relevant laws and regulations and then describes the good practices. Please note that while we do not provide good practices for all laws and regulations, insurers must still ensure that they are able to comply with all statutory requirements. The relevant laws and regulations are described in boxes.

Scope

This document refers to the outsourcing of critical or important activities, i.e. activities that are of material or fundamental importance for an insurer's operations. Impact is the defining factor, and this depends on an insurer's particular characteristics and circumstances.
Not all examples in this document can be applied to all insurers. They must make their own assessment of which measures are appropriate to manage or mitigate specific risks. Basic insurers, for example, may in some cases have to take less far-reaching measures compared to large insurers, since the EIOPA Guidelines on the system of governance do not apply to them. The diversity in types of business units within groups of insurers also results in differences in the types of activities and strategies deployed. Insurers can therefore opt to include a proportionality assessment in their risk analyses.

Insurers can use this Good Practices document as a guidance when outsourcing their critical or important functions, but it does not offer specific guidance on the management of these functions. Critical or important functions are fundamental to an insurer's ability to carry out its core activities, and the impact of outsourcing defines whether a function is to be regarded as critical or important. The functions mentioned in Articles 41, 44, 46 and 47 of the Solvency II Directive are in any case to be regarded as critical and are usually referred to as key functions: the risk management function, the compliance function, the internal audit function and the actuarial function.

EIOPA Guideline 60 – Critical or important operational functions and activities

1.113. The undertaking should determine and document whether the outsourced function or activity is a critical or important function or activity on the basis of whether this function or activity is essential to the operation of the undertaking as it would be unable to deliver its services to policyholders without the function or activity.

Insurers can use DNB's Information Security assessment framework, which includes a specific set of controls to manage outsourcing, to manage their outsourcing of IT and data. Examples of such controls include Manage third party and supplier services: monitoring and reporting of service level reports (14.1) and supplier risk management (14.2) and Internal control at third parties (16.3). Please refer to our Open Book on Supervision pages for more information: https://www.toezicht.dnb.nl/en/3/51-203304.jsp

This Good Practices document focusses on the elaboration of prudential regulations, which means Section 4(16) of the *Wft* (conduct supervision) falls outside its scope. Insurers can use this document in their capacity as an advisory or intermediary party.

Outsourcing also includes granting power of attorney to an intermediary (authorised agent). The insurer must ensure that the activities of such insurance intermediaries comply with the outsourcing requirements.

EIOPA Guideline 61 – Underwriting

1.114. When an insurance intermediary, who is not an employee of the undertaking, is given powers to underwrite business or settle claims in the name and for the account of an undertaking, the undertaking should ensure that the activity of this intermediary is subject to the outsourcing requirements.

Intra-group outsourcing falls within the scope of this Good Practices document.

EIOPA Guideline 62 – Intra-group outsourcing

1.115. If critical or important functions or activities are outsourced within the group, the participating insurance or reinsurance undertaking, the insurance holding company or the mixed financial holding company should document which functions relate to which legal entity and ensure that the performance of the critical or important functions or activities concerned at the level of the undertaking is not impaired by such arrangements. and ensure that the performance of the critical or important functions or activities concerned at the level of the undertaking is not impaired by such arrangements.

1 Outsourcing policy

An insurer first drafts an outsourcing policy before outsourcing any activities. The policy document sets out the considerations underlying the decision to outsource and the preconditions that apply. As a basic principle, the insurer is and remains responsible for the outsourcing of activities.

Solvency II Directive 2009/138/EC – Article 49 - Outsourcing

1. Member States shall ensure that insurance and reinsurance undertakings remain fully responsible for discharging all of their obligations under this Directive when they outsource functions or any insurance or reinsurance activities.
2. Outsourcing of critical or important operational functions or activities shall not be undertaken in such a way as to lead to any of the following:
   a. materially impairing the quality of the system of governance of the undertaking concerned
   b. unduly increasing the operational risk
   c. impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations
   d. undermining continuous and satisfactory service to policy holders.
3. Insurance and reinsurance undertakings shall, in a timely manner, notify the supervisory authorities prior to the outsourcing of critical or important functions or activities as well as of any subsequent material developments with respect to those functions or activities.

1.1 Policy process

An insurer establishes an outsourcing policy in writing, taking into account the impact of outsourcing on its operational management and applying the principle of proportionality. The outsourcing policy addresses all stages of the outsourcing process and describes how the outsourcing of activities ties in with the insurer's operational strategy, the associated risks and how they are managed. Prior to outsourcing activities, an insurer first carries out a systematic risk analysis, which may also include a proportionality assessment.

Legislative framework

Article 247(1) of the Solvency II Regulation provides that an insurer must establish a written outsourcing policy, which takes into account the reporting and monitoring arrangements to be implemented in cases of outsourcing. The insurer describes the approach and processes applying to outsourcing, with a particular focus on the aspects referred to in EIOPA Guideline 63: a materiality assessment, the service provider process and monitoring/evaluation of performance, contractual requirements and the insurer's business continuity process.

EIOPA Guideline 63 – Outsourcing written policy

1.116. The undertaking that outsources or considers outsourcing should cover in its policy the undertaking's approach and processes for outsourcing from the inception to the end of the contract. This in particular should include:

a. the process for determining whether a function or activity is critical or important
b. how a service provider of suitable quality is selected and how, and how often its performance and results are assessed
c. the details to be included in the written agreement with the service provider taking into consideration the requirements laid down in Commission Delegated Regulation 2015/35
d. business contingency plans, including exit strategies for outsourced critical or important functions or activities

Good practices

An insurer starts by carrying out a systematic risk analysis and defining the purpose and scope of outsourcing, describing which activities can be outsourced, which activities must not be outsourced, as well as the reasons why. The insurer establishes the objectives and considerations underlying the decision to outsource and the preconditions that apply. Where possible, the insurer also describes the considerations for terminating the outsourcing of activities.

