EIOPA-BoS-19-247

10 July 2019

Opinion on the supervision of the management of operational risks faced by IORPs

1. Legal basis

1.1. The European Insurance and Occupational Pensions Authority (EIOPA) provides this Opinion on the basis of Article 29(1)(a) of Regulation (EU) No 1094/2010[1]. 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 Directive (EU) 2016/2341[2] (the IORP II Directive), in particular in relation to Articles 25, 28, 31 and 49 thereof.

1.3. This Opinion is addressed to the competent authorities (CAs), as defined in point (i) of Article 4(2) of Regulation (EU) No 1094/2010.

1.4. The Board of Supervisors has adopted this Opinion in accordance with Article 2(7) of its Rules of Procedure[3].

2. Context and objective

2.1. The IORP II Directive introduced new requirements for IORPs[4] to put in place effective risk management system, which include operational risk management, in accordance with Article 25. Furthermore, IORPs need to assess operational risks as part of their own-risk assessment, as set out in Article 28. Within the supervisory review process, as set out in Article 49, CAs are required to assess the risks IORPs

1 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.

2 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), OJ L 354, 23.12.2016, p. 37.

3 Decision adopting the Rules of Procedure of EIOPA's Board of Supervisors, https://eiopa.europa.eu/Publications/Administrative/EIOPA-BoS-11-002_EIOPA-BoS-Rules%20of%20Procedure-Rev3.f.pdf.

4 Including the occupational retirement provision business of life insurance undertakings subject to Article 4 of the IORP II Directive.

face and IORPs' ability to assess and manage those risks.

2.2. In Article 31(3) the IORP II Directive includes new provisions on the outsourcing of key functions and other activities specifying that outsourcing should not lead to unduly increasing IORPs' operational risk and should not discharge IORPs of their responsibility for that operational risk. Depending on their nature and size, IORPs may not have internal resources to manage all activities. Therefore, they tend to rely more on outsourcing, thereby exposing themselves to asymmetric information problems, which necessitate robust and effective governance to monitor and control any potential misalignments.

2.3. EIOPA conducted a mapping exercise among CAs that identified cyber risk as a challenging operational risk that requires further supervisory attention. This concern echoes G7 guidance recognising the continued pervasiveness of cyber risks and the need for sustained efforts to enhance cybersecurity in the financial sector.[5] The supervision of operational risks should be forward-looking by factoring in new market and regulatory developments such as the shift from defined benefit (DB) to defined contribution (DC) pensions, the emergence of new forms of IORPs, or reforms facilitating early pension access. Although new market and regulatory developments should generally improve occupational pensions, they may also result in greater complexity in terms of retaining supervisory oversight of the full range of activities performed and/or outsourced by IORPs to deliver the pensions of members and beneficiaries.

2.4. The objective of this Opinion is to promote consistent supervisory practices by providing CAs with guidance on the supervision of IORPs' management of operational risks, including the assessment and management of outsourcing and cyber risks.

2.5. This Opinion further aims to facilitate risk-based and proportionate supervision of IORPs. In this context, CAs may take into account the national specificities of the IORP sector to determine the requirements necessary for implementing this Opinion considering a risk-based and proportionate approach[6].

3. IORPs' operational risks

Definition and classification

3.1. Operational risk is defined as the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events.[7]

3.2. Operational risks include compliance/legal risks, but exclude reputational, strategic and political/regulatory risks. However, all three excluded risks are in many respects closely related to operational risk. For example, a political/regulatory risk could affect IORPs' existing activities, triggering legal risk, which would impact

[5] G7 Fundamental Elements of Cybersecurity for the Financial Sector, 11 October 2016, https://ec.europa.eu/info/system/files/cybersecurity-fundamental-elements-11102016_en.pdf

[6] For further guidance on risk-based and proportionate supervision: EIOPA (2017) A common supervisory culture, https://eiopa.europa.eu/Publications/Speeches%20and%20presentations/A%20Common%20Supervisory%20Culture.pdf

[7] In line with the definition in Article 13 of Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance, OJ L 335, 17.12.2009, p.1.

the operational risk. CAs should take into account these related risks when reviewing IORPs' assessment and management of operational risks.

3.3. IORPs may carry out the two core operational activities, pension administration and investment management, internally or delegate them to an external service provider. As operational risk may arise from internal activities, including within the IORP's management and key functions or from external events, operational risks can be further broken down in the following subcategories relating to[8]:

- 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. Annex 1 explains these subcategories in more detail and provides examples for each of them, distinguishing the origin of the operational risk events. The examples do not represent an exhaustive list of operational risks. Moreover, not all examples will be relevant for all IORPs.

Forward-looking supervision of the management of IORPs' operational risks

3.5. To ensure that supervision is based on a risk-based and forward-looking approach, in accordance with Article 47(2) of the IORP II Directive, CAs should assess and review the operational viability of IORPs.

