



Policy Department

**CONFIDENTIAL**

**DRAFT**

15 February 2019

## **DRAFT OPINION OF THE EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY**

of [date Month YYYY]

on the Supervision of the Management of Operational Risk by IORPs

### **1. Legal basis and scope**

- 1.1. The European Insurance and Occupational Pensions Authority (EIOPA) provides this Opinion on the basis of Article 29 on Common supervisory culture of Regulation (EU) No 1094/2010<sup>1</sup> (hereafter the 'EIOPA Regulation'). This Article mandates EIOPA to play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union by providing opinions to competent authorities.
- 1.2. EIOPA delivers this Opinion on the basis of Article 25.2(e), Article 28.2(g) and Article 31 of Directive (EU) 2016/2341<sup>2</sup> (hereafter the 'IORP II Directive'). Article 25.2(e) specifies that the risk-management system shall cover, amongst others and where applicable, in a manner that is proportionate to their size and internal organisation, as well as to the size, nature, scale and complexity of their activities, operational risks which can occur in IORPs or in undertakings to which tasks or activities of an IORP have been outsourced. Article 28.2(g) provides that a qualitative assessment of operational risks shall be included in the own-risk assessment to be carried out and documented by IORPs. Article 31 prescribes, among others, that the outsourcing of key functions or other activities shall not impair the quality of the system of governance, unduly increase operational risk, impair the ability of competent authorities to monitor the compliance of the IORP with its obligations and undermine the continuous and satisfactory service to members and beneficiaries. To that end, IORPs shall ensure the proper functioning of the outsourced activities through the process of selecting a service provider and the ongoing monitoring of the activities of that service provider. IORPs have to enter into a legally enforceable agreement with the service provider, clearly defining the respective rights and obligations. IORPs should notify competent authorities in a timely manner of any outsourcing of the activities covered by

---

<sup>1</sup> Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/79/EC (OJ L 331, 15.12.2010, p. 48).

<sup>2</sup> Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs) (recast).

the IORP II Directive and of any subsequent important developments. Where the outsourcing relates to the key functions or the management of IORPs, this shall be notified to the competent authorities before the outsourcing agreement enters into force.

- 1.3. This Opinion concerns the supervision of the management of operational risks by IORPs, including the assessment and management of outsourcing risk.
- 1.4. This Opinion is addressed to the competent authorities (CAs), as defined in point (i) of Article 4(2) of the EIOPA Regulation.
- 1.5. The Board of Supervisors has adopted this Opinion in accordance with Article 2(7) of its Rules of Procedure<sup>3</sup>.

## **2. Context and objective**

- 2.1. The recast IORP II Directive entered into force on 12 January 2017 and had to be transposed into national law by 13 January 2019. The IORP II Directive introduces new requirements at EU level on the management and assessment of operational risk of IORPs. The IORP II Directive also puts forward more extensive provisions on the outsourcing of activities of IORPs. IORPs often delegate activities to external service providers or the sponsoring undertaking. Such outsourced activities are subject to operational risk, but outsourcing does not discharge IORPs of their responsibility for that operational risk.
- 2.2. EIOPA conducted a mapping exercise among NCAs that identified cyber risk to be a challenging operational risk, which requires further supervisory attention. The G-7 developed a set of fundamental elements for the effective assessment of cybersecurity, recognising the continued pervasiveness of cyber risks and the need for sustained efforts to enhance cybersecurity in the financial sector.<sup>4</sup>
- 2.3. Operational risk is relevant for IORPs providing all kinds of pension schemes, ranging from defined benefit (DB) to defined contribution (DC) plans. A defining feature of (pure) DC schemes is that market risks are explicitly borne by members and beneficiaries, but the same is normally not true for operational risk. Being the only risk that is borne by the institutions itself, operational risk is of particular importance for IORPs providing DC schemes and, given the strong trend from DB towards DC pension provision, the IORP sector as a whole.
- 2.4. The IORP II Directive recognises the importance of NCAs reviewing IORPs' risk management strategies, processes and reporting, including an assessment of the system of governance, the risk exposure of IORPs and their ability to assess and manage those risks, of NCAs having the necessary powers to require IORPs to remedy weaknesses or deficiencies identified.<sup>5</sup>
- 2.5. In addition, the IORP II Directive already puts forward a high-level framework for IORPs' risk management. It recognises that a proper system of governance lies at the heart of sound risk management<sup>6</sup>. Moreover, IORP II emphasises and explains the roles of the risk management function and the risk management system.<sup>7</sup>
- 2.6. The objective of this Opinion is to provide NCAs with guidance on the supervision of IORPs' management of operational risk, including outsourcing risk and cyber risk, within the overall governance and risk management structure laid down in the IORP II Directive. The

<sup>3</sup> Decision adopting the Rules of Procedure of EIOPA's Board of Supervisors, available at: [https://eiopa.europa.eu/Publications/Administrative/EIOPA-BoS-11-002\\_EIOPA-BoS-Rules%20of%20Procedure-Rev3.f.pdf](https://eiopa.europa.eu/Publications/Administrative/EIOPA-BoS-11-002_EIOPA-BoS-Rules%20of%20Procedure-Rev3.f.pdf).

<sup>4</sup> G7 Fundamental Elements of Cybersecurity for the Financial Sector, October 2016.

<sup>5</sup> Article 49 IORP II Directive (EU) 2016/2341.

<sup>6</sup> Article 21 IORP II Directive (EU) 2016/2341.

<sup>7</sup> Article 25 IORP II Directive (EU) 2016/2341.

guidance is high-level in nature, recognising the diversity of the IORP landscape in Europe and allowing NCAs to impose further rules on IORPs to suit the specificities of the national IORP sector.

- 2.7. In establishing its Opinion, and in line with its task to foster cross-sectoral consistency, EIOPA considered and drew on existing principles and guidelines in the area of operational risk for other parts of the financial sector, in particular for the banking and insurance sectors.<sup>8</sup> In general, there is broad agreement on the key ingredients for sound management of operational risk, including outsourcing and cyber risk, irrespective of the type of financial institution. From this high-level perspective, this Opinion is consistent with similar principles and guidelines for other parts of the financial sector. Still, the latter may contain guidance that is more detailed, consider specificities of other financial institutions not relevant for IORPs, use different terminologies and put emphasis on different principles or formulate principles in a different way.

### 3. Taking the above into consideration, EIOPA is of the opinion that

#### 3.1 Definition and classification

- 3.1. To promote a common supervisory culture with respect to the supervision of the management of operational risks, including the risk of outsourcing, NCAs should recognise as a starting point that operational risk is defined as the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events.<sup>9</sup>
- 3.2. Operational risk has, compared to other risk categories, the distinctive characteristic of being asymmetric in nature. Operational risk events are most often associated with losses rather than gains to the detriment of the IORP, sponsor, members and beneficiaries.
- 3.3. A further classification may assist NCAs in identifying the key operational risks of IORPs under their supervision and on which their attention should focus. Operational risk can be further broken down in the following subcategories relating to<sup>10</sup>:
- Internal fraud;
  - External fraud;
  - Employment practices and workplace safety;
  - Relations with sponsors, members and beneficiaries;
  - Damage to physical assets;
  - Operational disruption and system failures;
  - Trading/transaction processing and process management.
- 3.4. The two core operational activities of IORPs are normally pension administration and investment management, which the IORP may carry out in-house or delegate to an external service provider. Still, operational risk may also arise from within other activities, including the IORP's Board and key functions, or external events. Annex 1 explains the seven subcategories in more detail and provides examples for each of them, distinguishing the origin of the operational risk events. The examples should not be construed to represent an exhaustive list of operational risks, but rather be interpreted as illustrations.

<sup>8</sup> See for example: BCBS/BIS, "Principles for the Sound Management of Operational Risk, June 2011, EBA, "Draft Guidelines on Outsourcing arrangements", Consultation Paper, EBA/CP/2018/11, 22 June 2018, and IAIS, Draft Application Paper on Supervision of Insurer Cybersecurity, 2 May 2018 (Members only version).

<sup>9</sup> [Insert references to other financial sector regulations to make clear that this is a widely used definition.]

<sup>10</sup> See Annex 9 of BCBS/BIS, International Convergence of Capital Measurement and Capital Standards – A Revised Framework, June 2006.

- 3.5. The definition of operational risk includes compliance/legal risk, but excludes reputational, strategic and political/regulatory risk (see Annex 1 for a definition and examples). The latter are in many respects closely related to operational risk. NCAs should take into account these related risks when reviewing IORPs assessment and management of (operational) risks.

### **3.2 Supervision of IORPs' assessment and management of operational risk**

- 3.6. NCAs should consider IORPs' assessment and management of operational risk as an integral part of their supervision activities. NCAs should ensure that IORPs embed operational risk effectively in their risk management strategy and system to optimise resilience against operational risk.