An insurer updates its risk analysis on an annual basis, or more frequently if prompted to do so by incidents.

An insurer lays down its outsourcing strategy for the next five years in a strategy document, which demonstrates that strategic considerations underly the decision to outsource activities.

The insurer defines an outsourcing strategy aimed at achieving its objectives, taking into account the associated outsourcing risks as well as the measures to manage these on an ongoing basis.

The strategy document has been formally approved, signed and dated by the organisation's policymakers. The opinion of the second-line risk management function is an integrated part of decision-making about strategy. The strategy document has been shared with the employees within the organisation.

The outsourcing policy covers all aspects of outsourcing, and the insurer involves all relevant departments such as Risk Management, Legal Services, Compliance, all relevant business units and, if applicable, the IT and Operations departments.

The outsourcing policy describes the service provider selection process, the selection criteria applied and the decision-making moments. It also describes the service provider evaluation process, and the minimum requirements to be included in the outsourcing agreement.

An insurer lays down in its policy that it performs a materiality assessment to assess whether the activities to be outsourced must be regarded as important or critical, i.e. activities that are of material or fundamental importance for an insurer's operations. Impact is the defining factor, and this

depends on an insurer's particular characteristics and circumstances. An insurer uses the following criteria to assess the materiality of outsourcing:

- The critical nature and inherent risk profile of the activity the insurer wishes to outsource. The insurer must consider whether the activity is vital to its operational management, business continuity or viability and to its obligations towards its customers or policyholders. This means that the insurer would be unable to provide its services (or vital parts of it) without this activity.
- The immediate operational consequences that interruptions of the activity may have, and the associated legal and reputation risks.
- The impact that a disruption in the activity may have on the insurer's anticipated revenues.
- The impact that a breach of confidentiality or integrity, or unavailability of data may have on the insurer or its customers, members or policyholders.

An insurer that outsources specific activities or functions with a high impact on a part of its policy holders classifies this activity or function as critical, since it would be unable to provide its services to part of its policy holders without this function or activity. The prudential impact determines whether the outsourced activity qualifies as critical.

An insurer's management board approves the policy and its supervisory board or other supervisory body assesses the policy.

An insurer lays down in its policy that it includes the classification and security and continuity of its systems and data in its assessment of the risks.

The insurer uses outsourcing guidelines and procedures (business units, IT, authorised agents) that are in accordance with its general outsourcing policy. The insurer informs its staff of its outsourcing policy.

An insurer's outsourcing policy ensures that activities can only be outsourced to a service provider if that service provider's policy with respect to information security and business continuity management (BCM) equals or exceeds the standards of the insurer's own internal policy with respect to these areas, or if there are alternative measures to safeguard the desired results and there are no unacceptable risks.

1.2 Business continuity management (BCM)

An insurer designs its business continuity management based on its established BCM policy and strategy. While service providers will make every effort to ensure the continuity of their service provision, there is always a chance of things going wrong. An insurer drafts a business continuity plan, including all outsourced activities, in order to be prepared for such situations. Service providers also have their own business continuity plans.

Legislative framework

Solvency II Directive 2009/138/EC – Article 41(4) - General governance requirements

Insurance and reinsurance undertakings must take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, the undertaking must employ appropriate and proportionate systems, resources and procedures.

Solvency II Regulation (EU) 2015/35 – Article 274.5

The insurance or reinsurance undertaking that is outsourcing critical or important operational functions or activities shall fulfil all of the following requirements:

a. ensure that relevant aspects of the service provider's risk management and internal control systems are adequate to ensure compliance with Article 49(2)(a) and (b) of Directive 2009/138/EC
b. adequately take account of the outsourced activities in its risk management and internal control systems to ensure compliance with Article 49(2)(a) and (b) of Directive 2009/138/EC
c. verify that the service provider has the necessary financial resources to perform the additional tasks in a proper and reliable way, and that all staff of the service provider who will be involved in providing the outsourced functions or activities are sufficiently qualified and reliable
d. ensure that the service provider has adequate contingency plans in place to deal with emergency situations or business disruptions and periodically tests backup facilities where necessary, taking into account the outsourced functions and activities

EIOPA Guideline 63 – Outsourcing written policy

1.116. The undertaking that outsources or considers outsourcing should cover in its policy the undertaking's approach and processes for outsourcing from the inception to the end of the contract. This in particular should include:

Business contingency plans, including exit strategies for outsourced critical or important functions or activities

Good practices

An insurer defines and takes decisions on continuity measures. Outsourced material activities are part of these continuity measures. This means both the service provider and the insurer take continuity measures that are commensurate with the risk profile of their data and systems – and which include back-up facilities at different locations, with an appropriate distance between them.

An insurer drafts a business continuity plan (BCP) which addresses the outsourced activities, the consequences of disruptions at the own organisation or that of the service provider and the measures in place to minimise the impact of such disruptions.

In consultation with its service providers, an insurer periodically assesses whether the continuity plans and continuity measures in the outsourcing chain are still in line with one another. The insurer analyses any deviations from the requirements and takes appropriate adjustment measures. If necessary, the insurer adjusts its continuity plan, thereby mitigating the risk that the entire outsourcing chain fails if there is a disruption in one of its links.