3.6. CAs should verify that the responsibilities for operational liabilities are clearly defined for all types of IORPs. This is in particular important as operational risk events and errors are most often detrimental to the IORP, sponsors, members and beneficiaries, not only directly e.g. loss and costs from an operational risk incident but also indirectly e.g. damage to the IORP's reputation.

3.7. This includes, but is not limited to, defining clear responsibilities for operational liabilities:

- between the IORP and the sponsor(s) regarding the collection of contributions, for instance in the form of a service level agreement with sponsors;
- of the IORP regarding the investment of contributions, in particular for DC schemes where a delay in investing contributions has an immediate impact.

3.8. CAs should also take account of the new forms of IORPs, such as IORPs established by service providers with a commercial purpose to provide occupational

[8] Annex 9 of BCBS/BIS, International Convergence of Capital Measurement and Capital Standards – A Revised Framework, June 2006, http://www.bis.org/publ/bcbs128.pdf.

pensions for multiple unrelated employers ('multi-sponsor IORP providers').[9]

3.9. Whilst the emergence of multi-sponsor IORP providers contributes to meeting the evolving sponsor demand for occupational pensions, it also raises new questions about operational viability and ultimate responsibility for operational obligations, which may have been less prominent in the past for IORPs traditionally sponsored by a single or multiple connected employers where risks are shared.

3.10. CAs should also assess that there are appropriate means in place for covering operational liabilities and regarding future operational viability, e.g. insurance cover, requirement of the "funder" or guarantor of the IORP to cover set-up costs, request and assessment of the IORP's business plan, prudential requirement on capital reserves.

3.11. CAs should take necessary steps as part of their supervisory review process to include an appropriate assessment of the operational viability for these new forms of IORPs. In the context of registration or authorisation set out in Article 9 of the IORP II Directive, CAs should review the robustness of the business strategy and continuity plans for these IORPs, including the likelihood of winding-up and capital buffers in case of financial difficulties.

3.12. To assess IORPs' operational resilience, CAs should verify that IORPs take reasonable steps to ensure continuity and regularity in the performance of their activities. This includes reviewing IORPs' contingency plans and assessment of plausible disruptive scenarios in their risk management systems (e.g. failure to make pensions payments in time due to a disruption in the banking system or an internal, critical IT system).

3.13. CAs should encourage IORPs to put in place contingency plans, which describe their strategies, recovery and resumption procedures as well as communication plans to inform all stakeholders, including staff, members and beneficiaries, sponsors and supervisors in the event of operational risk incidents.

3.14. CAs should verify that IORPs have a policy in place as regards reporting material operational risk incidents to them, including the appropriateness of thresholds for incident reporting.

Immediacy of operational DC risks and retroactivity of operational DB risks

3.15. When assessing IORPs' operational resilience, CAs should pay attention to the immediacy of operational risks with regard to DC pensions. In contrast to DB schemes, the effect of an operational failure or error is more immediately visible to DC members in terms of accumulated pension capital and future projections, thereby making the risk identification even more important.

3.16. For instance, CAs should review IORPs' operational ability to collect and invest DC contributions accurately and on time as late or incorrect payments of DC contributions stemming from operational failures may have significant impact on members' future pensions.

[9] This emerging trend breaks with the traditional image of IORPs established by a sponsor or a group of sponsors (e.g. for industry-wide schemes) to manage pensions on a not-for-profit basis (source: EIOPA, 2017 Market development report on occupational pensions and cross-border IORPs, EIOPA-BOS-18/013, 30 January 2018, https://eiopa.europa.eu/Publications/Reports/EIOPA-BOS-18-013-2017%20Market%20Development%20Report.pdf)

3.17. Given the immediate impact of operational losses or errors on DC members, CAs should verify that the responsibilities for operational DC liabilities are clearly defined.

3.18. CAs should also pay attention to the retroactive implications of administrative errors when assessing IORPs' operational resilience. CAs should verify that IORPs identify and correct administrative errors in a timely fashion regardless of the scheme types. The less immediate nature of DB schemes also implies a risk of late identification of operational errors (e.g. over-/under-payment of benefits identified decades later) with potentially significant retroactive (cost) implications.

3.19. CAs should assess that IORPs have put in place effective internal controls and other mitigation techniques.

3.20. As poor record-keeping can lead to administrative errors, CAs should consider further specifying their supervisory expectations on IORPs' record-keeping regardless of the types of scheme managed, such as describing what data IORPs should hold or establishing measures and targets for IORPs to improve the quality and completeness of scheme records.