- 3.7. NCAs should conduct regular evaluations of IORPs' (operational) risk management:

- policies;
- processes; and
- systems.

These evaluations should go beyond checking whether IORPs are complying with regulation and internal procedures and include a review of the effectiveness of the (operational) risk management system.

- 3.8. NCAs should use a range of supervisory techniques to assess IORP's management of operational risks. These can be applied both off- and on-site, also at any external service provider to which IORPs have outsourced activities. NCAs should use the tools most suited to the particular circumstances of the IORP, including (stress) tests to assess the IORP's resilience to particular operational risks. Some NCAs may choose to use external auditors in these assessment processes.
- 3.9. NCAs should ensure that there are appropriate mechanisms in place to ensure that they remain up to date of developments at the IORPs. In order that supervisors receive current information on operational risk, they may wish to establish reporting mechanisms directly with IORPs and external auditors (i.e. internal reports could be made available on a regular basis). IORPs could also be required to proactively report incidents that do arise, beyond an appropriate threshold. This will help NCAs to become better informed of sector-wide risks, such as emerging cyber risks, that might otherwise go undetected for longer.
- 3.10. NCAs should stimulate IORPs to continually improve their operational risk management as the IORPs gain knowledge and experience. NCAs should continue to take an active role in encouraging ongoing internal development efforts by monitoring and evaluating an IORP's recent improvements and plans for prospective developments. These efforts can then be compared with other IORPs to provide the IORP with useful feedback on the status of its own work. Where there are identified reasons why certain efforts have proved ineffective, such information could be provided in general terms to assist in the development process.
- 3.11. NCAs should ensure that deficiencies in IORP operational risk management are responded to in a proportionate manner.

### **3.3 Review of integration of operational risk in IORPs' risk management system**

- 3.12. NCAs should evaluate whether IORPs fully and effectively integrated operational risk in their system of governance and risk management system. Therefore, NCAs should consider in their supervisory review the following key elements of IORP's risk management:

#### **(1) Strong risk management culture**

- 3.13. NCAs should verify that IORPs have in place an effective system of governance which provides for sound and prudent management of their activities. That system should include an adequate and transparent organisational structure with a clear allocation and appropriate segregation of responsibilities and an effective system for ensuring the transmission of information.<sup>11</sup>
- 3.14. It is the responsibility of the Board<sup>12</sup> to ensure that the IORP operates within a strong risk management culture that gives due recognition to staff's responsibility for a sound management of risks, including operational risk.
- 3.15. Elements that will contribute to a strong risk management culture:
- Clear definition of roles and responsibilities so that management and staff responsible for risk management are able to perform their tasks effectively;
  - Allocation of staff with sufficient knowledge and skills to execute their risk management duties and ensuring that relevant staff receive appropriate training;
  - Remuneration policies aligned with the IORP's objectives, appropriately balancing risk and reward and avoiding incentives for excessive risk taking.

## **(2) Risk-management system**

- 3.16. NCAs should check that IORPs have in place a risk-management system for which they should adopt strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report to the Board regularly the risks, at an individual and aggregated level, and their interdependencies. The risk-management system should be effective and well-integrated into the organisational structure and in the decision-making process of the IORP.<sup>13</sup>
- 3.17. An effective risk-management function should facilitate the risk-management system.<sup>14</sup> The risk-management function can be carried out by a single person or an organisational unit.<sup>15</sup> It should be able to undertake its duties effectively in an objective, fair and independent manner.<sup>16</sup> The risk-management function should report any material findings and recommendations to the Board.<sup>17</sup>
- 3.18. The risk-management system should be complemented by an effective internal control system<sup>18</sup>, ensuring sound administrative and accounting procedures, compliance with regulation and internal procedures, a clear segregation of duties and appropriate reporting arrangements.
- 3.19. The internal audit function should include among its activities a review of the adequacy and effectiveness of the risk management system.
- 3.20. The management of operational risk should be fully integrated into the IORP's overall risk management system, in a manner that is proportionate to the size and internal organisation of the IORP as well as to the size, nature, scale and complexity of its

---

<sup>11</sup> Article 21,1 IORP II Directive (EU) 2016/2341.

<sup>12</sup> The term 'Board' here and hereafter means the highest decision-making body of the IORP, referred to as the 'management or supervisory body' in the IORP II Directive (EU) 2016/2341. Art 21.6 of the IORP II Directive provides that IORPs should have at least two persons who effectively run the IORPs. Member States may allow that only one person effectively runs the IORP, on the basis of a reasoned assessment conducted by the NCA.

<sup>13</sup> Article 25.1 IORP II Directive (EU) 2016/2341.

<sup>14</sup> Article 25.1 IORP II Directive (EU) 2016/2341.

<sup>15</sup> Article 24.3 IORP II Directive (EU) 2016/2341.

<sup>16</sup> Article 24.1 IORP II Directive (EU) 2016/2341.

<sup>17</sup> Article 24.4 IORP II Directive (EU) 2016/2341.

<sup>18</sup> Article 21.4 IORP II Directive (EU) 2016/2341.

activities.<sup>19</sup> The IORP II Directive also states that IORPs must regularly carry out an own-risk assessment<sup>20</sup>, which includes a qualitative assessment of operational risk.

- 3.21. Operational risk should first and foremost be addressed at the operational level, such as pension administration and investment management, including at service providers to which activities have been outsourced. The operational unit is in the best position and responsible for managing the risks inherent in its activities, processes and systems. The IORP's risk management function should monitor and challenge the risk reporting from the operational level and maintain an overall view of the IORP's exposure to risks, including their interdependencies. Independent reviews of the risk management system by the internal audit function should complete detect inefficiencies and white spots, for instance by adopting a "three lines of defence" model.

### **(3) Board's approval, implementation and review**

- 3.22. NCAs should verify that IORPs establish and apply written policies in relation to risk management<sup>21</sup>, including the strategies, processes and reporting procedures underlying the risk-management system. The written policies should be subject to prior approval by the IORP's Board and should be reviewed at least every three years and adapted in view of any significant change in the system or area concerned.<sup>22</sup>

3.23. NCAs should verify that:

- the Board carries the overall responsibility for the functioning of the risk-management system, its implementation and periodic review. Depending on the governance model, the IORP may have in place a senior management team to which certain responsibilities may be delegated, such as implementing and maintaining throughout the organisation the risk management policies to ensure that the risk tolerance limits are respected. Particularly in the case of operational risk, the management of the operational units, including service providers carrying out outsourced activities, will be responsible for the implementation of risk management policies and compliance with the IORP's risk tolerance limits.
- The Board is kept up-to-date through regular risk reporting, including reporting of operational risks, to ensure pro-active management of (operational) risks. Where necessary, the Board is proactive in seeking extra information from the risk management function.

- 3.24. The periodic review of the risk management policies should take into account independent reviews by internal and external auditor as well as the NCA, experience with the current risk management system and recommendations by the risk management function and the identification of new and emerging risks, such as cyber threats.

### **(4) Risk tolerance statement**

- 3.25. NCAs should check that IORPs have a risk tolerance statement as part of the written risk management policies. Approved by the Board, the risk tolerance statement articulates the nature, types, and levels of risk that the IORP is willing to assume, including the limits on the various categories of operational risk.
- 3.26. Risk tolerance should be interpreted as the maximum level of risk, for each risk category,

<sup>19</sup> Article 25.2 IORP II Directive (EU) 2016/2341.

<sup>20</sup> Article 28 IORP II Directive (EU) 2016/2341.

<sup>21</sup> Article 21.3 IORP II Directive (EU) 2016/2341.

<sup>22</sup> Article 21.3 IORP II Directive (EU) 2016/2341.



that the IORP is willing to operate within expressed as a risk limit that, where possible, is based on a measurable limit of the risk remaining, after taking into account, where relevant, the risk mitigants for the risk.

- 3.27. Risk tolerance limits express the restrictions the IORP imposes on itself when looking to manage and mitigate risks. The risk tolerance limits defined for all relevant risk categories should guide day-to-day operations of the IORP's activities.

## **(5) Identification and assessment of operational risks**

- 3.28. NCAs should check that IORPs' risk-management systems ensure the identification and assessment of the operational risk inherent in all IORP activities, processes and systems to make sure the inherent risks and incentives are well understood.
- 3.29. The risk management systems should make use of available tools for identifying and assessing operational risks, like internal and external experience with operational losses, operational process mappings, risk assessments and scenario analyses.
- 3.30. The frequency and severity of operational risks are usually hard to quantify. Therefore, the assessment of the probability and expected losses of operational risks may have to be expressed in a qualitative manner, like "high", "medium" and "low" scores. The severity of operational risks may also be categorised in terms of "critical" versus "non-critical" to indicate whether a particular risk threatens to interrupt essential operations.
- 3.31. A risk register with identified operational risks together with an assessment of their probability/impact before and after risk mitigation measures will contribute to a comprehensive overview of the IORP's exposure to risks and their interdependencies. A risk register should not be treated as a static document. The identification and assessment of operational risk should be ongoing and forward looking in order to capture new and emerging risks.