An insurer tests its BCM measures on a regular basis, preferably in close cooperation with the relevant service providers to which the activities have been outsourced. The insurer also takes the results of BCM tests performed by the service provider into account.

An insurer looks into alternative solutions for outsourced activities and develops and implements exit and transition plans based on its exit strategies. An insurer makes agreements with its service providers about what happens to its data after termination of the outsourcing agreement. The insurer also assigns tasks and responsibilities for the management of exit and transition plans and for the transitional activities to be implemented in the event of an exit, including the return and destruction of stored data (production and back-up) from the service provider.

An insurer performs scenario analyses including the outsourced services in order to gauge the impact of operational damage in various scenarios, such as natural disasters, DDoS attacks and cybercrime (malware, ransomware, etc.)

An insurer has a transparent and verifiable exit policy in place to terminate an outsourcing agreement with a non-performing service provider or to make the decision not to renew the agreement.

The insurer investigates which resources are needed to transfer the outsourced activities to another service provider or to perform them itself again (implementation of the exit plan). An insurer ensures it has sufficient in-house knowledge to assess a service provider's performance, to control and adjust the outsourcing process and to take over and perform activities itself again if necessary.

An insurer drafts exit plans, possibly in collaboration with other customers of the same service provider, to prepare for a situation in which the service provider is unable to deliver, for example because of a bankruptcy.
The agreement must specify when and under what conditions the data is returned or made available to the insurer in the event of bankruptcy or takeover of the service provider. Alternative strategies must be recorded in an exit plan or exit procedure - or both. Examples include insourcing, escrow rights, takeover of shares, continuing on-site (subject to the liquidator's consent).

An insurer sets up a system for monitoring the operational effectiveness of the service provider's BCM and BCP measures. Monitoring also includes the timely collection of data that may indicate flaws in a service provider's performance or continuity.

2 Governance of outsourcing and outsourcing agreement

The outsourcing policy and the governance system in place provide a directional framework and translate into an outsourcing agreement complying with all statutory requirements, conditions and the insurer's own requirements and preferences. The duties and responsibilities of both the insurer and the service provider are described and recorded.

2.1 Compliance of outsourcing with statutory requirements

The outsourcing policy ensures compliance with all statutory requirements for all outsourced activities. It is a policy framework that sets the conditions and requirements for outsourcing and the limits that apply when entering into commitments. The management board ensures that the insurer complies with the applicable rules and regulations.

Legislative framework

Solvency II Regulation (EU) 2015/35 – Articles 274(1), 274(2) and 274(3)

1. Any insurance or reinsurance undertaking which outsources or proposes to outsource functions or insurance or reinsurance activities to a service provider shall establish a written outsourcing policy which takes into account the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented in cases of outsourcing. The undertaking shall ensure that the terms and conditions of the outsourcing agreement are consistent with the undertaking's obligations as provided for in Article 49 of Directive 2009/138/EC
2. Where the insurance or reinsurance undertaking and the service provider are members of the same group, the undertaking shall, when outsourcing critical or important operational functions or activities take into account the extent to which the undertaking controls the service provider or has the ability to influence its actions.
3. When choosing the service provider referred to in paragraph 1 for any critical or important operational functions or activities, the administrative, management or supervisory body shall ensure that:
   a. a detailed examination is performed to ensure that the potential service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily, taking into account the undertaking's objectives and needs
   b. the service provider has adopted all means to ensure that no explicit or potential conflict of interests jeopardize the fulfilment of the needs of the outsourcing undertaking
   c. a written agreement is entered into between the insurance or reinsurance undertaking and the service provider which clearly defines the respective rights and obligations of the undertaking and the service provider
   d. the general terms and conditions of the outsourcing agreement are clearly explained to the undertaking's administrative, management or supervisory body and authorised by them
   e. the outsourcing does not entail the breaching of any law, in particular with regard to rules on data protection
   f. the service provider is subject to the same provisions on the safety and confidentiality of information relating to the insurance or reinsurance undertaking or to its policyholders or beneficiaries that are applicable to the insurance or reinsurance undertaking.

Pursuant to Article 49(3) of the Solvency II Directive and Guideline 64 of the EIOPA Guidelines for the System of Governance an insurer must notify DNB in time of any critical or important outsourcing activities, in order to allow DNB to assess whether there are any prudential obstacles.

Solvency II Directive 2009/138/EC – Article 49 - Outsourcing

3. Insurance and reinsurance undertakings shall, in a timely manner, notify the supervisory authorities prior to the outsourcing of critical or important functions or activities as well as of any subsequent material developments with respect to those functions or activities.

EIOPA Guideline 64 – Written notification to the supervisory authority

In its written notification to the supervisory authority of any outsourcing of critical or important functions or activities the undertaking should include a description of the scope and the rationale for the outsourcing and the service provider's name.
When outsourcing concerns a key function, the information should also include the name of the person in charge of the outsourced function or activities at the service provider.

Good practices

In its outsourcing policy, an insurer records that it notifies DNB in writing of the outsourcing of material or critical activities and of important adjustments to outsourcing agreements, including subcontracting.

An insurer notifies DNB of the outsourcing of activities and submits a risk analysis prior the start of service provision, also if the services will be provided in stages or in project form. See also our Open Book on Supervision pages (https://www.toezicht.dnb.nl/en/2/5/51-230433.jsp).

An insurer clearly describes the duties, powers and responsibilities and ensures that it has sufficient expertise available within its organisation to prevent operational risk from increasing and to safeguard ongoing compliance with rules and regulations when engaging in outsourcing agreements, including subcontracting.