Information to review IORPs' assessment and management of operational risks

3.21. To review IORPs' assessment and management of operational risks, CAs should obtain and use the governance documents prescribed in the IORP II Directive, but also prepared by IORPs as part of their risk management practices. Relevant documents include, but are not limited to:

- own-risk assessment (ORA):As the frequency and severity of operational risks may be difficult to quantify, CAs should encourage IORPs to provide in their ORA an assessment of the probability and expected losses of operational risks (e.g. using "high", "medium" and "low" scores) as well as an evaluation of the severity of operational risks (e.g. using the terms "critical" versus "non-critical" to indicate whether a particular risk threatens to interrupt essential operations);

- a risk register (or other equivalent document) which identifies all risks of operational loss/failure/events together with an assessment of their probability/impact before and after risk mitigation measures[10]. The risk register should be a living document that gives a comprehensive overview of the IORP's exposure to existing and new, emerging risks and their interdependencies;

- A risk tolerance statement (or other equivalent document[11]) which articulates specific maximum risk that an IORP is willing to take regarding each relevant risk, as well as the risk limits it is not prepared to infringe. Risk limits may also be set to notify an IORP of any breach of tolerable risks. Risk tolerance can be expressed in absolute terms, e.g. 'The IORP will not accept a delay in investing contributions that exceeds x days'. An

[10] In case of cyber risks, the assessment should also be expressed in terms of threat and vulnerability.
[11] This may be part of a more comprehensive document e.g. risk appetite policy.

IORP's risk tolerance can also be limited by legal or regulatory requirements, e.g. 'The IORP has zero tolerance on fraud'.

3.22. When verifying that IORPs regularly monitor and report on operational risks, CAs should request operational risk reports and other relevant evidence that includes but is not limited to:

- 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.

3.23. CAs should also verify 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.

3.24. Further guidance on the use of governance documents in the supervision of IORPs can be found in the Opinion on the use of governance and risk assessment documents in the supervision of IORPs, BoS-19-245, 25 June 2019.

Assessment of operational risks for the full range of activities performed and/or outsourced by IORPs

3.25. To supervise IORPs' operational risks, CAs should have a complete overview of the full range of activities performed and/or outsourced by IORPs and assess their complexity. They should also verify that the identification and assessment of the operational risk inherent to all IORP activities are well understood.

3.26. CAs should also identify essential and core functions and operational complexity[12] within the full range of activities performed and/or outsourced by IORPs. CAs' assessment of IORPs' operational resilience should in particular focus on any operational functions and activities which are essential for but not limited to:

- timely and accurate collection of contributions;
- timely investment of contributions;
- safekeeping of assets;
- timely and accurate payment of pension benefits;
- protection of members' future pension benefits e.g. against external fraud;
- service continuity of the IORP's operations.

3.27. IORPs may not have sufficient internal resources to perform part or all activities necessary to deliver the pensions of members and beneficiaries. Therefore, they are more likely to outsource their activities, hence making them more exposed to outsourcing risks.

3.28. As a result, in the area of operational risks CAs should cooperate and share information with other relevant CAs and public authorities supervising other entities

[12] For example, the more variables (e.g. number of service providers interacting with the IORP and with each other) that need to be monitored and controlled, the more complex operations are. Diversity in the outsourced activities (e.g. mixed IORPs with different types of pension schemes) may also result in more complex operations.

involved in delivering all or part of IORPs' activities (e.g. competent authority supervising IORPs' asset managers, public authorities in relation to crime-related operational risks such as cyber threats and money laundering).

3.29. CAs should also pay attention to how market and regulatory developments may affect the range of activities performed and/or outsourced by IORPs' and potentially change their exposure to operational risks.

3.30. For instance, CAs should consider how regulatory changes (e.g. reforms on early pension access or abolishing compulsory annuitisation) may impact on the activities performed and/or outsourced by IORPs and IORPs' exposure to operational risks (e.g. operational risks from delivering new services to support decumulation phase, external fraud risk resulting from early pension access).

3.31. Market trends such as the shift from DB to DC and the emergence of new IORP forms mean that IORPs are likely to change some of their activities. CAs should therefore 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 risks, should be part of the decision-making process relating to significant new activities, processes and systems.

3.32. 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 cross-border activities or transfers;
- new IT solutions/systems that may be vulnerable to cyber risks;
- automation of processes, for instance for pension transfers;
- outsourcing of activities or change of service provider, which will be subject to operational risks.

4. IORPs' outsourcing risks

4.1. Annex 2 to this Opinion provides guidance for the CAs on the supervision of IORPs' management of outsourcing risks. 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. Article 31 of the IORP II Directive also allows for the outsourcing of the management of IORPs and key functions.

5. IORPs' cyber risks

5.1. Annex 3 to this Opinion provides guidance for the CAs on the supervision of IORPs' cyber risks. Because of the rapid evolution and potential impact of cyber risks, CAs should focus their attention to how IORPs assess and manage cyber risks. Cyber risks are part of CAs' assessment of IORPs' information security risk which, for instance, aims to verify that IORPs maintain an inventory of the data that is stored and processed and have effective processes for the back-up of business-critical data to ensure service continuity.