## **(6) New activities, processes and systems**

- 3.32. NCAs should verify that the identification and assessment of operational risks is not restricted to existing activities, processes and systems. A proper integral risk analysis, including operational risk, should be part of the decision-making process relating to significant new activities, processes and systems.<sup>23</sup>
- 3.33. Examples of new activities, processes and systems include but are not limited to:
- New pension products/schemes that may increase operational risk due to added complexity;
  - New IT solutions/systems that may be vulnerable to cyber risk;
  - Outsourcing of activities or change of service provider, which will be subject to operational risk.
- 3.34. NCAs should check that IORPs carried out due diligence before taking on new activities, also encompassing operational risk aspects of the proposal. The due diligence process should be well documented.

## **(7) Monitoring and reporting**

- 3.35. NCAs should check that IORPs' risk-management system contains processes to regularly monitor operational risk profiles and material exposures to losses, including the ongoing

---

<sup>23</sup> Article 28.2(a) IORP II Directive (EU) 2016/2341 requires IORPs to provide a description of how own-risk assessment is integrated into the management process and into the decision-making process of the IORP.

monitoring of outsourced activities through a service provider.

3.36. Appropriate reporting mechanisms should be in place at the Board and at the management of operational units that support proactive management of operational risk.

3.37. Operational risk reports should include details of:

- breaches of operational risk tolerance;
- material operational risk losses or events since the last report;
- external developments and events, such as new cyber threats, that may have a bearing on the operational risk exposure of the IORP.

## **(8) Control and mitigation**

3.38. NCAs should verify that IORPs' risk-management system includes a strong risk control environment in which appropriate risk mitigation and/or transfer strategies are implemented.

3.39. An effective operational risk control environment requires an appropriate segregation of duties, for example avoiding conflicts of interests. Other examples of controls and mitigating measures include:

- Clearly established approval processes;
- Access restrictions to confidential/sensitive information and critical IT systems;
- Appropriate staffing and training to ensure sufficient(ly) competent staff;
- Leave policy requiring staff to take a holiday of reasonable length to discourage internal fraud or encourage its detection.

## **(9) Continuity of activities & contingency plans**

3.40. NCAs should check that IORPs take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To that end, IORPs should employ appropriate and proportionate systems, resources and procedures.<sup>24</sup>

3.41. Their risk-management system should model and assess plausible disruptive scenarios. For example, a failure to make pensions payments in time due to a disruption in the banking system or an internal, critical IT system.

3.42. Their contingency plans should establish strategies, recovery and resumption procedures as well as communication plans to inform all stakeholders, including staff, members and beneficiaries, sponsors and supervisors.

## **(10) Disclosure**

3.43. NCAs should verify that the IORP's assessment of operational risk features in the ORA document.<sup>25</sup> In the EIOPA Opinion on Governance Documents, EIOPA is of the opinion that NCAs should encourage IORPs to disclose the ORA document to relevant stakeholders in order to promote greater transparency on how they manage pension risks.

3.44. NCAs should check that IORPs have a policy in place as regards reporting operational risk incidents to them. Overall, IORPs should have a policy in relation to the requirements for incident-driven ad-hoc reporting and need to consider appropriate thresholds for incident

<sup>24</sup> Article 21.5 IORP II Directive (EU) 2016/2341.

<sup>25</sup> Article 28 IORP II Directive (EU) 2016/2341.



reporting.<sup>26</sup>

### **Cooperation and information sharing**

3.45. NCAs should cooperate and share information with other NCAs and, where appropriate, public and private stakeholders as regards the supervision of operational risks:

- Cooperation with other NCAs may be necessary with respect to the outsourcing of IORP activities to other financial institutions, like asset managers, particularly in cross-border situations;
- Cooperation and information sharing with public authorities will be necessary to supervise in an effective way crime-related operational risks, like cyber threats and money laundering.

### **Proportionality**

3.46. As part of conducting proportional supervision, NCAs should determine the frequency and depth of their supervision of IORPs' management of operational risk, given their supervisory priorities and prudential objective of protecting the rights of members and beneficiaries and ensuring the stability and soundness of IORPs. In doing so, NCAs should take into account the IORPs' characteristics, i.e. the operational complexities of their activities and how these may affect their future resilience, and the importance of operational risks relative to other potential risk exposures of IORPs. EIOPA's Questions and Answers (Q&A) regarding the proportional supervision of IORPs provide further detail.

### **Outsourcing risk**

3.47. NCAs should integrate EIOPA's guidance on IORPs' management of outsourcing risk in their supervision (see Annex 3). Many IORPs, also compared to other financial institutions, outsource activities to external service providers, like asset managers. The pension administration of single-employer IORPs is often entrusted to the sponsoring company. The IORP II Directive also allows for the outsourcing of the management of IORPs and key functions.<sup>27</sup>

3.48. The outsourcing of activities does not "outsource" the responsibility of IORPs to manage and contain the (operational) risks relating to those activities. IORPs remain fully responsible for compliance with their obligations under the IORP II Directive when they outsource key functions or any other activities.<sup>28</sup> Outsourcing should not be undertaken in such a way as to lead to:

- Impairing the quality of the system of governance of the IORP concerned;
- Unduly increasing the operational risk
- Impairing the ability of the NCAs to monitor the compliance of the IORP with its obligations;
- Undermining continuous and satisfactory service to members and beneficiaries.<sup>29</sup>

### **Cyber risk**

3.49. NCAs should integrate EIOPA's guidance on IORPs' management of cyber risks in their supervision. The use of information technology will contribute to reducing operational risk since automated processes are less prone to error than manual ones. However, the use of ICT also introduces new operational risk, in particular cyber risk.

---

<sup>26</sup> BCBS/BIS, "Principles for the Sound Management of Operational Risk, June 2011. Page 18

<sup>27</sup> Article 31.1 IORP II Directive (EU) 2016/2341.

<sup>28</sup> Article 31.2 IORP II Directive (EU) 2016/2341.

<sup>29</sup> Article 31.3 IORP II Directive (EU) 2016/2341.

3.50. Cyber risk refers to any threat to information, information systems and operational processes that jeopardises the 'confidentiality', 'integrity' and 'availability' of information, information systems and operational processes.

- IORPs dispose of large amounts of data of their staff, sponsors, members and beneficiaries. Access to these confidential data by unauthorised individuals/organisations will result in financial and reputational losses for the IORP;
- Integrity means the accuracy and consistency of information and systems over the entire life-cycle. Inaccurate or inconsistent data may compromise IORPs' operations. For example, if records are incomplete, IORPs may not be able to calculate accrued pensions of members and beneficiaries or send pension benefit statements. Similarly, manipulated internal risk or actuarial models may lead to wrong investment or policy decisions;
- Interruptions to the availability of technology may halt core processes of IORPs and also be a source of financial and reputational losses. For example, the IORP may not be able to pay retirement benefits in time, invest DC members' contributions or roll over derivative hedging arrangements.

#### **4. Monitoring by EIOPA**

4.1. [To be drafted]

4.2. This Opinion will be published on EIOPA's website.

Done at Frankfurt am Main, XX Month 2019

[signed]

Gabriel Bernardino

Chairperson

For the Board of Supervisors

## Annex 1: Classification of operational risk and related risk

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
<b>OPERATIONAL AND RELATED RISKS:</b>	<b>Investment management</b>	<b>Pension administration</b>	<b>Other activities, incl. key functions and management of the IORP</b>	<b>Investments, pension administration and other activities</b>	
<b>I OPERATIONAL RISK</b> Losses arising from inadequate or failed internal processes, personnel or systems, or from external events.					
Subcategories:					
<b>(1) Internal fraud</b> Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or the IORP's policy, excluding diversity/discrimination events, which involves at least one internal party.	- Fraud and improper actions (misappropriation & misallocation) by employees	- Fraud and improper actions (misappropriation & misallocation) by employees	- Fraud and improper actions (misappropriation & misallocation) by employees	- Fraud and improper actions (misappropriation & misallocation) by employees	
<b>(2) External fraud</b> Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.				- Service provider engaged in illegal activities	- Breakdown of IT infrastructure and communications due to cyber-attack - Access to confidential information (incl. data of members and beneficiaries) due to hacking - Sponsoring companies involved in illegal activities are making