An insurer sets up a coordinating organisation for monitoring larger outsourcing operations and describes the required knowledge and expertise in order to check and balance the service provider and to take back control over the outsourced activity if necessary.
An insurer involves second-line risk management in defining and designing new control measures at the insurer and its service providers. The internal audit function is also consulted to assess the new situation: what else must be arranged, and are the necessary resources available? The insurer records these observations and uses them when selecting a suitable service provider and drafting the agreement, and in the translation to the service level agreement.

An insurer is able to guide the service provider and make additional or new agreements on the service provider's performance and results (Deming cycle: Plan > Do > Check > Act). The insurer has alternatives for outsourcing from the start of the services, e.g. migration to another service provider or taking back control.

The written agreement with the service provider includes clauses on security and data protection as well as a processing agreement. The insurer takes compliance with applicable laws and regulations into account, including the General Data Protection Regulation (GDPR).

2.2 Outsourcing agreement

An insurer's outsourcing policy also describes the terms and conditions governing the outsourcing agreement. When selecting a service provider, the insurer establishes which statutory requirements must be met and records these, for example in a model outsourcing agreement.

After – or if possible during – the process of selecting a service provider, the insurer concludes an agreement or draft agreement with the service provider to lay down the agreements about the activities to be outsourced. The agreement serves to ensure that the service provider performs the activities in accordance with agreements made.

Legislative framework

Article 274.3(c) the Solvency II Regulation stipulates that an insurer must record the outsourcing agreement in writing. Article 274(4) of the Solvency II Regulation prescribes the elements that must be included in the outsourcing agreement.

Solvency II Regulation (EU) 2015/35 – Article 274(4)

4. The written agreement referred to in paragraph 3c to be concluded between the insurance or reinsurance undertaking and the service provider shall in particular clearly state all of the following requirements:
   a. the duties and responsibilities of both parties involved
   b. the service provider's commitment to comply with all applicable laws, regulatory requirements and guidelines as well as policies approved by the insurance or reinsurance undertaking and to cooperate with the undertaking's supervisory authority with regard to the outsourced function or activity
   c. the service provider's obligation to disclose any development which may have a material impact on its ability to carry out the outsourced functions and activities effectively and in compliance with applicable laws and regulatory requirements
   d. a notice period for the termination of the contract by the service provider which is long enough to enable the insurance or reinsurance undertaking to find an alternative solution
   e. that the insurance or reinsurance undertaking is able to terminate the arrangement for outsourcing where necessary without detriment to the continuity and quality of its provision of services to policyholders
   f. that the insurance or reinsurance undertaking reserves the right to be informed about the outsourced functions and activities and their performance by the services provider as well as a right to issue general guidelines and individual instructions at the address of the service provider, as to what has to be taken into account when performing the outsourced functions or activities
   g. that the service provider shall protect any confidential information relating to the insurance or reinsurance undertaking and its policyholders, beneficiaries, employees, contracting parties and all other persons
   h. that the insurance or reinsurance undertaking, its external auditor and the supervisory authority have effective access to all information relating to the outsourced functions and activities including carrying out on-site inspections of the business premises of the service provider
   i. that, where appropriate and necessary for the purposes of supervision, the supervisory authority may address questions directly to the service provider to which the service provider shall reply
   j. that the insurance or reinsurance undertaking may obtain information about the outsourced activities and may issue instructions concerning the outsourced activities and functions
   k. the terms and conditions, where applicable, under which the service provider may sub-outsource any of the outsourced functions and activities
   l. that the service provider's duties and responsibilities deriving from its agreement with the insurance or reinsurance undertaking shall remain unaffected by any sub-outsourcing taking place according to point k)

Solvency II Directive 2009/138/EC – Article 38 – Supervision of outsourced functions and activities

Without prejudice to Article 49, Member States shall ensure that insurance and reinsurance undertakings which outsource a function of an insurance of reinsurance activity take the necessary steps to ensure that the following conditions are satisfied:

a. the service provider must cooperate with the supervisory authorities of the insurance and reinsurance undertaking in connection with the outsourced function or activity
b. the insurance and reinsurance undertakings, their auditors and the supervisory authorities must have effective access to data related to the outsourced functions or activities
c. the supervisory authorities must have effective access to the business premises of the service provider and must be able to exercise those rights of access.

Good practices

The outsourcing agreement that an insurer concludes with a service provider contains a clear term of operation and evaluation frequency. It describes the activity or activities to be outsourced and the terms and conditions of outsourcing, including compliance with legislation and regulations.

The insurer will assess on a regular basis whether its standard and model agreements are still in compliance with current legal and regulatory requirements.

It contains a specification of the mutual exchange of information and the service provider's control and reporting requirements, including service level reports, assurance statements and certificates. The requirements include the service provider's duty to notify the insurer of any continuity threats or changes to the service provider's ownership structure.

An insurer records the reasons for terminating the agreement, manner of transition/migration and the liability and best-efforts obligation of the service provider. The insurer lays down extensive rights to terminate/dissolve the agreement if the service provider's performance is not in line with the agreements about quality.

If a service provider is to process sensitive data, an insurer concludes a processing agreement with the service provider. The insurer also makes agreements about the ownership of the data.

Before entering into an outsourcing agreement, the insurer has checked the legal aspects of outsourcing. An insurer checks that the agreements made are not counter-productive or conflicting. The agreement is signed at board level.

Subcontracting means that the service provider to whom the insurer has outsourced activities also fully or partially outsources these activities itself.