5.2. The use of information and communication technology (ICT) can contribute to

reducing operational risks since automated process are less prone to error than manual ones. However, the use of ICT also introduces other types of operational risks, in the area of information security risks and in particular cyber risks. Prevention only is not sufficient as IORPs, like any other entities, can be subject to cyber incidents that may jeopardise the 'confidentiality', 'integrity' and 'availability' of information, information systems and operational processes:

- 'confidentiality'[13] relates to the protection of communications or stored data against interception and reading by unauthorised persons. 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'[14] means the confirmation that the data, which has been sent, received, or stored are complete and unchanged. Inaccurate or inconsistent data my 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;
- 'availability'[15] refers to the fact that data is accessible and services are operational. 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.

6. Proportionality

6.1. CAs should determine the frequency and depth of their supervision of IORPs' management of operational risks, in line with 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, CAs should take into account the IORPs' characteristics, e.g. 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. For instance, CAs should consider the diversity of IORPs' activities. Many IORPs only have a single purpose of delivering occupational retirement benefits and tend to outsource most or all of their activities to service providers.

6.2. CAs should also recognise that exposure to cyber risks may differ between IORPs, for instance, it may depend on whether an IORP provides access to personal accounts of members and beneficiaries and carries out online transactions.

[13] FSB Cyber Lexicon; www.fsb.org/wp-content/uploads/P121118-1.pdf. ENISA glossary; www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary
[14] FSB Cyber Lexicon; ENISA glossary.
[15] FSB Cyber Lexicon; ENISA glossary.

7. Monitoring by EIOPA

7.1. Two years following the publication of this Opinion, EIOPA will look into the supervisory practices of the CAs with a view to evaluate supervisory convergence.

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

Done at Frankfurt am Main, 25 June 2019

[signed]

For the Board of Supervisors

Gabriel Bernardino

Chairperson

Annex 1: Classification of operational and related risks

ORIGIN OF RISK:	**INTERNAL ACTIVITIES**			**OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR**	**EXTERNAL**
OPERATIONAL AND RELATED RISKS:	**Investment management**	**Pension administration**	**Other activities, incl. key functions and management of the IORP**	**Investments, pension administration and other outsourced activities**	
I OPERATIONAL RISK Losses arising from inadequate or failed internal processes, personnel or systems, or from external events.					
Subcategories:					
(1) Internal fraud 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		
(2) External fraud Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party.				- Fraud and improper actions (misappropriation & misallocation) by employee - Service provider engaged in illegal activities - Access to confidential information (incl. data of members and beneficiaries) by non-authorised employees	- 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 pension contributions derived from illicit activities to the IORP ('money laundering')

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
OPERATIONAL AND RELATED RISKS:	**Investment management**	**Pension administration**	**Other activities, incl. key functions and management of the IORP**	**Investments, pension administration and other outsourced activities**	
(3) Employment practices and workplace safety Losses arising from acts inconsistent with employment, health or safety laws or agreements from payment of personal injury claims, or from diversity / discrimination events.	- Fines or damages to be paid to staff for not observing employment laws or collective labour agreements - Fines or damages to be paid to (potential) staff for engaging in discriminatory employment or hiring practices	- Fines or damages to be paid to staff for not observing employment laws or collective labour agreements - Fines or damages to be paid to (potential) staff for engaging in discriminatory employment or hiring practices	- Fines or damages to be paid to staff for not observing employment laws or collective labour agreements - Fines or damages to be paid to (potential) staff for engaging in discriminatory employment or hiring practices		
(4) Relations with sponsors, members and beneficiaries 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.	- Failure to execute member investment decisions (DC) - Failure to provide members with appropriate investment options (DC) - Failure to meet the requirements in the SIPP	- Untimely and/or incorrect payment of benefits due under the scheme - Member leaving service option forms not issued within statutory timescales - Untimely or erroneous communication with members/beneficiaries and sponsor - Untimely or inadequate follow-up in response to communication from members/beneficiaries - Unsatisfactory service towards members and beneficiaries due to insufficient or insufficiently competent staff	- Failure to put in place appropriate default investment strategy (DC) in accordance with fiduciary duty or regulation - Failure to provide members with appropriate investment options (DC) - Member invested in inappropriate investment funds (DC) - Failure to fully insure death in service benefits in line with the benefits payable under the terms of the pension scheme - Member communications do not effectively manage benefit expectations	- All previous examples at outsourced activities of the IORP - Service provider does not comply with its obligations towards members and beneficiaries laid down in the outsourcing agreement	

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
OPERATIONAL AND RELATED RISKS:	**Investment management**	**Pension administration**	**Other activities, incl. key functions and management of the IORP**	**Investments, pension administration and other outsourced activities**	
		- Unclear or erroneous communication to members and beneficiaries leads to misinterpretation of benefits for which IORP is liable	- Non-compliance with national and international laws and regulations - Excessive costs and charges		
(5) Damage to Physical Assets 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)
(6) Operational disruption and system failures Losses arising from disruption of operational 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	
(7) Trading/transaction processing & Process Management 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	- Member records not complete or inaccurate - Lack of transparency in own systems and/or systems operated by service providers - Non-compliance with	- If the IORP is set up under a Trust Deed then the trustees might fail to follow what the Trust Deed specifies, or might fail to understand what the terms of the Trust	- All previous examples at outsourced activities of the IORP - Service provider does not comply with its obligations relating to execution, delivery and	- Sponsor is late in remitting contributions to the IORP - Sponsor is late in remitting data of the members to the IORP