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
					pension contributions derived from illicit activities to the IORP
<b>(3) Employment practices and workplace safety</b> Losses arising from acts inconsistent with employment, health or safety laws or agreements from payment of personal injury claims, or from diversity / discrimination events.	<ul style="list-style-type: none"> <li>- Fines or damages to be paid to staff for not observing employment laws or collective labour agreements</li> <li>- Fines or damages to be paid to (potential) staff for engaging in discriminatory employment or hiring practices</li> </ul>	<ul style="list-style-type: none"> <li>- Fines or damages to be paid to staff for not observing employment laws or collective labour agreements</li> <li>- Fines or damages to be paid to (potential) staff for engaging in discriminatory employment or hiring practices</li> </ul>	<ul style="list-style-type: none"> <li>- Fines or damages to be paid to staff for not observing employment laws or collective labour agreements</li> <li>- Fines or damages to be paid to (potential) staff for engaging in discriminatory employment or hiring practices</li> </ul>	<ul style="list-style-type: none"> <li>- Service provider does not comply with its obligations relating to employment practices and workplace safety laid down in the outsourcing agreement</li> </ul>	
<b>(4) Relations with sponsors, members and beneficiaries</b> Losses arising from an unintentional or negligent failure to meet a professional obligation to specific sponsors, members and beneficiaries (including fiduciary and suitability requirements) or the nature or design of a pension product.	<ul style="list-style-type: none"> <li>- Failure to execute member investment decisions (DC)</li> <li>- Failure to provide members with appropriate investment options (DC)</li> </ul>	<ul style="list-style-type: none"> <li>- Untimely and/or incorrect payment of benefits due under the scheme</li> <li>- Member leaving service option forms not issued within statutory timescales</li> <li>- Untimely or erroneous communication with members/beneficiaries and sponsor</li> <li>- Unsatisfactory service towards members and beneficiaries due to insufficient or insufficiently competent staff</li> </ul>	<ul style="list-style-type: none"> <li>- Failure to put in place appropriate default investment strategy (DC)</li> <li>- Failure to provide members with appropriate investment options (DC)</li> <li>- Member invested in inappropriate investment funds (DC)</li> <li>- Failure to fully insure death in service benefits in line with the benefits payable under the terms of the pension scheme</li> <li>- Member communications do not effectively manage benefit expectations</li> <li>- Non-compliance with national and international laws and</li> </ul>	<ul style="list-style-type: none"> <li>- All previous examples at outsourced activities of the IORP</li> <li>- Service provider does not comply with its obligations towards members and beneficiaries laid down in the outsourcing agreement</li> </ul>	

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
			regulations - Excessive costs and charges		
<b>(5) Damage to Physical Assets</b> Losses arising from loss or damage to physical assets from natural disaster or other events.	- Staff (intentionally or unintentionally) damages physical assets - Malfunctioning appliance causes fire	- Staff (intentionally or unintentionally) damages physical assets - Malfunctioning appliance causes fire	- Staff (intentionally or unintentionally) damages physical assets - Malfunctioning appliance causes fire	- Staff (intentionally or unintentionally) damages physical assets - Malfunctioning appliance causes fire	- External disaster (flood/fire)
<b>(6) Business disruption and system failures</b> Losses arising from disruption of business or system failures.	- Breakdown of IT infrastructure and communications - Breakdown of payment systems and interface with bank infrastructure - Breakdown of internal/external reporting and performance systems	- Breakdown of IT infrastructure and communications - Breakdown of payment systems and interface with bank infrastructure - Breakdown of internal/external reporting and performance systems	- Breakdown of IT infrastructure and communications - Breakdown of internal/external reporting and performance systems	- Breakdown of IT infrastructure and communications - Breakdown of payment systems and interface with bank infrastructure - Breakdown of internal/external reporting and performance systems	
<b>(7) Execution, Delivery &amp; Process Management</b> Losses from failed operations processing or process management, from relations with counterparties and vendors & suppliers.	- Key operational requirements are missed, like the timeline for the investment of contributions - Errors in trading execution - Errors in settlement of transactions - Errors in asset valuation - Failure to comply with decision procedures on investments, including ESG/sustainability - Substandard quality of performance reporting	- Member records not complete or inaccurate - Lack of transparency in own systems and/or systems operated by service providers - Non-compliance with internal governance codes	- If the IORP is set up under a Trust Deed then the trustees might fail to follow what the Trustees specifies, or might fail to understand what the terms of the Trust Deed means. - Insufficient monitoring of third party service providers - No clear record of how and why important financial management or significant decisions were at by the trustees - Lack of engagement of	- All previous examples at outsourced activities of the IORP - Service provider does not comply with its obligations relating to execution, delivery and process management laid down in the outsourcing agreement	- Sponsor is late in remitting contributions to the IORP

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
	and accounting - Wrong decisions on risk mitigation in dealing with derivatives - Failing processed for maintenance and legal responsibility in relation to (direct) property investments - Non-compliance with internal governance codes		appropriate advisors - Failure to identify and manage conflicts - Failure to maintain the confidentiality of the schemes affairs - Failure to secure competitive and value for money investment and other services - Lack of compliance with legislation (or misinterpret legislation) - Administrator not registered with the national supervisory authority		
			- Lack of quality and/or breakdown of internal models for: risk assessment, investment decision support and analysis, performance measurement and cash flow analysis and forecasting. - Non-compliance with internal governance codes - Non-compliance with national and international laws and regulations - Inappropriate actuarial valuation methods and assumptions		



ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
Related risks:					
<b>II REPUTATIONAL RISK</b> Losses resulting from damages to an IORP's reputation.	Reputational risk may arise from any operational risk by resulting in a loss of reputation of the IORP, instead of a direct financial loss for the IORP, sponsor(s) and/or members and beneficiaries, but reputational losses can derive from broader risks than just operational risk. Reputational losses may result in future financial losses, e.g. if the reputational damage leads to a reduced market share of the IORP. Not-for-profit IORPs - which do not operate on a market per se - may lose their privileged position under national social and labour law.				
<b>III STRATEGIC RISK</b> Losses resulting from the strategic choices/ decisions of the IORP.	- Strategic decisions relating to investments that (in hindsight) proved not to pay off	- Strategic decisions relating to staff that (in hindsight) resulted in insufficient or insufficiently competent staff - Strategic decision to introduce a more complex pension plan involving more choice for and interaction with plan members that resulted in operational difficulties	- Inadequate objectives and strategies - Inappropriate strategic asset allocation decisions	- All previous examples at outsourced activities of the IORP - Service provider does not comply with its obligations relating to strategic decisions laid down in the outsourcing agreement	
<b>IV REGULATORY / POLITICAL RISK</b> Losses resulting from adverse changes in the regulatory framework within which the IORP is operating. This could involve a change in either the general regulatory framework applicable to the IORP or in its own relationship with its specific regulator/supervisor (or both).					- A negative shift in regulation or government policy - A change in national regulations affecting transfer values of IORPs - EU imposes Solvency II valuation standards and capital requirements on IORPs

## Annex 3: Supervisory guidance on outsourcing risk

### 1. Definitions

- 1.1. Outsourcing is an arrangement of any form between an IORP and a service provider, by which the service provider performs a process, a service or an activity which would otherwise be performed by the IORP itself. An IORP should establish whether an arrangement with a third party falls under the definition of outsourcing. The outsourcing is related to the core business of the IORP. Therefore, the acquisition of services (e.g. advice of an architect regarding the premises, legal representation in front of the court and administrative bodies), goods (e.g. purchase of office supplies, or furniture) or utilities (e.g. electricity, gas, water, telephone line) that are not normally performed by the IORPs are not considered outsourcing (Recital 61 of the IORP II Directive).
- 1.2. Important and critical functions or activities: Key functions that are included in the system of governance of IORPs are always to be considered as important and critical functions. In all other respects, IORPs are responsible for determining whether the relevant function or activity is important and critical. The issue of whether a function or activity is important and critical would be assessed on a case-by-case basis.
- 1.3. Service provider means a third party entity that is undertaking an outsourced process, service or activity, or parts thereof related to the core business of the IORP, under an outsourcing arrangement. The service provider itself may or may not be a regulated entity.
- 1.4. Sub-outsourcing means a situation where the service provider under an outsourcing arrangement further transfers a process, a service or an activity, or parts thereof, to another service provider.