In the outsourcing agreement, an insurer records that subcontracting is only permitted if this does not withdraw the subcontracted activities from supervision. The insurer also records the conditions and agreements of subcontracting, for example the duty to inform the insurer in time to make a

risk assessment and take appropriate measures and any other statutory requirements that apply to outsourcing.

In the event of subcontracting, an insurer includes appropriate measures in the agreement terms and conditions to mitigate the risk that a subcontractor is unable to meet its obligations.

An insurer stipulates in the agreement that the service provider must notify the insurer of any intended major changes with respect to the subcontractors listed in the original agreement, or the services that are subcontracted out. The notification period is determined in such a way that the insurer has sufficient time to assess the risk ensuing from the proposed changes and if necessary take appropriate measures or terminate the agreement with the service provider. The insurer must have the option to activate the exit clause if it does not wish the work to be performed by this particular subcontractor.

An insurer demands that the main service provider unconditionally ensures DNB's right to examine and the insurer's right to audit, and that these rights must also be included in its agreements with subcontractors through the entire chain. If possible through a framework agreement in which this is recorded.
The actual exercise of the right to examine and the right to audit must not be limited by contractual arrangements. To enable on-site checks, service providers must allow full access to all information about outsourced activities and functions, as well as to business premises (headquarters and operational centres), including all provisions, systems, networks and data that the service provider uses to deliver the outsourced services.

2.3 Critical and sensitive data

An insurer must handle critical and sensitive data carefully. In the event of outsourcing, it ensures that the availability, integrity, confidentiality and security of its critical and sensitive data is safeguarded.

Legislative framework

Article 274(3)(e) of the Solvency II Regulation stipulates that the outsourcing does not entail the breaching of any law, in particular with regard to rules on data protection, such as the GDPR. Pursuant to Article 274(3)(f) Solvency II Regulation, the service provider and its subcontractors are subject to the same provisions on the availability, integrity and confidentiality of information that are applicable to the insurer, i.e. their information security and business continuity management policy are at an equal or higher level. The insurer is responsible for ensuring that it complies with the applicable information security requirements, and that the service providers to which it has outsourced activities also comply with these requirements. See Open Book on Supervision[1].

1 See http://www.toezicht.dnb.nl/en/3/51-203304.jsp and http://www.toezicht.dnb.nl/en binaries/51-236703.pdf

Solvency II Regulation (EU) 2015/35 – Article 274(3)

3. When choosing the service provider referred to in paragraph 1 for any critical or important operational functions or activities, the administrative, management or supervisory body shall ensure that:
   e. the outsourcing does not entail the breaching of any law, in particular with regard to rules on data protection
   f. the service provider is subject to the same provisions on the safety and confidentiality of information relating to the insurance or reinsurance undertaking or to its policyholders or beneficiaries that are applicable to the insurance or reinsurance undertaking.

Good practices

An insurer defines and takes decisions on appropriate security measures about the availability, integrity and confidentiality of data. An insurer investigates whether specific measures are needed with respect to data that is transmitted, processed and stored (production and back-up), such as the application of strong authentication and encryption techniques combined with an appropriate set-up of encryption key management. The insurer monitors the measures as well as any incidents.

An insurer monitors the service provider's access to critical and sensitive data on an ongoing basis, e.g. with the help of security logs or other monitoring instruments.

An insurer exercises restraint in engaging in and managing agreements with parties outside the European Economic Area (EEA) with a view to the potential risks associated with the location of data and data processing. The insurer assesses and addresses the potential consequences of risks, including impediments for supervision in connection with the countries where the data are stored. The insurer is transparent towards relevant parties if their sensitive data are stored outside the EEA.

An insurer is transparent towards relevant parties about the outsourcing and provision of personal data to third parties.

An insurer ensures that the rights of relevant parties are not restricted or hampered.

An insurer is able to establish that the service provider complies with the GDPR. Non-compliance with the GDPR and the agreements made can be a reason for the insurer to terminate the agreement with the service provider.

3 Selection process

Once an insurer has established which activities it wishes to outsource, and the statutory requirements that must be met, it initiates a selection process to find a suitable service provider. The insurer checks whether the insurer complies with both the statutory requirements and the insurer's own requirements and preferences.

3.1 Selection of service provider

The service provider to be selected must be able to carry out the activities, and a process must be in place to ensure that the service provider selected is capable of doing so.

Solvency II Regulation (EU) 2015/35 – Article 274(3)

3. When choosing the service provider referred to in paragraph 1 for any critical or important operational functions or activities, the administrative, management or supervisory body shall ensure that:
   a. a detailed examination is performed to ensure that the potential service provider has the ability, the capacity and any authorisation required by law to deliver the required functions or activities satisfactorily, taking into account the undertaking's objectives and needs
   b. the service provider has adopted all means to ensure that no explicit or potential conflict of interests jeopardize the fulfilment of the needs of the outsourcing undertaking
   c. a written agreement is entered into between the insurance or reinsurance undertaking and the service provider which clearly defines the respective rights and obligations of the undertaking and the service provider
   d. the general terms and conditions of the outsourcing agreement are clearly explained to the undertaking's administrative, management or supervisory body and authorised by them

Solvency II Regulation (EU) 2015/35 – Article 274.5

The insurance or reinsurance undertaking that is outsourcing critical or important operational functions or activities shall fulfil all of the following requirements:

c. verify that the service provider has the necessary financial resources to perform the additional tasks in a proper and reliable way, and that all staff of the service provider who will be involved in providing the outsourced functions or activities are sufficiently qualified and reliable

EIOPA Guideline 63 – Outsourcing written policy

1.116. The undertaking that outsources or considers outsourcing should cover in its policy the undertaking's approach and processes for outsourcing from the inception to the end of the contract. This in particular should include:
b. how a service provider of suitable quality is selected and how, and how often its performance and results are assessed

Good practices

The selection of a service provider is preceded by a risk analysis which addresses concentration risk and legal risk with respect to the service provider and includes a due diligence assessment. The insurer considers the risks ensuing from various scenarios, e.g. a situation in which a service provider is unable to deliver, activities abroad, competition, growth, loss of knowledge in the organisation, etc.