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
OPERATIONAL AND RELATED RISKS:	**Investment management**	**Pension administration**	**Other activities, incl. key functions and management of the IORP**	**Investments, pension administration and other outsourced activities**	
	- 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 and accounting - Wrong decisions on risk mitigation in dealing with derivatives - Failing processes for maintenance and legal responsibility in relation to (direct) property investments - Non-compliance with internal governance codes	internal governance codes - Failing processes because of lack of control in absence of key control register or due to inadequate control over key controls - Failing operational process leads to uncertainty about legal liability	Deed means - Insufficient monitoring of third party service providers - No clear record of how and why important financial management or significant decisions were arrived at by the trustees - Lack of engagement of appropriate advisors - Failure to identify and manage conflicts - Failure to maintain the confidentiality of the scheme's 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	process management laid down in the outsourcing agreement	
			- Risk management systems and/or documents do not fit the specificities of the IORP's organisational parts or of external		

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
OPERATIONAL AND RELATED RISKS:	**Investment management**	**Pension administration**	**Other activities, incl. key functions and management of the IORP**	**Investments, pension administration and other outsourced activities**	
			service providers - 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		
Related risks:					
II REPUTATIONAL RISK 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 or in a loss of confidence in 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.				
III STRATEGIC RISK Losses resulting from the strategic choices/ decisions of the IORP.	- Strategic decisions relating to investments that (in hindsight)	- Strategic decisions relating to staff that (in hindsight) resulted in insufficient or insufficiently competent	- Inadequate objectives and strategies - Inappropriate strategic asset allocation	- All previous examples at outsourced activities of the IORP - Service provider does	

ORIGIN OF RISK:	INTERNAL ACTIVITIES			OUTSOURCED ACTIVITIES, INCLUDING AT THE SPONSOR	EXTERNAL
OPERATIONAL AND RELATED RISKS:	**Investment management**	**Pension administration**	**Other activities, incl. key functions and management of the IORP**	**Investments, pension administration and other outsourced activities**	
	proved not to pay off	staff - Strategic decision to introduce a more complex pension plan involving more choice for and interaction with plan members that resulted in operational difficulties	decisions	not comply with its obligations relating to strategic decisions laid down in the outsourcing agreement	
IV REGULATORY / POLITICAL RISK Losses resulting from adverse changes in the regulatory framework within which the IORP is operating. This could involve a change either in 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 - A change in the EU legislation - Political crisis or change in developing country leads to decline in value of emerging market debt investments

Annex 2: Supervision of outsourcing risks

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. 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. 'Service provider' means a third party 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.

1.3. '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. CAs 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 of the supervision of IORPs' operational risks, CAs 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. IORPs should be able to influence the actions of its service provider and to give instructions at any time.

2.3. CAs should verify that outsourcing does not hinder their supervisory powers, functions and legal obligations. For instance, CAs should prescribe that the written agreement on outsourcing stipulates that the service provider has to grant full access to the CA of all relevant data. CAs should have the unrestricted right to conduct on-site inspections at the service provider's premises. CAs should be able to issue instructions to service providers via the IORP without being compromised.

2.4. CAs should verify that an IORP assesses the materiality of existing and new outsourcing arrangements including but 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, in particular 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;
- the degree of difficulty and time required to find an alternative service provider or to bring the business activity 'in-house'.

2.5. When reviewing IORPs' outsourcing risks, CAs should obtain and use relevant documents and evidence including but not limited to:

- written policy on outsourcing and record-keeping of outsourced activities in terms of their criticality and importance;
- procedures for the identification, assessment, management and mitigation of outsourcing risks and of potential conflicts of interest;
- 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;
- contingency planning to ensure the service continuity of essential and core outsourced functions or activities;
- the ORA documents describing the results of IORPs' analysis of outsourcing risks and, if relevant, any additional information on IORPs' risk analysis for important or critical outsourcing arrangements.

2.6. CAs should verify the completeness and accuracy of the information regarding outsourcing provided by IORPs[16].

2.7. CAs should communicate to IORPs their expectations for notifying them in a timely manner of any new outsourcing arrangements or significant changes. CAs should use the information to review whether new or changes to IORPs' outsourcing arrangements could materially and adversely affect their financial soundness and ability to fulfil their obligations to members and beneficiaries.

2.8. When a key function or the management of an IORP is outsourced, CAs should be informed before the agreement enters into force in order to consider the prudential implications of the proposed outsourcing and take appropriate action if necessary.

