



Public consultation on Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents

Fields marked with * are mandatory.

Introduction

The European Supervisory Authorities (EBA, EIOPA and ESMA) have published the second batch of Consultation Papers on the mandates stemming from the Digital Operational Resilience Act (DORA) with the aim to collect market participants' feedback on the proposed Joint Guidelines on the estimation of aggregated annual costs and losses caused by major ICT-related incidents.

Market participants are invited to provide their feedback to the Joint Guidelines by responding to the questions presented in this consultation paper.

The feedback received will be taken into account in the finalisation of the Joint Guidelines, which are due to be developed by 17 July 2024.

Comments are most helpful if they:

- respond to the questions stated; indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence (including relevant data, where applicable) to support the views expressed;
- reflect a cross-sectoral (banking, insurance, markets and securities) approach, to the extent possible;
- and describe any alternative approaches the ESAs could consider.

To submit your comments, please click on the blue “Submit” button in the last part of the present survey. Please note that comments submitted after 4 March 2024 or submitted via other means may not be processed.

Please clearly express in the consultation form if you wish your comments to be published or to be treated as confidential. A confidential response may be requested from the ESAs in accordance with the ESAs' rules on public access to documents. We may consult you if we receive such a request.

Any decision we make not to disclose the response is reviewable by the ESAs' Boards of Appeal and the European Ombudsman.

The protection of individuals with regard to the processing of personal data by the ESAs is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the ESA websites.

General Information

* Name of the Reporting Stakeholder

Dutch Federation of Pension Funds

Legal Entity Identifier (LEI), if available

* Type of Reporting Organisation

- ICT Third-Party Service Provider
- Financial Entity
- Industry Association/Federation
- Consumer Protection Association
- Competent Authority
- Other

* Financial Sector

- Banking and payments
- Insurance
- Markets and securities
- Other

* If other, please specify

Pensions

* Jurisdiction of Establishment

Netherlands

* Geographical Scope of Business

- EU domestic
- Eu cross-border
- Third-country
- Worldwide (EU and third-country)

* Name of Point of Contact

Martin van Rossum

* Email Address of Point of Contact

rossum@pensioenfederatie.nl

* No, please treat my response as confidential

- Yes, publish my response
 No, please treat my response as confidential

Questions

Question 1. Do you agree with paragraph 7 and 9 of the Guidelines on the assessment of gross and net costs and losses of major ICT-related incidents?

- Yes
 No

* 1b. Please provide your reasoning and alternative approach(es) you would suggest.

Because there are many categories of costs, the amount of €100,000.00 is quickly reached. In particular, identifying indirect costs takes a lot of effort and time. In most cases only a good estimate be made. The approach to estimations needs to be flexible and pragmatic, because in many cases as the cost level will not be immediately clear. Rigid cost calculations will go at the expense of incident resolution in a crisis operation.

The ESAs should provide strict delineations of how to determine "losses due to forgone revenues" when estimating the gross costs and losses. For example, economic projections should not have to be included.

Finally, it will be difficult for financial entities to report on cost and losses of incidents from previous fiscal years. Cost recovery from insurance often takes months, often running across accounting years. In many cases, there will therefore be a complicated audit trail between gross and net losses to relate the compensation to the cost. Moreover, a final report one month after the incident will not have conclusive certainty on whether costs are incurred or recovered.

Question 2. Do you agree with paragraphs 5, 6 and 8 of the Guidelines on the specification of the one-year period, the incidents to include in the aggregation and the base of information for the estimation of the aggregated annual gross and net costs and losses of major ICT-related incidents?

- Yes
 No

* 2b. Please provide your reasoning and alternative approach(es) you would suggest.

Setting the start and end date to be identical with the accounting year of the financial entity creates the lowest administrative burden because it is consistent with the fiscal year of the company in question. However, internal financial accounting processes must be modified to meet the reporting requirement. Custom and detailed accounting is also required to show costs and losses. Most companies have a fiscal year from January 1 to December 31. Nevertheless, there will be differences, which makes comparison more difficult. A pragmatic approach is desirable, such as referring to the general ledger.

Question 3. Do you agree with paragraph 10 and 11 and the annex of the Guidelines on the reporting of annual costs and losses of major ICT-related incidents?

- Yes
 No

* 3b. Please provide your reasoning and an alternative approach(es) you would suggest.

There must be a balance between reporting and incident resolution. The requirement to report within a month of the final report is disproportionate.

Regarding the relation between the pension fund and its service providers, it is important that service providers can report in a uniform way for all its clients. Duplication of cost reporting for each financial entity should be avoided.

We note it is impossible to determine the exact 'economic impact'. This will always be an estimate. The Guidelines should reflect this fact.

4. Do you have any further comment you would like to share?

Contact

[Contact Form](#)