When selecting a service provider, the insurer checks whether the service provider complies with both the statutory requirements and the insurer's own requirements and preferences. The insurer does so based on a sound risk assessment, using a uniform set of standards. The service provider selection and assessment process addresses the following aspects:

- financial situation of the service provider and possible conflicts of interests
- professional background and expertise of service provider staff
- employee screening (criminal records check)
- size of the contract in relation to the size of the service provider
- existence of litigation or legal procedures against the service provider
- track record of the service provider
- quality of subcontractors
- standard certification, audit and assurance reports
- information security policy of the service provider
- continuity policy of the service provider
- compliance policy of the service provider
- privacy policy
- incident reporting policy of the service provider
- applicable law and country of incorporation of the service provider
- data security
- data storage location, if applicable:
- safeguards for the performance of supervisory duties
- ongoing compliance with legal and regulatory requirements.

The service provider selection process includes process steps, selection criteria and a decision-making process, leading to clear mandates for the service provider, with the insurer's management board bearing ultimate responsibility. Based on the selection criteria, the insurer requests information from service providers and creates a longlist. Based on the outcomes of an assessment of the aspects listed above, the longlist is then reduced to a shortlist. The insurer initiates contract negotiations with service providers whose risk profile matches the insurer's risk appetite. If the insurer cannot find a suitable service provider, it again considers its reasons for outsourcing and the selection criteria, and analyses whether outsourcing is the best option.

The insurer documents the service provider selection and assessment process in a formal document that can be objectively verified by third parties.

An insurer that selects a cloud provider is aware of the specific risks related to cloud services and has sufficient knowledge to make agreements with the service provider on indicators for adequate management of these risks. Examples include vendor lock-in, data location, data access and concentration. These are part of the 10 subjects selected by DNB that insurers must as a minimum include in their risk analysis when submitting a notification of outsourcing to DNB. They should then supplement their risk analyses with risks that are relevant to the institution itself.
Please refer to our Open Book on Supervision pages for more information: https://www.toezicht.dnb.nl/en/2/5/51-230431.jsp

With respect to concentration of services, an insurer is aware that the data it submitted to different main service providers may be stored and managed by the same service provider due to subcontracting.

An insurer is aware that the standard service provision of cloud providers may not in all cases meet the standards that the insurer requires. In all links of the outsourcing chain, the levels of security and continuity must be in line with the levels defined in the insurer's own policy. “A chain is only as strong as its weakest link".

4 Monitoring

After entering into an outsourcing agreement, the insurer monitors whether the service provider is able to deliver the services agreed. The insurer monitors the execution of activities, the operational effectiveness of security and control measures and compliance with laws and regulations. If necessary, the insurer takes immediate appropriate measures.

4.1 Monitoring of outsourcing

An insurer adjust its internal processes in order to monitor outsourced activities and has in place adequate procedures, measures, expertise and information.

Legislative framework

Solvency II Regulation (EU) 2015/35 – Article 274(5)

The insurance or reinsurance undertaking that is outsourcing critical or important operational functions or activities shall fulfil all of the following requirements:

a. ensure that relevant aspects of the service provider's risk management and internal control systems are adequate to ensure compliance with Article 49(2)(a) and (b) of Directive 2009/138/EC
b. adequately take account of the outsourced activities in its risk management and internal control systems to ensure compliance with Article 49(2)(a) and (b) of Directive 2009/138/EC

Good practices

An insurer's management board takes the outsourced activities into account in its risk management and internal control systems, to monitor performance and ensure compliance with statutory and regulatory requirements. An insurer regularly checks the operational effectiveness of internal control measures in place for risks related to outsourcing and reports the findings to its management board.

The insurer monitors the risks related to outsourcing such as operational and concentration risk on an ongoing basis and compares the information from the service provider with specified critical risk indicators (CRIs) for outsourcing risks, with the aim of timely identifying changes to the service provider's risk profile.
Examples of CRIs include:

- the number of disruptions with an immediate operational impact on service provision or expected earnings
- number of complaints from policy holders
- number of data incidents
- level of compliance with statutory and regulatory requirements
- level of operational effectiveness (%) of internal control measures in place to manage outsourcing risks
- concentrations on service providers

An insurer sets up a coordinating organisation for monitoring larger outsourcing operations that is proportionate to the nature, scale and complexity of the insurer as well as the outsourced activities.

An insurer sets up a system for monitoring the operational effectiveness of the service provider's control measures. Monitoring also includes the timely collection of data that may indicate flaws in a service provider's performance or continuity.

An insurer describes the required knowledge and expertise to check and balance the service provider (see part 1, policy). The insurer also describes the specific competencies required to properly assess KPI/CPI reports. This also applies to the assessment of service level reports (4.2) and assurance reports (4.3).

The risk management function collects, aggregates and reports information about outsourced activities to the management board at least on a quarterly basis. The information allows the management board to effectively manage the operational risks related to the outsourced activities.