2.9. Examples of information to provide CAs in the event of essential and core 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;

[16] Further guidance on the use of governance documents in the supervision of IORPs: EIOPA Opinion on the use of governance and risk assessment documents in the supervision of IORPs, BoS-19-245, 25 June 2019.

- main reasons for outsourcing the specific function or activity.

2.10. Notification to CAs 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.

2.11. Where concerns with a significant material impact on IORPs' outsourcing risks are identified, CAs should take appropriate action, which may include limiting or restricting the scope of the functions and activities outsourced or requiring exit from one or more outsourcing arrangements, taking into account the need for ensuring service continuity of the IORP's operations.

3. Holistic assessment of IORPs' outsourcing risks

3.1. CAs should conduct a holistic risk assessment of IORPs' outsourcing risks seeking to evaluate all significant risks resulting from outsourcing essential and core functions or activities to service providers, in terms of their criticality and operational complexity. 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, CAs should monitor the development of such risks and evaluate their potential impact on other IORPs;
- the extent to which the IORP controls the service provider or has the ability to influence its actions or vice versa;
- conflicts of interest between the IORP and the service provider.

4. Accountability of the IORP

4.1. CAs should verify that IORPs are ultimately responsible for the effective management of risks arising from outsourcing.

4.2. Elements that CAs should pay attention to when reviewing IORPs' responsibilities for and effective management of outsourcing risks include but are not limited to:

- evidence of clear responsibility in-house for monitoring the conduct of the service provider and for delivering respective reports to the management body;
- evidence of the IORP approving and regularly reviewing its outsourcing policy;
- evidence of the IORP approving frameworks for reporting to the management body on matters relating to outsourced activities;

- evidence that an assessment takes place on how the IORP's risk profile will be impacted by the outsourcing of essential and core functions or activities;
- evidence of the IORP approving the outsourcing of an essential and core function or activity;
- evidence that the IORP has conducted an assessment of service providers;
- evidence of the IORP taking or authorising appropriate action in case of performance or compliance issues with the service provider of the outsourced functions or activities.

5. The nature of the outsourcing relationship

5.1. In supervising IORPs' outsourcing risks, CAs should take into consideration the nature of the relationship of the IORP with different types of service providers. The outsourcing of IORPs' activities can be broadly summarised in the following situations:

i. the sponsoring undertaking (or other entities of the group of the sponsoring undertaking) provides services to the IORP (e.g. IT services);

ii. the sponsoring undertaking providing services to the IORP is a financial services institution (e.g. insurance undertaking);

iii. the service provider of the IORP's outsourced activities is owned by the IORP (e.g. asset management);

iv. the service provider of the IORP (e.g. consultancy firm, insurance undertaking) owns the IORP;

v. there is no connection between the IORP and the service provider of the IORP's outsourced activities.

5.2. In situations i. to iv., CAs 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 v. 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 four cases, CAs should take specific circumstances into consideration, such as the extent to which the IORP controls the service provider or has influence on its actions (and vice versa). CAs should therefore verify that:

- the selection of the service provider by the 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; and
- there is 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 iv.), CAs should assess:

- the level of independence of the persons effectively running the IORP from the management board of the service provider;
- whether 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, CAs should verify that IORPs conduct appropriate due diligence in selecting their 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, CAs should require 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 CAs 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, CAs should verify that IORPs have formalised their outsourcing arrangement with service providers in the form of a written agreement between the IORP and the service provider. Such written contract between the 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 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 IORP to transfer the outsourced function to another service provider or the reincorporation into the IORP (e.g. in-house investment).

7.2. CAs should also verify that the outsourcing agreement specifies whether sub-outsourcing is permitted. If so, CAs should verify 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), CAs should verify compliance with appropriate information security standards.

8. Assessment of the conflicts of interest

8.1. CAs should verify that IORPs properly identify, assess and take appropriate measures to manage the conflicts of interests arising from outsourcing its activities. In doing so, they should consider different conflicts of interest depending on the nature of the relationship between the 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.

8.2. Outsourcing-specific conflicts of interest may especially arise in case of IORPs outsourcing key functions to the sponsoring undertaking. If the sponsoring

undertaking is for instance a financial institution such as an insurance undertaking (see situation ii. in paragraph 5.1.), CAs should pay attention to potential conflicts of interest, for instance if the actuarial function is carried out by the sponsoring undertaking.

8.3. According to Articles 24 and 28 of the IORP II Directive the single person or organisational unit (within the IORP) has to 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[17].

8.4. For any identified conflict of interests, CAs should review 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, CAs should oversee if an IORP has ensured that the conditions, including financial conditions, for the outsourced service are set at arm's length.

8.5. Where IORPs have no employees and outsource all key functions and activities to the services provider owning the IORP (see situation iv. in paragraph 5.1.), CAs should verify that the remuneration policy concerning the persons effectively running the IORP includes appropriate measures to avoid conflicts of interest.

8.6. Moreover, CAs should review the internal audit function's evaluation of the effectiveness of risk management, control and governance processes with respect to the IORP's outsourced activities and in relation to the identification and management of conflicts of interest.