### 2. Supervision of IORPs' assessment and management of outsourcing risks

- 2.1. In line with guidance 3.2 of the supervisory opinion, NCAs should analyse IORPs' outsourcing risks within their supervisory review process, including as part of registering or authorising new IORPs, off-site activities or on-site inspections.
- 2.2. As part the supervision of IORPs' operational risks, NCAs should verify in particular that outsourcing arrangements do not hamper the ability of an IORP to meet its regulatory requirements and its legal and/or contractual obligations. For example, outsourcing should not undermine the continuous and satisfactory service to members and beneficiaries. An outsourcing IORP should be able to influence the actions of its service provider and to give instructions at any time.
- 2.3. NCAs should check that outsourcing does not hinder their supervisory powers, functions and legal obligations. For instance, NCAs should prescribe that the written agreement on outsourcing stipulates that the service provider shall grant full access to the Competent Authority of all relevant data. NCAs should have the unrestricted right to conduct on-sight inspections at a service provider's premises. NCAs should be able to issue instructions to service providers via the outsourcing IORP without being compromised.
- 2.4. NCAs should verify that an IORP assesses the materiality of its outsourcing arrangements which may include but are not limited to:
  - the impact of the outsourcing arrangement on its finances, reputation and operations;
  - IORP's ability to maintain appropriate internal controls and meet regulatory and legal requirements, particularly if the service provider were to experience problems;

- IORP's net risk does not materially increase as a result of outsourcing compared to if the IORP carried out the function or the activity itself;
  - the risk of potential loss, of access to important data; and
  - the degree of difficulty and time required to find an alternative service provider or to bring the business activity 'in-house'.
- 2.5. IORPs should also document the results of their analysis of outsourcing risk including when they conduct the Own-Risk Assessment (Article 28 of the IORP II Directive).
- 2.6. NCAs should verify the completeness and accuracy of the information regarding outsourcing provided by IORPs (Article 50 of the IORP II Directive). Such information would include a general written policy on outsourcing (Article 21 of the IORP II Directive) that is:
- Approved by the persons effectively running the IORP;
  - Consistent with the IORP's strategy; and
  - Regularly reviewed and adjusted accordingly in case of material changes in the area of outsourcing.
- 2.7. Elements of the outsourcing policy include but are not limited to:
- Review procedures for the identification, assessment, management and mitigation of outsourcing risk and of potential conflicts of interest;
  - Review procedures for the assessment of the service provider's ability to provide the services outsourced;
  - Specification of the internal units or individuals that are responsible for monitoring and managing each outsourcing arrangement.
  - Documentation and record keeping of activities related to outsourcing.
  - Duty to develop emergency plans for outsourced important and critical functions or activities that deal with problems occurring with the service provider.
- 2.8. The outsourcing policy should specify each activity that is outsourced, with a clear distinction between key functions and other activities e.g. fiduciary management, and identification of critical and important activities and reasoning.
- 2.9. If necessary for the purposes of supervision, NCAs may ask IORPs to provide additional information on their risk analysis, in particular for important or critical outsourcing arrangements.
- 2.10. IORPs should be transparent with respect to its outsourcing arrangements and always disclose to NCAs any matter, which could materially and adversely affect the financial soundness of the IORP and its ability to fulfil its obligations to its members and beneficiaries. All books and records pertaining the important and critical functions or other activities being outsourced and draft of outsourcing agreement should be made available to NCAs upon their request.
- 2.11. Outsourcing IORPs should notify in a timely manner new or significant changes to their outsourcing arrangements to NCAs (Article 31 of the IORP II Directive).
- 2.12. When a key function or the management of an IORP is outsourced, NCAs should be informed before the agreement in respect of any such outsourcing enters into force in order to consider the prudential implications of the proposed outsourcing and take appropriate action if necessary.
- 2.13. Examples of information to provide NCAs in the event of important and critical functions or activities being outsourced include but are not limited to:

- Function or service that is being outsourced;
  - Name and address of the service provider (indicating whether this firm is part of the regulated entity's group and its regulatory status, if any);
  - Location where the outsourced activity will be carried out whether in the home state or outside of it;
  - Date of commencement and expiration of outsourcing agreement;
  - Main reasons for outsourcing the specific function or activity; and
  - The name of the competent person at the service provider side.
- 2.14. Notification to NCAs of the premature termination of an outsourcing agreement should, at a minimum, include the name of the service provider, date of termination, reason for termination and how the outsourced function or activity will be performed.
- 2.15. If an outsourcing IORP fails to meet the supervisory requirements, the NCAs must take the necessary and appropriate measures. Where concerns are identified that lead to the assessment that IORPs do not any longer have robust governance arrangements in place or do not comply with regulatory requirements, NCAs should take appropriate action, which may include limiting or restricting the scope of the functions outsourced or requiring exit from one or more outsourcing arrangements. In particular, taking into account the need of the IORP to operate on a continuous basis, cancellation of contracts could be required, if the supervision and enforcement of regulatory requirements cannot be ensured by other measures.

### 3. Holistic assessment of IORPs' outsourcing risk

- 3.1. NCAs should conduct a holistic risk assessment of IORPs' outsourcing risk seeking to evaluate all significant risks resulting from outsourcing of important and critical functions or activities. Examples of such risks to be taken into account include but are not limited to:
- the operational risk posed by the outsourcing arrangement;
  - reputational risk resulting from outsourcing;
  - concentration risks within the IORP, caused by multiple outsourcing arrangements with a single service provider or connected service providers or multiple outsourcing arrangements within the same business area;
  - concentration risks at a sectoral level, e.g. where multiple IORPs make use of a single or small group of service providers; where concentration risks are identified, NCAs should monitor the development of such risks and evaluate their potential impact on other IORPs;
  - the extent to which the outsourcing IORP controls the service provider or has the ability to influence its actions or vice versa; and
  - conflicts of interest between the IORP and the service provider.

### 4. Accountability of the IORP

- 4.1. In accordance with the prudential and regulatory conditions to proportional supervision (see also Q&A on proportional supervision of IORPs), NCAs should ensure and verify that outsourcing IORPs are ultimately responsible for the effective management of risks arising from outsourcing (Article 20 of the IORP II Directive). The outsourcing of the IORP's activities to third parties does not mean "outsourcing" the IORPs' responsibility to comply with its obligations with respect to these activities. IORPs should establish clear

responsibility in-house for monitoring the conduct of the service provider and for delivering respective reports to the management body.

4.2. The following list provides non-exhaustive guidance to NCAs on the areas for which the outsourcing IORP remains ultimately responsible:

- Approving and regularly reviewing of the outsourcing policies;
- Approving of frameworks for reporting to the management body on matters relating to outsourced activities;
- Ensuring that an assessment takes place on how the IORP's risk profile will be impacted by the outsourcing of important and critical functions or activities;
- Approving the outsourcing of an important and critical function or activity;
- Verifying that an assessment of service providers is conducted; and
- Taking or authorising appropriate action if it appears that the service provider may not be carrying out or cannot carry out the outsourced important and critical functions or activities effectively or in compliance with applicable legal and regulatory requirements.

## **5. Considering the nature of the outsourcing relationship**

5.1. In supervising IORPs' outsourcing risks, NCAs should pay specific attention to the nature of the relationship of the outsourcing IORP with different types of service providers. The outsourcing of IORPs' activities can be broadly summarised in the following four situations:

- i. The sponsoring undertaking provides services to the IORP (e.g. IT services)
- ii. The service provider of the IORP's outsourced activities is owned by the IORP (e.g. asset management)
- iii. The service provider of the IORP's outsourced activities is owned by the IORP (e.g. insurance undertaking)
- iv. There is no connection between the outsourcing IORP and the service provider of the IORP's outsourced activities

5.2. In situations i) to iii), NCAs should verify that the performance of the outsourced key function or other activity of the IORP is not impaired by such arrangements. In these cases, outsourcing is not necessarily different from outsourcing to an unconnected service provider as described in situation iv). More flexibility in the selection process may be permitted, but it should not be seen as automatically requiring less care and oversight than outsourcing to an unconnected service provider.

5.3. In the first three cases, NCAs should take specific circumstances into consideration, such as the extent to which the outsourcing IORP controls the service provider or has influence on its actions (and vice versa). NCAs should therefore check that:

- The selection of the service provider by the outsourcing IORP is based on objective reasons
- The conditions of the outsourcing arrangement are set at arm's length and explicitly deal with conflicts of interest that such outsourcing may entail
- The regular review of the outsourcing arrangement e.g. conflicts of interest, service continuity and satisfaction of members and beneficiaries

5.4. Where IORPs have no employees apart from the persons effectively running the IORP (e.g. board of the IORP) and have fully outsourced the key functions to the service provider owning the IORP (situation iii), NCAs should assess:

- The level of independence of the persons effectively running the IORP from the management board of the service provider; and
- If the outsourcing is only operational and does not also cover the definition of the IORP's strategy

## **6. Due diligence process for the selection of service providers**

6.1. Regardless of the nature of the IORP's relationship with its service providers, NCAs should verify that outsourcing IORPs conduct appropriate due diligence in selecting its service providers.