An insurer has a comprehensive overview of the full outsourcing chain. The monitoring reports comprise the full scope of services. The insurer receives information about the subcontracted services directly from the subcontractor or through the main service provider on a regular basis. Depending on the materiality of the service, this concerns incident reports, service level reports and assurance reports on the quality of service provision and the effectiveness of internal controls.

An insurer keeps a central register of information about the activities it outsources. The register contains the details of all outsourcing relations including relevant subcontracting relations. The insurer records the following details of the service providers:

- name and addresses of the service providers and their subcontractors (if applicable)
- chamber of commerce registration data
- description of the outsourced activities
- start date and end date or renewal date of the outsourcing agreement
- spplicable law governing the outsourcing agreement
- country or countries where the service is provided and data storage location (if applicable)
- outcome and date of the materiality assessment
- own classification of availability, integrity and confidentiality of data
- proof of approval from the management board ensuring that the outsourcing complies with statutory requirements and the insurer's own selection criteria.
- assessment of whether an alternative service provider is available (in terms of easy, difficult or impossible) and if so, their details.
- date of most recent service provider evaluation
- date of most recent renewal date of the outsourcing agreement (if applicable)

4.2 Service level reports (SLRs)

An insurer receives reports about the service provider's performance. They allow the insurer to monitor the quantity and quality of outsourcing and manage the outsourcing risks.

Legislative framework

Pursuant to Article 258(1 h,i,k) of the Solvency II Regulation, General governance requirements, an insurer must establish information systems and reporting lines that ensure the prompt transfer of complete and clear information about the internal organisation and the risks to all persons who need it.

Good practices

An insurer uses a service level agreement (SLA) to record performance agreements between the insurer and the service provider, including the mutual responsibilities ensuing from the outsourcing agreement. Detailed working agreements are recorded in an Agreement and Procedures Document. This document describes the following:

- contact persons
- how to contact them
- how to submit changes
- schedule and frequency of agreements
- operational, tactical and strategic consultations
- dispute resolution
- escalation procedure

An insurer has recorded all agreements in a service level agreement (SLA). The performance and risk indicators (CPIs/CRIs) in this agreement match the insurer's risk appetite

The SLA describes how the service provider implements the agreement and how performance is managed: performance indicators, measurements, frequency, standards (tolerance limits). An insurer makes agreements on the following performance indicator and sets a standard that must not be breached:

- operating hours
- availability (%)
- numbers and nature of incidents: security, cybercrime, data issues
- incident response time
- incident recovery time
- user support
- complaints
- problem recovery and maintenance rounds
- security level: dealing with sensitive data, training and instruction
- transaction numbers
- transactions volumes
- backlogs
- time to delivery

An insurer verifies that the outsourced services continue to meet the agreed performance and quality standards on the basis of regular service level reports with predefined performance indicators. The reporting frequency – quarterly, monthly or ongoing based on tooling in which the insurer and the service provider cooperate – is appropriate to the nature and scale of the outsourced activities. The SLA and/or the Agreement and Procedures Document include agreements on information exchange, checks, service level reports, regular consultations and a complaints and incidents process with reporting moments and standards.

An insurer ensures that the critical performance indicators (CPIs) in the SLA are in line with the outsourcing policy objectives, and that its risk appetite matches the critical risk indicators (CRIs) applied.

An insurer monitors and assesses the effectiveness of the services and ensures that the risks stay within the limits of the risk appetite in order to allow the service provider to take appropriate remedial action when needed. The insurer uses a combination of quantitative and qualitative indicators based on recent operational service provider data to assess the effectiveness of the services.

4.3 Quality of outsourced services (internal control)

An insurer receives reports about the service provider, both from the service provider in question and from independent third parties. They allow the insurer to monitor the quality of outsourcing and process management at the service providers in the chain, to manage the outsourcing risks.

Good practices

In the outsourcing agreement, the insurer agrees with the service provider that the latter provides regular assurance about its internal management system, e.g. based on an assurance report compiled by an independent assurance provider or based on an audit that the insurer performs or has performed at the service provider.

An insurer ensures that the scope of assurance provided and the period to which it pertains is in accordance with the services provided. The insurer opts for an assurance report on design, existence and operating effectiveness pertaining to a specified period.

In the event of IT services, the insurer opts for a SOC2 type II report, possibly supplemented by a SOC3 report (management objectives with a focus on security, availability, processing integrity, confidentiality and privacy), or an extensive ISAE 3000 report. For assurance about the outsourcing of services related to annual financial statements, the insurer opts for an ISAE3402 type II or SOC1 type 2 report. The assurance report relates to the quality of the services throughout the chain. The insurer receives aggregated assurance reports from the main service provider, or separate reports from all individual service providers. The insurer actively monitors the follow-up of findings from the assurance reports. The insurer checks and balances the findings with its own observations and complaints and incident reports. The insurer makes a risk assessment, takes appropriate measures and records them.

An insurer ensures that a sufficient level of knowledge and expertise is available in the organisation to assess the assurance reports, e.g. a multidisciplinary team.

An insurer performs audits at service providers if no assurance report is available, or to supplement an assurance report that insufficiently matches the services provided.

When evaluating an assurance report, the insurer checks that the services provided are included in the scope of the report as well as the sample.

The external auditor establishes the correct, complete and timely operation of controls based on a representative sample. If necessary, the insurer performs its own, supplemental audit.

An insurer with insufficient audit resources at its disposal can organise a joint audit with other customers of the same service provider or cloud service provider. This will help the parties to deploy their audit resources more efficiently and at the same time reduces the organisational burden for the service provider. Cloud solutions are very complex technically speaking. The insurer verifies beforehand whether the auditor performing the audit has the required knowledge and skills to perform audits and/or assessments of cloud solutions in an effective and appropriate manner.