9. Assessment of the business continuity management

9.1. When IORPs outsource essential and core functions or activities, CAs should verify that both the 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;

[17] 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.

- 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

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

i. legal and regulatory profile of the foreign jurisdiction: CAs should consider whether their powers to issue orders or instructions to the 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;

ii. 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, CAs should prescribe that the written agreement on outsourcing stipulates that the service provider of the outsourced function or activity has to grant access to the CA of the IORP for all relevant data in its possession and that the CA of the 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;

iii. right to carry out on-site inspections: CAs should prescribe that the written agreement on outsourcing stipulates that the service provider will not oppose to an on-site inspection on request of the Home CA should the case arise. This contractual obligation should provide the Home CA of the IORP with sufficient legal certainty to have access to the premises of the service provider, where necessary.

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

10.3. CAs should also verify that 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 its services effectively for the IORP. CAs should also consider 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 Regulation (EU) 2016/679[18], IORPs, when outsourcing abroad, including to third countries, should take into account differences in national provisions on data protection. The outsourcing arrangement should include the obligation of the service provider to protect confidential, personal or otherwise sensitive information and comply with all legal requirements regarding data protection.

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1.

Annex 3: Supervision of cyber risks

1. Definitions

1.1. CAs should understand the meaning of relevant cyber security and cyber resilience terminology through the descriptions provided in the Financial Stability Board's cyber lexicon, in the absence of common EU definitions e.g. ENISA glossary.

Cyber risk	The combination of the probability of cyber incidents occurring and their impact
Cyber incident	A cyber event that: i. jeopardises the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not
Cyber event	Any observable occurrence in an information system
Cyber resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents
Cyber threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security
Cyber security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation

1.2. Because cyber risks can evolve rapidly, CAs should keep abreast of relevant EU legislation that may be passed in this area, and use new and revised definitions, which may be developed at EU level in the future.

2. Holistic assessment of IORPs' cyber risk exposure

2.1. CAs should identify the types of threats and issues likely to make IORPs (more) vulnerable to cyber risks. Depending on the characteristics of IORPs, CAs should identify what the critical assets and activities of IORPs are. These include but are not limited to:

- member data;
- financial assets;
- physical assets (e.g. IT systems, computers);
- reputation.

2.2. To identify and assess IORPs' cyber risk exposure, CAs should develop an overview of typical data and information flows for all the activities performed and/or outsourced by IORPs. Data and information flows include but are not limited to:

- internally (e.g. emails);
- to / from sponsors (e.g. payment schedule of contributions);
- to / from other IORPs and financial entities (e.g. individual pension transfers, retirement income providers);
- to / from NCAs and other public authorities (e.g. data reporting, tax);
- to / from service providers to the IORP (e.g. pension administrator, IT supplier, asset managers, custodian, external audit);
- to / from members and beneficiaries (e.g. benefit payments, queries).

2.3. CAs should recognise that IORPs' cyber resilience requires joint efforts from all parties involved in IORPs' activities, because entities tend to underestimate cyber threats and cyber attacks and therefore do not completely internalise cyber risks (also known as 'negative externality' in economics terms). NCAs should therefore consider how cyber risk exposure borne by other entities involved in IORPs' activities could indirectly affect IORPs' operational risks (e.g. cyber security incident on the sponsor resulting in late payments of contributions). A loss stemming, for example, from a cyber attack against a service provider of an IORP, may affect the entire network of entities involved in the IORPs' activities, including the IORP.

2.4. Furthermore, many of IORPs' systems and processes are directly or indirectly interconnected with numerous third parties, such as cloud service providers and providers of outsourced services. The cyber security of these providers may significantly affect the cyber risks that IORP faces.

2.5. CAs should also develop an overview of IORPs' cyber risk profile for key operational areas exposed to cyber risks, arising from both internal and external sources and 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, e.g. use of wireless access, volume of network devices, extent of cloud services, 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 e.g. online and mobile delivery channels may present increased levels of risk to an IORP;
- organisational characteristics: these characteristics include but are not limited to the number of users with privileged access, changes in IT environment, locations of operations and data centres (including legacy systems), and reliance on third party service providers, including cloud service providers.

- external threats: the volume, type and sophistication of attacks (attempted or successful) reflect and affect an IORP's cyber risk exposure.

3. Forward-looking and cross-sectoral supervision of cyber risks

3.1. As cyber threats are continually evolving, NCAs should keep abreast of developments with regard to the cyber risk landscape and likelihood for IORPs to become more vulnerable in the future.

3.2. CAs should gather information on systemic and evolving cyber risks that would affect IORPs. CAs should also collect, centralise and use IORPs' unsolicited reporting of devastating cyber incidents.

3.3. CAs should coordinate and share relevant information on cyber security issues[19] with other regulators across the financial sector, and collaborate with other specialist public and private actors to improve the oversight of cyber risks but also be aware of their own exposure to cyber risks.

3.4. CAs should design and adapt their risk-based supervision to fulfil the prudential objective of fostering IORPs' resilience against cyber risks[20], hence protecting member data (both at rest and in transit) and promoting operational security. CAs should conduct cyber security assessments using tools, individually or in combination, including but not limited to:

- on-site inspections;
- desktop reviews;
- self-assessments;
- red team testing[21];
- technical reviews;
- thematic reviews;
- cyber security exercises.

4. Raising IORPs' awareness of cyber risks

4.1. CAs should raise IORPs' awareness of the necessity to integrate cyber risks in their risk-management systems, by identifying, measuring, monitoring, managing and reporting cyber risks and having in place effective internal controls facilitated by the IORP's risk-management function.

4.2. Raising awareness is a step toward building IORPs' cyber resilience and developing their capability to identify, detect, act and respond to cyber threats (e.g. incident management and recovery).

4.3. Where there is low level of awareness, CAs should provide guidance and information on how to demonstrate cyber resilience, including what to require from

[19] For instance, using centralised information of IORPs' unsolicited reporting of devastating cyber incidents.

[20] BaFin's Circular 10/2018 Supervisory Requirements for IT in Insurance Undertakings: https://www.bafin.de/SharedDocs/Downloads/EN/Rundschreiben/dl_rs_1810_vait_va_en.pdf?__blob=publicationFile&v=5.

[21] Examples for assessment techniques and testing methods, TIBER-EU: www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html www.dnb.nl/binaries/TIBER-NL%20Guide%20Second%20Test%20Round%20final_tcm46-365448.pdf

service providers of outsourced activities and how to monitor their performance. Taking into account the characteristics of the domestic IORP sector, CAs should consider the possibility to launch an information campaign targeting relevant IORPs and, if applicable, their service providers.

4.4. As cyber risks may evolve rapidly, CAs should signpost IORPs, regardless of awareness levels, to where they can find latest information on the cyber risks landscape. European Union Agency for network and information security (ENISA)[22] provides useful information and resources on cyber security in Europe, including an annual publication on the top cyber threats, cyber security training, information pack for SMEs, cyber risks management tools and methods, cloud computing risk assessment.

4.5. CAs should also encourage IORPs to participate in security information-sharing platforms or forums to strengthen their cyber resilience.

4.6. Cultivating awareness of IORPs on cyber risks is a first step toward incentivising IORPs to embed cyber security in their risk management and regularly evaluate their cyber risk profile vis-à-vis their risk tolerance and overall objectives.

5. IORPs' assessment and management of cyber risks

5.1. As IORPs generally tend to have limited or no in-house resources, CAs should recognise that IORPs are very likely to rely on outsourcing of cyber security. Testing resilience to cyber risks may be carried out by the IORP's internal audit function, or be outsourced to specialist consultants.

5.2. When reviewing IORPs' resilience to cyber risks, CAs should verify that IORPs have identified their assets, assessed their cyber footprint[23] and put effective measures in place, including with relevant third parties involved in delivering part or all of the IORP's activities, to protect their assets.

5.3. An identification and maintenance of a current inventory of their 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 assets that support their operational functions and processes. A risk assessment of those assets should be carried out in order to classify them in terms of criticality.

5.4. Effective cyber risk management involves:

- being more resilient against attacks;
- detecting attacks;
- being able to respond timely; and
- recovering in case of an attack.

5.5. Therefore, a classification of identified operational functions and processes in terms of criticality, should guide the prioritisation of IORPs' protection, detection,

[22] www.enisa.europa.eu

[23] Cyber footprint refers to the digital presence and hence trail of information that all the parties involved in the IORP, and service providers (e.g. cloud service providers) unknowingly give away and therefore creates vulnerabilities for the IORP.

response, and recovery efforts.

5.6. CAs should verify that cyber risks appear in IORPs' risk register (or other relevant document).

5.7. CAs should verify that IORPs regularly monitor risk profiles and material exposures to losses, including processes for cyber security monitoring to rapidly detect cyber incidents. Early detection gives IORPs sufficient time to mount appropriate counter-measures against a potential breach, and allows proactive containment of actual breaches. Examples of testing methodologies to validate the effectiveness of a cyber security framework include but are not limited to[24]:

- vulnerability assessment;
- scenario-based testing;
- penetration tests;
- red team tests.

5.8. CAs should verify that IORPs have put effective controls to support early detection and enhance cyber security. Examples 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 protection legislation and guidance.

5.9. When assessing IORPs' contingency planning to ensure continuity and regularity in the performance of their activities, CAs should review how the IORP will respond to and recover from any identified cyber incidents.

[24] IAIS Draft Application Paper on Supervision of Insurer Cybersecurity: https://www.iaisweb.org/page/consultations/closed-consultations/2018/application-paper-on-cyber-security/file/75304/draft-application-paper-on-supervision-of-insurer-cybersecurity