6.2. According to Article 31 of the IORP II Directive, IORPs shall ensure the proper functioning of the outsourced activities inter alia through the process of selecting a service provider. Thus, NCAs should require outsourcing IORPs to perform in writing a due diligence assessment of a service provider before entering into the initial outsourcing agreement in order to ensure that the service provider has appropriate and sufficient ability, capacity, resources and organisational structure to perform the outsourced key function or any other activity in a reliable and professional manner over the duration of the proposed contract.

6.3. Examples for NCAs to verify IORPs' due diligence process in the selection of service providers include but are not limited to:

- human, financial and technical resources (including information technology systems) to effectively undertake the outsourced tasks;
- ability to safeguard the confidentiality, integrity and availability of information entrusted;
- corporate governance, risk management, security, internal controls, reporting and monitoring processes;
- reputation, complaints or pending litigation;
- business continuity arrangements and contingency plans;
- reliance on and success in dealing with sub-contractors.

## **7. Formalised outsourcing arrangement**

7.1. Regardless of the nature of the IORP's relationship with service providers, NCAs should verify that outsourcing IORPs have formalised their outsourcing arrangement with service providers in the form of a written agreement between the IORP and the service provider (Article 31 of the IORP II Directive). Such written contract between the outsourcing IORP and its service provider should at least contain:

- A clear definition of the function or activity that is to be outsourced.
- The specification and documentation of the precise requirements concerning the performance of the service. The service provider's ability to meet performance requirements in both quantitative and qualitative terms should be assessable in advance.
- A definition and specification of the respective rights and obligations of the IORP and the service provider. This should also serve to ensure compliance with laws and supervisory regulations.



- The inclusion of the obligation of the service provider to identify, disclose, monitor and manage conflicts of interest.
- The protection of confidential information and the obligation of the service provider to notify the IORP in respect of any breach in data and information security.
- The authority of the IORP to control and issue instructions to the service provider.
- The obligation of the service provider to allow the IORP full and unrestricted rights of inspection and auditing of its data.
- The obligation on the service provider to immediately inform the IORP, of any material changes in circumstances which could have a material impact on the continuing provision of services.
- The inclusion of provisions allowing the outsourcing IORP to cancel the contract by contractual notice of dismissal or extraordinary notice of cancellation if so required by the supervisory authority.
- The inclusion of provisions allowing the outsourcing IORP to transfer the outsourced function to another service provider or the reincorporation into the IORP (e.g. in-house investment).

7.2. NCAs should also verify that the outsourcing agreement specifies whether or not **sub-outsourcing is permitted**. If that is the case, NCAs should check that the IORP takes into account:

- **the risks associated with sub-outsourcing, including the additional risks that may arise if the sub-contractor is located in a third country or a different country than the service provider;**
- **the risk that long and complex chains of sub-outsourcing reduce the ability of an IORP to oversee the outsourced function or activity and the ability of the competent authority to effectively supervise them.**

7.3. For outsourced activities involving the handling or transfer of sensitive data (e.g. cloud or other ICT outsourcing), NCAs should verify compliance with appropriate information security standards

## **8. Assessment of the conflicts of interest**

8.1. NCAs should verify that outsourcing IORPs properly identify, assess and take appropriate measures to manage the conflicts of interests arising from outsourcing its activities (Articles 24 and 28 of the IORP II Directive). In doing so, they should consider different conflicts of interest depending on the nature of the relationship between the outsourcing IORP and the service provider. Conflicts of interest may also arise when the same person or organisational unit within the IORP performs multiple tasks, for example, when a key function holder performs multiple functions at the same time. Outsourcing-specific conflicts of interest may especially arise in case of IORPs outsourcing key functions to the sponsoring undertaking. According to Articles 24 and 28 IORP II Directive the single person or organisational unit (within the IORP) shall be different from the one carrying out a similar key function in the sponsoring undertaking. If allowed by national law IORPs can exceptionally carry out key functions through the same person or organisational unit as in the sponsoring undertaking, provided the IORPs can explain how they prevent or manage any conflicts of interest with their sponsoring undertaking<sup>30</sup>.

---

<sup>30</sup> To be precise: The person or organisational unit within the IORP being responsible for the evaluation and assessment of the performance of the outsourced key function can only be the same one carrying out a similar key function in the sponsoring undertaking, when the IORP can explain how it prevents or manages any conflicts of interest with its sponsoring undertaking.

- 8.2. For any identified conflict of interests, NCAs should check that the IORP's decision on the outsourcing arrangement and its oversight are performed with a sufficient level of objectivity in order to appropriately manage conflicting interests. To this end, NCAs should oversee if an IORP has ensured that the conditions, including financial conditions, for the outsourced service are set at arm's length.
- 8.3. Moreover, NCAs should check that the internal audit function of outsourcing IORPs carry out an independent review of outsourced activities to evaluate the adequacy and effectiveness of the IORP's internal control system and other elements of the system of governance, including outsourced activities (Article 26 of the IORP II Directive).
- 8.4. NCAs should verify the outsourcing IORP's audit plan and programme which should include, in particular, the outsourcing arrangements of important and critical functions or activities, including the appropriateness of data protection measures, controls, risk management and business continuity measures implemented by the service provider.
- 8.5. With regard to outsourcing, the internal audit function should at least ascertain:
- that an IORP's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk appetite and with the decisions of the management board;
  - the adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risks remain within the risk appetite;
  - the risk tolerance limits, risk management and control procedure of the service provider are in line with an outsourcing IORP's strategy;
  - the appropriate involvement of governance bodies;
  - the appropriate monitoring and management of outsourcing arrangements;
  - Formal follow-up procedure to all audit recommendations and findings and record keeping of their effective and timely resolution.
- 8.6. NCAs should also verify that appropriate and adequate skills and knowledge are used to perform relevant audits and/or assessments effectively, especially where the outsourcing arrangement carries a high level of technical complexity e.g. cloud outsourcing.

## **9. Assessment of the business continuity management**

- 9.1. When IORPs outsource important and critical functions or activities, NCAs should verify that both the outsourcing IORP and its service provider have established and maintained specific business contingency plans for each outsourcing arrangement in order to address the potential consequences of a business disruption or other problems at the service provider.
- 9.2. Examples of what business contingency plans can comprise include but are not limited to:
- Specification of the service provider's measures for ensuring the continuation of the outsourced service in the event of problems;
  - The obligation of the service provider to inform the IORP of material changes to its business continuity plans;
  - Definition of timeframes for the execution of regular test runs and exercises in accordance with the risks of the relevant unit or process;
  - A clear definition of tasks, accountabilities and duties to inform in the event of a business disruption or other problems at the service provider;

- A termination and/or exit strategy in the event that the service provider can no longer effectively carry out the outsourced important and critical function or activity.
- Estimation of the costs of alternative options that include changing the service provider or moving the outsourced activity back to IORP.

## 10. Cross-border outsourcing<sup>31</sup>

10.1. Cross-border outsourcing in the EEA has important implications for an effective prudential supervision. NCAs should therefore consider additional issues when assessing cross-border outsourcing with respect to:

- Legal and regulatory profile of the foreign jurisdiction:** NCAs should consider whether their powers to issue orders or instructions to the outsourcing IORP can be reliably enforced without being compromised by instructions issued by other supervising authorities to the service provider of the outsourced function or activity.
- Right to request information from service providers about outsourced key functions or any other activity:** To ensure the right to request information from service providers about outsourced key functions or any other activity, the NCAs should prescribe that the written agreement on outsourcing stipulates that the service provider of the outsourced function or activity shall grant access to the Competent Authority of the outsourcing IORP for all relevant data in its possession and that the Competent Authority of the outsourcing IORP should be able to obtain promptly from the service provider any relevant books, records and other information relating to the outsourced activity, regardless whether the service provider is a regulated or unregulated entity.
- Right to carry out on-site inspections:** NCAs should prescribe that the written agreement on outsourcing stipulates that the service provider of the outsourced function or activity will not oppose to an on-site inspection on request of the Home Competent Authority should the case arise. This contractual obligation should provide the Home Competent Authority of the outsourcing IORP with sufficient legal certainty to have access to the premises of the service provider of the outsourced function or activity, where necessary.

10.2. In Member States where outsourcing outside of EU/EEA is permitted, NCAs should pay even greater supervisory attention to the outsourcing to third countries. They should follow, to the extent possible, considerations highlighted in points i) to iii).

10.3. NCAs should also verify that outsourcing IORPs may additionally assess the economic, legal and political conditions of the third country that might adversely impact the service provider's ability to perform effectively for the outsourcing IORP. NCAs should also take special care to possible data protection risks, compliance risks as well as risks concerning the effective supervision of outsourced activities located outside the EEA.

10.4. Without prejudice to the GDPR, IORPs, when outsourcing abroad, including to third countries, should take into account differences in national provisions regarding the protection of data. The outsourcing agreement should include the obligation of the service provider to protect confidential, personal or otherwise sensitive information and comply with all legal requirements regarding the protection of data that apply to the IORP.

<sup>31</sup> These recommendations are based on Part III Chapter 3 of the Annex to the Board of Supervisors Decision on collaboration of the competent authorities of the Member States of the European Economic Area (EEA) with regard to Directive (EU) 2016/2341 of the European Parliament and of the Council of 14 December 2016 on the activities and supervision of institutions for occupational retirement provision (IORPs).

## Annex 4: Supervisory guidance on cyber risk

### 1. Definition and classification

- 1.1. To promote a common supervisory culture with respect to the supervision of IORPs' management of cyber risks, NCAs should understand cyber risk to mean any risks (of loss, disruption or damage) that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information. Cyber risks include both internal risks (e.g. from staff) and external risks (e.g. hacking). The cyber risk related to an IORP's information and communication technologies is one of the many operational risks.
- 1.2. In addition, cybersecurity refers to strategies, policies, and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities, and policies regarding the security of an IORP's operations.
- 1.3. Finally, cyber footprint constitutes the digital presence of all the parties involved in the IORP, and service providers (e.g. cloud service providers), which creates vulnerabilities for the IORP.

### 2. Supervision of IORP's management of cyber risk

- 2.1. The assessment of IORP's cyber risks should be considered by NCAs as an integral part of their ongoing supervision. NCAs should regularly review whether IORPs incorporate cyber risk in their risk management system to foster resilience against cyber risks, protecting the data of members and beneficiaries and promoting operational security.
- 2.2. NCAs should use a range of assessment techniques and methods available to reflect the specific breadth, depth of coverage, or maturity sought in a given assessment. A non-exhaustive "toolkit" for cybersecurity assessments might include among other techniques and methods: on-site inspections, desktop reviews, self-assessments, threat-based penetration testing, technical reviews, thematic reviews, and cybersecurity exercises<sup>32</sup>. These tools can be used either singly or in combination.<sup>33</sup>
- 2.3. When planning and designing programs for conducting cybersecurity assessments, NCAs should establish clear assessment objectives and communicate those objectives to the IORPs. This approach provides clarity of motivation to both assessor and assessed IORP.
- 2.4. Not only should NCAs raise awareness and educate IORPs on cyber risks, encouraging IORPs to take the cyber risk very seriously owing to the high impact and possible disruption in case of cyber incidents. NCAs need to be aware of their own exposure to cyber risk.
- 2.5. NCAs should in this context request IORPs to report unsolicited on devastating cyber incidents. NCAs should use their overall oversight position to gather information on

---

<sup>32</sup> Examples for assessment techniques and testing methods:

- TIBER-EU:

[file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/Q59M7D3U/ecb.tiber\\_eu\\_framework.en.pdf](file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/Q59M7D3U/ecb.tiber_eu_framework.en.pdf)

- TIBER-NL: [file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/Z3AJ8COQ/TIBER-NL%20Guide%20Second%20Test%20Round%20final\\_tcm46-365448.pdf](file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/Z3AJ8COQ/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf)

- CBEST threat-led assurance testing:

<file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/Z3AJ8COQ/cbest-implementation-guide.PDF>

<sup>33</sup> See BaFin's Circular 10/2018 Supervisory Requirements for IT in Insurance Undertakings: [file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/LLDVDTKK/dl\\_rs\\_1810\\_vait\\_va\\_en.pdf](file:///C:/Users/kalakaniha/AppData/Local/Microsoft/Windows/INetCache/IE/LLDVDTKK/dl_rs_1810_vait_va_en.pdf).

systemic and evolving cyber risks and disseminate that information to IORPs.

### **3. Review of integration of cyber risk in IORPs' overall risk management**

3.1. NCAs should evaluate whether IORPs fully integrated operational risk in their system of governance and risk management system. Therefore, NCAs should consider in their supervisory review the following key elements of IORP's risk management:

#### **(1) Strong risk management culture**

3.2. NCAs should verify that the Board promotes a strong risk management culture, which also recognises that staff at all levels have important responsibilities in ensuring the IORP's cybersecurity.

3.3. Important elements for the Board to achieve this include but are not limited to:

- cultivating awareness of and commitment to cybersecurity;
- providing staff with training appropriate to their role at an adequate frequency;
- clearly defining the roles and responsibilities and facilitating the performance of staff implementing, managing, and overseeing the effectiveness of the risk management system in general and cybersecurity strategies in particular.

#### **(2) Risk-management system**

3.4. NCAs should check that IORPs have in place an effective and well-integrated risk-management system, identifying, measuring, monitoring, managing and reporting risks and their interdependencies. The risk-management system should be complemented by an effective internal control system and facilitated by a risk-management function.

3.5. NCAs should verify that the management of cyber risks is fully integrated in the IORP's overall risk-management system. This recognises that an IORP's cybersecurity strategies are likely to overlap with the policies, procedures, and controls that it has established to manage other types of risks, especially operational risks. For example, cyber risk should also be a consideration in an IORP's physical security framework (e.g., to limit access to critical information and communication technology infrastructure) and its human resource policies (e.g., to manage "insider" threats).

3.6. Cyber risk management comprises the protection of data both when at-rest and when in-transit throughout data lifecycle.

3.7. It involves assessing the cyber risk, align it with its risk tolerance, then take appropriate measure to:

- be more resilient against attacks;
- detect attacks;
- be able to respond timely; and
- recover in case of an attack.

3.8. Analogous to other operational risks, cybersecurity should first and foremost be safeguarded at the operational level, including at service providers to which activities have been outsourced. Operational units are primarily responsible for safeguarding confidentiality of data, integrity of information and systems and the availability of technologies used for their activities.

3.9. NCAs should verify that the IORP's risk-management function monitors and challenges the (cyber) risk reporting of the operational units. Where the risk-management function constitutes a unit, rather than a single person, the IORP may consider designating a specific information security officer with specific experience with and knowledge of cybersecurity.

3.10. NCAs should also check that the internal audit function regularly evaluates the effectiveness of the risk-management system, including the management of cyber risk.

### **(3) Approval, review and implementation of risk management system**

3.11. NCAs should verify that IORPs establish and apply written policies in relation to risk management, including strategies, processes and reporting procedures for the risk-management system. The written policies should be subject to prior approval by the IORP's Board and should be reviewed at least every three years and in view of any significant change in the system or area concerned.

3.12. NCAs should check that the IORP's Board is ultimately responsible for the implementation and reviews of the risk-management system, also covering cyber risks. As such, the Board should include knowledge and skills appropriate to its oversight role with respect to the management of cyber risks. The Board should also not refrain from seeking expert advice and information on cyber security.

3.13. Particularly cybersecurity strategies may benefit from the periodic review of the risk-management system, as cyber risk may evolve rapidly. The review should take into account the lessons learned from cyber events, both 'successful' ones and near misses, that have occurred within and outside the organisation, the outcomes of cybersecurity assessments and testing programmes, internal and external audit report and evaluations by the NCA.

### **(4) Risk tolerance statement**

3.14. When reviewing IORPs' risk tolerance statement approved by the Board, NCAs should verify that the statement tolerance limits relating to cyber risks.

### **(5) Identification and assessment**

3.15. NCAs should check that the risk-management system ensures the identification and assessment of cyber risks inherent in the IORPs' activities, processes and systems. To that end, it should make use of available tools for identifying and assessing cyber risks, such as mappings of processes, including access rights, technologies/systems and operational functions in combination with risk analyses and assessments.

3.16. Cyber threats to be considered should include those, which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. A IORP should consider threats to the confidentiality, integrity, and availability of its business processes, data of its beneficiaries and members, and to its reputation. Threats arising from both internal and external sources, such as employees or third-party service providers, respectively, should be considered.

3.17. A cyber risk profile identifies key operational areas exposed to cyber risk, arising from both internal and external sources, focussing on the following categories:

- Technologies and connection types: Certain technologies and connection types may pose a higher cyber risk depending on the complexity and maturity, connections, and nature of the specific technology products or services of the IORP. For example, it may be appropriate for an IORP to assess the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the presence and number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices by IORP's staff;
- Delivery channels: Some delivery channels for products and services may pose a heightened cyber risk depending on the nature of the specific product or service offered. Cyber risk increases as the variety and number of delivery channels increases. For



example, online and mobile delivery channels may present increased levels of risk to an IORP.

- Organisational characteristics: Those characteristics include the number of users with privileged access, changes in information technology (IT) environment, locations of operations and data centres (including legacy systems), and reliance on third party service providers, including cloud service providers.
- External threats: External threats, particularly the volume, type and sophistication of attacks (attempted or successful), reflect and affect an IORP's cyber risk exposure.

- 3.18. The identification of operational functions and supporting processes and the conduct of a risk assessment enhance the understanding of the importance of each function and supporting processes, and their interdependencies, in performing the functions. A classification of identified operational functions and processes in terms of criticality, should guide the prioritisation of its protection, detection, response, and recovery efforts.
- 3.19. An operational impact analysis for cyber risks identifies threats, vulnerabilities, likelihoods and impacts to establish the risks and prioritization of risk responses.<sup>34</sup>
- 3.20. An identification and maintenance of a current record of both individual and system access rights is allows IORPs to ensure that access rights are no broader than necessary, and to facilitate identification and investigation of anomalous activities.
- 3.21. An identification and maintenance of a current inventory of its information assets and system configurations, including interconnections and dependencies with other internal and external systems (for example third party service providers) allows IORPs to know at all times the information assets that support its operational functions and processes. A risk assessment of those assets should be carried out in order classify them in terms of criticality.
- 3.22. NCAs should check that cyber risks appears in the IORP's risk register. They should also review that IORPs assess and understand their cyber footprint, i.e. the extent of the digital presence of all the parties involved in the IORP, and the risk posed by these parties. These can be both internal and external and include the sponsoring employers, other advisors (auditor, actuaries, investment manager or consultant, lawyers), members (especially if offering online access) as well as service providers.

## **(6) New activities, processes and systems**

- 3.23. NCAs should verify that the identification and assessment of risks, including cyber risks, is part of the IORPs' decision-making process relating to new activities, processes and systems.
- 3.24. Many of IORP's systems and processes are directly or indirectly interconnected with numerous third parties, including cloud service providers and providers of outsourced services. The cybersecurity of those providers may significantly affect the cyber risk that an IORP faces.
- 3.25. Due diligence should be carried out before engaging with third-party service providers in order to verify that they have implemented appropriate administrative, technical, and physical controls and measures to protect and secure the confidentiality of data, the integrity of information and systems and the availability of technology-driven key operational processes.

## **(7) Monitoring and reporting**

---

<sup>34</sup>

General information to BIA see: ISO/TS 22317:2015: <https://www.iso.org/standard/50054.html> .

- 3.26. NCAs should check that the IORPs' risk-management system contains processes to regularly monitor risk profiles and material exposures to losses, including processes for cybersecurity monitoring to rapidly detect cyber incidents.
- 3.27. They should review that the IORP periodically evaluates the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises. The testing and auditing functions should be appropriately independent from staff responsible for implementing and managing the cybersecurity program.
- 3.28. The recognition of signs of a potential cyber incident, or detection that an actual breach has taken place, is essential to strong cybersecurity. Early detection provides IORPs with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the impact of the attack – for example, by preventing an intruder from gaining access to confidential data or exfiltration of such data.
- 3.29. A IORP's detection capabilities should also address misuse of access by third-party service providers, potential insider threats, and other advanced threat activity.
- 3.30. Testing programs aim to validate the effectiveness of all elements of its cybersecurity framework. The results of the testing program are used to support the ongoing improvement of cybersecurity. The Board should be appropriately involved in such testing programs (e.g. as part of crisis management team) and informed of test results.
- 3.31. Available state-of-the-art testing methodologies include the following elements<sup>35</sup>:
- Vulnerability Assessment;
  - Scenario-based testing;
  - Penetration tests; and
  - Red team tests.
- 3.32. NCAs should check that the Board regularly appraises the IORP's cyber risk profile to ensure that it remains consistent with the IORP's risk tolerance as well as the IORP's overall objectives. This also means that the Board should receive regular updates on cyber risks, incidents and controls.

## **(8) Control and mitigation**

- 3.33. NCAs should check that the IORPs' risk-management system includes a strong risk control environment in which appropriate risk mitigation and/or transfer strategies are implemented.
- 3.34. An IORP should put in place sufficient and proportionate controls to minimise the risk of a cyber incident occurring. It should work with all relevant parties (e.g. in-house functions, third party service providers and sponsoring undertakings) to define these controls.
- 3.35. Examples of controls to enhance cybersecurity include but are not limited to:
- acceptable use of devices (including removable and personal devices), email and internet (including social media);
  - use of passwords and other authentication;
  - home and mobile working;
  - data access, protection (including encryption), use and transmission, in line with data

---

<sup>35</sup> See IAIS Draft Application Paper on Supervision of Insurer Cybersecurity, Page: 28 ([file:///H:/Dokumente/VA%2054/EbAV%20II-RL/PSC%20PG/Documents%20for%20draft%20guidance/cyber%20risks/Draft\\_Application\\_Paper\\_on\\_Supervision\\_of\\_Insurer\\_Cybersecurity.pdf](file:///H:/Dokumente/VA%2054/EbAV%20II-RL/PSC%20PG/Documents%20for%20draft%20guidance/cyber%20risks/Draft_Application_Paper_on_Supervision_of_Insurer_Cybersecurity.pdf)).

protection legislation and guidance.

## **(9) Continuity of activities & contingency plans**

- 3.36. NCAs should verify that IORPs take reasonable steps to ensure continuity and regularity in the performance of the IORP's activities, including the development of contingency plans.
- 3.37. A written incident response and recovery plan indicates how the IORP will respond to and recover from any identified cyber incidents.
- 3.38. Elements to be contained in a written response plan would include but are not limited to:
- a scenario-based incident management on what to do after a cyber attack, data breach incident etc.;
  - the definition of clear roles and responsibilities in the event of an incident;
  - thorough assessment of the nature, scope and impact of a cyber incident;
  - containment of the incident and mitigation of its impact;
  - information on in-crisis communication that need to take place in the event of an incident (incident reporting procedure) including how and when reporting will be made to the board of management;
  - notification of internal and external stakeholders, (e.g., the supervisory authority, the affected beneficiaries and members, etc.);
  - resumption and recovery actions.
- 3.39. The response and recovery plan should be subject to review and improvement. It should be actively updated based on current cyber threat intelligence, information-sharing, and lessons learned from previous events.
- 3.40. Cyber incident recovery arrangements should be designed to enable IORPs to resume operations safely with a minimum of disruptions to beneficiaries, members and business operations. As an example, a IORP's recovery plan could provide to maintain an uncorrupted "golden copy" of critical data, to be used in the restoration of impacted systems and data.
- 3.41. The recovery of operations that are interrupted by a cyber incident should occur once operational stability and integrity are assured.
- 3.42. The recovery plan should include strategies and processes to rapidly isolate cyber incidents and compromised locations so as to mitigate the IORP's exposure to the new vulnerabilities detected.
- 3.43. As an IORP's systems and processes are often interconnected with the systems and processes of third parties, NCAs should check that the IORP understands its third party suppliers' incident response processes.
- 3.44. The recovery plan should provide for cyber incidents to be documented and major incidents to be followed by a post-incident review.

## **(10) Disclosure**

- 3.45. NCAs should check that the IORP's ORA document features the IORP's assessment of operational risk including cyber risks.<sup>36</sup> In the EIOPA Opinion on Governance Documents, EIOPA is of the opinion that NCAs should encourage IORPs to disclose the ORA document to relevant stakeholders in order to promote greater transparency on how they manage pension risks.

---

<sup>36</sup> Article 28 IORP II Directive (EU) 2016/2341.

#### **4. Cooperation and information sharing**

- 4.1. Cross-sectoral exchange of information between regulators as well as collaboration with other specialist public and private actors within and outside the financial sector contribute to improving the oversight of cyber risks.
- 4.2. NCAs should not only regularly coordinate and share relevant cybersecurity information among themselves (supervisory cooperation and collaboration in dealing with cyber risks) in order to achieve a better supervision of cyber risks. They are also advised to strengthen communication and partnership with the industry and other stakeholders, including cooperation with public and private communities, specialist regulators, working groups etc. to exchange relevant information on cybersecurity issues in order to better monitor cyber threats across the financial sector and help the entities to become more resilient against cyber attacks.
- 4.3. NCAs are also advised to strongly encourage IORPs to participate in security information-sharing platforms or forums to strengthen their cyber resilience.

#### **5. Proportionality**

- 5.1. While cyber security is necessary for all IORPs, there is no one-size-fits-all prescription for the supervision of IORPs cyber risks. Supervisory measures should be appropriate to attain the supervisory objectives and should not go beyond what is necessary to achieve those objectives. EIOPA's Questions and Answers regarding the proportional supervision of IORPs provide further detail.