An insurer acknowledges the posibilities and limitations of the various types of assurance and certification (e.g. ISO). Certification is aimed at the quality of the design of processes. While certification guarantees the existence of a PDCA process, it does not guarantee ongoing operational effectiveness of controls. Where necessary, an insurer takes measures to verify the operational effectiveness of processes.

5 Evaluation process

Over time, an insurer gains more experience of the processes surrounding the outsourced activities and the quality of the service providers. At regular intervals, or when necessary, the insurer evaluates her own policy and processes and the performance of the service provider.

Legislative framework

Article 41 of the SII Directive and Article 258(6) of the SII Regulation stipulate that insurers must evaluate their governance system on a regular basis, including the outsourcing of activities. Guideline 63 of the EIOPA Guidelines for the System of Governance also addresses how, and how often a service provider's performance and results are assessed.

Solvency II Directive 2009/138/EC – Article 41 - General governance requirements

1. Member States shall require all insurance and reinsurance undertakings to have in place an effective system of governance which provides for sound and prudent management of the business. That system shall at least include an adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities and an effective system for ensuring the transmission of information. It shall include compliance with the requirements laid down in Articles 42 to 49. The system of governance shall be subject to regular internal review.
2. The system of governance shall be proportionate to the nature, scale and complexity of the operations of the insurance or reinsurance undertaking.
3. Insurance and reinsurance undertakings shall have written policies in relation to at least risk management, internal control, internal audit and, where relevant, outsourcing. They must ensure that those policies are implemented. Those written policies must be evaluated at least annually. They must be subject to prior approval by the administrative, management or supervisory body and be adapted in view of any significant change in the system or area concerned.

Solvency II Regulation (EU) 2015/35 – Article 258

6. Insurance and reinsurance undertakings shall monitor, and on a regular basis evaluate, the adequacy and effectiveness of their system of governance and take appropriate measures to address any deficiencies.

EIOPA Guideline 63 – Outsourcing written policy

1.116. The undertaking that outsources or considers outsourcing should cover in its policy the undertaking's approach and processes for outsourcing from the inception to the end of the contract. This in particular should include:
e. how a service provider of suitable quality is selected and how, and how often its performance and results are assessed

5.1 Evaluation in all stages of the outsourcing process

An insurer not only evaluates the service providers to which it outsources activities, but also its own outsourcing policy (see 1) and the outsourcing processes: selection (3) monitoring (4) and evaluation (5). Does the internal reporting lines structure facilitate timely notification of incidents at the service provider, do processes and controls still match the insurer's policy and does the standard for outsourcing agreements still comply with current legal and regulatory requirements??

Good practice

An insurer evaluates its policy on a regular basis, and at least once a year. The insurer documents the outcome of its evaluation and informs the management at the correct level about deviations and appropriate measures. Based on the outcome, the insurer adjusts its outsourcing policy if necessary and checks whether any existing outsourcing agreements must be adjusted or terminated as a result of adjusting the policy.

An insurer evaluates its policy based on a management report containing a clear performance overview of all service providers. Based on the management report, policymakers can decide to adjust or terminate outsourcing agreements with service providers, and to adjust the outsourcing policy or existing procedures and measures.

5.2 Evaluation of service providers

An insurer evaluates the performance of its service providers on a regular basis, or when prompted by monitoring signals. The insurer also evaluates whether the outsourced activities still match its strategic policy and risk appetite.

Good practices

During the term of the outsourcing agreement, the insurer evaluates the performance of its service providers in line with the approach and frequency established in its policy. The insurer evaluates critical or important outsourcings at least annually. This includes the achievement of performance and results agreements and the evaluation of major

changes at the service provider, such as changes to the strategy, profitability, ownership structure or other aspects that may affect the service provider's ability to meet its contractual obligations.
The evaluation results in a decision at the correct management level to continue, change or terminate the outsourcing. The central question is whether the insurer wishes to continue working with the service provider or find another service provider who better fits its mission, vision and strategy.

An insurer appoints organisational units or individuals responsible for auditing, managing and evaluating all outsourced activities. Preferably, the insurer appoints a multidisciplinary team for this purpose.

An insurer checks the original outsourcing business case against its policy.

As part of its evaluation, an insurer checks whether the service provider and outsourcing still meets the requirements, matches its risk appetite and contributes to its strategy and objectives. The following aspects are evaluated as a standard:

- financial situation of the service provider and possible conflicts of interests
- professional background and expertise of service provider staff
- size of the contract in relation to the size of the service provider
- existence of litigation or legal procedures against the service provider
- track record of the service provider
- quality of subcontractors
- monitoring system
- standard certification, audit and assurance reports
- information security policy of the service provider
- continuity policy of the service provider
- compliance policy of the service provider
- incident reporting policy of the service provider
- data storage location, if applicable

DISCLAIMER

This Good Practices document presents non-binding recommendations to insurers for implementation of the Solvency II Directive and Regulation, the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft – Bpr*) and the EIOPA Guidelines for risk management. It sets out our expectations regarding observed or envisaged behaviour in policy practice that reflects an appropriate application of the rules to which this Good Practices document pertains.

We encourage insurers to take our expectations into account in their considerations and decision-making, without them being obliged to do so, while also taking into consideration their specific circumstances. The Good Practices document is only indicative in nature and therefore does not alter the fact that some financial institutions should apply the underlying regulations differently, and possibly more strictly. It is the institution's responsibility to take this into account.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl