JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

Report on the feasibility for further centralisation of reporting of major ICT-related incidents

Article 21 of REGULATION (EU) 2022/2554

Contents

Executive Summary

1. DORA under article 21 requires that European Supervisory Authorities (ESAs) prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for ICT-related incident reporting. To this end, this report presents the results of the study performed to understand and assess the options of further centralisation of incident reporting under DORA. This study has also been carried out concurrently with the drafting of DORA technical standards on incident reporting.

2. Considering the DORA legal mandate for this work, the report serves as a guide for exploration and comprehension of further centralisation of incident reporting. Accordingly, the report aims at informing any further discussions towards centralisation of incident reporting and thus any future decision to set up a further centralised solution would require further technical implementation studies and DORA amendments.

3. The report was prepared by the ESAs in collaboration with the Competent Authorities (CAs), who provided significant input in view of their existing experience and incident reporting solutions. The ESAs also collaborated closely with the European Central Bank (ECB) and Single Resolution Board (SRB), as per the DORA mandate, they are key stakeholders and receivers of incidents in the DORA reporting regime. Further, the European Union Agency for Cybersecurity (ENISA) also participated due to its expertise in cybersecurity and its EU role particularly in incident reporting and management. This collaborative approach ensured a comprehensive perspective, drawing on the insights from both financial and cybersecurity viewpoints.

4. The structure of the report mirrors the methodology used to perform this feasibility study. It includes a thorough analysis of the DORA legal basis and the incident reporting flows and roles and responsibilities established therein, comprehensive stock-taking exercises both on existing incident reporting regimes in the financial sector at EU level, as well as different available solutions, the general minimum high level requirements of an incident reporting system, the identification of the three scenarios to be assessed, the assessment based on the elements identified in Article 21(2) and the subsequent cost and benefit analysis, as well as the overall conclusion. The report thus presents comprehensive information on each of these elements, with additional supporting information and analyses in the technical annexes.

5. The identification of the different scenarios with increasing levels of centralisation, as well as the definition of the baseline scenario, are derived from DORA, particularly Recital 55 and Article 21:

    a. the baseline,

    b. the data sharing (baseline encompassing also other national authorities, such as the NIS authorities); and

    c. the fully centralised model (single EU hub)[1].

[1] It is important to highlight that although DORA Recital 55 includes two centralisation scenarios, in general terms, for the purposes of this study, we will refer to the EU-Hub as the most centralised solution.

6. The baseline scenario is the model which implements the existing DORA incident reporting flows, as per Article 19, and which according to DORA should be operational from 17 January 2025. This model remains largely decentralised, where financial entities report directly to the designated competent authorities in accordance with the reporting modalities and tools in place at national level. The competent authorities then transmit these reports onwards to other national and European authorities, with the ESAs then disseminating the incidents to relevant competent authorities.

7. The data sharing is a model based on the baseline solution, but where financial entities (FEs) would continue to report to the competent authority responsible for their supervision, in accordance with the reporting modalities and tools in place at national level. The main difference, however, is that in this scenario, decentralised dissemination is no longer required. Once the report is submitted to the single solution available to competent authorities, it is automatically disseminated both nationally and at the European level to the relevant stakeholders, according to their respective responsibilities.

8. The fully centralised model envisages financial entities reporting directly to the EU hub, which is accessible to stakeholders based on their specific roles and responsibilities and from which they receive notifications. This model also allows for the development of enhanced analytical capabilities, eliminating the need to duplicate such capabilities at a decentralised level. In this scenario, while the financial entities will report onto a centralised system, the competent authorities are still expected to be a first point of contact from the perspective of supervisory engagement, response, and follow-up. This solution would aim at facilitating the collection, dissemination and offering of advanced analytical capabilities of the incidents and at creating efficiencies at EU level.

9. The assessment across these three models was performed considering the elements identified in Article 21(2) on technical and legal prerequisites for the establishment of the EU hub, limitations and risks , especially related to the high concentration of sensitive information, capabilities to ensure interoperability with other reporting schemes, operational management, conditions of membership, technical arrangements for access of financial entities and national competent authorities, and preliminary assessment of financial costs incurred.

10. The report also identified the key limitations of the analysis, in view of important known unknowns at the time that the assessment was performed. Specifically, those relate to unknown number of total major ICT-related incidents expected, unknown specific design and development needs, interoperability with NCAs IT systems used for supervisory response and follow-up, and unknown timelines for the decision to move to a fully centralised solution.

11. Regarding the risks related to the high concentration of sensitive information, the report identifies that the fully centralised solution would be exposed to a higher risk of loss of the incident data availability, under the assumption that the data is not replicated at national level. This risk would warrant comprehensive information security controls to be built-in such centralised solution, and could result in higher complexity and cost, in a way that it is not possible to estimate in a precise manner at this stage. It is also worthwhile noting that in terms of loss of confidentiality and integrity risk, that in the baseline scenario the information on reporting would be already stored in a database centralised at ESAs

level, and thus already subject to such risks. Overall, this makes the information security risks (confidentiality, integrity, availability, when data is replicated at national level-) associated with the fully centralised solution only marginally higher in comparison to the baseline scenario.

12. The report concludes that all three models are feasible, noting that the baseline scenario already has to be implemented in 2025. For the other two models, their implementation is considered feasible within 3 years for the data sharing solution, given this could be implemented progressively from the baseline solution and from 5 years onwards for the fully centralised hub. This timeline considers the amendments that would need to be made to DORA to enable these models, as well as the complexity of other elements (technical, operational, governance) that would need to be in place.

13. In terms of costs, the analysis shows that there is no significant difference among the three scenarios assessed and from overall cost perspective[2] all three solutions are in a similar range. Specifically, for the fully centralised scenario, in absolute terms, would normally be able to ensure some savings, considering that the implementation of one platform would be less costly than the implementation of many At the same time, taking into account the costs linked to the implementation of the baseline solution, which was inevitable given the legal requirement to have a decentralised DORA ICT-related reporting in January 2025, potential saving opportunities would materialise only in the longer term.

14. The report also highlights that certain features of the fully centralised solution potentially offer advantages that are either exclusive to the centralised model or can only be fully realised through its implementation. Those features and capabilities include streamlining reporting channels by avoiding parallel reporting; features shortening report dissemination time and response time for cross-border incidents; shortening onwards dissemination times to all stakeholders, which would be an important prerequisite towards the operation of a cybersecurity crisis management framework and early warning; as well as advanced analytical capabilities or even direct access for FEs for analytical purposes (contributing to the objective of increasing data available to (re)insurers in line with EIOPA's strategy on Cyber Underwriting of 2020[3]).

15. Further, considering also the many known unknowns and limitations in the assessment, as highlighted above and the ongoing implementation of the DORA incident reporting solution, the report also highlights the importance of further analysis towards informing the decision on a fully centralised system. Any decision about future centralisation should prioritise and have as a guiding principle in the design of such a solution the fundamental objective of incident reporting linked to the collection, analysis, dissemination, and response to such incidents.

16. Finally, the study clearly shows further centralisation and a single EU Hub scenario is feasible and brings certain benefits. At the same time, local solutions have already been or are in the process of being built at national level to enable reporting by 17 January

[2] The overall cost perspective includes estimation of costs already sustained by competent authorities to implement their national solutions to comply with DORA requirements and those relating to the implementation of the new solutions. The latter are reported in terms of CAPEX and OPEX.
[3] Cyber underwriting strategy - EIOPA

2025, in accordance with DORA requirements. Therefore, while there are also some envisaged advantages and cost reductions in absolute terms for the fully centralised scenario, it inevitably becomes less attractive with limited advantage and incentives for changing the existing reporting channels; considering also that CAs would anyway need to continue to invest in infrastructures enabling supervisory response and follow-up at national level, even if a solution were to centralise fully incident data collection, validation and analytical capabilities. It is thus important that co-legislators continue to assess and consider further centralisation into a single EU hub, having regard to the different elements and aspects highlighted in this report, especially also considering minimising costs for transition to a fully centralised EU hub solution. In addition, such centralisation would be more beneficial and would be worth considering within a wider context of EU ICT-related incident reporting, beyond DORA.

1 Background

18. In the rapidly digitising global landscape, Information and Communication Technology (ICT) has become an integral pillar of not only the society and the economy but also of the global financial market. Concurrently, there has been a notable surge in ICT-related incidents, from cybersecurity attacks to significant data breaches. These incidents pose severe consequences for individuals, and financial entities. Across the European Union, national competent authorities of the financial entities put a lot of effort into getting a detailed overview over threats and incidents to assess and minimise risks and impact of incidents on the financial market.

19. At the moment of drafting this report, the landscape for reporting ICT-related incidents in the financial sector is fragmented across member states but also across different pieces of legislation, resulting in different reporting methods.

20. However, the Digital Operational Resilience Act (DORA) establishes a consistent incident reporting framework across the Union for financial entities and requirements for major ICT-related incidents to be forwarded to the relevant competent authorities in other Member States and at EU level to be applied by 17 January 2025. DORA also requires, under article 21, that European Supervisory Authorities (ESAs) prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU Hub for ICT-related incident reporting and submit it to the co-legislators by 17 January 2025. This meant that the work on implementing DORA major ICT-related incident reporting under Article 19 of DORA needed to be performed in parallel with the preparation of the feasibility report exploring further centralisation of incident reporting. The feasibility report explores whether an EU Hub could facilitate the flow of ICT-related incident reporting, reduce associated costs, support effective incident response, and underpin thematic analyses with a view to enhancing coordination and supervisory convergence.

21. Potential benefits of an EU Hub could be to aim to potentially foster more effective cross-border coordination and facilitate a more rapid, informed, and efficient response to incidents. By streamlining the reporting process, this EU Hub could also potentially enhance the collective understanding of the evolving threat landscape and bolster the Union's cybersecurity posture in the financial sector. The potential benefits, limitations and risks of further centralisation will be explored in this report.

22. This report contains a feasibility study on options to further centralise incident reporting under DORA, covering the aspects detailed in Article 21(1) of the said legislation, and all those additional elements that are considered useful for the correct contextualization and elaboration of the study. The ultimate objective is, therefore, to analyse the feasibility of further centralisation as required under Article 21(1) by exploring different alternatives described in this document.

23. The report was prepared by the ESAs in collaboration with the Competent Authorities (CAs). The ESAs also collaborated closely with the European Central Bank (ECB), given its pivotal role in the EU's financial infrastructure and its vested interest in maintaining

robust ICT security. Further, the European Union Agency for Cybersecurity (ENISA) also participated due to its expertise in cybersecurity and its EU legal role particularly in incident reporting and management as well as its technological capabilities in this field.[4] This collaborative approach ensures a comprehensive perspective, drawing on the insights from both financial and cybersecurity viewpoints.

1.1 Legal mandate

24. DORA is establishing a significant step forward in the harmonisation and strengthening of ICT security, including with regard to incident reporting, within the EU's financial sector.

25. In this context, Article 21 of DORA mandates the ESAs to prepare a joint report assessing the feasibility of further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting by financial entities. Such joint report shall explore ways to facilitate the flow of ICT-related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence. This involves assessing prerequisites, benefits, limitations, risks, and financial costs of such an initiative, indicating a comprehensive examination prior to any conclusive action.

26. It is important to note that the task assigned to ESAs under Article 21 does not go beyond assessing the feasibility for a possible further centralisation of incident reporting. Therefore, the mandate requires to explore, comprehend, and assess the possible further centralisation of incident reporting, but it does not require the setting up a centralised reporting solution (as also confirmed in recital 55 of DORA). This lack of a legal mandate for setting up a single EU Hub, if found to be feasible, means that the potential decision to set up such a hub lies in the future, contingent upon the findings of the mandated study and the provision of an appropriate legal basis for any potential option.

27. Although the EU Hub referred to in Article 21 of DORA is intended primarily as a centralised system where financial entities report directly to a centralised solution, recital 55 considers also an additional scenario, where the centralised system acts as a coordination mechanism. For the purposes of this report, we will refer to the EU Hub as the fully centralised scenario (please refer to section 7, Identification overview of potential options).

28. Additionally, the rest of articles under Chapter III of DORA, which set out the requirements for ICT-related incident management, classification and reporting further delineate the reporting obligations and feedback mechanisms concerning ICT incidents, emphasising the importance of harmonisation, feedback, and expanded scope, respectively. The articles under Chapter III of DORA contain elements that could inform the technical specification and operational design of such a hub given that they will support effective incident reporting under the existing DORA framework.

[4] ENISA plays a critical role in several pieces of legislation that are geared towards enhancing digital operational resilience in the context of incident reporting. See Directive (EU) 2022/2555 (NIS2) Article 23(9), NIS2 Recital 106, Directive (EU) 2018/1972 (EECC) Article 40, and Regulation (EU) No 910/2014 (eIDAS) Article 19. ENISA also maintains CIRAS, the Cybersecurity Incident Reporting and Analysis System

29. Article 19 of DORA provides a robust blueprint for the types of reports that a central hub might process, specifying elements like time limits for notification and details for establishing the relevance of reporting for other Member States. The development of common draft regulatory and implementing technical standards, as outlined in Article 20 of DORA, will also serve as a guiding framework for defining the standard forms, templates, and procedures a central hub should utilise. This would be particularly relevant in handling ICT-related incidents and significant cyber threats.

30. The supervisory feedback mechanisms referred to in Article 22 of DORA, with the provision of anonymised information and intelligence, are another essential element that could inform the technical specifications of a central hub, as they would support the goal of creating a centralised system that can effectively track and respond to ICT related incidents across the EU.

31. Furthermore, the provision of Article 23 of DORA for operational or security payment-related incidents concerning credit institutions, payment institutions, account information service providers, and electronic money institutions could directly contribute to the scope and operations of a central hub, ensuring it covers a wide range of financial entities.

32. In summary, while these articles of DORA do not legislate the creation of a single EU hub, they can provide crucial technical and operational insights that could guide its design, should its establishment be decided upon in the future.

33. In conclusion, in the current DORA framework, if the European Commission, the Council and the European Parliament, to whom this report is addressed, decide to proceed with further centralisation of incident reporting through the establishment of a single EU Hub, a separate and specific legal mandate or a delegation project would be necessary.

1.2 Methodology and structure of the report

34. The methodology used for this feasibility study aims to provide a well-informed, objective assessment of the feasibility of establishing a centralised solution for ICT-related incident reporting. This report is based on the current DORA Level 1 requirements and is carried out concurrently with the drafting of additional technical standards on incident reporting that are relevant for such deliverable. Therefore, the assumptions of such study may slightly change after the finalisation of the legislative process.

35. At the same time, the considerations regarding the baseline scenario are based on the functional requirements and the reporting workflows expected for the tool that will be operational at the beginning of 2025.

36. The study consists of eight main sections, in addition to the background.

- In Section 2, the reporting process under DORA is described, along with the roles and responsibilities of the various competent authorities involved in the process.
- Section 3 analyses some examples of current frameworks and systems implemented at both the European and national levels, as well as different available commercial alternatives.

- During the drafting process, it was considered beneficial to gather information through additional methods, particularly questionnaires and requests for information.
    I. During the initial phases of the analysis (Q2 2023), a survey was circulated among the various competent authorities to gather qualitative and quantitative information regarding the incident reporting. This survey aimed to obtain valuable insights and data pertaining to the incidents reported, including their nature, frequency, and impact. By gathering this information, the study sought to gain a preliminary understanding of the incident reporting landscape and provide a solid foundation for further analysis of the feasibility of additional centralisation of the reporting process.
    II. Another questionnaire was shared with the entities represented in the stakeholder groups of the three ESAs during Q3 of 2024 (primarily financial entities, industry associations, academia and user representatives).
    III. The results of these questionnaires are summarised in Section 4 and detailed in the annexes. The information gathered has informed the cost-benefit analysis included in Section 8.
- The analysis of requirements presented in Section 5 is a preliminary and high-level overview of functional and non-functional requirements of a general incident reporting system and it should be further explored in case of the adoption of any of the proposed solutions. Depending on the outcome of the detailed requirements analysis the solutions proposed in this paper may need to be adapted at later stages.
- To investigate whether commercial (off-the-shelf) solutions are available on the market that can meet DORA's data collection, assessment, analysis, dissemination and notification requirements, a market scan was conducted, the results are also included in section 6 and the description of the methodology for this request for information is also included in the annex.
- The identification of the different centralisation options, as well as the definition of the baseline scenario, are derived from the information contained in DORA, particularly Recital 55 and Article 21. More information about this process can be found in Section 7.
- Section 8 includes the assessment results:
    I. To assess and compare the different scenarios the criteria listed in DORA Art 21(2) were used, a summary of the assessment is included in this section. An additional assessment of the three scenarios performed by and independent firm (Gartner Consulting) is included in the annex.
    II. A cost-benefit analysis was carried out considering different stakeholder groups in order to obtain a holistic view of the different scenarios and to analyse the different impacts of the scenarios on these different groups.
    III. In the same section possible considerations for future implementation have been included, these considerations aim to elaborate on the feasibility of the various options beyond the elements for the assessment identified in DORA and the functional requirement.

- Once the assessment is presented, the report's conclusions are elaborated in Section 9.

37. The Report also includes an Annex where more detailed information is presented, in particular expanding the content of Sections 3, 4 and 8.

2 Competent authorities under DORA: Roles and responsibilities

38. The reporting process outlined in Article 19 aims to facilitate effective incident management, enhance transparency, and enable the competent authorities to take appropriate measures to safeguard the resilience of the financial sector.

39. Article 19 of the DORA establishes a comprehensive reporting process for incidents within the financial sector. This process ensures that financial entities promptly notify the relevant competent authorities of any major ICT-related incidents. Under Article 19, once an incident is detected, financial entities shall report it to their respective Competent Authority[5] (CA). The CA then evaluates the severity and potential impact of the incident and collaborates with other competent authorities, both at the national and European levels, to coordinate incident response activities and information sharing.

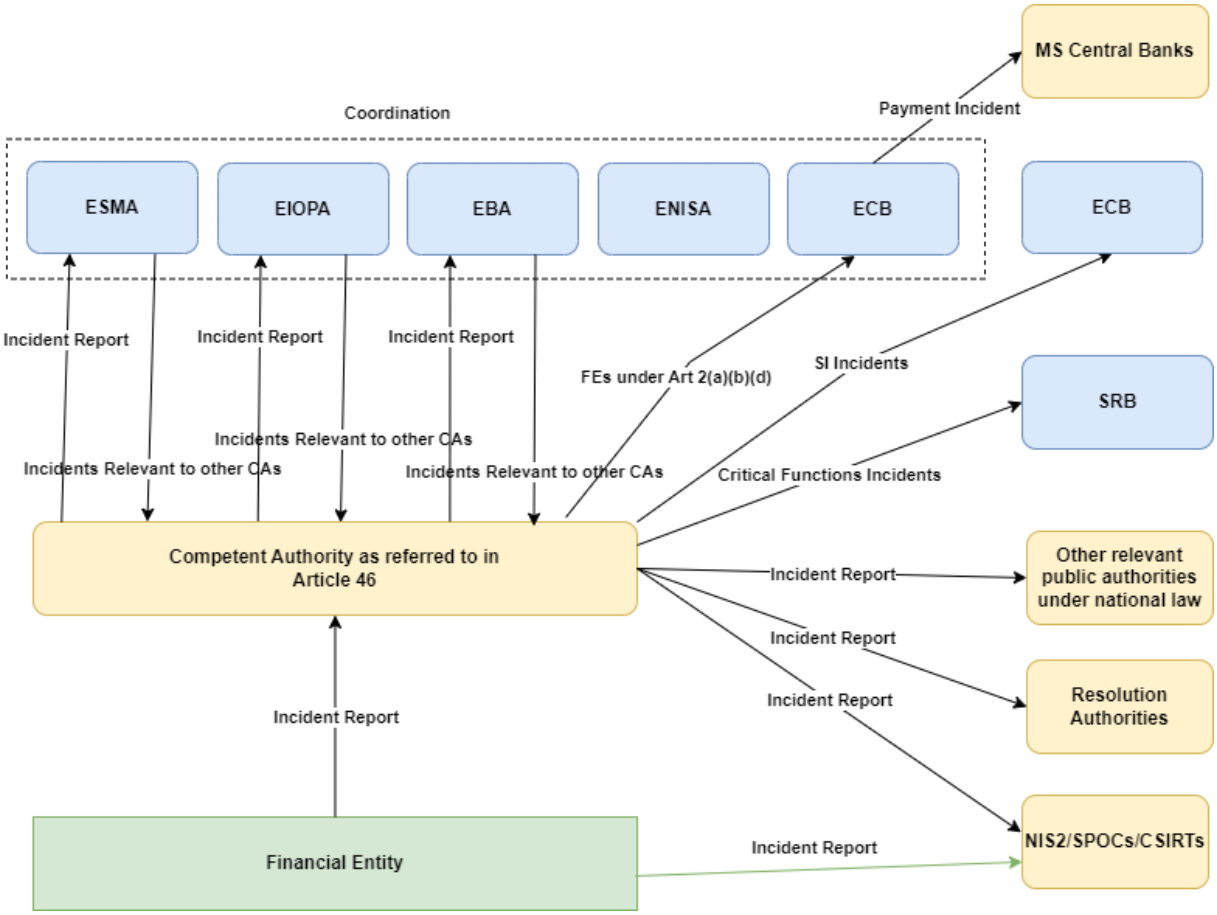
40. This section focuses on the roles and responsibilities of the competent authorities involved in incident reporting under this regulation. These competent authorities, designated at both the national and European levels, play vital roles in establishing reporting mechanisms, receiving incident notifications, assessing incident severity, and coordinating incident response. Their collaboration and expertise contribute to a comprehensive incident reporting framework that enables prompt and effective management of incidents in the financial sector.

41. Before analysing the role and responsibilities of each competent authority, it is important to understand and explain the reporting process foreseen by DORA. This process encompasses the requirements and procedures set for financial entities to promptly report incidents to the relevant competent authorities. By understanding the reporting process, we can gain insights into how the various competent authorities fulfil their roles and responsibilities in incident reporting.

2.1 Incident reporting under DORA

42. Effective incident reporting including the classification, management and reporting of incidents is one of the basic pillars of DORA and Chapter III of this regulation is dedicated to it. Within this chapter, Article 19 defines, first, the flow of reports from financial institutions to the competent authorities and then the flow of information from the latter to other stakeholders.

[5] The list of Competent Authorities is identified in Article 46 of DORA



43. Figure 1 identifies the main reporting lines[6] for the different actors involved in the process, which can be summarised in two main steps, as follows:

I. The beginning of the reporting flow starts at the financial entities, which (directly or through a third-party service provider) shall report to the relevant competent authority (as set out in Article 46), for incidents considered major, the initial notification (and subsequently the intermediate and final reports) using the templates set out in Article 20 and within the time period set out in the same article.

II. This reporting shall be made to a single authority, notwithstanding that in certain countries such information shall also be forwarded to the competent authorities or the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555.

III. Credit institutions classified as significant, in accordance with article 6(4) of Regulation (EU) 1024/2013, shall report to the relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit that report to the ECB.

IV. Member States may additionally determine that some or all financial entities shall also report to the competent authorities, or the computer security incident response teams

[6] The reporting has three phases, initial, intermediate and final report, the reporting lines are equivalent for any phase of the report.

(CSIRTs) designated or established in accordance with NIS2 Directive (green arrow in Figure 1).

V. The competent authorities, upon receipt of the initial notifications, shall forward them, as applicable and depending on the type of financial institution, to:

(a). EBA, ESMA or EIOPA.

(b). ECB.

(c). the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;

(d). resolution authorities and the Single Resolution Board (SRB);

(e). other relevant public authorities under national law.

VI. Once this initial notification is received, the 3 ESAs in coordination with the ECB and ENISA shall assess whether the major incident is relevant for other authorities in other member states. If so, the EBA, ESMA and EIOPA shall notify the competent authorities (with certain considerations with respect to ESMA and central securities depository as set out in Article 19 point 8).

VII. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system.

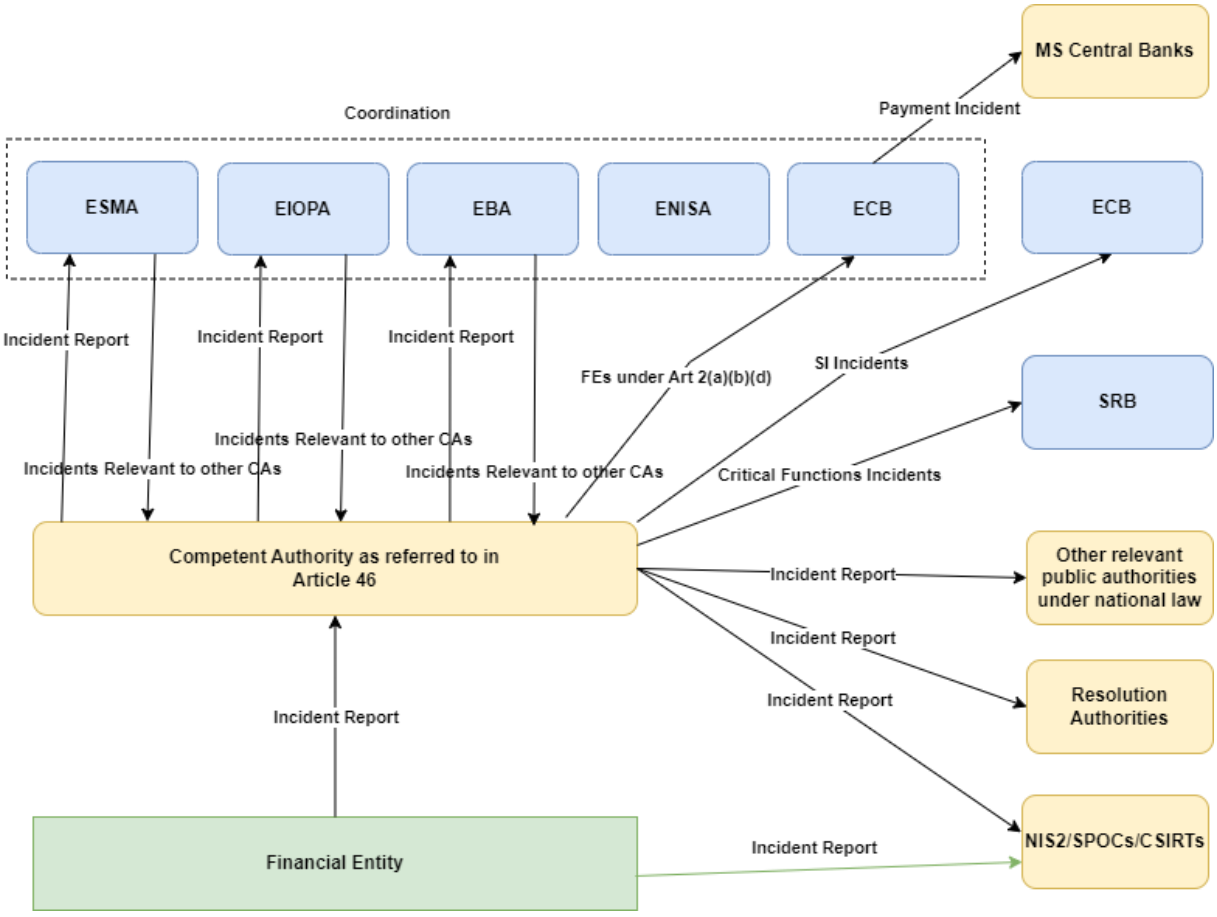


FIGURE 1 INCIDENTS DATA FLOW UNDER DORA

44. As can be seen in the graph and in the high-level description of the reporting flow, there may be multiple channels of data exchange between different authorities and from financial entities in the process, depending on the nature of the incident. Any incidents that are local to a Member State (MS) will be dealt with by MS, with other Union authorities kept informed as appropriate. It is relevant to note that in some MS the competent authority may have different roles (e.g. central banks, resolution authorities, etc) and therefore in these countries the incident flow may avoid additional communications at MS level. This is currently the case for many of the incidents reported. Any incidents that have a cross border impact, will be notified to the relevant competent authorities in other MS. The purpose of this study will therefore be to analyse the possibility of advancing towards further centralisation of incident reporting, and with a view to facilitating the flow of ICT related incident reporting, reduce associated costs and underpin thematic analyses with a view to enhancing supervisory convergence.

2.2 Competent authorities

45. Once explained the reporting flow of major incidents, we will delve deeper into the specific roles and responsibilities of each competent authority, providing comprehensive insights into their contributions to the incident reporting process as outlined in Article 19 and Article 21 of DORA.

46. The competent authorities responsible for ensuring that financial entities comply with DORA are set out in Article 46 of DORA. This is done by reference to a number of provisions of European law. Depending on the type of financial entity, these provisions reserve supervisory competence either to national competent authorities or to European competent authorities (European Supervisory Authorities: EBA, ESMA or to the ECB).

47. National competent authorities should be understood as the competent authorities that ensure compliance of financial entities with DORA and that have been designated for this function in each Member State for a given category of financial entities in accordance with the provisions referred to in Article 46 of DORA. National competent authorities under DORA are responsible for the supervision of most of the categories of financial institutions:[7]:

- credit institutions and institutions exempted pursuant to Directive 2013/36/EU;
- payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;
- electronic money institutions, including those exempted pursuant to Directive 2009/110/EC;
- account information service providers;
- investment firms;
- crypto-asset service providers and issuers of asset-referenced tokens;

[7] The list is not exhaustive with respect to the regulation referred to a possible exceptions, for further details on this point please refer to Article 46 of DORA.

- central securities depositories;
- central counterparties;
- trading venues;
- data reporting service providers constituting approved reporting mechanisms and approved publication arrangements with a derogation in accordance with art. 2.3 of Regulation (EU) No 600/2014;
- managers of alternative investment funds;
- management companies;
- insurance and reinsurance undertakings;
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
- institutions for occupational retirement provision;
- administrators of national critical benchmarks
- crowdfunding service providers.

48. On the other hand, the European competent authorities, ECB, EBA and ESMA, are responsible for the supervision of:

- credit institutions classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013 (ECB);
- issuers of significant asset-referenced tokens (EBA);
- data reporting service providers other than approved reporting mechanisms and approved publication arrangements with a derogation in accordance with art. 2.3 of Regulation (EU) No 600/2014 (ESMA);
- trade repositories (ESMA);
- credit rating agencies (ESMA);
- administrators of European critical benchmarks (ESMA);
- securitisation repositories (ESMA).

2.2.1 National competent authorities and other relevant authorities and MS level

Bodies acting as national competent authorities in the Member States

49. Different Member States may have different arrangements for the competent authorities responsible for the supervision of financial market entities. First, supervisory responsibilities for many categories of financial market entities may be consolidated in a single competent authority, as is, for example, the case with the Polish Financial Supervision Authority. The latter is responsible for the national supervision of banks, insurance companies and financial market entities.

50. Conversely, in some Member States different authorities may be responsible for supervising different categories of financial market entities. An example is Croatia, where the Croatian National Bank is responsible for the supervision of credit institutions whereas the Croatian Financial Services Supervisory Agency is responsible for the supervision of investment firms. In many countries, supervisory responsibilities are also exercised by central banks (e.g., in Belgium by the National Bank of Belgium for credit institutions, insurance undertakings, payment institutions, electronic money institutions, central securities depositories and some types of investment firms).

Roles and responsibilities of national competent authorities regarding incident reporting under DORA

51. DORA imposes a number of obligations on competent authorities in relation to incident reporting. According to Article 19(1) of DORA, competent authorities (including national competent authorities) remain responsible for receiving notifications of major ICT-related incidents from financial entities. This includes the submission by financial entities to the national competent authority of an initial notification, an intermediate report and a final report. Article 19(4)(b) of DORA also gives competent authorities the power to request an intermediate report on a major ICT-related incident from a financial entity, in order to obtain additional information on the incident that is particularly important for the competent authority.

52. Article 19(6) of DORA also obliges competent authorities to forward initial notification and intermediate and final reports of major ICT-related incidents to the European and national authorities mentioned in the provision. The provision emphasises that the competent authority should share incident reports with the relevant authorities, taking into account their respective competences. This assessment is an additional responsibility of the competent authority as part of the process of communicating information to other recipients as provided for in Article 19(6) DORA. Additional recipients of incident reports include:

    (a) EBA, ESMA, EIOPA;

    (b) ECB;

    (c) the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;

    (d) the resolution authorities and the Single Resolution Board (SRB);

    (e) other relevant public authorities under national law.

53. The exchange of information on major ICT-related incidents between national competent authorities and EBA, ESMA and EIOPA is bilateral for incidents that have cross-border implications. Upon receipt of an ICT-related incident report, EBA, ESMA or EIOPA and the ECB carries out an analysis to assess whether the incident is relevant for competent authorities in other Member States. In case of a positive assessment, EBA, ESMA or EIOPA notifies the relevant national competent authority or authorities of the incident. Such notification provides national competent authorities with an additional source of information on ICT-related incidents in other Member States that may have cross-border impact. EBA, ESMA and EIOPA consults with ENISA and cooperates with the relevant

competent authority when assessing the impact of a major ICT-related incident on other Member States.

54. The provisions of DORA also provide for the competence of national competent authorities to provide feedback to financial entities in relation to reports on major ICT-related incidents. Upon receipt of the initial notification and of each report as referred to in Article 19(4) of DORA, the competent authority acknowledges their receipt and may, to the extent possible, provide appropriate and proportionate feedback or high-level guidance to the financial entity in a timely manner, in particular by providing any relevant anonymised information and intelligence on similar threats, and may discuss countermeasures taken at the level of the financial actor and ways to minimise and mitigate negative impacts across the financial sector. This does not, however, mean that national competent authorities are delegated to deal with ICT-related incidents or their consequences. As emphasised in Article 22(1) of DORA, financial entities remain fully responsible for the handling and consequences of ICT-related incidents.

55. Taking into account the Article 23 of DORA, the above responsibilities of the national competent authorities also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.

2.2.2 EBA, ESMA and EIOPA

56. The ESAs are tasked with relevant roles under Article 19, Paragraphs 6-8 of DORA, which focuses on the reporting of major ICT related incidents in the financial sector. Such roles in incident reporting, risk evaluation, and information dissemination are fundamental to ensuring a well-coordinated and effective response to major ICT-related incidents within the EU's financial sector.

57. Upon the initial notification of a major ICT-related incident, the competent authority forwards details of the incident to several entities, including the pertinent ESA (EBA, ESMA, or EIOPA), as laid out in Paragraph 6 of Article 19. This distribution of information allows for a comprehensive, coordinated response and fosters a unified approach to address the incident across the European Union.

58. Upon the receipt of this information, in consultation with ENISA and in cooperation with the relevant competent authority, the ESAs should assess the potential relevance of the major ICT-related incident for authorities in other Member States. After this evaluation, the ESAs are then tasked with notifying relevant competent authorities in other Member States, thereby facilitating a cross-border information flow and response mechanism. This notification responsibility should also be aligned with the cooperation arrangements among competent authorities related to the supervision of financial entities.

59. In addition to their duties under Article 19, Article 22 of DORA lays out additional responsibilities for the European Supervisory Authorities (ESAs). This Article operates under the principle that feedback, even at a high level, can provide valuable guidance for mitigating the adverse impact of ICT-related incidents across the financial sector. It

envisions a dynamic relationship between competent authorities and financial entities, where information exchange becomes the cornerstone of managing ICT-related risks.

60. Moreover, the second part of Article 22 extends the ESAs' role beyond incident management to proactive risk analysis and communication. Through the Joint Committee, the ESAs are required to prepare an annual report, which includes information on the number, nature, and impact of major ICT-related incidents, remedial actions taken, and costs incurred. These anonymised and aggregated data gives the ESAs a comprehensive view of the landscape of ICT-related incidents.

61. Their report, therefore, becomes a valuable source of insights for financial entities and regulatory authorities alike. Additionally, the ESAs are also entrusted with the task of issuing warnings and producing high-level statistics to support ICT threat and vulnerability assessments. This proactive role of the ESAs underlines their importance in maintaining the stability and integrity of the EU financial sector.

62. The feasibility study explores the benefits of further centralisation of reporting major ICT-related incidents. The study would explore also whether and how further centralisation would improve incident data analysis at ESA level, as well as the facilitate the establishing of a cyber crisis communication framework.

2.2.3 ECB

63. Under Article 19 of DORA the ECB also has a specific role. Firstly, with regard to the reporting of incidents by credit institutions classified as significant (Article 19(1) paragraph 3). These financial institutions shall report directly to the relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU, and this national competent authority shall transmit this information to the ECB.

64. It is important to note that such reporting should be done **immediately**. This approach differs from the general information flow in Article 19(6) from Competent Authorities to other stakeholders, where the text provides for reporting in a "timely manner".

65. In point 6 the ECB is also part of the recipients of this general information flow, in particular for incidents related to credit institutions, payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366; and electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC.

66. The ECB under point 7 of the same article shall participate in the analysis of the relevance of incidents received for competent authorities in other member states.

67. Under the same point, the ECB shall also notify the members of the European System of Central Banks on issues relevant to the payment system.

68. It is therefore worth noting that the ECB's role as receiver and distributor of incidents is twofold and the reporting line is also duplicated depending on the type of incident and the financial institution.

2.2.4 SRB

69. The SRB, together with the resolution authorities, is the recipient of the subset of incidents related to the entities referred to in Articles 7(2), (4)(b) and (c) and (5) of Regulation (EU) No 806/2014 if such incidents pose a risk to ensure critical functions. Critical functions being understood as those activities, services or operations the discontinuance of which is likely in one or more Member States, to lead to the disruption of services that are essential to the real economy or to disrupt financial stability due to the size, market share, external and internal interconnectedness, complexity or cross-border activities of an institution or group, with particular regard to the substitutability of those activities, services or operations.

2.2.5 ENISA

70. ENISA's role in the incident flow is primarily consultative. ENISA shall be consulted in the process that assesses the relevance of an ICT-related incident for competent authorities in other Member States.

3 Existing Systems: Frameworks and IT systems

71. Incident reporting, whether ICT-related or of other types, is part of the information flow between financial sector entities and the various competent authorities. This is the case both for systems at EU level and for systems implemented at Member State level.

72. Such a framework around the receipt of incidents not only has certain processes and tasks associated with it, but often relies on technological solutions to support them. In this section we briefly elaborate on some (pre-DORA) use cases at both EU and national level to try to get an overview of the current state of incident reporting for some of the stakeholders involved in the incident reporting process in DORA.

73. A more detailed overview of the different use cases can be found in the Annex III: Existing Systems.

3.1 Existing frameworks and IT systems at EU Level

3.1.1 ESMA

74. ESMA plays an important role in incident reporting within the EU financial markets. It has both direct and shared supervisory responsibilities. ESMA directly oversees EU Credit Rating Agencies, Trade Repositories, Securitisation Repositories, certain Data Reporting Services Providers, specific benchmark administrators, and Tier 2 third-country Central Counterparties. These entities are governed by various regulations such as the CRA Regulation, EMIR, SFTR, MiFID II, the Benchmark Regulation, and EMIR 2.2.

75. ESMA has also issued guidelines for some of its supervisory mandates on periodic information reporting, providing the legal basis for ICT-related incident reporting. ESMA and NCAs work together, forming a comprehensive framework for incident reporting and management. This collaboration aims to enhance the resilience of the financial market infrastructure against ICT-related threats.[8]

76. ESMA has developed procedures for the full lifecycle of each incident, from its initial reporting by supervised entities to its monitoring and assessment. Supervised entities are requested to report incidents to ESMA according to a specific process and in a designated template. The reporting process starts with an initial notification, followed at a later stage by a full notification, both sent via an online portal.

77. This process is partially supported by a technology solution that allows the incidents to be logged and monitored in an appropriate manner, as well as by visualisation tools that provide a complete picture of the status of the situation for a particular incident as well as for the incidents as a whole.

[8] In the new proposed reporting guidelines, which are out for public consultation in the moment of drafting this report, incident reporting is now defined as to be performed in line with the template set out in the relevant Commission Implementing Regulation to be adopted pursuant to DORA, this is to facilitate compliance for reporting entities subject to DORA as opposed to creating a separate template.

3.1.2 EBA

78. The revised Payment Services Directive (PSD2) conferred the EBA with the mandate to collect and disseminate reports on major security or operational payment-related incidents. Since 2018, the EBA has been receiving major incident reports impacting payment service providers (PSPs), including credit institutions, payment institutions, and e-money institutions. The reporting flow involves PSPs submitting initial, intermediate, or final reports to their Competent Authorities, which are then forwarded to the EBA and the ECB. Upon receipt of these reports, the EBA, ECB, and the submitting CA assess the incident's relevance to other Member States and notify the respective CAs. Additionally, the EBA, in collaboration with the ECB and the home Member State's competent authority, assesses the incident's relevance to other Union and national authorities and notifies them accordingly.

79. The classification and reporting provisions of major incidents under PSD2, including classification criteria, materiality thresholds, reporting templates, data field descriptions, and instructions, are outlined in the EBA Guidelines on major incident reporting under PSD2. Based on the reports received, the EBA and the ECB monitor high-level reporting trends, leading to the revision of guidelines, organisation of industry workshops, and informing policy development related to incident mandates under DORA.

80. The European Centralised Infrastructure for Supervisory Data (EUCLID) platform is the current system for banking and financial data in the EU's financial sector which is place since its implementation 2021. EUCLID keeps evolving in terms of scope of reporting entities and functionalities, with a data dissemination platform being launched during Q4 2023 and Q1 2024 (phase 1 and 2, respectively). In addition, it is complemented with the EBA's public registers, namely the Credit Institutions Register (CIR) and the Payments Institutions register (PIR) under the Payments Service Directive (PSD2), and possibly with a critical Third-Party Providers register in coming years.

81. The current reporting scope to the EBA covers over 10,000 reporting entities including EU/EEA credit institutions banking groups, investment firms, investment firms' groups, resolution groups, payment and e-money institutions.

3.1.3 EIOPA

82. EIOPA has been taking several initiatives to monitor risks and identify opportunities in the context of the cyber underwriting. Acknowledging the critical role of a comprehensive incident reporting system, EIOPA recognises the invaluable insights derived from incident data for cyber risk assessment and management. The incident reporting data is essential for cyber underwriting processes, enabling the development of tailored insurance policies that reflect the market's specific cyber risk profile. Thus, it is important that the incident data collected as part of DORA reporting framework will be made available to cyber

underwriters (insurance and reinsurance undertakings and intermediaries) in line with EIOPA's strategy on cyber underwriting[9].

3.1.4 ENISA

83. ENISA maintains an incident reporting tool, called CIRAS (Cybersecurity Incident Reporting and Analysis System), for the authorities, where they can upload reports, and search for and study specific incidents. At the moment, the main use for CIRAS is to support the annual summary reporting for NIS Directive, EECC Art. 40 and eIDAS Art. 19.

84. Both the data flow and the data typology supported by this solution are very similar to those established in DORA. The tool has capabilities to receive reported incidents and disseminate them to relevant stakeholders. Moreover, its scope of action is similar, as it works mainly with incidents in the field of cybersecurity.

3.1.5 ECB

85. As mentioned under section 3.1.2, the ECB has been receiving major incident reports impacting payment service providers (PSPs), including credit institutions, payment institutions, and e-money institutions, in accordance with the provisions under the PSD2 (and as outlined in the EBA Guidelines on major incident reporting under PSD2). The reporting flow involves PSPs submitting initial, intermediate, or final reports to their Competent Authorities, which are then forwarded to a reporting platform hosted by the EBA (to which both EBA and ECB have access).

86. Upon receipt of these reports, the ECB, along with the EBA and the submitting CA assesses the incident's relevance to other Member States as well as other Union and national authorities and notifies them accordingly. In addition, the EBA and the ECB monitor high-level reporting trends (see also section 3.1.2).

87. The SSM Cyber Incident Reporting Framework has been established as a central mechanism to collect, analyse, and draw actionable insights from significant cyber incidents, helping to monitor credit institutions and to uphold the resilience of the financial system. The entities in scope of the SSM Cyber Incident Reporting Framework are Significant Institutions[10] that are supervised by the ECB ("Supervised Institutions"). These institutions report cyber incidents that fulfil the reporting criteria at the highest level of consolidation (within the SSM). The objectives of the framework focus primarily on: i) assessing the impact to the bank in an immediate follow-up, identifying critical cyber incidents that could potentially lead to a crisis situation and ii) drawing potential conclusions from the cyber incident for the supervisory assessment of the overall cyber risk of the bank.

[9] In order to allow for sound pricing, underwriting and cyber risk management, the availability of data on cyber incidents should be broadened and appropriately standardised, while safeguarding the level playing field and data confidentiality. Ultimately, the access to cyber incident database(s), potentially a European Database, could be seen as a public good and underpin the further development of the European cyber insurance industry and act as an enabler of the digital economy. EIOPA Digital Underwriting, Strategy, 2020, p.3

[10] https://www.bankingsupervision.europa.eu/banking/list/html/index.en.html

88. At its core, the framework establishes a streamlined procedure and a database, set up as a centralised repository for significant cyber incidents. Supervised Institutions report directly to the ECB or, for some countries with pre-existing national cyber incident reporting regulations, via their National Competent Authorities (NCAs). The incidents are reported via a standardised Excel-based template, to ensure collection of consistent information across all incidents. Details about the current reporting process are explained in Section 3.3.1.3.

89. The ECB's Cyber Incident Team is set up to operate the reporting process, bridging communications among banks, NCAs, and the JSTs. Its role also includes gauging the impact of each incident, invoking and running the dedicated Cyber Incident Emergency Process (CIEP), with participation of experts across the ECB and NCA functional areas, in cases of highly critical ("major") incidents. The ECB's Cyber Incident Team is acting both in capacity of an expert function, providing support to JSTs in specific cases, and as an analytical function, providing insights on a cross-bank level.

3.2 Existing systems at National Level

90. In the same way that the different incident reporting frameworks have generated different frameworks and technological solutions at the European level, the competent authorities in the different member states have developed their own frameworks and systems to meet their needs.

91. In this section we briefly present some examples, although these are not exhaustive as each Member State has been able to opt for different models, both in terms of procedures and technological solutions, derived from their needs and the various competent authorities and their degree of integration.

92. It is important to note that often the competent authorities in the member states operate as a middle point between the reporting entities and other bodies at the European level, in a similar way to that established for incident reporting in DORA.

3.2.1 Roles and responsibilities of national competent authorities regarding incident reporting under national laws

93. National competent authorities may have other roles and responsibilities under national law with regard to incident reporting. Such roles and responsibilities often involve cooperation with other competent authorities at Member State level.

94. An example of this type of regulations can be found in particular in the provisions implementing the NIS Directive (replaced by the NIS2 Directive) in each Member State. NIS Directive provides for operators of essential services to notify the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Its scope of application covers several economic sectors, in order to achieve a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. It also covers certain entities in the banking sector (credit institutions) and financial market infrastructures (operators of trading venues and central counterparties).

95. The NIS Directive requires Member States to designate one or more national competent authorities for network and information systems security. The main task of the NIS competent authorities is to monitor the application of the Directive at national level.

96. At the same time, it introduces an obligation to designate a single point of contact for network and information system security in each Member State. This is intended to facilitate cross-border cooperation. The provisions of the NIS Directive also provide for other mechanisms for cooperation with national authorities. For example, competent authorities should, whenever appropriate and in accordance with national law, consult and cooperate with relevant national law enforcement authorities and national data protection authorities.

97. The NIS Directive also requires the designation of one or more Computer Security Incidents Response Teams (CSIRTs) in each Member State. The provisions of the NIS Directive provide for a number of cybersecurity-related tasks for those teams, including:

    (a) monitoring incidents at a national level;

    (b) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;

    (c) responding to incidents;

    (d) providing dynamic risk and incident analysis and situational awareness;

    (e) participating in the CSIRTs network.

3.2.2 Collaboration with other competent authorities at the national level and cross-border incident reporting and cooperation

98. Depending on national arrangements, in some Member States, the role of the NIS Directive competent authority for operators of essential services from sectors of banking and financial market infrastructures, as well as the related role of the CSIRT, may be performed by national competent authorities responsible for ongoing financial market supervision (Poland may be an example of such a country - see the case study section below for more information). If, on the other hand, the role of the NIS Directive competent authority or the role of the CSIRT under NIS Directive is performed by another national authority, cooperation between these authorities and the competent national authorities responsible for the day-to-day supervision of the financial market in the area of incidents in financial market entities is essential. This may also involve national resolution authorities or national authorities responsible for macro-prudential supervision.

99. In addition to cooperation on incident reporting at national level, competent authorities in Member States can also participate in cross-border cooperation mechanisms in this area. These include the arrangements provided for in the NIS Directive, such as the Cooperation Group on Security of Networks and Information Systems and the CSIRTs Network.

100. The Cooperation Group is composed of representatives of the Member States, the Commission and ENISA, and some of its tasks are directly related to incident reporting issues, such as exchanging best practices on the exchange of information related to incident reporting, producing annual summary incident reports based on anonymised and

aggregated data, collecting best practice information on risks and incidents, or discussing modalities for reporting incidents. In turn, the members of the CSIRTs Network include representatives of the Member States' CSIRTs and CERT-EU, and most of the tasks of the CSIRTs Network are incident related. These include, inter alia:

- exchanging and discussing non-commercially sensitive information related to the incident and associated risks, at the request of a representative of a CSIRT from a Member State potentially affected by an incident;
- exchanging and making available on a voluntary basis non-confidential information concerning individual incidents;
- discussing and, where possible identifying a coordinated response to an incident that has been identified within the jurisdiction of the Member State, at the request of a representative of a Member State's CSIRT;
- providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance; or
- discussing, exploring and identifying further forms of operational cooperation, including in relation to categories of risks and incidents as well as principles and modalities for coordination, when Member States respond to cross-border risks and incidents.

101. Information exchange on incidents involving financial market entities can also take place through other cooperation mechanisms, in particular the Single Supervisory Mechanism (SSM). It should be noted that not all national competent authorities of the Member States are involved in the cooperation under this mechanism. It only applies to countries.

3.2.3 Use Case: Polish Financial Supervision Authority

102. The Polish Financial Supervision Authority (PFSA) is an example of a national competent authority with tasks connected with incident reporting.

103. These obligations derive primarily from the National Cyber Security System Act, which implements the NIS Directive. Pursuant to Article 41 of the Act, the PFSA remains the competent authority for the sector of banking and financial market infrastructure. In addition, a sector-level CSIRT team (CSIRT KNF) has been established within the PFSA for the relevant sector. This team, in addition to the national CSIRTs, receives major incident reports from operators of essential services in the banking and financial market infrastructure sector.

104. The team's tasks also include assisting operators of essential services in handling cybersecurity incidents, as well as analysing major incidents, finding links between incidents and drawing conclusions from incidents handling. As part of its tasks, the sector-level CSIRT team cooperates with the CSIRT teams at national level to coordinate the handling of major incidents.

105. Entities classified as operators of essential services are required to report security incidents to the relevant national level CSIRT team and sector level CSIRT. Reporting to the national and sector level CSIRT teams is done via a dedicated web form on the

website, or via a prepared PDF form sent via email. In the case of emailing, an additional mechanism is used in the form of PGP encryption.

106. The incident handling process uses the well-known open source RTIR (Request Tracker for Incident Report) solution - the use of the tool allows the handling of reported incidents to be organised and structured. PSD2 incidents are reported directly to the Competent Authority using a dedicated and pre-differentiated form in an XLS file. Files are sent using the government's ePUAP system.

4 Stock-taking and stakeholder consultation

4.1 Stock taking exercise with CAs

107. To gather the necessary insights and information for the feasibility study, a data collection exercise has been conducted during March 2023, primarily through the utilisation of a survey. It is important to consider that the results obtained during the survey may have changed by the time the report was completed. This survey has enabled ESAs to obtain valuable input from key stakeholders (i.e. competent authorities at national and EU level), facilitating a thorough understanding of their reporting needs and preferences. This survey has encompassed a wide range of topics related to incident reporting, including existing reporting processes, data flows, data quality, reporting volumes, and key challenges faced by CA when it comes to reporting.

108. A detailed presentation of the answers to each of the sections can be found in the Annex V. We present here information regarding the overall benefits and risks identified with future further centralised reporting.

4.1.1 Views on the establishment of the single EU Hub for incident reporting under DORA

109. The final section of the survey focused on obtaining the views of the different CAs on the future adoption of a single EU Hub to further centralise reporting, the feasibility analysis of which is the subject of this document. With a view to being able to analyse the data, certain categories were created where respondents could rank the main challenges and risks on the one hand, and the main benefits on the other.

110. Focusing on the risks, most CAs emphasised the nature of the data and the considerations needed to protect the information, but also aspects related to the governance and integration of any future solutions as well as the possible suboptimal integration between DORA and NIS authorities. Although not presented in the graph below, several CAs expressed concerns about possible delays in receiving information from financial entities they are responsible for supervising and the possible loss of immediate contact between financial entities and their competent authorities in the event of further centralisation of reporting.

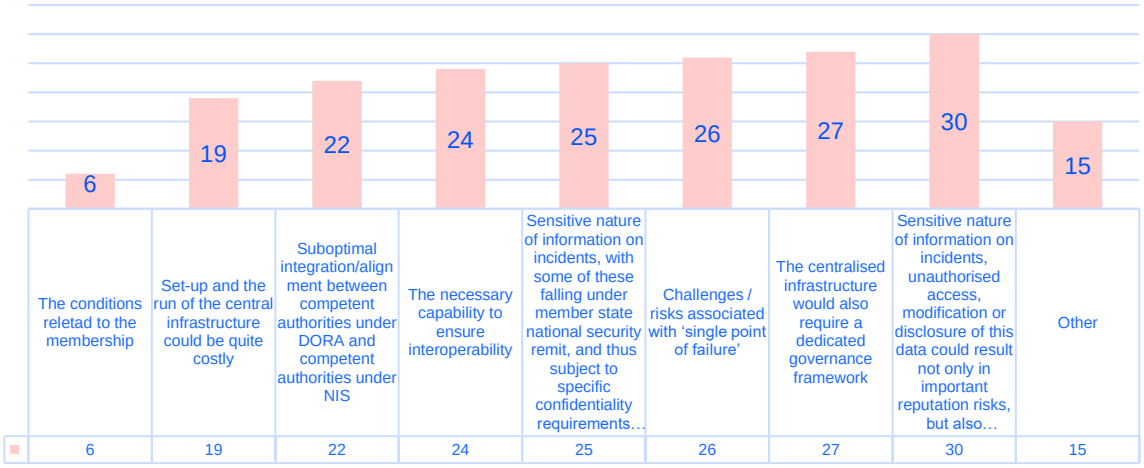


FIGURE 2 POTENTIAL RISKS LINKED TO FURTHER CENTRALISATION

111. On the other hand, several benefits related to the establishment of a centralised Hub were also identified. Simplification of reporting, elimination of duplication and quicker access to information on incidents under DORA by all relevant authorities were the main benefits identified as being linked to the implementation of a future solution with a higher degree of centralisation.

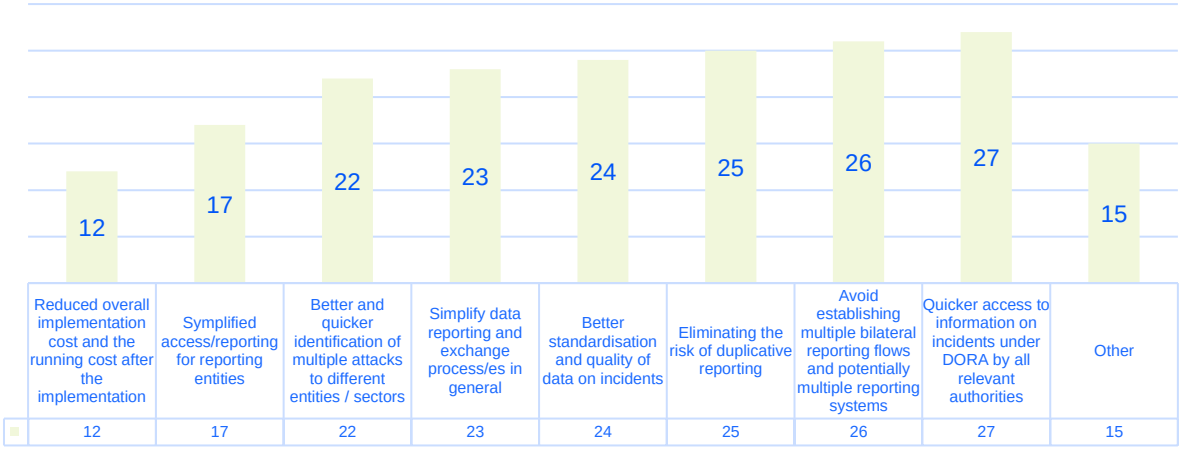


FIGURE 3 POTENTIAL BENEFITS LINKED TO FURTHER CENTRALISATION

4.2 Stakeholder Questionnaire

112. During Q3 2024, a questionnaire was distributed through the stakeholder groups of the three ESAs to gather feedback from market participants on the key elements considered for this feasibility report. Special emphasis was placed on the benefits and risks of each of the different scenarios identified in DORA (and further explained in section 24).

113. Regarding the composition of the responses, the stakeholders' groups of the three ESAs participated in the process[11], with representation from the following groups:

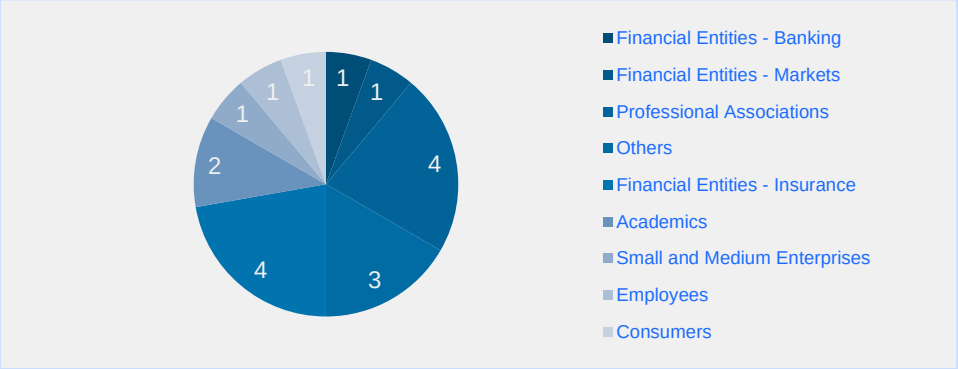
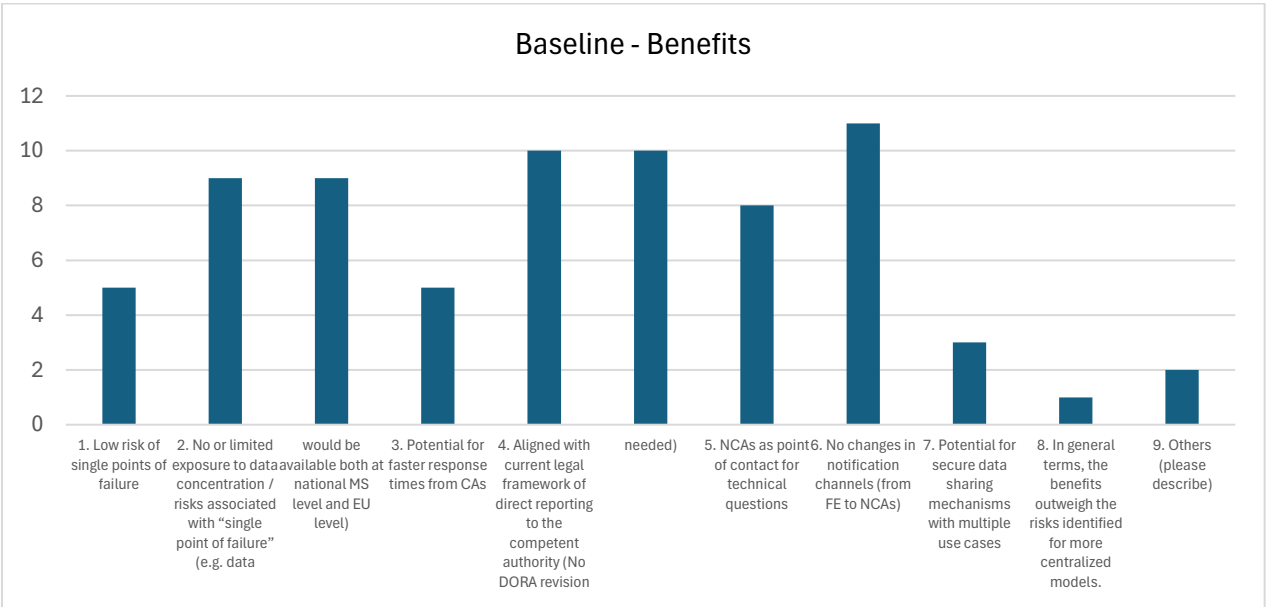


FIGURE 4 STAKEHOLDERS REPRESENTED

114. A total of 18 individual responses were received, along with one aggregated response from the Banking Stakeholders Group (BSG)[12]. One of the respondents belongs to both the BSG and the SMSG. The professional associations represented include three at the EU level and one at the Member State level.

115. An extended version of the analysis of the responses received can also be found in the annex of the document. Here, we highlight the key benefits and risks associated with each scenario, as well as the main conclusions.



[11] Banking Stakeholders Group, Securities and Markets Stakeholders Group, Occupational Pensions Stakeholder Group and Insurance and Reinsurance Stakeholder Group

[12] The BSG's joint response to the questionnaire is included in the Annex.

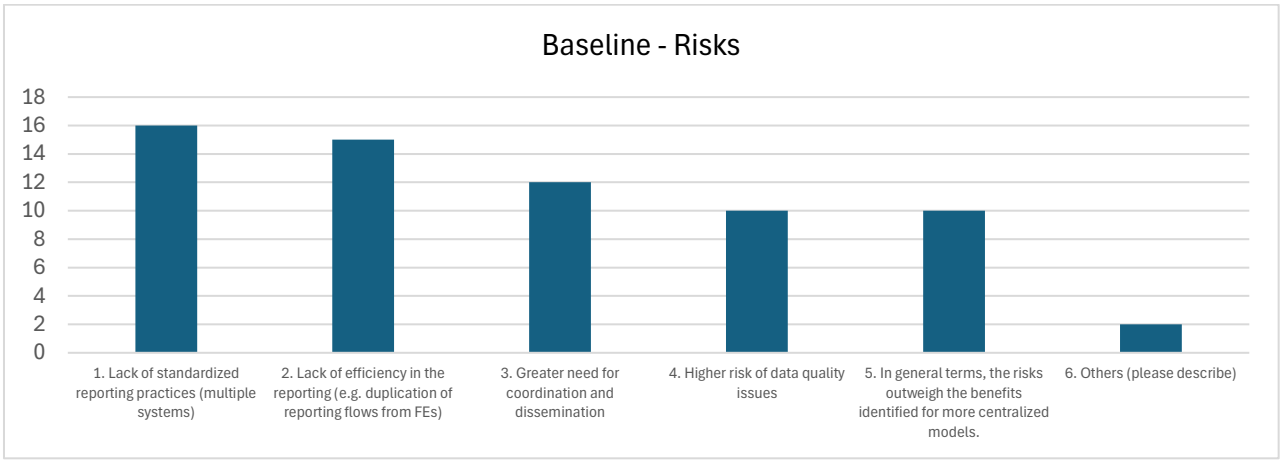
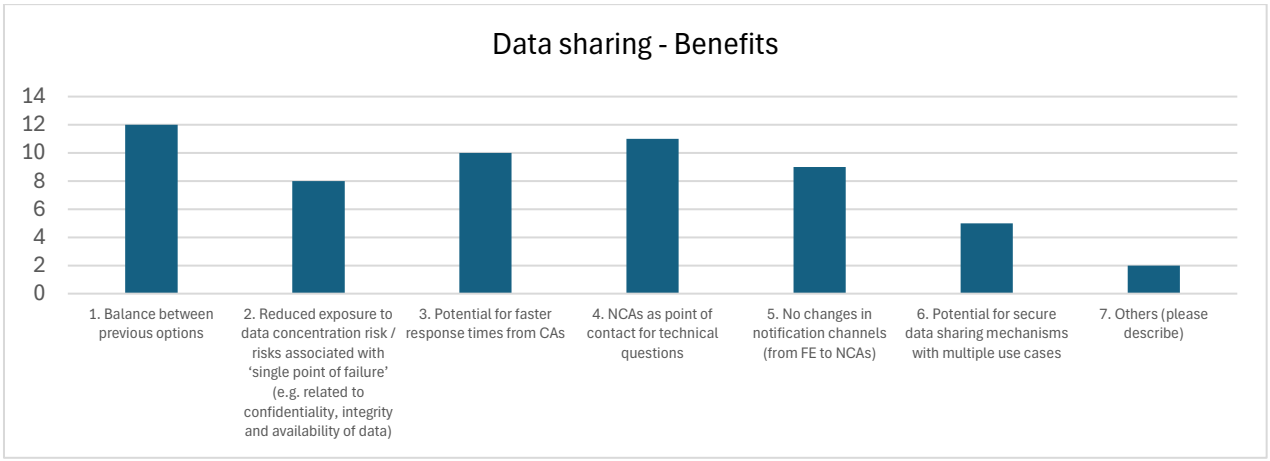


FIGURE 5 BENEFITS AND RISKS - BASELINE



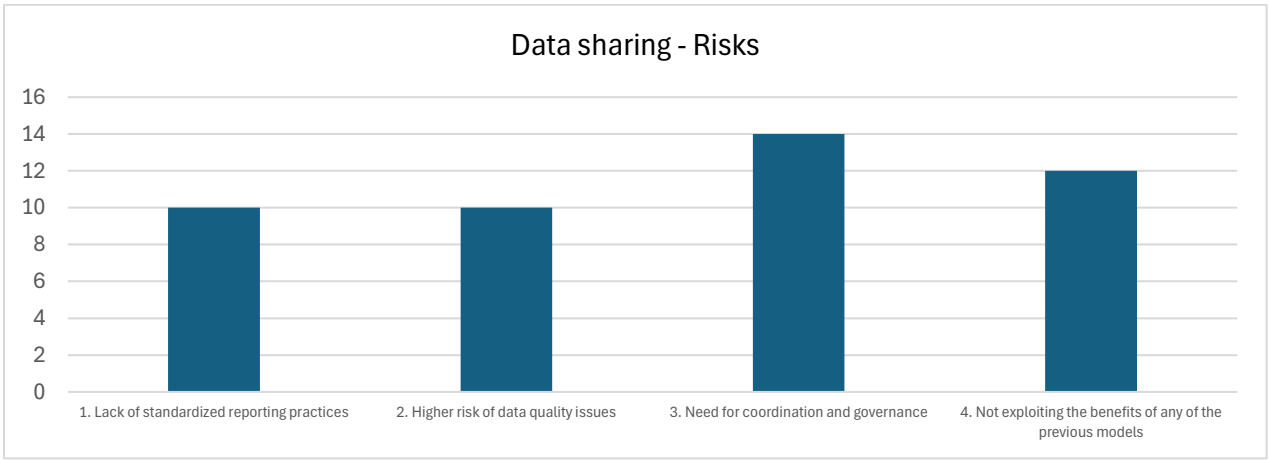


FIGURE 6 BENEFITS AND RISKS - DATA SHARING

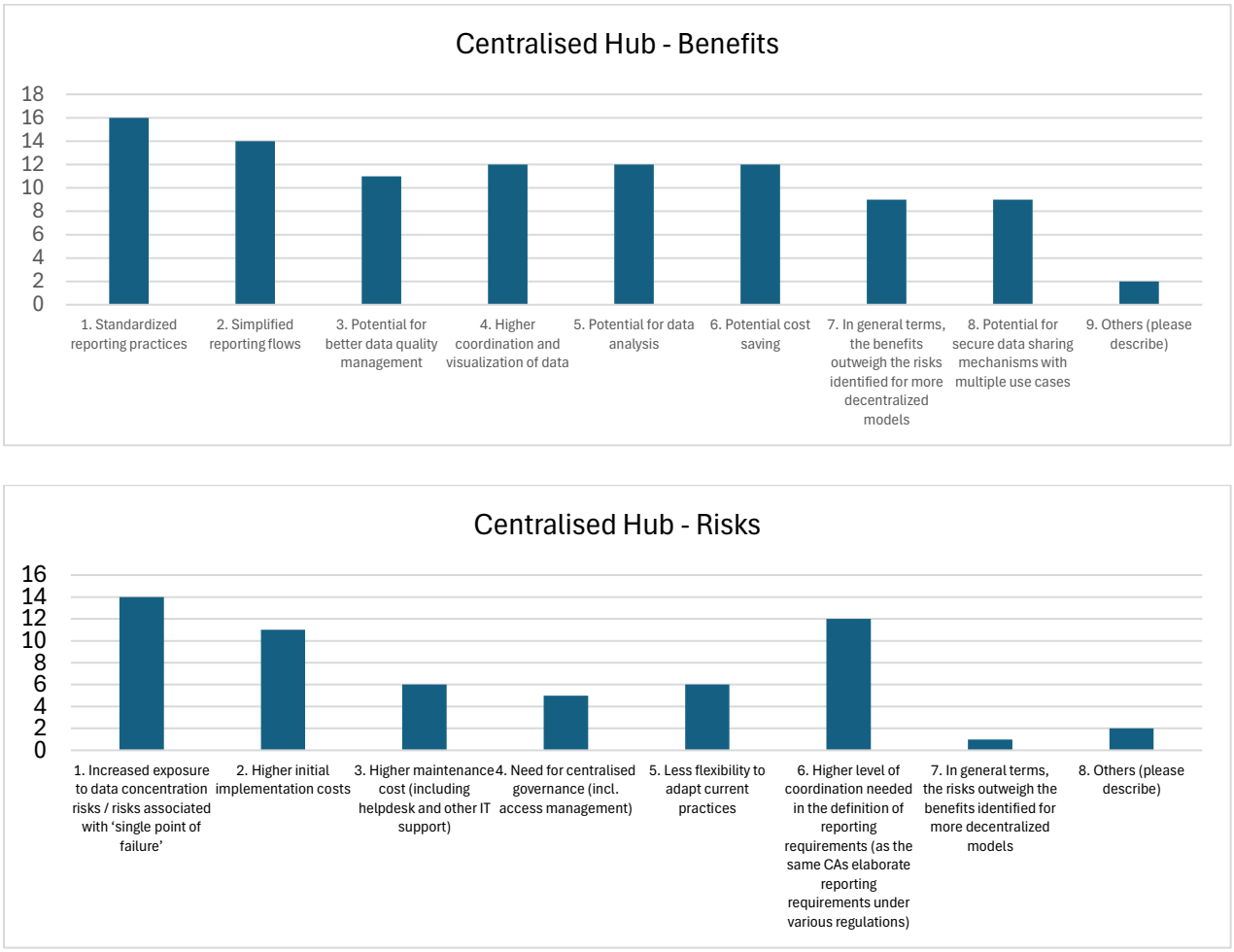


FIGURE 7 BENEFITS AND RISKS – CENTRALISED

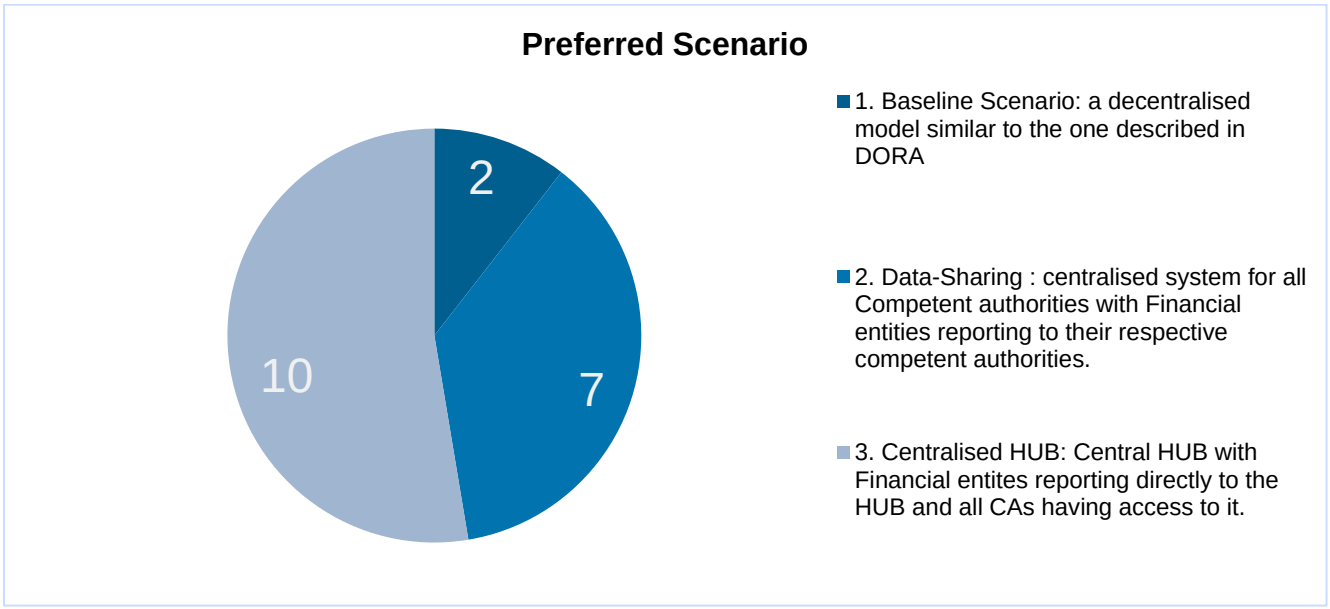


FIGURE 8 PREFERRED SCENARIO

116. Members of the stakeholder groups were asked about their preferred scenario, and the majority supported the most centralised model.

- Baseline Scenario: Least favourite option, only supported by two members of the OPSG.
- Data-Sharing: This is seen as the best option by 7 different members, which are part of three different stakeholder groups, SMSG, BSG and OPSG.
- Centralised HUB: This option is the one with more support, with 10 different members expressing their preference for this scenario. A respondent opted for either the Data-Sharing or the Centralised model. Members supporting this model are members of three different stakeholder groups, OPSG, IRSG and BSG.

5 High level business requirements

117. In conducting the feasibility study outlined by Article 21, various options for further centralisation of the reporting of major ICT-related incidents can be considered. Despite the diversity of potential approaches, there are likely to be common business requirements that would underpin all these structures, enabling a standardised, efficient, and secure incident reporting and management across the European Union. These potential specifications, inferred from the regulatory requirements mentioned in the regulation and from the views of the different competent authorities, would shape the technical backbone of any such centralised system.

118. These requirements will serve as the foundation for evaluating the feasibility of further consolidation and will inform subsequent stages of the study. The identified high-level requirements will encompass both functional and non-functional aspects, taking into account the needs of different stakeholders, regulatory compliance, scalability, and technological considerations.

119. The following requirements should therefore be present in any of the options identified within this study, as they are considered the essential elements from a business requirements perspective.

120. The study will not delve into detailed technical requirements, as they are considered beyond its scope. The requirements have been divided into functional and non-functional. Functional requirements have been grouped according to the phases of the incident reporting and analysis process[13].

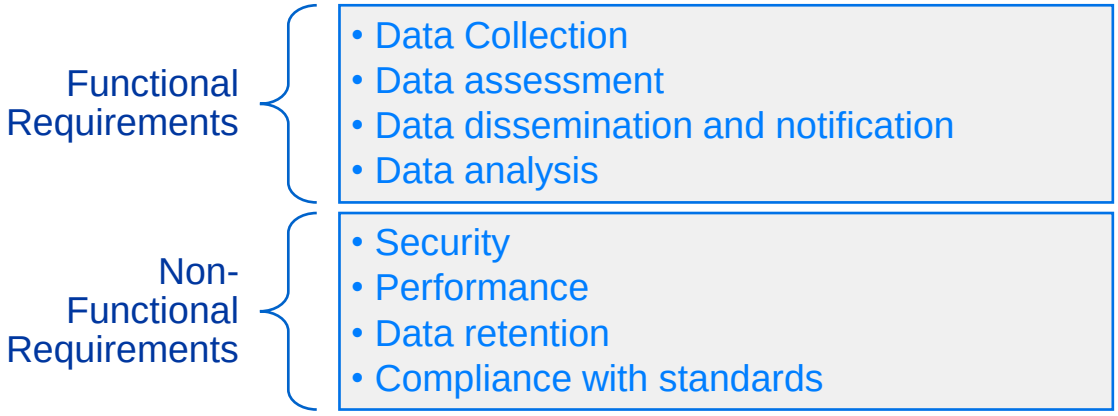


FIGURE 9: HIGH LEVEL FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

[13] For the purpose of the identification of the business requirements, the “reporting entity” can be either a Financial Entity or the CA, depending on the level of centralisation.

121. FUNCTIONAL REQUIREMENTS	
122. Data Collection	
1	The solution shall support the collection of all versions of ICT-related incident reports from the reporting entity in a timely manner (as defined in DORA and RTS/ITS on Incident reporting), and at any rate in a very short timeframe (to be agreed with CAs).
2	Each reporting entity shall be able to submit incident reports to the solution using the templates, taxonomy and respective data point model developed based on the RTS/ITS on Incidents reporting.
3	The solution shall identify and link the different messages related to every reported incident as per Art 19 (4) of DORA.
4	The solution shall provide unique reference number and timestamp for all submitted reports and link the reference numbers of subsequent reports (initial notification, intermediate and final report) in line with Requirement 3.
5	The solution shall register the date and the time when the CA or FE (depending on the reporting agent) reported the incident and track all actions taken on reports.
6	The solution shall allow unintentional or erroneous submissions to be cancelled, modified, or reversed by the submitting CAs/FEs (depending on the reporting agent) or system administrators.
7	The solution shall perform data validation checks against the taxonomy, technical specifications set by the ESAs when implementing technical package for RTS/ITS on Incident reporting or a predefined set of validations created ad hoc.
8	The solution shall acknowledge the reception of the incident to the reporting entity, following the reception of a report/notification file, in very short timeframe. The acknowledgement shall include the successful collection of the report or the need to revise/resubmit the report, where the validation and completeness checks have not been passed, (indicating the fields that didn't pass the validation). In relation to validation, this should happen immediately and in parallel to the process of uploading the information into the system (i.e. at the moment this information is available in the system, to avoid iteration loops as far as possible).
9	The solution shall support the ESAs in collecting significant cyber threats reports from the reporting entity. (Although the notification of cyber threats is voluntary, it is considered that any solution should be able to accommodate the reporting of these threats)
10	The solution shall enable machine to machine reporting (e.g. through APIs) from and to the systems of the reporting entity, as well as the possibility of manual

	reporting (as some reporting entities will have less sophisticated IT systems). At the same time the IR IT system shall support bulk file upload.
Data assessment	
11	The solution shall support the manual and automated assessment of incident reports in order to identify whether the major ICT-related incident is relevant to stakeholders other than the reporting entity based on specific data fields from the incident report.
12	The solution shall support rule-engines that can be enabled and configured through pre-defined structured data fields to assess and disseminate incident messages/information to relevant users in a timely manner (very short timeframe to be agreed with CAs).
Data dissemination and notification	
13	The solution shall allow forwarding or providing access to incident reports to relevant stakeholders following the Data assessment phase.
14	The solution shall support the notification of the flagged reports to relevant stakeholders and shall provide the stakeholders with access to them, including all intermediate reports.
15	The solution shall allow the export of reports.
16	The solution shall facilitate the communication process among the different stakeholders through specific communication channels.
Data analysis	
17	The solution shall support manual and automated analysis of the incident data in a way that allows using all reported data for the purposes of the preparation of the annual report or to be used in sectorial risk assessment by the ESAs, in accordance with Article 22.2 paragraph 1 of DORA.
18	The solution shall support the analysis of the incident data in a way that allows using all reported data for the purposes of the ESAs issuing of warnings (the IT system itself does not have to generate the warnings but support the process), and the production of high-level statistics, in accordance with Article 22.2 paragraph 2 of DORA (e.g. through data visualisation).
NON - FUNCTIONAL REQUIREMENTS	
Security	

19	Incident data to be classified and the solution shall treat it in accordance with the relevant EU policies linked to this level of confidentiality.
20	The solution shall include a comprehensive user management system that allows for seamless registration, authentication, authorisation, and profile management. The solution system shall allow for managing access to the system and its data, based on roles and responsibilities (for example, role-based access control, including user profiles and user groups) for the different stakeholders (i.e. CAs, ESAs, FEs, ECB). The solution shall allow each CA to maintain the details of the FEs reporting to them and other data management tasks, including which other authorities should receive reports submitted to them. The principle of least privilege, where individuals have only the access necessary to perform their roles, shall apply. In the case of FEs having direct access to the system, the solution shall support additional identity and access management complexity, since an important number of different access profiles would need to be supported.
21	The solution shall ensure the integrity of the data.
22	The solution shall guarantee the availability of the data.
23	The solution shall maintain a high uptime.
24	The solution shall ensure that the personal data contained in the incident reports is protected in line with the GDPR and EDPR requirements.
Performance	
25	The solution shall be capable of handling a volume of incidents to be determined, but it would likely scale to several thousand per year. The estimated volume could be derived from actual volumes received prior to the implementation of the solution. The number of cross-border incidents per year, which is estimated on a best-efforts basis to be around 20% of total incidents reported
26	The solution shall provide quick response time, processing data in a timely manner (timeframe to be agreed with CAs).
27	The solution shall accommodate future increases in reported incidents, ensuring seamless expansion of functionalities, while supporting effective change management processes
28	The system shall support a large number of users accessing the system, in the order of several thousands
Data retention	

29	Incident reporting files and other related data (audit logs, user data, etc.) shall be maintained for 5 years.
Compliance with standards	
30	The solution shall comply with generally accepted data reporting standards and data communication protocols and should allow a consistent approach with data reporting standards and communication protocols for ICT-related incident under the Directive (EU) 2022/2555 (NIS2).
31	The solution shall comply with EU Web Accessibility Directive [Directive (EU) 2016/2102]
32	The solution should guarantee Interoperability, understood as the ability to exchange and make use of information, whether it's data from financial entities, national competent authorities, or other EU institutions. The solution should be built using open standards and protocols, allowing it to interface effectively with the variety of systems used by different stakeholders.

TABLE 1 HIGH LEVEL BUSINESS REQUIREMENTS

6 Commercial solutions

123. Based on an initial high-level analysis, the market scan demonstrated that there may be off-the-shelf commercial solutions that exist with a high degree of functional and non-functional fit (see for details of these requirements chapter section 5). The ESAs and CAs identified a total of 10 technological solutions with the potential to accommodate the incident flow in DORA and its specifications. Four vendors responded to the Request for Information (RfI).

Vendor A: ~25 employees

- The solution proposed offers an open-source enterprise-level ticket management system. Organizations of all sizes use the solution to track and manage workflows, customer requests, and internal project tasks of all sorts. With seamless email integration, custom ticket lifecycles, configurable automation, and detailed permissions and roles. The solution builds on all the features and provides additional tools to correlate key data from incident reports, find patterns and link incident reports, and manage communication to multiple interested parties.

Vendor B: ~200 employees

- The vendor offers IT Service Management (ITSM) solutions. The Incident Management solution has been developed in-line with the ITIL Best Practices Framework and has been verified in Incident Management for IT Service Management (ITSM). The solution covers functionalities such as activity tracking on incident request, attaching multiple incidents to a problem request, full traceability on all activities, sharing incident resolutions with various stakeholders, etc.

Vendor C: ~500 employees

- The vendor offers cloud-based software specialised in risk management, integrating governance, risk, compliance software and ethics & compliance learning resources. The proposed solution allows organisation to improve their speed and efficiency to report on, respond to, and resolve any incident. It offers functionality such as multimodal incident reporting, automated end-to-end investigations, real-time access to one central data repository.

Vendor D: >>10000 employees

- The vendor offers a cloud-based solutions. The proposed Incident Management solution provides the necessary tools to identify and track incidents and collaborates with the relevant involved parties. The solution offers functionalities such as event monitoring, automation of repetitive tasks, centralised workspace, broadcast communication for internal teams and customers, reporting and dashboards, etc.

124. All vendors seem to offer strong capability coverage across the functional requirements, most specifically in Data Collection, Data Dissemination and Notification. Based on the available information the vendors were able to provide only rough (order of magnitude)

price indications – the indicative prices were ranging from 125k€ to 180k€ per year, depending on the solution and the deployment method selected it refers to a service fee or a recurring annual software maintenance fee. Based on the available information, 3 out of the 4 participating vendors estimate that the implementation of their solutions could take up to 6 months what covers the setup and integration of the solution. One vendor was not able/willing to provide an estimate based on the available information.

125. In the Request for Information (RfI), the vendors were asked to score their solutions against the DORA requirements listed in chapter 5. The scores in the table below are based on these vendors self-assessment and aggregated across all functional and non-functional requirements which are equally weighted for the aggregation. 100% means the requested requirements can completely be covered by the standard functionality provided by the solution.

Aggregated Score	Functional Requirements	Non-Functional Requirements
Solution A	87%	94%
Solution B	100%	100%
Solution C	100%	99%
Solution D	100%	94%

TABLE 2 COVERAGE OF FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

126. All solutions cover all functional and non-functional requirements - the difference between the solutions is to which degree this is a standard functionality of the solution or how much effort is needed to customise the solution for the use in the context of DORA. In general, all solutions can cope with all functional and non-functional requirements according to the vendors.

127. These results - the functional and non-functional coverage of the different solutions would need to be validated with the vendors during workshops as a next step. The level of granularity of the requirements used for the RfI was adapted to that of a feasibility study. To pursue a more detailed and informed assessment in next phases of this endeavour once a standard solution is sought, key use cases would need to be identified. In addition, and in order to validate the RfI results and to conduct a Request for Proposal (RfP) the following steps can be taken:

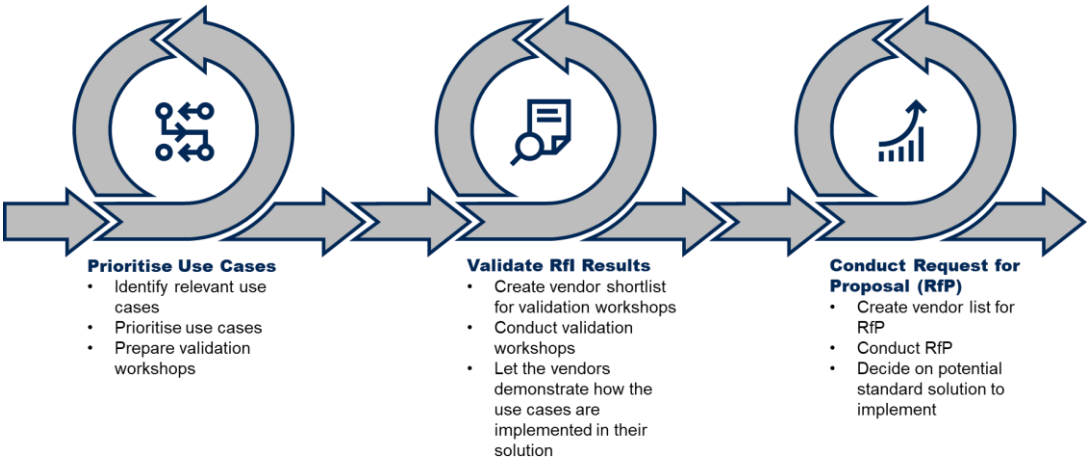


FIGURE 10 REQUEST FOR PROPOSAL (RFP) PROCESS

128.

7 Identification overview of potential options

129. This section identifies and presents three options:

- the baseline option, based on Article 19 and 22 of DORA and on input from the ongoing work performed by the ESAs together with the CAs to enable incident reporting in January 2025
- two potential options for further centralisation of incident reporting as defined in the recital 55 of DORA: Data Sharing solution and Centralised Hub (EU Hub).

130. The following sections describe each of the identified options.

FIGURE 11: OPTIONS CONSIDERED IN THIS REPORT

7.1 Baseline Scenario

131. The tasks assigned to the different stakeholders under DORA (see Incident reporting under DORA) warranted coordinated work for incident reporting from the perspective of the ESAs that could be ready during 2025. Based on this, the ESAs, in coordination with the member states, the ECB, ENISA, and the SRB, are developing a joint tool to meet the mandate established in Articles 19 and 22 of DORA which relates to facilitating incident reporting from the competent authorities in the various member states to these European authorities for relevant incident reports[14]. This system is under development at the time of finalisation of the present feasibility study and will be considered the "*Baseline scenario*". [15]

132. The Baseline Scenario is defined by the expected starting situation at the beginning of the incident reporting under DORA in 2025. By this time, the ESAs will have implemented a common tool to facilitate the reporting and dissemination of incidents from and to CAs. Under this Baseline scenario CAs will receive the incidents directly from the FEs.

133. This tool has been developed as part of the CIRAS system operated by ENISA.

[14] Incident reports are forwarded to other authorities based on their competence. All incident reports are not forwarded to any single EU authority

[15] The scenario is presented at a high level as defined for its implementation in 2025, without disregarding potential future changes that could impact it (in terms of governance, data management, etc.).

134. Thus, the reporting flows are fundamentally based on those established in DORA with the following modifications:

- The flow from the relevant competent authorities to the ESAs is common. That is, the same system allows for the reception of such incidents, ensuring access to the relevant ESA, depending on its competencies.
- This system, based on the information contained in the reported incident, is capable of notifying other competent authorities in other member states. These competent authorities can then access the system to consult or download the incident report.

135. The reporting flow from the competent authorities to the ECB is twofold:

- Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, will report to the CAs, which will immediately transmit that report to the ECB/SSM. The IT tool to accommodate this data flow is out of the scope of the solution developed by ESAs.
- Incidents related to financial entities under Article 2(1), points (a), (b) and (d) will be reported from the CAs to the ESAs System. This system will channel the reports to the ECB.

136. The reporting flow from the competent authorities to the SRB is simplified, the SRB will be notified in case an incident is related to Critical Functions directly from the ESAs solution. This way, CAs avoid notifying the SRB in parallel, achieving a certain level of centralisation.

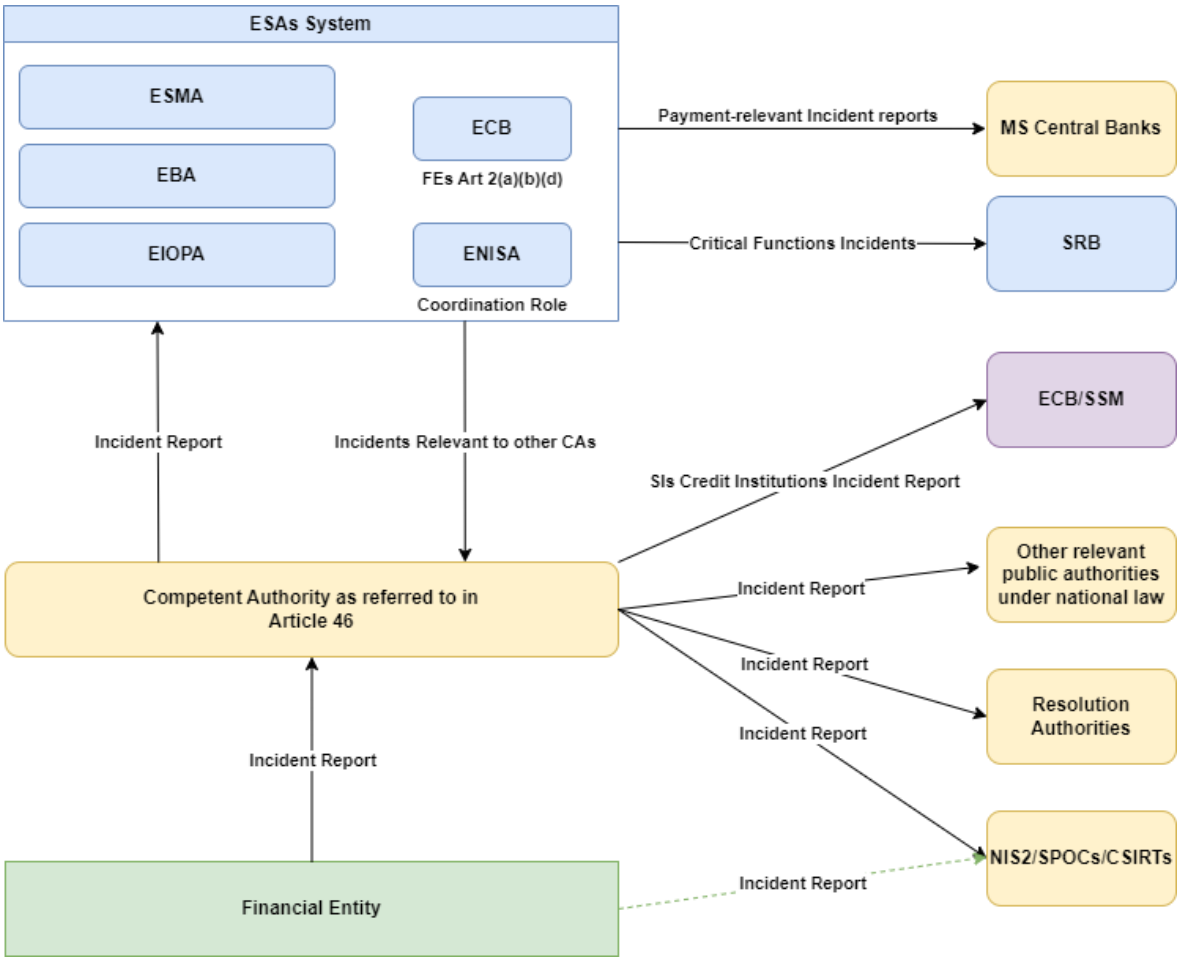


FIGURE 12 BASELINE SCENARIO - DATA FLOWS

137. Under this scenario there is still a proliferation of incident reporting flows:

- There is potential parallel reporting at the FE level under Article 19(1) paragraph 6 and Article 19(2) paragraph 3 (NIS2/SPOCs/CSIRTS authorities, represented by the green arrow in the figure). At the same time, it is relevant to consider that the situation may differ from one Member State to another, and can be avoided even in the baseline scenario, as the double reporting to DORA NCAs and NIS2 is subject to the decision at member state level, therefore the number of parallel reporting lines could be reduced.
- Potential parallel reporting at the group level of financial entities operating under the supervision of different CAs. Under DORA, each FE is assigned for reporting purposes to a single CA. However, for those groups of FEs supervised across multiple geographies or sectors, there is a potential duplication in the flow of incidents. The volume of incidents under this scenario is unknown at the time of drafting this report.
- There is identification of parallel onward transmission of reports by CAs to ESAs, ECB, and other national authorities. Although the baseline scenario already includes a certain degree of centralisation at the EU level, the CAs are required to forward the same incident report (depending on their responsibilities) to the ESAs system, the ECB, and/or other national authorities.

138. Regarding the graph shown above, the flows of data have been simplified at the member state level, as the represented structure will need to be replicated in all countries.

139. It is relevant to emphasise that reporting flows from Financial Entities to CAs are carried out under the systems and mechanisms implemented by said Competent Authorities. In other words, there is no additional centralisation in this area, and each CA establishes such mechanisms.

140. On the other hand, it is also important to note that the reporting will be based on what is established in the RTS and ITS on content, timelines, and templates on incident Reporting.

141. To delve into the standardisation of reporting, the competent authorities, in collaboration with the ESAs, have developed the data model, validations, and other aspects related to the Data management for the flow between CAs and the ESAs System.

142. Similarly, the competent authorities have also participated jointly with the ESAs, ENISA, the ECB, and SRB in defining the business requirements for the solution implemented by the ESAs and were also involved in other relevant deliverables of this project.

143. The baseline scenario presented in this study could be slightly different from what is currently outlined, as it is still in the development phase, but the main characteristics and the data flow could be considered stable.

7.2 Identification of alternatives for further centralisation

144. The identification of the various options for further centralisation of incident reporting was based on the options already mentioned in DORA.

145. Firstly, in recital 55 of DORA, there is a reference to a model in which the relevant competent authorities remain as the primary point of contact for financial entities, with the HUB acting as a coordination mechanism, merely centralising relevant reports forwarded

by the national competent authorities. For the purposes of this study, we will refer to this alternative as the "**Data Sharing**".

146. Furthermore, recital 55 and the first point of article 21 of DORA identifies a fully centralised option through the establishment of a single EU Hub for major ICT-related incidents where financial entities directly report to the EU Hub. For the purposes of this study, we will refer to this alternative as the "**Centralised Hub**".

147. Other possible options not described in DORA were also considered but were initially discarded after preliminary discussions among ESAs and CAs. These alternatives were deemed unnecessary to pursue further, given that a high-level cost-benefit assessment indicated that the two options already identified in DORA were sufficient.

7.2.1 Data Sharing Scenario

148. This scenario identifies an intermediate model of centralisation, combining elements from the model established in DORA (and already included in the Baseline Scenario) with elements included in the Centralised Hub, and is based on the second of the scenarios identified in recital 55 of this regulation.

149. From DORA, it is extracted that Competent Authorities remain as the first point of contact for incident reporting from Financial Entities. Additionally, the responsibility of transmitting these reports to the Hub continues to stay with these competent authorities.

150. Centralisation occurs once the reports are reported to the Hub, which, acting as a coordination mechanism, makes the information available to the various stakeholders involved in the process.

151. Regarding the graph shown before, the flows of data represented at member state level have been simplified, as the represented structure will need to be replicated in all countries.

152. Under this scenario, the duplication of reporting flows is only maintained in the case of those groups of FEs operating under the supervision of more than one NCA (due to sectoral or geographical footprint reasons)

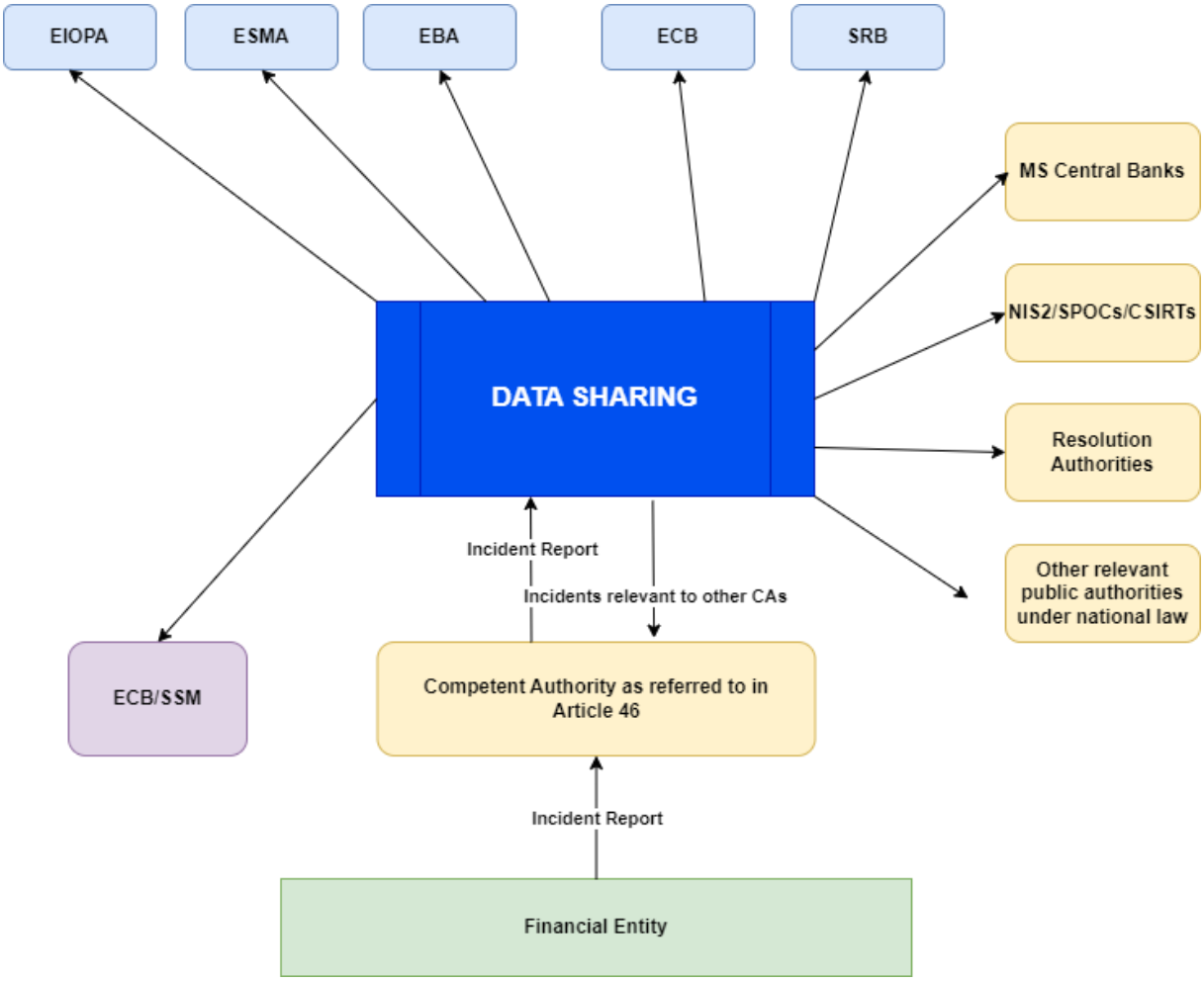


FIGURE 13 DATA SHARING SCENARIO - DATA FLOWS[16]

7.2.2 Centralised Hub Scenario

153. The Centralised Hub (single EU Hub) represents the most centralised model among the considered alternatives and is fundamentally based on the mandate established under Article 21 of DORA. This means a model where Financial Entities report directly to this new Hub, and the rest of the stakeholders to be receiving notifications, access to reports and consuming relevant information, based on their competences, through the Hub.

154. Such centralisation occurs both from the reporting and information dissemination perspectives, but also at the level of analysis. Under this model, various stakeholders would have access to centralised tools to assist in the analysis and follow-up processes. Therefore, the model should ensure access to key individuals within each organisation. For example, at the level of CAs, it should guarantee access to data and analytical tools to supervisors responsible for monitoring and analysing the reported incidents.

155. Based on the above, the flow established for incident reporting under Article 19 of DORA disappears and is replaced by a new model where all stakeholders, including Financial

[16] The black arrows indicate the initial flow from the FEs or CAs. The red arrows indicate the notification or the possibility of access to the data by the other stakeholders through the Data Sharing solution.

Entities, have access to the same information based on their competencies and responsibilities.

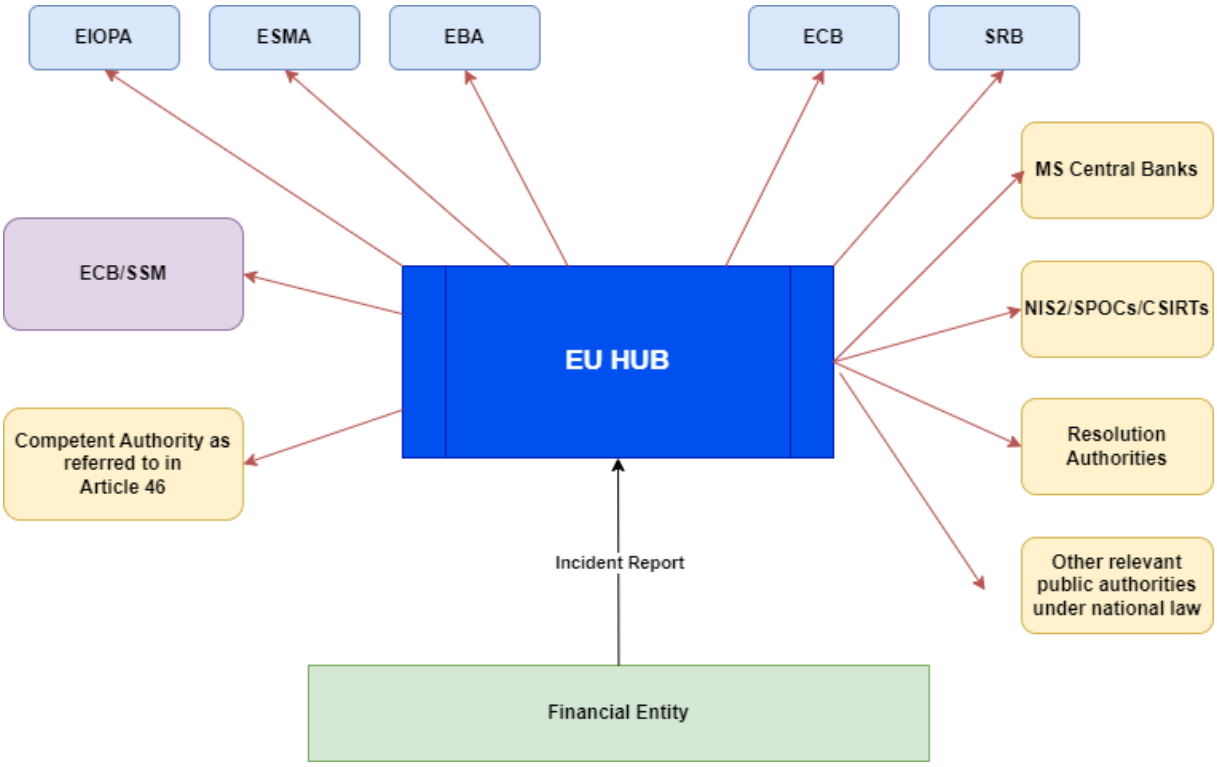


FIGURE 14 CENTRALISED SCENARIO - DATA FLOWS[17]

7.3 Differences between the Baseline Scenario and the Data Sharing Scenario

156. While the differences between the Baseline Scenario and the Centralised EU Hub Scenario are more pronounced, the Baseline and Data Sharing Scenario are similar. To facilitate the analysis, it is important to highlight the main two differences:

- The CAs that access the Data Sharing solution directly also could cover national NIS2 Authorities/SPOCs/CSIRTs hence the number of CAs having directly access is expected to be higher compared to the Baseline Scenario
- In the Data Sharing Scenario, all stakeholders except the FEs have direct access to the central solution for notification / dissemination purposes. This eliminates the need to notify incidents at the national level (e.g., to national NIS2 Authorities/SPOCs/CSIRTs, NCBs as members of the ESCB in their capacity as oversight authorities).). The same applies at the EU level, where in the Data Sharing

[17] The black arrow indicates the initial flow from the FEs. The red arrows indicate the notification or the possibility of access to the data by the other stakeholders through the HUB.

Scenario, all competent authorities at the European level consume information from the central solution.

8 Assessment

157. This section encompasses the limitations in the assessment performed, the identification of the elements considered for evaluation, a high-level cost-benefit analysis, and additional considerations for the potential implementation of scenarios beyond the baseline.

8.1 Limitations

158. With the information available, at the drafting of this report, conducting a detailed assessment for the three scenarios is highly complex. For example, even for the baseline scenario, currently under development, a more precise cost analysis is relatively difficult to obtain considering the different types of IT implementation in the different CAs and the current phase of the ongoing developments. Producing a comprehensive assessment and breakdown of the total costs for the data-sharing and centralised scenarios proves to be even more challenging due to the high uncertainty regarding factors that would impact such assessment and cost calculation. Nonetheless, the assessment performed, and the cost estimation are critical to the feasibility of each scenario—and therefore to the conclusions of this document. Additionally, identifying the primary cost areas is valuable for outlining financial implications.

159. Specifically, below we have identified the numerous variables (known unknowns) that could significantly alter the overall assessment and costs of centralisation, both at the ESA/EU and NCA level.

- **Unknown specific design and development needs:** Detailed design and functional requirements of the centralised approach cannot be more precise at this stage, than the analysis made above on the different requirements. This makes the cost calculation of the development effort quite abstract. This includes key design elements such as system technical design, system integrations and interdependencies, specific information security design aspects, amongst others, all of which could result in variations in complexity and cost.
- **Unknown number of total incidents:** currently we do not have a stable estimate on the number of incidents that would be reported, as this would be the first time such reporting will take place. We are also unclear on the proliferation of parallel channels (please refer to par. 137) of reporting, the reporting and management of which could indeed increase the costs of decentralised solutions depending on the frequency of such reports.
- **Legal and regulatory considerations:** there is a dependency on the key legal changes that could potentially influence the design of the proposed approach.
- **Interoperability with NCAs IT systems used for supervisory response and follow-up:** Each NCA operates unique systems with varying degrees of technical complexity, integration, sophistication and automation. And some NCAs may not operate any system and rely on manual submissions (e.g. via secure email). While reporting systems at NCAs may not be needed if reporting is centralised, NCAs may still need to integrate into the centralised solution any systems / functionalities of the system they use to conduct supervisory response and follow-up on major incidents (e.g. GRC systems). This could involve vastly different levels of effort and will increase the complexity in the design of such a centralised solution, as well as implementation.

- **Unknown timelines:** The lack of a detailed and concrete timeline creates uncertainty in terms of costs, planning, budgeting, resource allocation, and governance needs.
- **Ongoing costing:** Centralised models will lead to duplication of some technical, data and operational elements already present in the various CAs for other analogous reporting processes, as well as to continuous governance and maintenance.

8.2 Assessment areas

160. The mandate under Article 21 of DORA sets out the minimum elements to be considered in the feasibility study, namely its paragraph 2, points (a) to (g), lists 7 elements on which the feasibility study should at least elaborate. However, it is necessary to clarify them in more detail, to be able to establish an effective analysis and comparison of the different options considered.

161. The tables below further elaborate on the key elements considered in the evaluation of each of the criteria identified in Article 21(2) of DORA and its assessment. An additional analysis of each of these elements for each of the identified scenarios, elaborated by an independent expert (i.e. Gartner Consulting), is included in the Annex I: Assessment summary - .

Article 21(2)(a) Prerequisites for the establishment of a single EU Hub
Infrastructure and Technology Requirements: The initial technological requirements enabling the scenario, vary significantly, particularly in terms of the hardware and software needed from day one. These requirements depend on the desired level of centralisation and the necessary connectivity between the various stakeholders and the technological solutions they need to be connected to. In the context of these requirements, potential proliferation of IT systems serving the same purpose, as well as potential duplications were considered as factors. In general terms, the prerequisite is to ensure that competent authorities are provided with pertinent information without delay (e.g. requirements for an immediate and automatic alert and synchronisation in the access to incident), this is identified as a priority for each of the scenarios outlined given their supervisory responsibilities for incident response. In this context, a cloud computing -based implementation is considered appropriate, considering the requirements of the baseline solution, which is currently under implementation. The implementation should allow to have access without delays to the right data. **Information Security requirements**: In addition, in all scenarios, strong information security requirements are needed, to ensure confidentiality, integrity and availability of the reported data. The dataset has already been classified as Sensitive non-classified information for the purposes of the baseline scenario, and the ESAs would need to ensure compliance with the Cybersecurity Regulation at the institutions, bodies, offices**,** and agencies of the Union[18]. While, the fully centralised scenario is expected to have higher risks related mostly to the availability of the incident reporting information, all scenarios would require comprehensive information security controls in place, particularly but not limited to the identify and access management, to minimise the risks of unauthorised access, disclosure and/or modification of data. This is because even in the case of the baseline scenario, the information will be stored at national systems but also in a centralised database (ESAs hub). **Governance of centralisation (who host and manage the solution)**: While at the moment of drafting this feasibility report, it is not yet decided which EU body will store the data in their systems, at the same time two options are considered currently: an ESA's system, as well as ENISA, which will need to host similar dataset for other incident reporting regimes. Both options provide for solid implementations, considering technical prerequisites and information security requirements as identified above. **Legal prerequisites**: the necessary regulatory changes under DORA (as it forms the basis of the mandate) are considered, including some details on the specific articles and provisions that may need to be amended. The assessment took into consideration that the baseline scenario does not require changes to the legal framework. The Data-sharing scenario would require some minor changes, in particular with regard to reporting to NIS authorities. The centralised solution would require amendments to DORA and Level 2 regulation. Namely, legal changes required under the centralised solution, although not

[18] Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Article 21(2)(a) Prerequisites for the establishment of a single EU Hub

numerous in quantitative terms, will impact the current data flows from the FEs to the CAs, constituting a significant change in the existing process. Similarly, to fully leverage the benefits of the centralised solution, the aggregated incident reporting (a single report for incidents with cross-sector and cross-Member State impact) should be regulated (the aggregated reporting is only partially developed in Article 7 of the **ITS** in accordance with Article 20, first subparagraph, point (b) of DORA, hereinafter the 'ITS on forms, templates, and procedures'**),** the need for an agreement on these arrangements, particularly concerning the aggregated reporting, can also be considered a potential risk, as the successful implementation, particularly concerning the aggregated reporting, can also be considered a potential risk, as the successful implementation of such changes depends on achieving consensus among relevant stakeholders. Additionally**,** changes are needed in the legal provisions for alternative reporting mechanisms in cases of technical unavailability. The legal assessment has not considered potential legal changes, if any, for any of the scenarios at the Member State level.

Article 21(2)(b) Benefits, limitations and risks, including risks associated with the high concentration of sensitive information

This point is relatively heterogeneous; therefore, the assessment has been divided among the various elements included in the mandate. Here, we focus on the most relevant elements, with further elaboration provided in the annex.

In the baseline scenario, the focus of the assessment is on utilising the existing systems and processes of the CAs, along with the investments made to adapt to DORA, particularly in the short term. Regarding the other scenarios, it has been considered that the centralised scenario involves the creation and maintenance of a single infrastructure, which will involve additional costs to establish but could potentially result in economies of scale and efficiency for some stakeholders (e.g. groups of financial entities that report in more than one Member State,)) over the medium to long term. In this scenario, CAs will still operate reporting systems for different purposes/reporting frameworks. The data-sharing scenario emphasises the potential reuse of the CAs' systems and could be implemented as an expansion of the baseline. scenario. Equally important is the data flow between stakeholders. The flows from FEs and CAs have been considered and any changes to them, depending on the approach used.

In terms of supervisory convergence, the degree of standardisation increases with the centralisation of reporting. All scenarios (including the baseline) allow for standardisation (through taxonomies, formats, standardised validations)), but this standardisation becomes more evident as the centralisation of the flow increases. It has been also considered how the different levels of centralisation have the potential to generate inconsistent and asynchronous databases and the possibilities for allowing for an enhanced market overview through a consolidated database.

Identified limitations: In the centralised scenario, the CAs are no longer the first point of contact for the FEs and in some cases possible specificities relevant to them in the reporting flow may be lost. In the non-centralised scenarios, the limitation lies in the possible delays in accessing and consolidating information due to the two-stage process and the need for the Groups of FEs that report in a number of Member States or under different sectors to report through different systems. Language barriers should also be considered for all three scenarios, with relative advantages in the baseline model due to maintaining current reporting flows.

Risk Identification: At the operational and technical level, there are risks linked to the possible duplication of information and systems and lack of harmonisation on information security controls. Linked to this is the risk of data concentration and single point of failure in the centralised model, which should be mitigated with appropriate measures. This risk does not disappear completely in the decentralised models, as some information is still kept at the centralised (ESAs) and decentralised levels. Reputational risk, as the whole process takes place centrally, is the highest in the centralised scenario. Finally, the risk of delays in the consolidation of information from different sources in the decentralised models is reduced in the centralised model with only one reporting step in the process. Risk, though the ability of DORA and NIS competent authorities to escalate and respond in a timely manner might be less in a centralised scenario.

Article 21(2)(c) The necessary capability to ensure interoperability with regard to other relevant reporting schemes

Technical compatibility and existing systems: the assessment has considered a variation in interoperability in the baseline scenario for CAs. In the baseline scenario the CAs should connect to several solutions depending on the stakeholder to whom they shall notify incidents (ESAs, ECB, and if necessary other competent authorities at national level), in the data-sharing and centralised model, the need to connect to multiple systems is reduced to a single system. FEs should connect to the DORA CA (to multiple DORA CAs in case of Groups of FEs or parallel reporting to NIS authorities as identified in par 137) in the decentralised scenarios, and directly to the EU Hub in the centralised scenario. It is important to emphasise that the centralised scenario could allow CAs to access and consume/analyse the relevant information for their internal use.

Data sharing and harmonisation: in the Baseline and Data sharing scenarios, it is managed by the CAs in collaboration with the ESAs (and can be improved through detailed taxonomies, validations, etc.) with possible difficulties due to the two-step process and the different reporting pathways. In the centralised scenario it is managed in a single step.

Article 21(2)(d) Elements of operational management

Governance Structure: The complexity of the governance models for each of the scenarios has been considered. In the centralised model at EU level, the management of all FEs accessing the systems could concentrate the complexity in one central solution and could introduce a complex governance model as the underlying system is decentralised. Management of FEs still remains in decentralised (at MS/CA level) scenarios with potentiality of duplications.

Data Management Procedures: Data management procedures are duplicated in both Baseline and Data-sharing. Data management procedures are more complex in the centralised model.

Quality Assurance Measures: Two-stage heterogenous data quality assurance process established at national level by CAs and at EU level by the ESAs (it can be mitigated with taxonomy, validations, etc.).

Article 21(2)(e) Conditions of membership

Eligibility Criteria (type of stakeholder that can get access to the centralised EU solution): the main difference is that in the centralised scenario the FEs are also eligible and can also access the system (for both reporting and potentially consumption of data). This is not the case for the other scenarios, as it would potentially eliminate the benefits associated with decentralisation. The data-sharing and centralised hub allows a greater number of CAs at both EU and national level to access information.

Membership Application: under all three scenarios the CAs will have to apply for membership of the jointly operated solution. In the data-sharing and the centralised model, the number of staff of CAs accessing the single solution is higher, in the centralised scenario, the access could be for both reporting and analytical/supervisory purposes so the number of users will be increased. In the baseline scenario, CAs should connect for reporting purposes to several IT solutions, it is also assumed that the users of the CAs have access to the IT solutions operated by the CAs themselves. The main difference lies treatment reporting modalities for FEs, where for the centralised scenario, the FEs will report directly to a single solution in a centralised system, while in the other two more de-centralised scenarios, the FEs report into the different national systems set up for incident reporting or according to the reporting instructions of each NCA. The potential for heterogeneity in reporting systems among FEs across different countries in decentralised models has also been analysed.

Technical standards should specify the modalities and operational standards for the CAs to access the centralised HUB and the terms and conditions, the arrangements, and the required documentation under which access to a centralised EU Hub is granted. The conditions of membership of FEs should be also elaborated.

Authorisation process: Consideration given to the different degree of complexity and effort in the authorisation process for the FEs. In the centralised model managed centrally, with support from CAs, and in the other scenarios the authorisation will only need to be carried out by CAs.

Potential membership cost: potentially higher in decentralised models because of possible duplication, although even in the fully centralised scenario CAs will continue to operate systems for other purposes outside DORA Incident reporting.

Article 21(2)(f) Technical arrangements for financial entities and national competent authorities to access the single EU Hub
Identity & Access Management (IAM) Access by CAs: In the Centralised model CAs only have to access the HUB and there is no need to connect to other CAs' systems (at least for sharing in the context of DORA). It should be mentioned that the access should be for all those relevant members of the staff of the CAs, including supervisors, in the centralised model. Thereby, it should be ensured that CAs only have access to incident reports of financial entities they supervise. Moreover, while horizontal supervisors may have access to all incident reports of entities under the supervision of their CA, competent supervisors of one or multiple FEs only have access to incidents reports of FEs they supervise. **Access by FEs:** the IAM of FEs is a relevant and clearly differentiating factor between the different scenarios, the obvious difference being the need to manage access identification in a centralised or decentralised manner. There are arguments for both approaches, the difficulties derived from doing it centrally for a very large number of FEs should not be underestimated, while such centralisation allows for greater uniformity in the process and the security standards adopted. Similar arguments in the opposite direction apply for decentralised models. Role-based access control and authorisation credentials: the elements to be considered are similar to those of the previous point with some caveats. Although the process is more standardised at the centralised level, the FEs should continue to be registered in the national systems. The different of roles increase with centralisation as more stakeholders need to be onboarded, apart from CAs, ECB and SRB therefore also increases the complexity of the IAM implementation and operation On the other hand, the centralised model allows standardising the process for groups of FEs operating in different member states or under different sectors, while a strong IAM implementation is warranted for all there scenarios, given the nature of the dataset, as mentioned under the information security prerequisites (Article 21(2)(a))

Article 21(2)(g): Preliminary assessment of financial costs incurred by setting-up the operational platform supporting the single EU Hub, including the requisite expertise
Platform cost (set-up/maintenance): in decentralised models such costs are incurred at both CAs and EU level, the data-sharing model allows other CAs (at Member State and EU level) to rely on the hub and avoid associated costs. Please refer to section 8.3.2. Expertise capacity building: There are few differences at the business level, however at the technical level capacities should exist at national and EU level for decentralised models (although these may be mitigated by existing knowledge to operate current systems).

TABLE 3 ELEMENTS BASED ON DORA ART. 21 COVERED IN THE ANALYSIS OF THE SCENARIOS

8.3 High-level cost identification

162. Having highlighted the known unknowns, the report provides a high-level cost assessment identifying the primary cost areas and outlining key financial implications based on the information known to the ESAs at this stage, including data shared by CAs, assumptions made, and projections from similar solutions at ESAs level.

163. The assessment is performed both in absolute (Section 8.3.1) and relative cost terms (Section 8.3.2) and highlights the main cost lines related to the high-level business requirements listed in Section **Error! Reference source not found.**. The costs are specified in implementation (CAPEX) and running/maintenance costs (OPEX) and are based on specific assumptions, which are presented in the next sections.

8.3.1 High-level cost estimates in absolute terms

164. The table in this section highlights all the high-level costs estimations in absolute terms. This means that the total expense associated with each of the specific scenarios is considered as if they were independent projects to be decided upon at the outset of this exercise. The estimates are based on the following assumptions:

- **Operational costs:** the operational cost is calculated consistently for all three scenarios, as a fixed percentage of the CAPEX costs.
- **Sunk costs**: sunk costs are considered irrelevant for the cost's estimations in absolute terms since they are an expense that has already been incurred and cannot be recovered. It should be however factored in for the calculation of the cost estimates in relative terms, and thus considered in the conclusion of the total cost assessment.
- **Baseline scenario:** the baseline scenario estimates are based on the costs incurred by the ESAs in developing their joint solution, as well as extrapolations drawn from information shared by several CAs and ECB.
- **Data-sharing scenario:** the data-sharing scenario identifies a higher cost for the ESAs in relation to the baseline scenario. This is driven by the larger number of stakeholders involved and the additional design requirements necessary to accommodate the expanded scope of the scenario. At the MS level, the CAPEX, and consequently the OPEX, costs are reduced compared to the baseline scenario, as some of the associated responsibilities also disappear, there is no need for the CAs to establish mechanisms for proper routing or dissemination to multiple stakeholders; all the information received is channeled into a single system.
- **Centralised scenario:** cost estimates in the centralised scenario are based on assumptions regarding the number of stakeholders, expected incident volumes, insights gathered during the request for information (please refer to section 6), and the ESAs' experience with similar projects implemented in the past. The requirements and prerequisites of this scenario eliminate the need for collecting, assessing, routing, and disseminating reports at MS level; therefore, no costs at CAs level are identified related to the implementation of the high-level business requirements identified in the section 5 of this report. However, it should be noted that additional costs for local copies of incidents reported at national level would be only related to DORA supervisory activities, e.g. response, analysis, and follow-up, and such additional capabilities would be analogous for other scenarios. Therefore, no additional CAPEX is identified.

Type of cost on High level business requirement		Baseline	Data-sharing	Centralised
Implementation (CAPEX)	ESAs System	400,000 €	600,000 €	9,500,000 €
	CA Level	11,300,000 €	8,700,000 €	
	Total CAPEX	**11,700,000 €**	**9,300,000 €**	**9,500,000 €**
Maintenance (OPEX)	ESAs System	80,000 €	120,000 €	1,900,000 €
	CAs	2,260,000 €	1,740,000 €	
	Total OPEX/year	**2,340,000 €**	**1,860,000 €**	**1,900,000 €**

165. With these assumptions, the three solutions have similar costs range in absolute terms for both CAPEX and OPEX. Nevertheless, the baseline solution is slightly more expensive, in absolute terms, primarily due to the proliferation of systems at both the MS and EU levels, as well as the expanded duplicated capabilities of these systems and the need to operate them simultaneously, while the data sharing and centralised solutions as assessed as very close for both one-off setup and recurring maintenance costs. Although absolute costs are presented for comparative purposes, it should be noted that the baseline scenario represents sunk costs in the event of a migration to one of the additional scenarios, as explained in the next section.

8.3.2 Cost estimates in relative terms

166. The costs estimate in relative terms for the data sharing and centralised solutions should consider that the costs foreseen for the baseline scenario are already incurred, thus cannot be recovered.

167. With these assumptions and considering the sunk costs for the actual implementation, the centralised scenario seems to be the most expensive in relative terms, given that potential saving opportunities on yearly OPEX would materialize only in the long term, if ever (e.g. more than 20 years after the setup).

168. Hence, in that context it appears that the data sharing scenario is more cost effective, taking into consideration its' possible implementation as incremental improvements of the baseline scenario.

8.3.3 Additional cost considerations

8.3.3.1 BASELINE

169. The efforts already made to gather the business requirements and to select the Baseline Solution should also be considered, which add up to the total cost for the implementation of the Baseline Scenario. These costs will imply a better understanding of possible future needs and are therefore likely to reduce development costs in the other alternatives.

- In addition, the Baseline Solution needs help desk support in all CAs at both MS and EU level and additional second level support.
- At national level some jurisdictions may need to set-up new or adapt existing systems and maintain these systems in parallel. Also, the related necessary expertise capacity needs to be built, for those jurisdictions that don't have such systems. At the same time, it is expected that some jurisdictions may operate more manual modalities for receiving reports from FEs, as the number of incidents reported might not be high and a development of a dedicated tool would be unnecessary.

8.3.3.2 DATA SHARING

170. The Data Sharing Solution needs one help desk support and additional second level support.

- At national level some jurisdictions may need to set-up new or adapt existing systems and maintain these systems in parallel. Also, the related necessary expertise capacity needs to be built, for those jurisdictions that don't have such systems. At the same time, it is expected that some jurisdictions may operate more manual modalities for receiving reports from FEs, as the number of incidents reported might not be high and a development of a dedicated tool would be unnecessary.

8.3.3.3 CENTRALISED

171. The high cost associated with implementing the centralised solution arises from the onboarding of several thousand financial entities within scope and additional number of staff from CAs. Estimates are based on past onboarding processes for centralised solutions. However, the possibility to use innovative solutions for managing organisational credentials for financial institutions, like vLEI, which could significantly reduce the onboarding costs for the single EU hub, would also need to be explored. In the report, the figures are based on past ESAs data reporting projects, from where we drew the data available to support these estimates. Nonetheless, recent experiences in this area help quantify potential cost reductions associated with using this technology.

- In addition, the Centralised EU Hub needs only one help desk support in all EU languages and additional second level support.
- At national level, CAs will need to integrate their supervisory systems to the centralised system and build the related necessary expertise. At the same time, we expect that some jurisdictions may adapt more manual modalities for receiving reports from FEs, as the number of incidents reported is not high and a development of a dedicated tool would be an overkill.

8.4 High-level Cost Benefit Analysis

172. The following paragraphs present a high-level cost-benefit analysis of the different scenarios, incorporating perspectives from various actors, including stakeholders, ESAs, CAs and the independent assessment performed by Gartner Consulting. This analysis aims to capture the diverse viewpoints and feedback provided, recognising that each group has different perspectives, needs, priorities, and risks.

173. The identification of the elements for assessment mentioned in the previous chapter, along with the input gathered from two questionnaire consultations sent to the CAs and stakeholder groups (see section Stock-taking and stakeholder consultation), form the foundation of this analysis. Additionally, discussions held within the context of the DORA working groups further enriched this comprehensive evaluation.

174. The cost benefit analysis lists and performs a qualitative comparison of the associated benefits and costs/challenges. The cost/challenges considerations are based on the steady state costs

BENEFITS

BASELINE	DATA-SHARING	CENTRALISED
▪ **Minimum disruption:** Established data collection process and existing systems may be re-used. The systems adapted or developed for reporting under other mandates in force, as well as their associated processes, can be preserved. ▪ **Limited to no additional implementation cost as systems built for initial DORA implementation.** ▪ **No DORA amendments are needed:** this model can operate without modifications to either DORA Level 1 or Level 2. ▪ **CAs remain the first point of contact for FEs under their supervision:** this brings benefits related to the familiarity with the CA reporting framework and language or quicker scalability/response at CAs / national level. Any potential centralised applications at the Member State level—such as national hubs—are also retained. ▪ **High concentration of sensitive information:** Regarding the risks associated with the high concentration of sensitive information (as per Article 21(2)(b)), the analysis showed that in this scenario the risk of losing availability of the incident data is lower than that of the centralised scenario, as this data would also exist in the national systems. At the same time, the risk of unauthorised access and disclosure due to concentration still exists for this scenario and is similar to that of the Centralised Hub, as the baseline is implemented through a single ESAs hub which will receive, store and disseminate the incident reports.	▪ **Smooth transition and low disruption**: The scenario can be implemented as an extension of the existing baseline framework and can integrate more effectively with the solutions currently in place at national level, while offering some additional centralisation of reporting into the ESAs single hub. It may also provide a smoother transition as an intermediate solution to the centralised option while maximizing the benefits of the baseline. ▪ **Minimum disruption:** By maintaining the flows between CAs and FEs, some of the established data collection process and systems may be re-used. The systems adapted or developed for reporting under other mandates in force, as well as their associated processes, can be preserved. ▪ **Limited additional implementation cost** since it does not represent a significant change in the first phase of reporting (FEs → CAs). ▪ **Some potential economies of scale at national level** by avoiding the need for additional disseminations, both at member state and at the EU level which also makes it more cost effective than the fully centralised option, as per the analysis in Section 8.3.2. ▪ **CAs remain as the first point of contact for FEs under their supervision:** This brings benefits related to the familiarity with the CA reporting framework and language or quicker scalability/response at CAs level. ▪ **High concentration of sensitive information:** Regarding the risks associated with the high concentration of sensitive information (as per Article 21(2)(b)), the analysis showed that in this scenario the risk of losing availability of the incident data is lower than that of the centralised scenario, as this data would also exist in the national systems. At the same time, the risk of unauthorised access and disclosure due to concentration still exists for this scenario and is similar to that of the Centralised Hub, as the Data Sharing is implemented through a single ESAs hub which will receive, store and disseminate the incident reports.	▪ **Better alignment with the objectives linked to a Savings and Investments Union.** ▪ **Establishing deeper alignment with harmonisation objectives of DORA (DORA recitals 8 to 16).** ▪ **Enhanced EU level cybersecurity preparedness, coordination and response** through advanced analytical capabilities: while analytical capabilities can be provided in other models, the potential is greater in a system where all stakeholders are involved, and the database is consistent and synchronized. ▪ **A unified and consistent incident reporting process and standards across the EU, facilitated by a single unique system:** This ensures streamlined collection and dissemination for all stakeholders, irrespective of sector or Member State, promoting greater efficiency and alignment. ▪ **Limited data collection delays:** The system offers temporal synchronisation at the information level, eliminating risks of delays or inconsistencies from various reporting sources, ensuring timely data across the board. ▪ **Limited data inconsistencies**: A unified, consistent database for all European incident reports ensures that data is collected and managed according to a common standard, providing clarity and alignment across all stakeholders. ▪ **Potentially greater economies of scale** compared to the baseline solution, in the long run (please refer to Table 5). At the same time, this is attenuated considering the expense ESAs/CAs already had to incur to implement a solution enabling incident reporting in January 2025, as well as considering CAs would still need to implement solutions at national level for supervisory response and follow-up. ▪ **Reduced data dissemination times,** through a one-step data collection process that make the data available for all relevant CAs at the same time. ▪ **Shorter response time for cross-border incidents**, linked to the previous point, the ability to have consolidated and synchronised information allows for a shorter response time in the case of incidents occurring across multiple Member States. (temporal synchronization and content harmonization capabilities)

BENEFITS		
BASELINE	**DATA-SHARING**	**CENTRALISED**
		▪ **Opportunity to provide access to FEs:** the onboarding of FEs and consolidated database allow to provide access to European wide incident reporting data, with the appropriate security measures. In line with the EIOPA Strategy on Cyber Underwriting approved by the EIOPA Board of Supervisors in 2020[19].

TABLE 4 CBA: BENEFITS

– Future reduction or elimination or specific system adaptations for receiving and sending reports across all CAs involved in the process (which could be hundreds), even though the marginal cost to incorporate DORA reporting in the current systems reduced.
– Elimination of duplicate reporting flows to various stakeholders (this applies to NCAs as well as ESAs and other CAs at both national and European levels).
– Elimination of double reporting by groups of FEs (in cases of group-level or aggregated reporting).
– Overall operational costs, based on the estimation that overall, the operation of a single system is expected to be less costly than various systems at national level even if the implementation are more costly.
– Scalability: a centralised solution is easier to scale and modify, if necessary, Changes are implemented centrally, providing an easier expansion in capability, reduced incremental cost to escalate, uniform modifications and easier training and onboarding.
– Costs associated with quality: centralised and standardised solutions are more efficient in managing data quality and corrections, while the nature of more decentralised solutions would warrant duplicate cost for data quality purposes (e.g. data quality for x systems at EU level, as opposed to one).
– Consolidation in the visualisation of global data, which can facilitate related decision-making and faster response time through streamlined access to the data and reduced analysis time.
– Estimated economies of scale related to information security in general, linked to lower per-user-cost, lower operational/maintenance expenses and single cost-efficient implementation.
– Compliance cost: FEs and CAs operating a single system/process for all jurisdictions or sectors, reducing the need for specialised personnel, training, auditing and administrative overhead

TABLE 5 ECONOMIES OF SCALE FOR CENTRALISED MODEL

[19] EIOPA Strategy on Cyber Underwriting approved by the EIOPA Board of Supervisors in 2020 "" *In order to allow for sound pricing, underwriting and cyber risk management, the availability of data on cyber incidents should be broadened and appropriately standardised, while safeguarding the level playing field and data confidentiality. Ultimately, the access to cyber incident database(s), potentially a European Database, could be seen as a public good and underpin the further development of the European cyber insurance industry and act as an enabler of the digital economy*""

COSTS / CHALLENGES

BASELINE

- **Duplication / proliferation of incident reporting data flows as presented in par 137**: CAs would submit to ESAs, and other national authorities, while groups of FEs supervised by different CAs will need to report to several CAs.
- **Higher Maintenance Costs:** maintaining multiple systems across the EU, leading to increased spending compared to a single, centralised system.
- **Heterogeneity and proliferation of ICT-related incident reporting systems across the EU:** different national authorities will operate different systems for collecting and disseminating major ICT-related incidents. Many different systems will exist in the EU and within the EU member states, on top of the ESAs single Hub (baseline).
- **Delayed information sharing**: the two-step reporting process generates delays in completing the data collection and dissemination to all stakeholders and/or longer response times At the same time, this can be mitigated in the event of M2M implementation across all CAs. This is particularly important for incidents impacting multiple EU Member States
- **Higher risk of data inconsistencies and low data quality**: The proliferation of information flown, systems, reports, and data quality processes can potentially create inconsistencies in the information**. At** the same time, this **can** be mitigated with shared taxonomies)**.**
- **Different points of contacts for DORA incident reporting purposes:** there is an increase on the operational costs related to the management and communication with different point of contacts for reporting purposes**.**
- **Maintaining Different Reporting Standards:** In a decentralised model, different jurisdictions may require varying reporting standards, which increases complexity and costs. Even with efforts to minimize these differences through a shared data model, variations in data formats could persist. This

DATA-SHARING

- **Reduced incident reporting flows compared to the baseline**, while still multiple reporting flows are maintained, for example some FEs will be reporting to several CAs.
- **Heterogeneity and proliferation of ICT-related incident reporting systems across the EU:** different national authorities will operate different systems for collecting and disseminating major ICT-related incidents. Many different systems will exist in the EU and within the EU member states, on top of the ESAs single Hub (baseline).
- **Legal basis should be created first:** the Data-sharing scenario will require some minor modifications in the legal framework (mostly relating to the notifications to competent authorities).
- **Different points of contacts for reporting purposes:** there is an increase on the operational costs related to the management and communication with different point of contacts for reporting purposes (reduced compared to the Baseline)
- **Reduced compared to the baseline but still delayed information sharing:** the two-step reporting process generates delays in completing the data collection and dissemination to all stakeholders and/or longer response times. This is particularly important for incidents impacting multiple EU Member States
- **Reduced compared to the Baseline but still risk of data inconsistencies and low data quality:** The proliferation of information flows, systems, reports, and data quality processes can potentially create inconsistencies in the information. At the same time, it can be mitigated with shared taxonomies.
- **Maintaining Different Reporting Standards:** In a decentralised model, different jurisdictions may require varying reporting standards, which increases complexity and costs. Even with efforts to minimise these differences through a shared data model, variations in data formats could persist. This requires additional resources to manage and integrate diverse standards, including system customisations, staff training, and

CENTRALISED

- **Implementation costs:** a complex system that requires onboarding of all CAs, 'CAs' supervisors (at least for the financial sector) and FEs, in addition to the resources that would have been spent already for the baseline scenario. Particular cost points are the sophisticated identity & access management modules, and information security controls and arrangements that would need to be implemented, the operational costs, including the onboarding of many authorities and industry stakeholders, setting up helpdesk in different languages to support and the costs to accommodate the specific needs of the various CAs (both at the level of connectivity to national systems (if necessary), the analytical and monitoring capabilities required) and multi-language helpdesk. At the same time, we expect economies of scale to be achieved in the maintenance costs spent on such solutions in the EU level.
- **Sunk costs:** considering the sunk costs for the actual implementation, the centralised scenario seems to be the most expensive in relative terms, given that potential saving opportunities on yearly OPEX would materialize only in the long term.
- **Both at level 1 and level 2 legal basis should be created first:** The centralised solution would require amendments to Article 19 of DORA and to the ITS on forms, templates, and procedures to shift from the current reporting system to the central hub. To fully exploit the benefits of the centralised model, DORA amendments are needed to enable aggregated incident reporting at the cross-sector and cross-Member State level
- **High concentration of sensitive information and Single Point of Failure:** Regarding the risks associated with the high concentration of sensitive information (as per Article 21(2)(b)), the analysis showed that in this scenario the risk of losing availability of the incident data is the highest than on the other scenarios, as this data would only be available at centralised level. At the same time, the risk of unauthorised access and

COSTS / CHALLENGES

BASELINE	DATA-SHARING	CENTRALISED
requires additional resources to manage and integrate diverse standards, including system customizations, staff training, and data reconciliation efforts. Over time, this can lead to increased operational and compliance costs, as well as inefficiencies in data collection, analysis, and communication between stakeholders. High coordination needs and higher complexity Coordination and governance efforts at different levels (MS, EU, FEs). ▪ **Language of reporting of incidents:** estimated difficulties related with Incidents received in local languages and disseminated to other stakeholders in other Member States without translation**.**	data reconciliation efforts. Over time, this can lead to increased operational and compliance costs, as well as inefficiencies in data collection, analysis, and communication between stakeholders. ▪ **High coordination needs and higher complexity compared to the Centralised scenario:** Coordination and governance efforts at different levels (MS, EU, FEs). ▪ **Language of reporting of incidents:** difficulties linked with incidents received in local languages and disseminated to other stakeholders in other Member States without translation.	disclosure due to concentration still exists for this scenario and is similar to that of the Baseline and Data Sharing scenarios. ▪ **Operational difficulties linked to Identity & Access management:** under this scenario all FEs and all CAs' supervisors will have access to specific reports, on a scale of several thousand users ▪ **Cost and effort related to the creation of a new governance model**: the governance should be defined, being the number of modifications significant, and it uses a centralised approach for a reporting system that is not governed centrally ▪ **Highly disruptive as it would be the first time a centralisation of this type of incidents** would be done at such scale and with a mandatory character. This is a challenge at EU level and a cultural change would be required to make it work. ▪ **DORA incident reporting should not be looked at in isolation:** other systems will remain at national level towards enabling supervisory response and follow-up of incidents at national level. In addition, the centralised EU Single Hub would need to interoperate with other reporting systems and reporting regimes, posing thus further complexities and restrictions the fully centralised model ▪ **Language of reporting of incidents:** difficulties linked with the aggregate reporting of incidents and their analysis in the context of a centralised solution.

TABLE 6 CBA: COSTS / CHALLENGES

8.5 Considerations about future implementation

8.5.1 ESAs solution based on ENISA's incident reporting tool (Baseline Scenario) as starting point

175. The Baseline Scenario is scheduled for implementation and production in early 2025. This means that, regardless of the future scenario to be implemented, subsequent implementation/centralisation steps should consider the Baseline Solution as the starting point.

176. In this context, it is important to ensure business continuity of the incident reporting process in any transition to further centralised solutions, so that the flow of information to the CAs at both Member State and EU level responsible for supervision and incident response occurs in a timely and uninterrupted manner. For the fully centralised scenario, the transition should also guarantee that the relevant staff of CAs (e.g. supervisors, and other relevant staff) also get access to the information for monitoring, supervisory response and follow-up purposes, as well as interoperability aspects with the existing systems CAs may operate to perform supervisory analyses and risk assessment.

8.5.2 Legal considerations

177. The implementation of a different scenario beyond the Baseline Scenario may require amendments of DORA (please refer to the assessment of the legal implications in Annex I: Assessment summary). In this respect it is noted that the Baseline scenario may not require amendments to DORA, provided that the relevant authorities agree to use the ESAs system. The Data-sharing scenario will require some minor modifications in the legal framework, mostly linked to the amendments in the notification regime.

178. The centralised solution would require amendments to the structure of incident reporting under DORA and result in amendments to certain paragraphs in Article 19 of DORA and to the ITS on forms, templates and procedures (see Annex I for further information), and to regulate anew aggregate reporting in order to fully exploit the benefits of this scenario. Provided that amendments to DORA require their adoption by the Legislators, the time needed to finalise the related EU legislative process should be added to the time to implement any further centralised solution.

8.5.3 Costs

179. Moving from the baseline solution to any other scenario would involve additional costs to those already incurred for the implementation of the baseline scenario. This would have to be allocated and discussed with all relevant competent authorities.

180. The cost related to the implementation of the centralised scenario could have been lower if the initial expense of developing the baseline first and then moving to the centralised model could be avoided, e.g. CAs minimising their expenditure on existing or planned incident reporting solutions at EU level.

8.5.4 Data and user migration considerations

181. In both data sharing and centralised scenarios, there is an increase in the number of users of the system. In the data sharing solution only CAs' personnel need to be migrated to the new solution, the number will be higher than in the Baseline Scenario, but still in the same range (all EU supervisors will need swift access to these reports). In the centralised scenario, the number of users is significantly higher, as not only all CAs' supervisors but also all FEs (presumably multiple persons per FE) should be given access to the new solution.

182. By using a solution other than the Baseline Solution as a long-term solution, it will be necessary to migrate data to the new system in the future. Choosing a different solution requires careful consideration of the benefits of the new solution against the additional costs, effort and risks associated with migrating and transitioning from the Baseline Solution to the new solution. The longer it takes to decide to use a different solution, the more data will need to be migrated, in any case it should not be critical since the estimated number of incidents and users is reduced.

9 Conclusions

183. Following the assessment conducted, the report concludes the following key points.

184. Based on the identification of potential solutions and the assessment performed, all three scenarios are considered technically feasible. In addition, most of the potential risks associated with the different scenarios can be mitigated through additional measures, which will require additional investments.

185. The market scan performed in the context of this study and the assessment performed of the two alternative solutions suggests that there may be commercial off-the-shelf solutions with a high degree of functional and non-functional fit that offer a sound alternative to a self-developed solution.

186. In the short term (within 3 years from January 2025), only the Baseline Scenario, and possible enhancements of this scenario is feasible.

187. The implementation of the two scenarios offering further centralisation is considered feasible in medium (3 years onwards for data-sharing) and longer term (5 years onwards for fully centralised model), depending on the degree of the centralisation, the implementation of the required[20] policy and legislative change, and the extent to which they can be implemented as an extension to the solution currently being implemented to enable reporting in January 2025.

188. While the existing DORA provisions would allow to commence work towards increased centralisation, amendments and agreements regarding changes in DORA legal framework, as described in previous sections, would be warranted to exploit fully the benefits of the centralised model and ensure legal certainty on its governance, development and operation. At the same time, such agreements among CAs are very important, considering the topic of aggregated reporting aspects, that can be controversial. This means that the time required to perform these amendments and any subsequent policy work towards implementing a single EU Hub needs to be factored in.

189. Regarding costs, there are not significant differences between the three assessed scenarios and from an overall cost perspective all three solutions are in a similar range. A fully centralised scenario would normally have been able to ensure savings in absolute terms, considering that the implementation of one platform would be less costly than the implementation of many. At the same time, taking into account the costs linked to the implementation of the baseline solution, which was inevitable given the legal requirement to have a decentralised DORA ICT-related reporting in January 2025, potential saving opportunities would materialise only in the longer term. The case of the data sharing solution is similar, however with lower expected implementation costs, since it is envisaged to be implemented as an extension of the baseline scenario, and thus bearing potential OPEX savings for local implementations (as explained in Section 8.3.2).

190. Considering the above, which is further detailed in the analysis, as presented in Chapter 8, each scenario presents both benefits and challenges. Notwithstanding certain advantages of the baseline and data-sharing models over the fully centralized scenario,

[20] Please refer to par 8.2, 8.5.2 and Annex I: Assessment summary - Gartner Consulting

the latter shows many merits towards harmonisation, synergies, reducing industry burden, and with the objectives linked to a Savings and Investments Union and is also aligned with the objectives of harmonisation identified in DORA. At the same time, it is considered that a fully centralised scenario would bring full benefits, including for the market participants, in a wider context of aligning several sectorial and cross-sector incident reporting regimes.

191. Specifically, the report identified the following advantageous features that can be achieved to their full extent only with the implementation of a centralized single EU Hub model:

- avoidance of several parallel reporting channels as identified in paragraph 137 for the baseline scenario;
- benefits related to shorter dissemination time of the incident reports and potentially facilitating shorter response time, in case of cross-border incidents;
- the development of advanced and centralised analytical capabilities available to all users, including both CAs and FEs (also in line with the EIOPA Strategy on Cyber Underwriting approved by the EIOPA Board of Supervisors in 2020[21]);
- the potential reduction in onwards dissemination times to all stakeholders, which would be an important prerequisite towards the operation of a cybersecurity crisis management framework and early warning.

192. It is important to highlight that in any decision about future centralisation, the fundamental objective of incident reporting — linked to the reporting, analysis, dissemination and response to such incidents — should be prioritised and be a guiding principle in the design of the solution (in line with the prerequisites described in 8.2).

193. In addition, a lot of information has been still unknown or uncertain at the time the assessment was performed, given the implementation status of the baseline DORA incident reporting solution. This means that further analysis is required to better inform the decision and the design of a fully centralised solution. Such an analysis would include at least taking stock of the operation of the baseline solution post-January 2025, any further enhancements implemented on the baseline solution, and clarifying the elements that are unknown at this stage. Further, the need for CAs to still operate systems and solutions at national level, even if a solution were to centralise fully incident data collection, validation and analytical capabilities, would need to be considered.

194. Finally, the report concludes that further centralization and a single EU Hub scenario for DORA major ICT incident reporting is feasible and brings certain benefits. At the same time, the benefits of such centralisation are significantly attenuated in view of two key factors: the important effort and resources ESAs and CAs would have invested already for enabling DORA ICT-related incident reporting in January 2025, in line with the DORA requirements, and the resources that CAs would anyway need to continue to invest in infrastructures enabling supervisory response and follow-up at national level, even if the centralized solution were to be implemented. As mentioned above, it is thus important that co-legislators continue to assess and consider further centralisation into a single EU hub, having regard to the different elements and aspects highlighted in this report,

[21] Please refer to CBA in section 8.4

especially also considering minimising costs for transition to a fully centralised EU hub solution. In addition, such centralisation would be more beneficial and would be worth considering within a wider context of EU ICT-related incident reporting, beyond DORA.

Annex

Annex I: Assessment summary - Gartner Consulting

The following tables summarise the results of the assessment and comparison for the different scenarios performed by Gartner Consulting. The assessment provided by the Garter Consulting delivers an assessment grounded in expert judgement and access to relevant project information. While not intended as an exhaustive review, it nonetheless offers valuable insights based on a professional appraisal of key data. It is worth noting that some activities, such as in-depth interviews with primary stakeholders, were outside the assessment's scope.

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
Prerequisite for single EU Hub	Infrastructure & Technology Requirements	Duplicate decentralised software and hardware infrastructure on national as well as EU level FEs should be connected to the CA systems and the CA systems to Baseline Solution Biggest hardware and software need through decentralisation	Partially duplicate decentralised software and hardware infrastructure on national level for all CAs not accessing the Hub directly and the CAs under DORA On EU level there is no need to have duplicated solutions FEs should be connected to the CA systems and the CA systems to ESA solution based on Baseline Solution, a new commercial standard solution, or a new self-developed solution. Biggest hardware and software need through decentralisation (very similar to baseline scenario)	Centralised software and hardware infrastructure FEs and CAs should be connected to Baseline Solution Lowest hardware and software need through centralisation
	Legal Prerequisites (the legal assessment does not examine potential legal changes for any of the scenarios at the Member State level)	The current wording of Article 19 of DORA is compatible with this scenario. However, since Article 19 does not mandate the use of a common system by NCAs and the other authorities mentioned in it, the agreement of these authorities to use the common IT tool is necessary.	As for the baseline scenario, it can be considered that competent authorities may agree to use the Hub to dispatch major incident reports across the relevant authorities. Please note that however, since financial entities would still provide reports to	The centralised EU hub would substantially change the reporting flow compared to other options, since financial entities would have to report directly to the hub. In this case, a change to DORA provisions is needed to require financial entities to submit reports to the central hub.

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
		Considering that competent authorities expressed their interest to using the IT tool, we do not think that amendments in Article 19 of DORA to render the tool compulsory would be necessary. Should there be the intention to require the use of the IT tool, ad-hoc changes to Article 19 of DORA would be needed	the CAs, a duplication of reporting may take place with respect to the NIS 2 authorities, to which financial entities may be obliged to send the major incident reports if the national law so requires (Article 19(1), sixth subparagraph). Should there be the intention to require the use of the IT tool ad-hoc changes to Article 19 of DORA would be needed.	The amendments should cover Article 19(4), (6), (7), and (8) of .DORA. Also, amendments of the procedures to report incidents, covered in the ITS referred to in Article 20(b), would need to be enacted. In particular, it is probable, following exam of the Commission Implementing Act adopted in accordance with Article 20, that certain provisions on aggregated reporting would need to be added, to regulate reporting at the cross-sector and cross-Member State level. In this case, given the high number of reporting financial entities, the option of voluntary participation to the Centralised EU Hub is considered as not relevant.

TABLE 6: ASSESSMENT SUMMARY PREREQUISITES

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
Potential Benefits	Reduced costs, economies of scale and scope	Reuse of existing, if any, CA incident reporting tools No additional cost savings for CAs Partially reuse of Baseline Solution, an established system developed by ENISA for incident reporting Reporting flows will remain as described in DORA with minor modification Planned to be implemented by	Reuse of existing CA incident reporting tools Very limited cost savings for CAs Potential reuse of Baseline Solution, an established system developed by ENISA for incident reporting Reporting flows will remain as described in DORA with minor modification (potential changes on member state levels) Cross CA information	Centralised and standardised infrastructure Greatest overall cost savings through centralisation Potential reuse of Baseline Solution, an established system developed by ENISA for incident reporting Unified access to incident reporting information in a transparent and consistent way No double/multiple

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
		January 2025 Opportunity to use the same templates for any reporting flow based on RTS and ITS Lowest economies of scale and scope through duplications	exchange on member state level could be unified and simplified Cross CA information on EU level is unified and simplified Unified access to incident reporting information in a transparent and consistent way Limited number of additional credentials (only for CAs) on EU level compared to the baseline. Some potential economies of scale and scope for CAs	reporting needs for groups of FEs Standardised incident reporting Greatest overall economies of scale and scope after implementation
	Supervisory Convergence (shared data basis, …)	Low: 'Standardisation only on EU level between ESAs Less overall standardised data collection from data sources (FEs/member states) Decentralised potential inconsistent and asynchronous data basis	Medium: 'Standardisation on CA and EU level Less overall standardised data collection from data sources (FEs/member states) Decentralised potential inconsistent and asynchronous data basis	High: 'Standardisation on FE /CA and EU level Standardised data collection from data sources FEs directly Centralised consistent consolidated timely data basis
	Market Overview (consolidated database)	Duplicate incident reporting databases managed by the CAs and a consolidated database on EU level are required Decentralised potential inconsistent and asynchronous data basis should be consolidated	Duplicate incident reporting databases managed by the CAs and a consolidated database on EU level are required. Decentralised potential inconsistent and asynchronous data basis should be consolidated	Only one centralised incident reporting database is needed Centralised consistent consolidated timely data basis
	Opportunity to give FEs access to incident reporting data	Currently not planned Potential additional costs related to the necessary anonymisation of data	Currently not planned Potential additional costs related to the necessary anonymisation of data	FEs are onboarded and have access no additional efforts needed Potential additional costs related to the

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
		and implementation of additional roles Significant additional effort would be required to provide FEs access	and implementation of additional roles Significant additional effort would be required to provide FEs access	necessary anonymisation of data and implementation of additional roles

TABLE 7 ASSESSMENT SUMMARY: BENEFITS

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
Identified Limitations	Limitations	Potential delays due to two-step data collection process Double/multiple reporting of the same incidents through groups of FEs limits their potential to optimise their reporting processes Complex standardisation due to heterogenous infrastructure and decentralised processes	Potential delays due to two-step data collection process Double/multiple reporting of the same incidents through groups of FEs limits their potential to optimise their reporting processes Complex standardisation due to heterogenous infrastructure and mainly decentralised processes	Reporting flows need to be adapted to the new centralised reporting approach CAs are no longer the first point of contact of the FEs for incident reporting Country specific incident reporting features or information may get lost Through centralisation easy standardisation of processes, data and (analytical) functionalities
	Operational/Technical Risk	Potential inconsistencies due to duplicate data and systems D information security standards on CA level The data received by the ESAs is not received directly from the data source Inconsistent data due to multiple reporting of the same incident in different formats	Potential inconsistencies due to duplicate data and systems Different information security standards on CA level The data received by the ESAs is not received directly from the data source Inconsistent data	Need to manage a considerable amount of FEs providing information directly to the central hub Management of a significant number of login credentials centrally

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
			due to multiple reporting of the same incident in different formats	
	Security Risk (data concentration)	Duplicate databases on national and EU level with different information security standards	There are duplicate databases on national and EU level with different information security standards	Centralised database which creates a potential single source of failure, which need to be mitigated with appropriate measures
	Reputational Risk	Low - quality assured data is provided by the CAs	Low - quality assured data is provided by the CAs	High - the complete data collection process including the quality assurance is managed on EU level
	Others	Delayed consolidated data availability due to 2-stage data collection	Delayed consolidated data availability due to 2-stage data collection	

TABLE 8 ASSESSMENT SUMMARY: LIMITATIONS AND RISKS

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
Interoperability	Technical Compatibility/Connectivity with Existing Systems	Not standardised for FEs and CAs FEs need to connect to CAs CAs need to connect to Baseline Solution (central EU solution) CAs need to	Not standardised for the FEs and CAs not accessing the data hub FEs need to connect to CAs CAs need to connect to central EU solution (e.g. Baseline Solution)	Standardised FEs need to connect to the Central EU HUB CAs need to connect to the Central EU HUB Simplest (number and types)

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
		connect to other CAs. Most complex (number and types) connectivity requirements	CA s need to connect to other CAs Compared to Baseline Scenario simplified (number) connectivity requirements for CAs	connectivity requirements
	Data Harmonisation	Handled by the CAs in collaboration with the ESAs Complex data harmonisation due to decentral two-stage data collection, non-standardised first stage	Handled by the CAs in collaboration with the ESAs Complex data harmonisation due to decentral two- stage data collection, non-standardised first stage	Handled on EU level by the ESAs or other EU stakeholders Simple data harmonisation due to centralised data collection
Operational Management	Governance Structure	Complex governance structure Governed in a decentralised manner on national as well as on EU level	Complex governance structure Governed decentralised on national as well as on EU level	Simple governance structure Governed centrally on EU level
	Data Management Procedures	Complex duplicated data management procedures CAs and ESAs	Complex duplicated data management procedures CAs and ESAs and/or other EU stakeholders	Simple centralised data management procedures ESAs and/or other EU stakeholders
	Quality Assurance Measures	Two-stage heterogenous data quality management process established at national level by CAs and at EU level by the ESAs	Two-stage heterogeneous data quality management process established at national level by CAs and at EU level by the ESAs and/or other EU stakeholders.	One-stage data quality management established at EU level by the ESAs and/or other EU stakeholders.
Membership Conditions	Eligibility Criteria (type of stakeholder that can get access to the centralised EU solution)	CAs and ESAs are planned to get access to the EU database what is technical feasible Additional efforts are needed to	All CAs and ESAs are planned to get access to the EU database what is technical feasible (slightly higher number of CAs using the solution	All CAs, ESAs and FEs will have access to the centralised EU hub, the feasibility is assumed to be given but needs to be explored in more detail and the

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
		provide FEs access	compared to baseline scenario) Additional efforts are needed to provide FEs access	implications assessed
	Membership Application	Membership application need to be processed by CAs or ESAs Potentially more complex heterogeneous membership application process	Membership application need to be processed by CAs, ESAs and/or other EU stakeholders Potentially more complex heterogeneous membership application process	Membership application need to be processed by ESAs and/or other EU stakeholders The membership decision should be aligned with national requirements, which may become quite complex
	Confidentiality Measures	At CA or ESA level.	At CA or ESA/other EU stakeholder level.	At ESA and/or other EU stakeholder level Quite complex and effort intensive clearance process for the FEs
	Potential Membership Costs	At the CA or ESA level Through decentralisation and duplication potentially higher cost	At CA or ESA/other EU stakeholder level Through decentralisation and duplication potentially higher cost	At EU level Through centralisation potentially lowest cost

TABLE 9 ASSESSMENT SUMMARY: INTEROPERABILITY, OPERATIONAL MANAGEMENT, MEMBERSHIP CONDITIONS

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
IAM	Access by CAs	To local CAs and Baseline Solution Complex due to the need to directly interact with other CAs	To EU Hub Simplified due to the possibility to use the data sharing solution	To EU Hub Simple due to centralised hub

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
	Access by FEs	Managed by CAs Complex due to the need to provide reports to multiple CAs and partially in addition even NIS authorities	Managed by CAs Complex due to the need to provide reports to multiple CAs in different countries	Managed by ESAs or other European stakeholders Simple due to centralised reporting
	Assignment of roles for the different functionalities of the tool	Assigned by CAs and ESAs Complex due to decentralised data reporting to multiple CAs and partially in addition even NIS authorities	Assigned by CAs and ESAs/other European stakeholders Complex due to decentralised data reporting to multiple CAs	Assigned by ESAs or other European stakeholders Simpler and more consistent due to centralised data reporting
	Role Definition & Management	Defined and managed by CAs and ESAs Complex due to decentralised reporting and the need of the FEs to provide reports to multiple CAs	Defined and managed by CAs and ESAs/other European stakeholders Complex due to decentralised reporting and the need of the FEs to provide reports to multiple CAs	Defined and managed by ESAs/other European stakeholders Provision of enhanced functionalities will add additional complexity More consistent due to centralised reporting
	Credential Management	Managed by CAs & ESAs Complex due to decentralised reporting and the need of the FEs to provide reports to multiple CAs partially in addition even NIS authorities	Managed by CAs & ESAs/other EU stakeholders Complex due to decentralised reporting and the need of the FEs to provide reports to multiple CAs For CAs using the data sharing solution simplified	Managed by ESAs/other EU stakeholders Simple and consistent due to centralised EU Hub
Financial Costs	Platform Costs (set-up costs / maintenance)	At CA and ESA level	At CA and ESA/other European stakeholder level	At ESA/other European stakeholder level
	Expertise capacity building cost (Business)	Business expertise is required at country and EU level	Business expertise is required at country and EU level	Business expertise is required on EU level, only to a limited extent on national level

Categories	Criteria	Baseline Scenario (ESA Hub)	Data Sharing Scenario	Centralised EU Hub (Single EU Hub)
	Expertise capacity building cost (IT)	Technical solutions expertise is required at country and EU level	Technical solutions expertise is required at country and EU level	Technical solutions expertise is required at EU level
	Cost-Benefit Analysis Summary	See following sub chapter	See following sub chapter	See following sub chapter

TABLE 10 ASSESSMENT SUMMARY: IAM AND FINANCIAL COSTS

Annex II: Gartner Consulting CBA and Conclusions

CBA: PROs and CONs from an overall economic perspective – Gartner Consulting's point of view

BASELINE	DATA-SHARING	CENTRALISED
PROS ▪ Lean cost-efficient solution on EU level ▪ Established data collection process and systems may be re-used	**PROS** ▪ Established data collection process and systems may be re-used ▪ No need to share report information between CAs on national level ▪ Some potential economies of scale and scope for CAs	**PROS** ▪ Most cost efficient overall solution (lowest hardware and software need through centralisation) ▪ No redundant systems, capacity and data on EU/national level ▪ Greatest economies of scale and scope ▪ One consistent data base with all European incident reports ▪ Opportunity to provide Aadvanced analytical capabilities to all member states ▪ No redundant incident reportingTimely information basis (one-step data collection process
CONS ▪ Redundant systems, capacity and data on national level is needed ▪ Lowest economies of scale and scope ▪ Due to redundant incident reporting potentially inconsistent information ▪ Delayed information sharing (two-step data collection process)	**CONS** ▪ Redundant systems, capacity and data on national level is needed ▪ Due to redundant incident reporting potentially inconsistent information ▪ Delayed information sharing (two-step data collection process)	**CONS** ▪ A solid legal basis should be created first ▪ Potential Centralisation risks need to be mitigated

TABLE 11 GARTNER CONSULTING'S OPINION: PROS & CONS

- From an overall economic perspective, the scenario providing overall (most benefits / and could be associated with the lowest overall cost depending on the detail design (which was not part of the current project) is a Central EU HUB according to Gartner Consulting´s current point of view.

- No duplicate systems, capacity and data on EU/national level (cost efficient).
- A centralised, more sophisticated solution is still cheaper overall in the long run than multiple (dozens or even hundreds) simple local solutions.
- One consistent data base with all European incident reports
- No duplicate incident reporting as identified in the Baseline scenario
- Timely information basis (one-step data collection process)
- Potential opportunity (considering the current heterogenous environments and IT security standards in the member states) with an appropriate detail design to increase the IT security of the complete “Cybersecurity Incident Reporting Ecosystem”

- The Data Sharing solution and the Baseline Scenario both scenarios need duplicate infrastructure, data and other capacities on national and EU level
- In both scenarios due to duplicate incident reporting potentially inconsistent information and the risk of delayed information sharing due to the two-step data collection process)

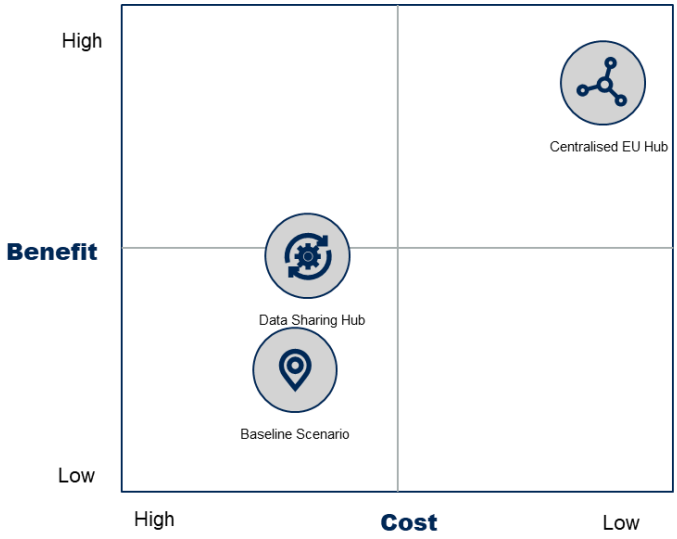
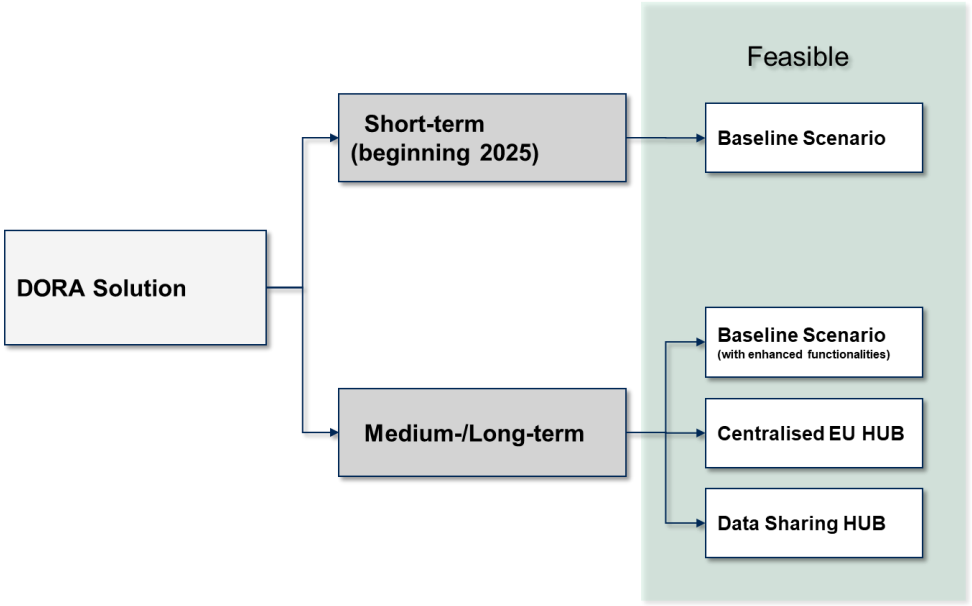


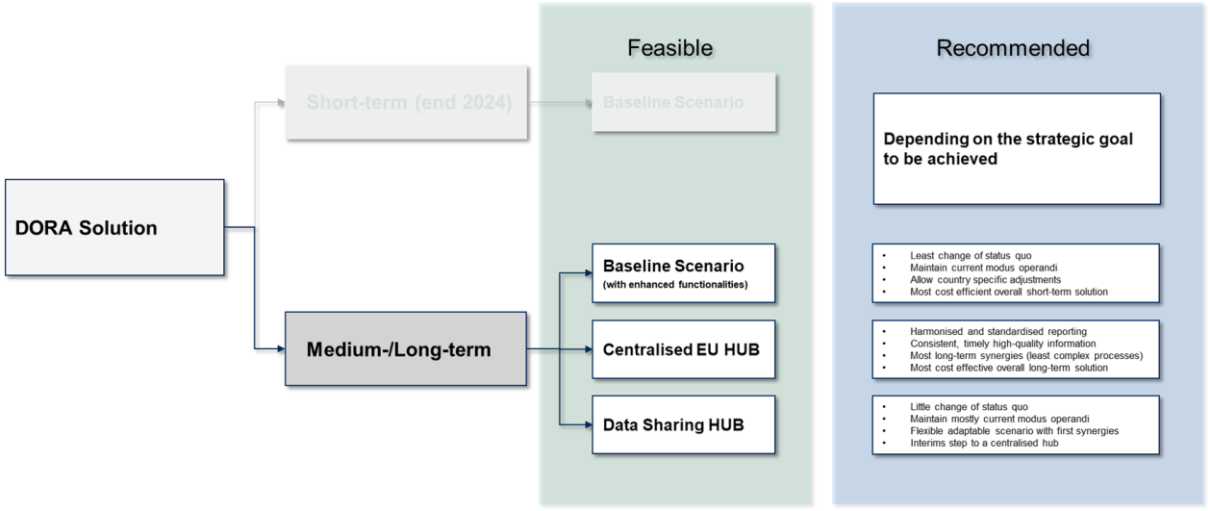
FIGURE 15 OVERALL PERSPECTIVE: HIGH-LEVEL OVERALL COST-BENEFIT ANALYSIS

Conclusions – Gartner Consulting’s point of view



Considering that a fully centralised EU Hub and an EU Data Sharing Solution cannot be implemented on the short term due to legal prerequisites which need to be created first, we conclude the following:

- In the short term, no scenario other than the Baseline Scenario is possible. In the medium to long term, all three scenarios are technically feasible, provided the legal requirements are created. There have been no obvious showstoppers identified
- The results of the assessments as presented in the previous sections show that overall, there is no dominant scenario, i.e. an absolute best scenario for all stakeholder groups and stakeholders involved according to all criteria listed in DORA (Article 21(2)).
- Therefore, the suitability of the three different scenarios depends on the strategic objectives to be achieved.



If the strategic goal is to change the existing reporting of incidents as little as possible, maintaining the current division of labour (modus operandi) between the ESAs and CAs,

to leverage the existing systems and to allow for country-specific adjustments, then the Baseline Scenario is the best solution. The downside of this scenario is that it is based on the most complex data collection and management process considering the necessary steps and the necessary number of interfaces between the involved different legal entities. It also provides the lowest supervisory convergence. Groups of FEs working in different EU countries may need to double/multiple report in this scenario the same incidents to multiple CAs potentially in different formats.

Is the strategic goal to have the best consistent and standardised high quality incident reporting data available on EU level in a timely manner and to simplify the incident reporting for the FEs the Central Hub is the best solutions. The data collection and management process are the least complex one of all scenarios. Such a central hub could also allow to provide all member state authorities the same sophisticated analytical tools which would allow to get valuable insights by leveraging the available information about cyber incidents in the best way. A central system would also allow to implement easier future changes and a high secure incident reporting ecosystem. This is easier to achieve with a centralised system compared to a decentral fragmented data collection approach based on systems with different technologies and different IT security standards. A potential concentration risk could be mitigated setting up appropriate IT security measures.

A central EU hub would allow to create most synergies through the centralisation of the necessary software and hardware infrastructure. Through centralisation of the data collection and quality assurance processes this scenario could also provide the best consistent timely consolidated incident reporting database on EU level. The standardisation of the incident reports and reporting processes could also provide the highest level of supervisory convergence of all scenarios. Depending on the detailed design of the Centralised Hub (technical solution as well as associated business and IT processes), these synergies (economies of scale) may vary in magnitude. (Note: the detailed solution design was not the subject of the Gartner Consulting project). To quantify such economies of scale, also the different characteristics of the NCAs (size of available infrastructure/capabilities) in the different member states should be taken into account. Gartner Consulting therefore recommends that all NCAs be more closely involved in the design phase of the detailed solution, which was not possible in the current phase given the scope of the Gartner Consulting project. Such an approach makes it possible to jointly design a centralised solution that creates maximum economies of scale for the common benefit of all NCOs, ESAs, FEs and other stakeholders and increases the overall IT security level of the entire Cyber Security Incident Reporting ecosystem."

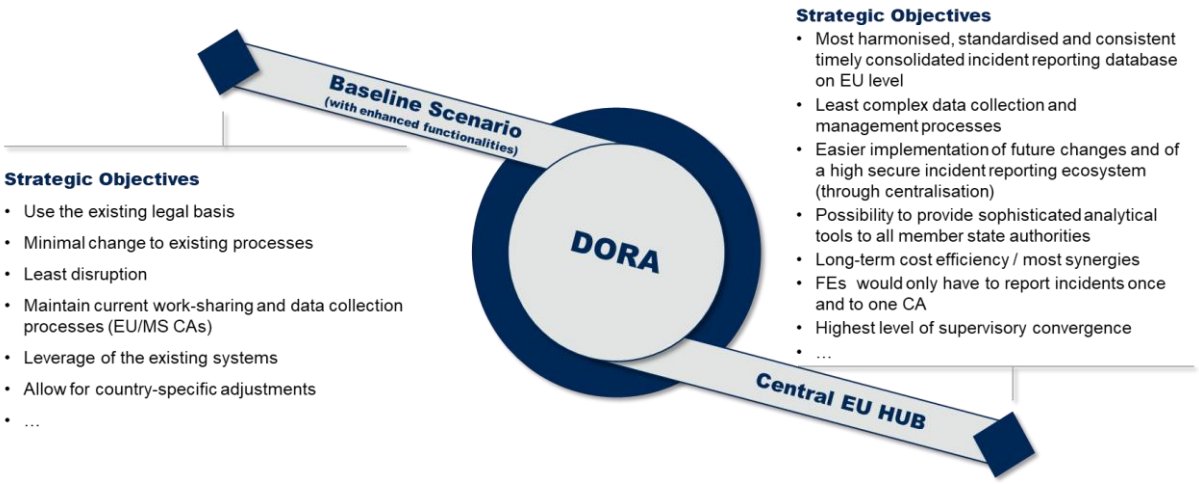
The Data Sharing Solution is a scenario which is a mix of the two other scenarios and provides some benefits for the CAs but still leveraging the existing incident reporting processes and tools to a far extent. This scenario could be seen as an interims step towards a centralised hub, it is very similar to the baseline scenario but provides CAs the possibility to access the information centrally and not through point-to-point data exchange with other CAs which may reduce on CA side significantly efforts but still may require groups of FEs working in different EU countries to double/multiple report the same incidents to multiple CAs potentially in different formats. The synergies for the NIS 2 CAs may also be limited since FEs may be legally obliged if national law requires them to submit

major incident reports directly to the relevant authorities. The data collection process is simpler compared to the Baseline Scenario, as this scenario at national level can, where legally possible, allow data to no longer be exchanged between CAs at national level. But the data collection process is still based on two stages which makes the data collection process much more complex compared to the Central Hub Scenario.

Risks were identified which need but also can be mitigated with appropriate measures, in particular in the case of a Centralised Hub the risks associated with the centralisation.

Standard solutions with a high degree of functional and non-functional coverage are available in the market as alternatives to self-developed solutions

Considering the increasing importance of timely high quality incident reporting data, the need to take aligned effective counter measures in time and the potential damage which could be created by delays in the context, the associated overall infrastructure cost seems to be neglectable low.



The "Data Sharing Hub" could be an intermediate step, keeping midterm the current processes but also creating gradually more benefits out of a centralised solution.

Annex III: Existing Systems

1. In order to effectively understand the possibilities towards a further centralisation of incident reporting under DORA, it is essential to understand the current responsibilities, procedures and systems in place at the national, EU, and commercial levels. This section delves into the existing frameworks and mechanisms that facilitate incident reporting within the financial sector. By examining the approaches adopted by various stakeholders, we can gain insights into the current landscape of incident reporting practices.
2. Furthermore, the main strengths and limitations of these existing systems will be explored, highlighting areas where improvements can be made. Through this analysis, the aim is to develop a comprehensive understanding of the current state of ICT incident reporting, paving the way for the formulation of more centralised frameworks which can be relevant for DORA.

Case Study 1 – ESMA

3. In the realm of incident reporting, the role of ESMA is notably twofold, encompassing both direct and shared supervisory responsibilities. ESMA's direct supervisory purview extends to all EU Credit Rating Agencies (CRAs), Trade Repositories (TRs), Securitisation Repositories (SRs), certain Data Reporting Services Providers (DRSPs), specific benchmark administrators, and Tier 2 third-country Central Counterparties (CCPs).
4. In contrast, the National Competent Authorities (NCAs) maintain supervisory responsibilities over all other market actors. This means that while ESMA has a significant role to play, its efforts are complemented by those of the NCAs, leading to a broad-based, multi-layered approach to incident reporting and management. The synergy between ESMA and the NCAs thus forms a comprehensive framework that addresses the diverse spectrum of entities operating within the EU's financial markets. The integration and cooperation of these bodies aim to enhance the overall robustness and resilience of the financial market infrastructure in the face of ICT-related threats.

ESMA - IT implementation

5. As a direct supervisor of certain types of financial entities, ESMA holds a significant role in the incident reporting process. ESMA is responsible for receiving initial notifications and subsequent reports of major ICT-related incidents from these entities. It is then required to assess the relevance and impact of the incident on a broader scale, taking into consideration other competent authorities in the EU. This involves a proactive analysis of the incident's potential ripple effects on the financial markets of other Member States, thus ensuring timely and relevant information exchange. As such, ESMA acts as a crucial link between the incident-affected entity and the collective response of the EU's financial market authorities.

6. For the purpose of this study, the focus will be limited to two types of ESMA's supervised entities that report the highest number of ICT incidents: Trade Repositories (TRs) and Data Reporting Services Providers (DRSPs).

7. The incident management process at ESMA level is composed by the following sub processes and tools supported by an IT implementation:

   (a) Incident Reporting

   (b) Incident Assessment (Incident Panel)

   (c) Incident follow-up

   (d) Pre-Enforcement

   (e) Reporting templates

   (f) Incident log

   (g) Incident dashboard

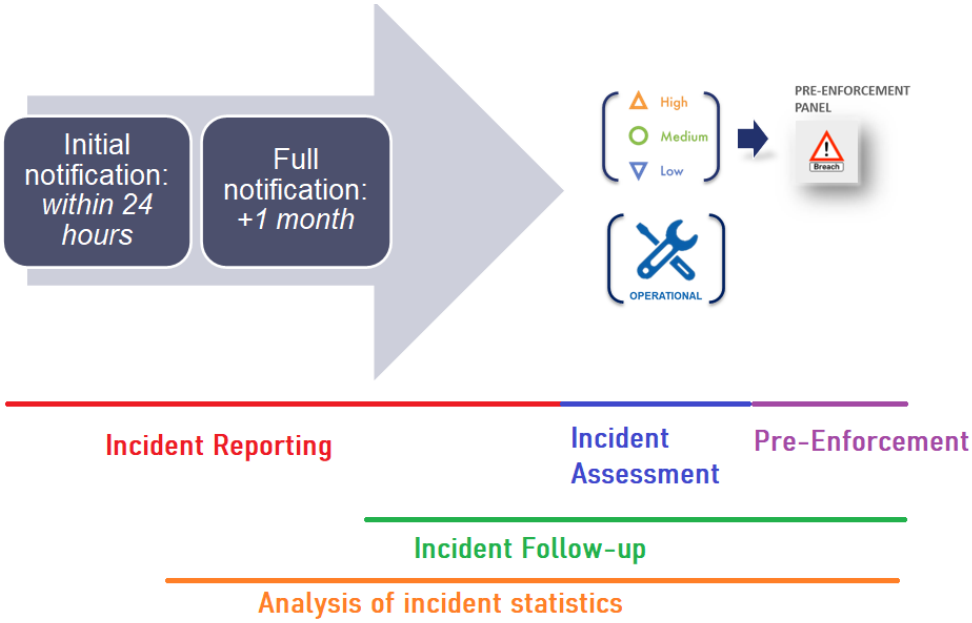


FIGURE 16: ESMA INCIDENT REPORTING FLOW

Case Study 2 – EBA

8. With regard to the incident reporting function at the European Banking Authority (EBA), the revised Payment Services Directive (PSD2) conferred a mandate to the EBA to collect and disseminate reports on major security or operational payment-related incidents.

9. Since 2018, the EBA has been tasked to receive major incident reports impacting payment service providers, including credit institutions, payment institutions and e-money institutions, (PSPs). The reporting flow requires PSPs to submit an initial, intermediate or

final report of a major incident to their CAs, which subsequently send it to the EBA and the ECB. Upon receipt of the major incident report, the EBA, ECB and the submitting CA are required to assess the relevance of the incident to other Member States and the EBA is required to notify and forward these incidents reports to the CAs from these relevant Member States. In addition, the EBA together with the ECB and in cooperation with the competent authority of the home Member State is required to assess the relevance of the incident to other relevant Union and national authorities and to notify them accordingly.

10. The provisions related to the classification and reporting of major incidents under PSD2, the specification of the classification criteria, materiality thresholds, as well as the reporting template, the description of the data fields and instructions how to populate the template are set out in the EBA Guidelines on major incident reporting under PSD2.

11. Based on the major incident reporting under PSD2, the EBA and ECB have been following high-level reporting trends and assessing the information received, which led to the revision of said Guidelines, organisation of an industry workshop on the trends and issues observed related to major payment-related incidents, and, crucially, as an input informing the policy development of the incident-related policy mandates under DORA.

EBA - EUCLID system

Overview

12. The European Centralised Infrastructure for Supervisory Data (EUCLID) platform is the current system for banking and financial data in the EU's financial sector which is place since its implementation 2021. EUCLID keeps evolving in terms of scope of reporting entities and functionalities, with a data dissemination platform being launched during Q4 2023 and Q1 2024 (phase 1 and 2, respectively). In addition, it is complemented with the EBA's public registers, namely the Credit Institutions Register (CIR) and the Payments Institutions register (PIR) under the Payments Service Directive (PSD2), and possibly with a critical Third Party Providers (cTTPs) register in coming years.

13. The current reporting scope to the EBA covers over 10,000 reporting entities including EU/EEA credit institutions banking groups, investment firms, investment firms' groups, resolution groups, payment and e-money institutions1.

Legal basis

14. The EBA EUCLID Decision2, sets out the scope, timing and modalities of the data submission and covers the reporting for all CAs to the EBA, for the different reporting modules including supervisory, resolution, investment firms and payments data.

Reporting process and CAs involvement

15. At the EBA, the supervisory data has two main flows, one for the master data needed for setting up the reporting calendar and one for the supervisory data. Concerning master data, CAs source them from their own national registers, internal supervisory activities or directly from reporting entities, later sending the required supervisory master data to the EBA.

16. In addition, reporting entities send the supervisory data to the relevant CA which forwards the information to the EBA. To ensure that data are submitted in the most efficient way, avoid duplication of reporting requirements and a smooth process for data transmission to the EBA, the sequential approach is place for supervisory and master data to ensure the consistency of data submitted to different authorities. In this respect the ECB and the SRB forwards, those data on behalf of CAs participating in the SSM, to the EBA.

17. For the transmission of files from CAs to the EBA, it was agreed to use the eXtensible Business Reporting Language (XBRL) standard for all supervisory files submitted. XBRL has the advantage of providing a high degree of flexibility in the creation of XBRL instance documents and provides a maximum level of harmonisation of the supervisory reporting among other things.

Data collection and analysis

18. Supervisory data are submitted according to the Data Point Model (DPM) specified by EBA and additional technical specifications provided. The DPM is a structured representation of the data identifying all the business concepts and its relations, as well as validation rules. It contains all the relevant technical specifications necessary for developing an IT reporting solution.

19. Additionally, with the aim of providing a uniform implementation of the reporting requirements, XBRL taxonomies are produced based on metadata in DPM to present the data items, business concepts, relations and validation rules in XBRL standard format.

Information sharing and collaboration

20. EBA collaborates with different EU supervisory authorities through memorandum of understanding (MoUs) on sharing data and continues to facilitate methods of exploiting the data. Additionally, the EBA also increased the number of data visualisations tools on a wide range policy areas aimed at presenting large amounts of data in a more comprehensive and dynamic manner.

21. On the EBA's website, the public can find user-friendly tools for different topics and risk areas, which allow users to explore comparable bank-by-bank figures through maps, tables and graphs to provide transparency on the EU financial system and enhance the role of the EBA's EU hub for banking data.

Main benefits

22. One of the main benefits is its scalability, among other aspects, whereas the number of files transmitted to the EBA since its inception has grown constantly proportionally to the number of reporting agents and modules, reaching over 244 000 files for 2022 reference dates.

23. From an analytical point of view, EUCLID allows the EBA to carry out deeper analyses of the EU-wide financial sector with the aim of enhancing its role as data-driven organisation in line with its data strategy.

Case Study 3 – ENISA Baseline Solution

Overview and legal framework

24. ENISA maintains an incident reporting tool, called CIRAS (Cybersecurity Incident Reporting and Analysis System), for the authorities, where they can upload reports, and search for and study specific incidents. At the moment, the main use for CIRAS is to support the annual summary reporting for NIS Directive, EECC Art. 40 and eIDAS Art. 19.

Reporting process

25. CIRAS is fully customisable and relies on defined taxonomies for the aforementioned pieces of legislation. All the information in the taxonomies may be customized to include for example additional information to be reported or different workflows, allowing for a dynamic and easily extensible incident reporting platform.

26. For the public, ENISA also offers an online visual tool, which is publicly accessible and can be used for custom analysis of the data: https://ciras.enisa.europa.eu/. This tool anonymises the country or operator involved.

27. The reporting template starts with an incident type selector and contains three parts:

    I. Impact of the incident –which communication services were impacted and by how much.

    II. Nature of the incident –what caused the incident?

    III. Details about the incident – detailed information about the incident, a short description, the types of network, the types of assets, the severity level etc.

28. The type selector distinguishes six types of cybersecurity incidents (see figure below). We explain the different types below.

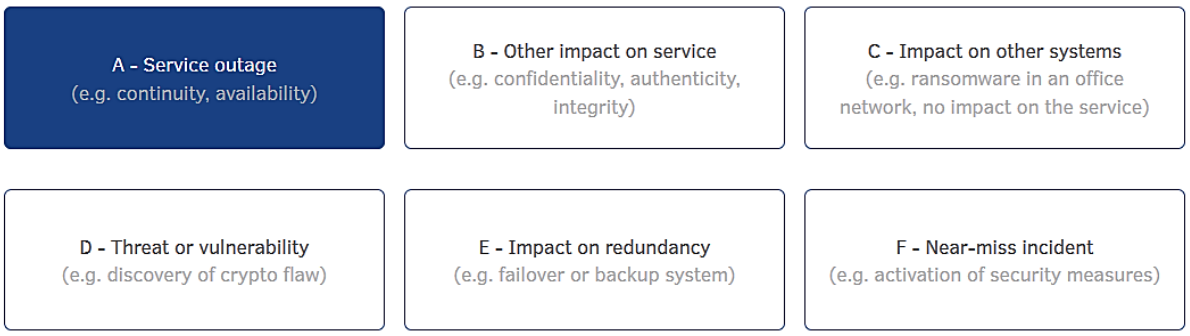


FIGURE 17 TYPE OF INCIDENT UNDER CIRAS

- **Type A:** Service outage (e.g. continuity, availability). For example, an outage caused by a cable cut due to a mistake by the operator of an excavation machine used for building a new road would be categorised as a type A incident.
- **Type B:** Other impact on service (e.g. confidentiality, authenticity, integrity). For example, a popular collaboration tool has not encrypted the content of the media channels, which are being established when a session is started, between the endpoints participating in the shared session. This leads to the interception of the media

(voice, pictures, video, files, etc.) through a man-in-the-middle attack. This incident would be categorised as a type B incident.

- **Type C**: Impact on other systems (e.g. ransomware in an office network, no impact on the service). For example, *a malware has been detected on several workstations and servers of the office network of a telecom provider*. This incident would be categorised as a type C incident.
- **Type D:** Threat or vulnerability (e.g. discovery of crypto flaw). For instance, *the discovery of a cryptographic weakness* would be categorised as a type D incident.
- **Type E:** Impact on redundancy (e.g. failover or backup system). For example, *when one of two redundant submarine cables breaks* would be categorised as a type E incident.
- **Type F:** Near-miss incident (e.g. activation of security measures). For instance, *a malicious attempt that ends up in the honeypot network of a telecom provider* would be categorised as a type F incident.

CA involved, information sharing and collaboration

29. The data on CIRAS version 1 and CIRAS Consolidated Reporting version 1 are anonymised and both visualisations are publicly available on the front page of CIRAS portal. Baseline CIRAS supports incident reporting by MS competent authorities, as well as analysis of the provided data.

30. CIRAS Consolidated Reporting functions:

- Custom analysis over the full dataset, per sector
- Multiannual statistics and trend graphs

31. When it comes to incident reporting, the following functionalities are supported:

- Create/view incident report for specific year and a list of sectors
- Create/view quarterly report
- Create/view annual report
- Cross border/article information
- Selection of one or more countries/articles
- Information remains in the tool
- Alert users via email
- Commenting, discussing incidents
- Search functionality
- Country profile, settings, authorised users & logs
- Status overview (annual, quarterly)
- Create/view supervision topics
- Administration options:
- Manage list of countries
- Manage users (assign / revoke roles)

- Import / export incidents
- Manage sectors and their mapping to articles
- Manage articles details
- Define the structure and logic of the incidents per article

FIGURE 18 EXAMPLE OF DASHBOARD IN CIRAS

32. CIRAS VISUAL functions:

- Custom analysis over the full dataset, per legislation
- Multiannual statistics and trend graphs

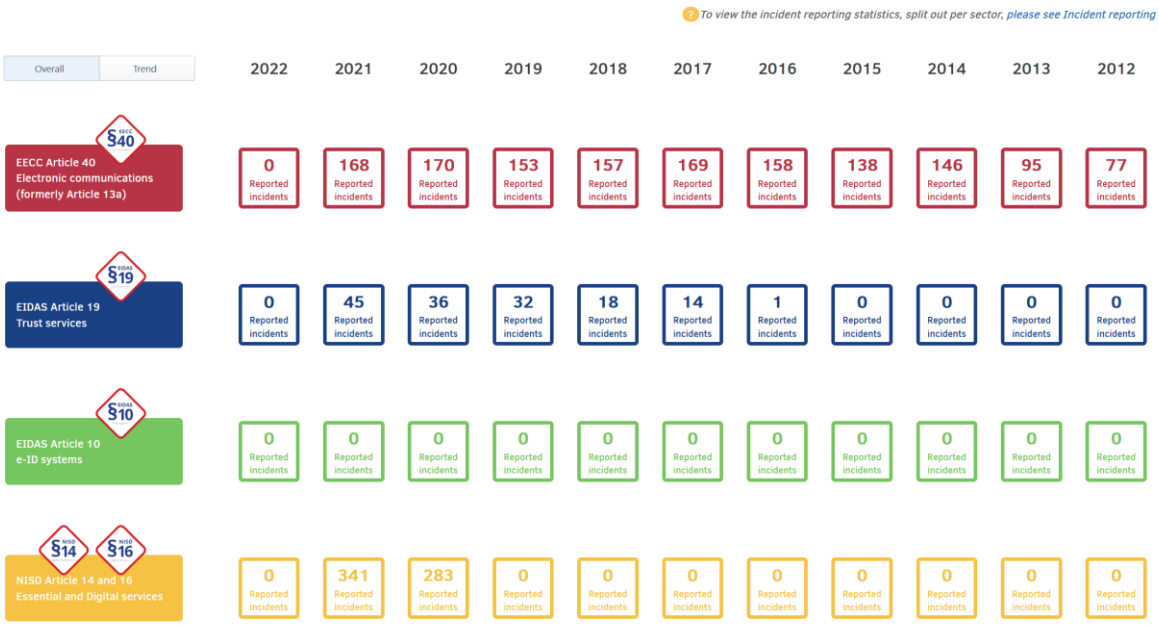


FIGURE 19 EXAMPLE OF INDICATORS UNDER BASELINE SOLUTION

33. Additionally, CIRAS provides the following functionalities:

- Cross-border incident notification: a MS may notify an incident as having cross-border impact and thus potentially affecting other countries. That incident may be marked as cross-border and all potentially affected countries may be marked down to receive an automated notification from CIRAS and commence a discussion with the reporting MS.
- Cross-country communication/discussion forum: following a cross-border incident notification, or on an ad hoc manner, CIRAS Solution supports a discussion forum for countries to exchange information and attachments about particular incidents. It is also possible to mark the status of the discussion and mark it as complete when the issue discussed has been resolved.

34. Issue tracker: the platform offers an issue tracker for users to register potential issues with the platform to be resolved by the administrators, namely ENISA.

Case Study 4 – ECB SSM

35. The SSM Cyber Incident Reporting Framework has been established as a central mechanism to collect, analyse, and draw actionable insights from significant cyber incidents, helping to monitor credit institutions and to uphold the resilience of the financial system. The entities in scope of the SSM Cyber Incident Reporting Framework are Significant Institutions[22] that are supervised by the ECB ("Supervised Institutions"). These institutions report cyber incidents that fulfil the reporting criteria at the highest level of consolidation (within the SSM). The objectives of the framework focus primarily on i) assessing the impact to the bank in an immediate follow-up, identifying critical cyber incidents that could potentially lead to a crisis situation and ii) drawing potential conclusions from the cyber incident for the supervisory assessment of the overall cyber risk of the bank.

36. At its core, the framework establishes a streamlined procedure and a database, set up as a centralised repository for significant cyber incidents. Supervised Institutions report directly to the ECB or, for some countries with pre-existing national cyber incident reporting regulations, via their National Competent Authorities (NCAs). The incidents are reported via a standardised Excel-based template, to ensure collection of consistent information across all incidents. Details about the current reporting process are explained in Section 3.3.1.3.

37. The ECB's Cyber Incident Team is set up to operate the reporting process, bridging communications among banks, NCAs, and the JSTs. Its role also includes gauging the impact of each incident, invoking and running the dedicated Cyber Incident Emergency Process (CIEP), with participation of experts across the ECB and NCA functional areas, in cases of highly critical ("major") incidents. The ECB's Cyber Incident Team is acting both in capacity of an expert function, providing support to JSTs in specific cases, and as an analytical function, providing insights on a cross-bank level.

[22] https://www.bankingsupervision.europa.eu/banking/list/html/index.en.html

ECB SSM Cyber Incident Reporting Framework (CIRF)

Overview and legal framework

38. The legal basis for the reporting of significant cyber incidents results from the decision of the ECB Supervisory Board to develop a Cyber Incident Reporting Framework (SB/15/37/09), with an aim to enhance the safety and soundness of Supervised Institutions and the stability of the financial system as per Article 10(1)(a) of Regulation (EU) No 1024/2013 and Article 141(1) of Regulation (EU) No 468/2014 of the European Central Bank[23]. In accordance with this overarching decision, each Supervised Institution has received an individual ECB Decision[24] that requires this Institution to report significant cyber incidents. These individual ECB Decisions include specific reporting instructions, reporting criteria and the template.

39. The framework comprises a database and process for handling significant cyber incidents, as well as a cyber incident emergency process (CIEP) for those incidents which may lead to a crisis situation for the affected bank. It serves a dual purpose: i) assessing the impact to the bank, identifying critical cyber incidents that could trigger the CIEP and ii) drawing conclusions from the cyber incident for the supervisory assessment of the overall cyber risk of the bank.

Reporting process

40. Banks should report incidents that are considered significant. In countries with pre-existing national incident reporting obligations, banks report incidents to their NCA first, which then transmits the relevant information to the ECB. In the remaining cases, Supervised Institutions are obligated to directly report to the ECB. The determination whether a cyber incident is significant and thus falls under the reporting obligation, is based on a set of criteria. An incident should be classified as significant in any of the following cases: a) it is publicly reported in the nation-wide or international media; b) the estimated financial impact equals or exceeds EUR 5M or 0.1% of CET1; c) it is internally escalated up to the top management - CIO or comparable position outside of regular reporting; d) the crisis management procedures are triggered, for example the Disaster Recovery and/or other measures in the Business Continuity Plan have been activated; e) the incident is reported to law enforcement, CERT or security authorities. Furthermore, banks should exercise their judgement, and may report incidents outside of the criteria, taking into account the extent of service disruption, reputational damage, legal and regulatory impact, competitive disadvantage or a potential systemic impact of the incident. Reporting is done by means of a standardised Excel template that is transmitted as a PGP-encrypted attachment via a notification email. In order to ensure that the initial information is shared timely, even if not much information may be available about the incident or its impact, the bank has to send an initial report within 2 hours of the exceedance of any of the reporting thresholds. The initial report asks for only the basic information about the incident. Additional information about the incident impact and scope

[23] Regulation (EU) No 468/2014 of the European Central Bank of 16 April 2014 establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (ECB/2014/17) (OJ L 141, 14.5.2014, p. 1).
[24] ECB Decisions can include formal obligations, imposed on the Supervised Institutions, and are enforceable – which means that the institutions can face sanctions or other enforcement measures if they fail to comply with the Decisions.

is requested in an interim report, which should be submitted within 10 working days of the first report, and a final report, which is to be submitted within 30 working days of the initial notification. The incident workflow is handled in Darwin – which is a central document repository of the ECB and the information exchange platform between the SSM supervisory authorities.

CA involved, information sharing and collaboration

41. The Cyber Incident Team receives the first notification of the incident either directly from the bank or indirectly via the NCA. The incident is timely shared with the Joint Supervisory Team (JST), which includes both the ECB as well as NCA members. The JST then classifies the incident according to its criticality and follows up if needed and monitors the development of the situation. Bank-specific issues (e.g. weaknesses, vulnerabilities, remediation actions, etc.) are discussed between the JST and the bank bilaterally when necessary. For incidents of the highest criticality ("major incidents"), a Cyber Incident Emergency Process is triggered, with involvement of the relevant SSM NCAs.

Data collection and analysis

42. Information is collected via the Excel templates and stored in a database in Darwin. All fields are mandatory. The initial report is limited to a general description of the incident, the interim report includes a more detailed description of the incident, identifying important aspects such as the type of incident, channels affected, information on the attacker, and the entry vector, while the final report includes additional information on aspects such as the crisis management procedure, weaknesses exploited and remediation actions.

43. Reports and supporting documents are exchanged via PGP-encrypted email, tied to a central ECB email address and dedicated users from the SI.

44. After the resolution, a holistic analysis takes place to enable a comprehensive understanding, consisting of i) an analysis by the supervisors of the impact and potential implications on the risk level of the institution, and on the institution side, any lessons learned; ii) a continuous assessment by the cyber incident team of potential trends, as well as the need for information sharing, and annual cross-institution and country benchmarking analysis.

Main benefits

45. The current cyber incident reporting framework streamlines and standardises information sharing. The implementation of a standardised template across all reporting stages - initial, interim, and final - facilitates a consistent workflow from data collection to analysis. The workflow is highly flexible yet time-sensitive, as the template is specifically designed for timely updates. While all information is required at the end of the incident lifecycle, it contains both open fields (free text) as well as multiple-choice or formatted fields (date/time, checkboxes etc), which can be populated as information becomes available. Moreover, while the core information is streamlined, supplementary documents can be attached and stored in the database, keeping all relevant information in one place.

Main challenges / risk

46. Ensuring a harmonised interpretation of the criteria for incident reporting is essential to establish a consistent incident analysis across supervised institutions and countries.

Another challenge is to obtain adequate data quality with respect to the submitted incident reports – that templates are unaltered and filled in with the requested and correct information. Technical issues with regard to the PGP encryption solutions are also causing additional operational burden as well as complicating streamlining of the process. The current cyber incident reporting framework, as it stands distinct from PSD2, could also potentially lead to fragmented incident handling.

Annex IV: Existing systems at National Level

Case Studies 1: Examples of National Competent Authorities' Use and Relevance of Transmitted Incident Information – Polish Financial Supervision Authority

1. The Polish Financial Supervision Authority (PFSA) is an example of a national competent authority with tasks connected with incident reporting.

2. These obligations derive primarily from the National Cyber Security System Act, which implements the NIS Directive. Pursuant to Article 41 of the Act, the PFSA remains the competent authority for the sector of banking and financial market infrastructure. In addition, a sector-level CSIRT team (CSIRT KNF) has been established within the PFSA for the relevant sector. This team, in addition to the national CSIRTs, receives major incident reports from operators of essential services in the banking and financial market infrastructure sector. The team's tasks also include assisting operators of essential services in handling cybersecurity incidents, as well as analysing major incidents, finding links between incidents and drawing conclusions from incidents handling. As part of its tasks, the sector-level CSIRT team cooperates with the CSIRT teams at national level to coordinate the handling of major incidents.

3. Based on the analysis of available information, including incident reports, the team takes actions to strengthen the cybersecurity of operators of essential services in the sector of banking and financial market infrastructure. These measures primarily include the issuing of warnings, recommendations and alerts. These are communicated to operators of essential services on an ongoing basis and address current cyber security threats, emerging vulnerabilities and ways to mitigate them. An example of this can be found in the Good practices in DDoS countermeasures[25]. They were prepared by the CSIRT KNF on the basis of experience and information gathered from incidents involving DDoS attacks, the scale of which increased significantly in Poland after Russia's aggression against Ukraine. They focus primarily on practical ways of reducing the threat posed by this type of attack to financial entities.

4. In addition, the sector-level CSIRT team also undertakes activities to share information extracted from incident reports (subject to data confidentiality requirements). Through the MISP platform, Indicators of Compromise are shared with operators of essential services. These are particularly helpful in mitigating cyber threats and vulnerabilities and in preventing incidents. Cooperation between the CSIRT KNF and operators of essential services, including in the area of incident reporting, is also being developed through the organisation of regular meetings to discuss current trends in cyber security incidents and threats as well as to discuss lessons learned. During such meetings, financial market entities can also indicate their needs and expectations in terms of incident handling support.

5. To summarise, incident reports enable the CSIRT KNF to gain situational awareness of the current cyber security situation in the financial market - current threats, attack methods, threat actors or exploited vulnerabilities. The information gained by the CSIRT

[25] https://www.knf.gov.pl/knf/pl/komponenty/img/Good_practice_against_DDoS_EN_78023.pdf

KNF from incident reports enables it to provide more effective cyber security support to operators of essential services and other financial entities.

Incident reporting in Poland

Overview and legal framework

6. The reporting of security incidents is mainly carried out on the basis of the PSD2 Directive and the Polish Act on the National Cyber Security System, which implements the NIS Directive in Poland. It assumes the existence of three national-level CSIRT teams, which are responsible for the security of citizens, government and military entities in the country. In addition, the Act also provided the possibility for competent authorities to appoint sector-level CSIRT teams. On 1 July 2020, the Polish Financial Supervision Authority appointed a sector-level CSIRT team for the financial market - the CSIRT KNF. This team is responsible for coordinating incident handling in the banking, financial markets and insurance sectors. The team is also responsible for monitoring and analysing cyber threats to financial entities.

Reporting process

7. Entities classified as operators of essential services are required to report security incidents to the relevant national level CSIRT team and sector level CSIRT. The national level CSIRT teams and the sectoral CSIRTs cooperate with each other in the analysis of incidents and cyber threats. They also have the authority to pass on sensitive information as part of incident handling. Reporting to the national and sector level CSIRT teams is done via a dedicated web form on the website, or via a prepared PDF form sent via email. In the case of emailing, an additional mechanism is used in the form of PGP encryption. CSIRT teams make public PGP keys available on their websites to encrypt communications. The incident handling process uses the well-known open source RTIR (Request Tracker for Incident Report) solution - the use of the tool allows the handling of reported incidents to be organised and structured. PSD2 incidents are reported directly to the Competent Authority using a dedicated and pre-differentiated form in an XLS file. Files are sent using the government's ePUAP system.

CA involved

8. The Competent Authority (Polish Financial Supervision Authority) accepts information on PSD2 incidents. The Competent Authority has also set up a sectoral CSIRT team of the PFSA (CSIRT KNF) responsible for coordinating the handling of incidents arising from the NIS Directive. The establishment of the team has streamlined the incident handling and coordination processes and also facilitated communication with the other CSIRT teams in the country.

Data collection and analysis

9. Information on major incidents reported is contained in a dedicated and structured form, the fields of which are derived from the NIS Directive or PSD2 Directive. In addition, technical information on IOCs (Indicators of Compromise) related to incidents or cyber

threats is transmitted using the STIX2 language in the MISP (Malware Information Sharing Platform). The use of the STIX2 language allows information to be exchanged in a standardised and structured manner. This information is usually transferred via STIX2 information sharing platforms.

Information sharing and collaboration

10. National-level CSIRT teams and sectoral CSIRTs exchange information on a daily basis on potential cyber threats and common security incidents. To facilitate communication, the Mattermost system is used, which allows direct working contact between individual staff members of all CSIRT teams. Technical information on the threats themselves is sent through a dedicated open-source system MISP. The system was initially used to exchange information on malware samples but is currently used by CSIRT teams to systematise the exchange of information on existing threats in the form of IOCs. The system is developed and maintained by the Luxembourg CSIRT LU team. The Traffic Light Protocol (TLP) standard is used to ensure that information is only shared with those who need to know.

Main benefits

11. Current practice in incident handling and response to cyber threats shows that an efficient exchange of information between the various actors involved in an incident is an essential element of the process. Working communication between security analysts should be simplified as much as possible and stripped of redundant formulas to make it faster and more efficient. The systems currently in use allow communication to be facilitated and streamlined. An important element in the exchange of technical information is the use of a standardised and predictable language. The use of the STIX2 standard makes it possible to communicate structured information that can be used by both the analyst and the information systems.

Main challenges / risk

12. Harmonisation and unification of incident handling processes resulting from different legislation (NIS, PSD2). Adequate communication with supervised entities in order to fine-tune the interpretation of criteria for incident reporting. Development of clear and efficient incident reporting and handling processes.

Annex V: Stock taking exercise with CAs

About the respondents

1. During March and April 2023, a stock-taking exercise was conducted between different competent authorities under the DORA framework. The main objective was to gather qualitative and quantitative information from the CAs that could be relevant to feed into the feasibility study, particularly in its initial phases. It is important to consider that the results obtained during the survey may have changed by the time the report was completed. The exercise was primarily attended by national authorities present in the

JC SC DOR[26], as well as NIS authorities and Resolution authorities. Figure 6 below shows the number of authorities that participated in the exercise and the number of countries represented in the sample.

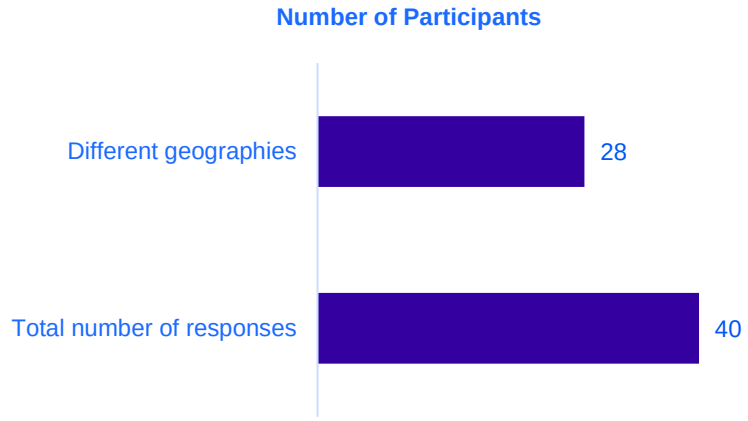


FIGURE 20 NUMBER OF CAS PARTICIPATING IN THE DATA COLLECTION EXERCISE

2. As can be observed, and despite the fact that the survey was carried out on a best effort basis, numerous competent authorities from numerous member states participated in the process (including authorities at EU-Level). In this way, although the results are not representative of all competent authorities, they do allow certain conclusions and useful information to be drawn for the preparation of this document. It is important to note that at the time the survey was conducted, there was a certain degree of uncertainty surrounding the regulatory developments linked to incidents (fundamentally around the classification of incidents and the instructions and templates related to reporting to the competent authority) and also the baseline scenario for enabling incident reporting in January 2025.

3. Also related to the representativeness of the sample, it is important to highlight that the responses correspond to authorities with responsibilities in different sectors and that they currently receive incidents from the entities under their competences with the support provided under multiple regulations. In the following graphs, can be seen both the sectors and activities represented in the sample as well as the different regulations under which they operate[27].

[26] Join Committee Sub-Committee DORA
[27] Note that in certain member states the same authority operates in multiple sectors and under multiple regulations

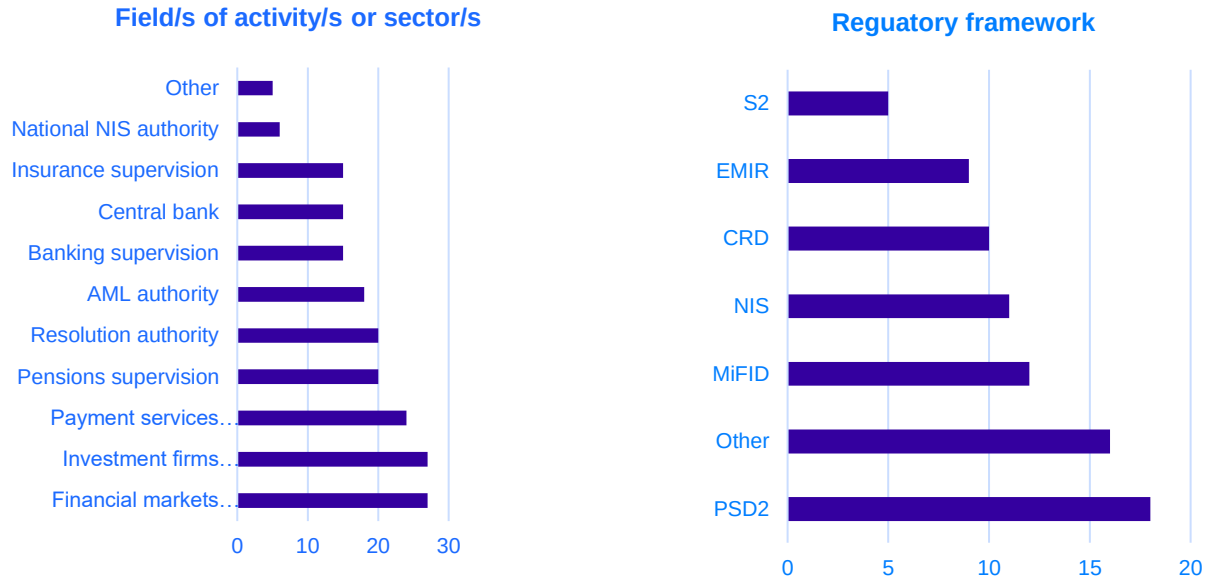


FIGURE 21 SECTORS AND REGULATORY FRAMEWORKS FOR THE EXERCISE

Existing incident reporting frameworks in place in the Member States for the financial sector

4. One of the questions introduced in the survey concerned the typology of financial institutions already subject to reporting among the member states that participated in the sample. The objective was to capture the extent to which all the typologies of entities listed in article 2 of DORA were already subject or not to some kind of online incident reporting requirement to be established by this regulation[28].

[28] It is important to highlight the limitations linked to the completeness of the sample present in the survey.

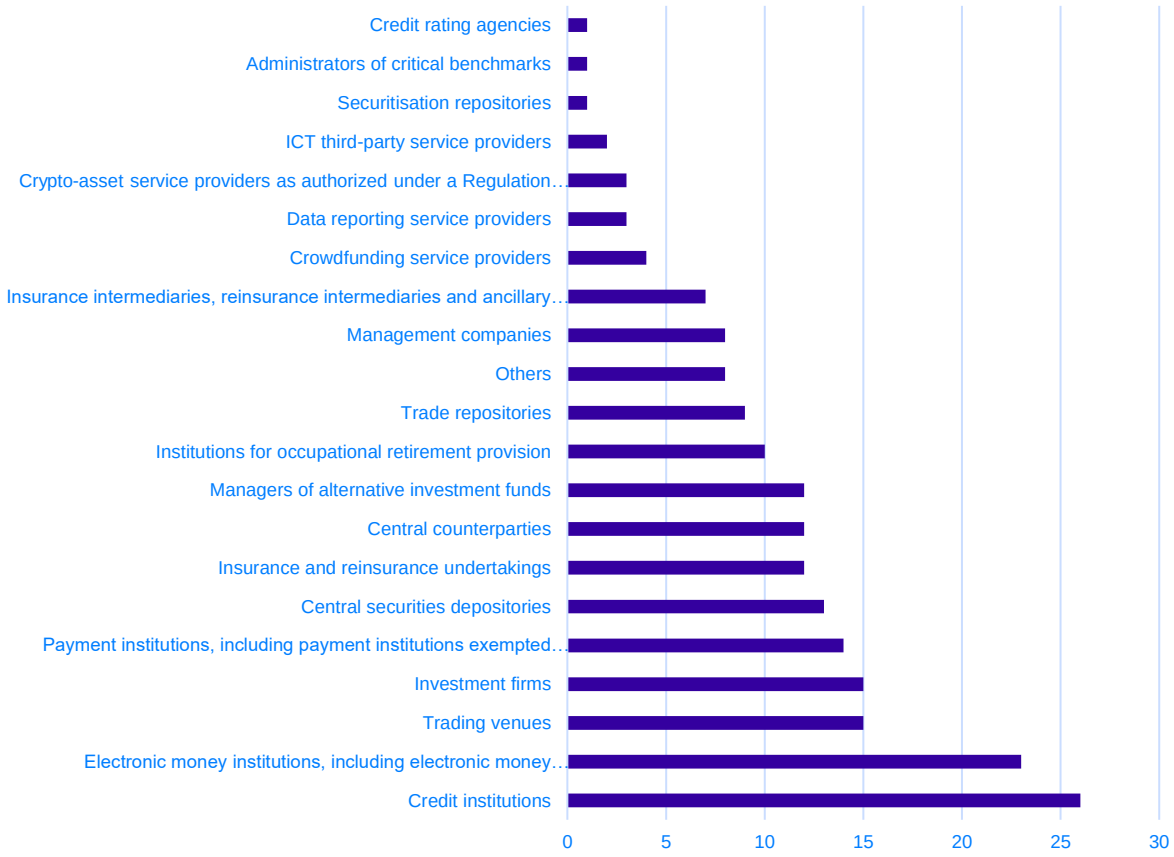


FIGURE 22 INSTITUTIONS SUBJECT TO INCIDENTS REPORTING INFORMATION

5. With the caveats related to the sample used, it can be observed that some sectors within financial activities are already subject to incident reporting requirements in the area of digital operational resilience in multiple or all of the geographies represented. This is particularly noticeable in the case of credit institutions and electronic money institutions. However, many other sectors within the scope of DORA will now be subject to support obligations that they did not have prior to the implementation of this regulation. This aspect is particularly important for the correct dimensioning of any future solution, as the number and type of institutions have increased, both from the point of view of the users of the reporting system and from the point of view of the volume of information to be exchanged. Efforts aimed at simplification of reporting and analysis of related information will obviously have a relevant impact.

Existing solutions/hubs for the reported incident information by financial entities

6. One of the most relevant aspects of the stock-taking exercise was to find out how the competent authorities currently manage the flow of information related to incident reporting. Both from the point of view of the exchange itself, as well as from the point of view of the information to be submitted. Regarding the first point, it was found that many competent authorities already have some kind of solution or hub dedicated to incident

reporting, with more than 60% of the authorities responding to the survey stating that such a solution already exists at Member State level.

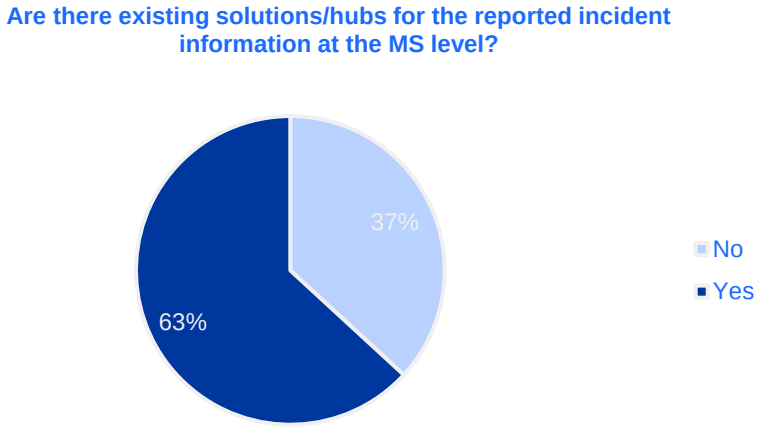


FIGURE 23 EXISTING SOLUTIONS FOR INCIDENT REPORTING

7. However, when we analyse the degree of centralisation of these solutions, it can be seen that only around 34% of the solutions implemented are centralised at member state level.

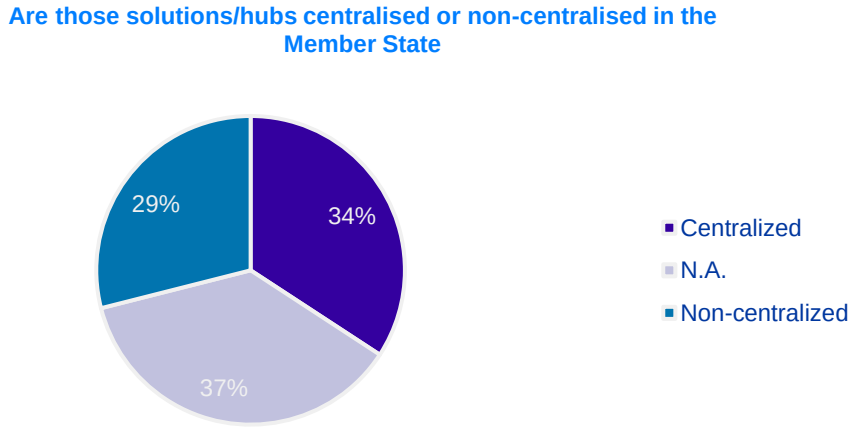


FIGURE 24 CENTRALISATION OF EXISTING SOLUTIONS

Processes and systems for financial sector incident reporting to competent authorities existing at Member States (or under development)

8. With regard to the option adopted to transmit this information from the financial institutions to the competent authorities, it can be observed that in very similar percentages, either email or specific portals are used where the information to be sent is uploaded. The result presented takes into account the method of submitting the initial notification.

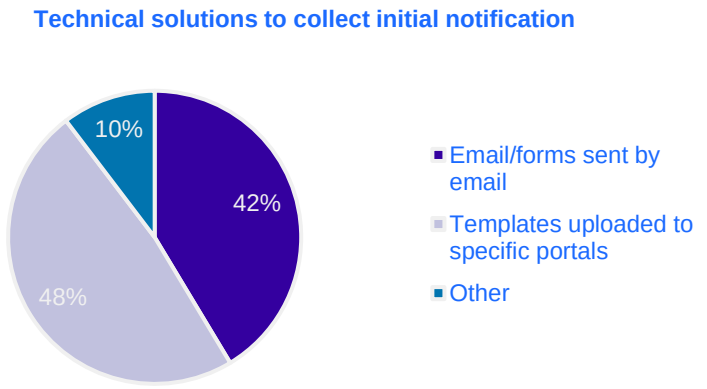


FIGURE 25 DATA EXCHANGE SOLUTIONS

9. From the point of view of the information to be transmitted, it is also important to know the degree of standardisation of the information. In this standardisation process, the first step can be defined as the definition of specific templates or models for reporting, the next step as the definition of a data glossary and finally the establishment of more detailed and sophisticated reporting taxonomies such as a data point model based on XBRL. Most of the CA already have specific templates (82% of the sample presented), 65% also have a data glossary (at least for some of the reporting phases), but only 11% have also defined a data point model.

10. As important as knowing the degree of standardisation is to know whether such standardisation occurs in a homogeneous manner in the Member State, or whether the different competent authorities present in a jurisdiction have established mechanisms that are not shared within that jurisdiction. Thus, based on the sample, 44% of the templates are not harmonised and 73% of the data glossaries are not harmonised at country level.

11. In general terms, it is therefore possible to describe a situation in the different jurisdictions with a certain degree of standardisation and homogenisation at member state, which decreases with the degree of complexity of such standardisation.

12. Given that in many CAs some form of dedicated incident reporting hub or system already exists and given that in some CAs such systems already have a certain degree of sophistication, it is important to know from the point of view of these authorities, whether their current systems would be sufficient to support the new incident reporting under DORA. Here it is important to introduce the limitations derived from the absence of information related to this process at the time of responding to the survey (March 2023) and to highlight that the respondents answered on a best effort basis on the basis of known information.

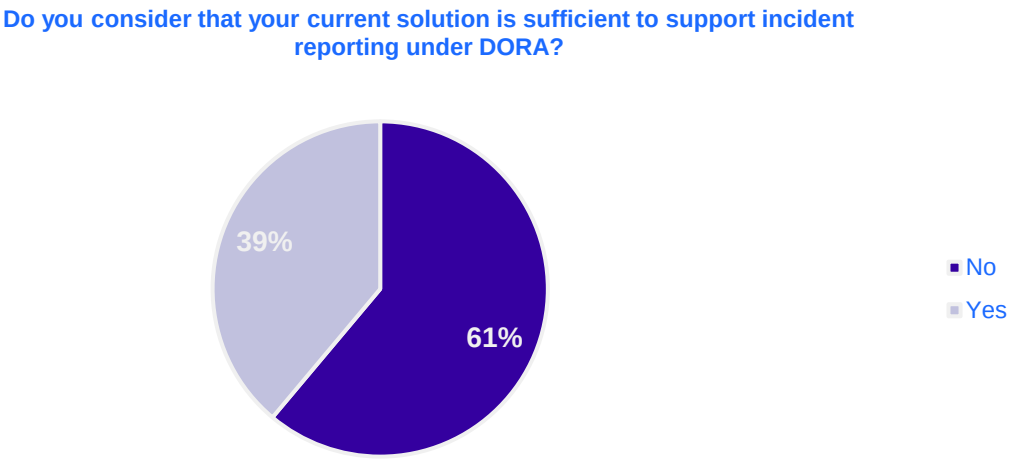


FIGURE 26 READINESS OF CURRENT SOLUTIONS

13. With all these caveats in place, respondents to the survey considered that their current solution (with or without changes to bring it into line with the new framework) was in 40% of cases ready to support incident reporting under DORA. It is important to note that in both cases, multiple CAs were already planning the necessary developments to make their systems ready to take on this new reporting.

Reporting volumes pertaining to the year 2022

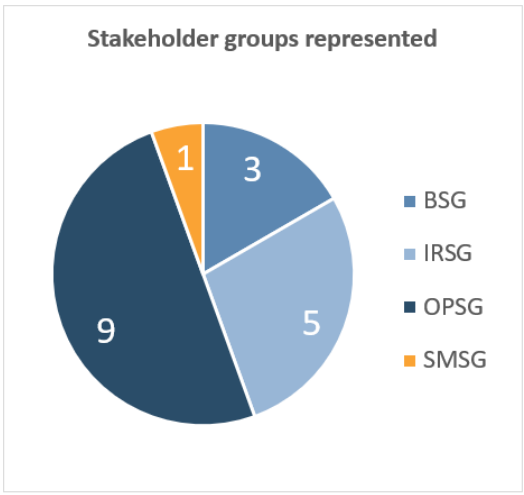
14. The stock taking exercise introduced quantitative questions related to the volume of incidents reported and the financial entities involved. Information relating to the year 2022 was requested. Here it is important to reintroduce the limitations associated with the information available, the number of CAs that have responded to this part of the survey, the possible duplications between authorities in the same member state and the different interpretations of the definition of an incident and its classification.

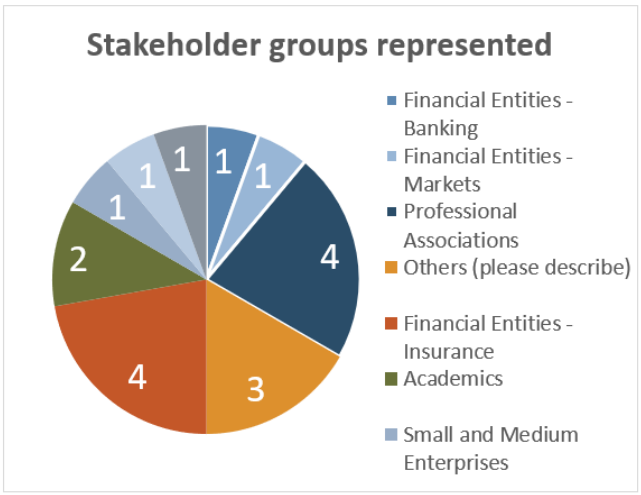
15. For all these reasons it is difficult to introduce an exact number of entities that have reported incidents similar to those established under DORA and the number of associated incidents for the reference period.

16. Thus, with regard to the number of entities subject to reporting, an initial estimate of more than 20 thousand entities can be assumed.

17. Regarding the volume of incidents, the results are equally difficult to extrapolate for the reasons mentioned above. The definition of incident, and of major incident under DORA were not entirely clear and establishing assimilations in the current reporting frameworks was difficult. In any case, taking into account related incidents reported to the various ESAs and the preliminary figures shared by member states, any tool implemented at the European level should be able to cope with incident reporting in the order of thousands per year.

Annex VI: Stakeholders Questionnaire

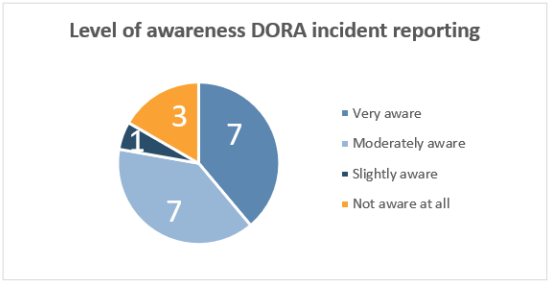




17 individual responses have been received + **1 aggregated response from the BSG**

1 of the respondents belongs to both BSG and SMSG

FIGURE 27 STAKEHOLDERS REPRESENTED



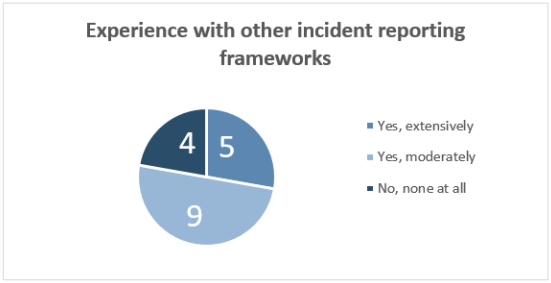


FIGURE 28 LEVEL OF AWARENESS AND USE

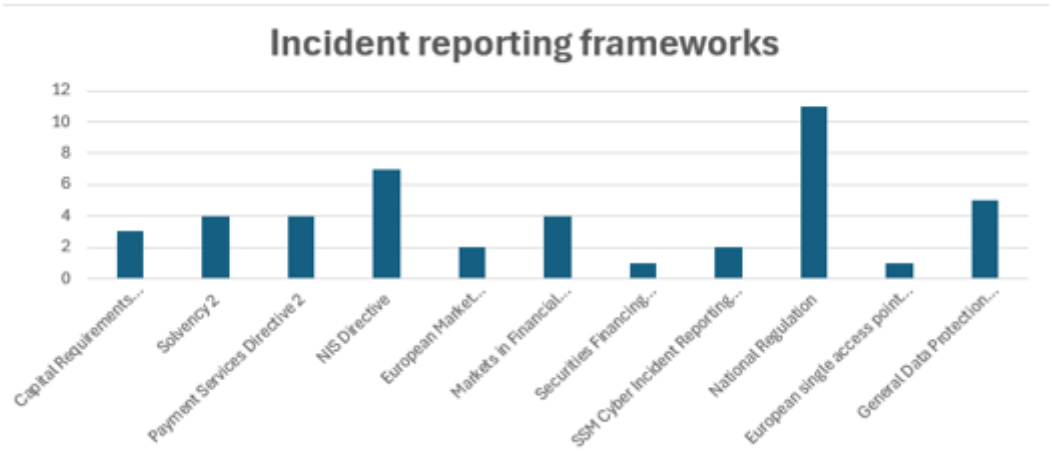
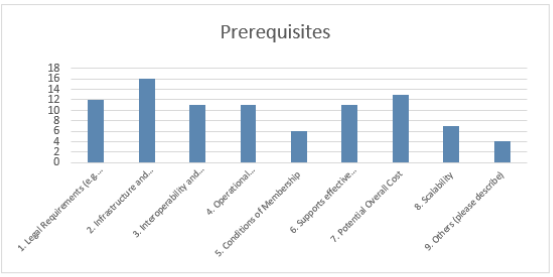
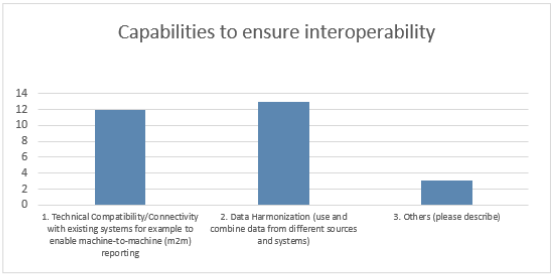


FIGURE 29IR REPORTING FRAMEWORKS UNDER WHICH RESPONDENTS CURRENTLY REPORT

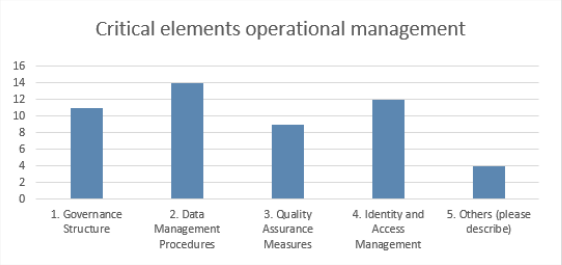


- Most respondents qualify legal requirements (e.g. DORA revision), infrastructure & technology requirements, interoperability and integration, operational management (governance, data management), effective response from CAs and potential overall costs as essential prerequisites for the EU hub

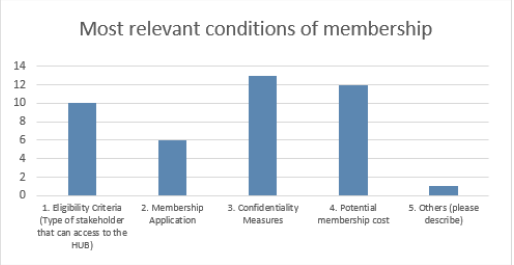


- Most respondents qualify technical compatibility/connectivity with existing systems (e.g. M2M reporting) as an essential capability to ensure interoperability.
- Consider a holistic approach, considering the wider regulatory landscape

FIGURE 30 ELEMENTS FOR THE ASSESSMENT

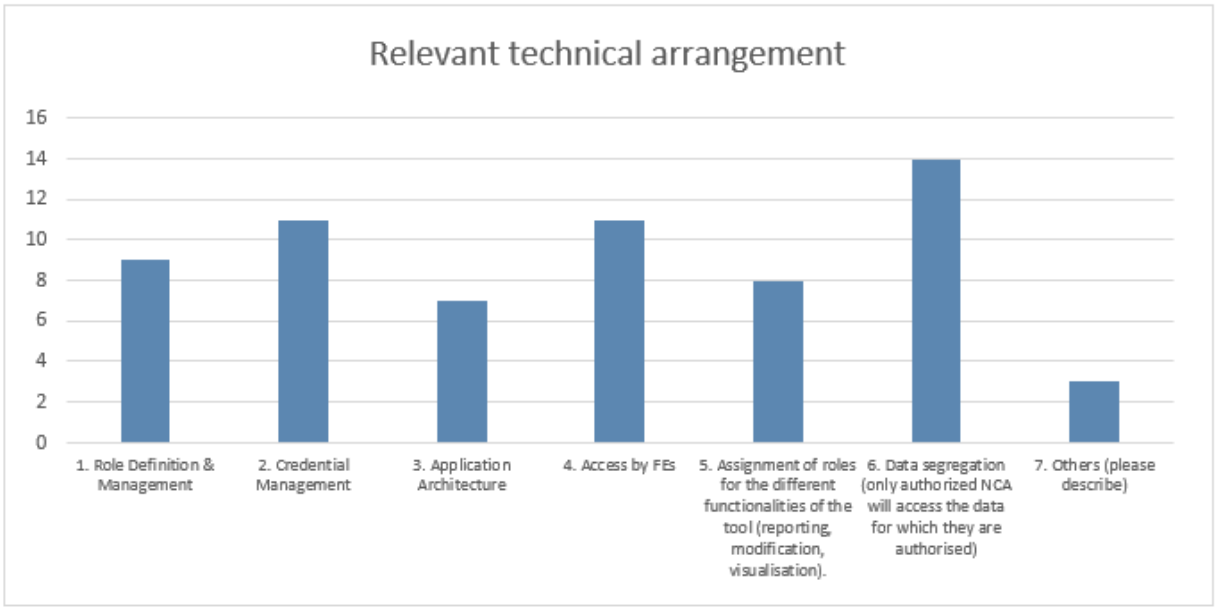


- Majority of the respondents qualifies all proposed elements as critical



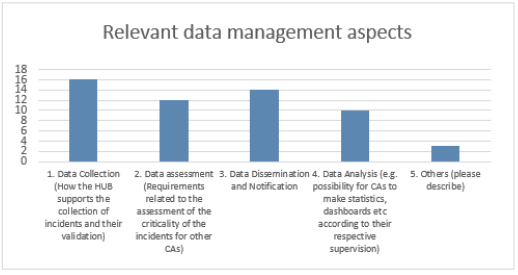
- All respondents consider confidentiality measures essential for membership. Most also selected "potential membership costs"

FIGURE 31 ELEMENTS FOR THE ASSESSMENT (II)

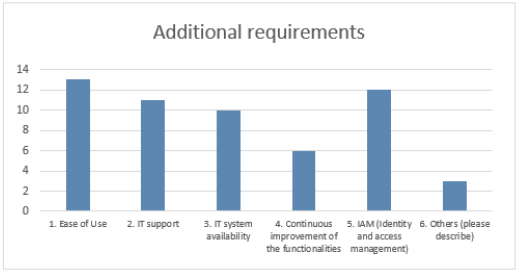


- Majority of respondents qualifies access by Fes, data segregation, assignment of roles for different functionalities, credential management, and role definition & management as relevant

FIGURE 32 ELEMENTS FOR THE ASSESSMENT (III)

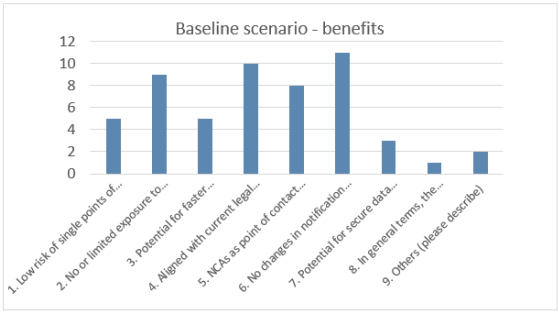


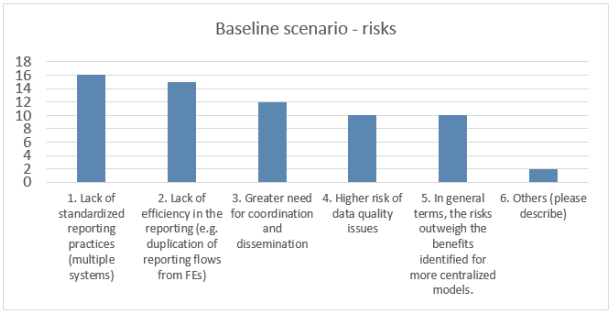
- Respondents seem to qualify all suggested options relevant, although some do not view data analysis possibilities for CAs as relevant
- Coordinated responses, aggregated analysis for FEs and the important of Regional country specific analysis are also mentioned



- Respondents seem to qualify ease of use, IAM, and IT support as the most relevant
- IT system availability, training and continuous improvement of functionalities are also mentioned

FIGURE 33 BUSINESS REQUIREMENTS

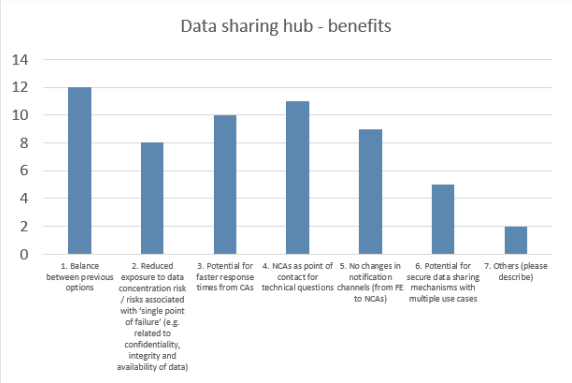


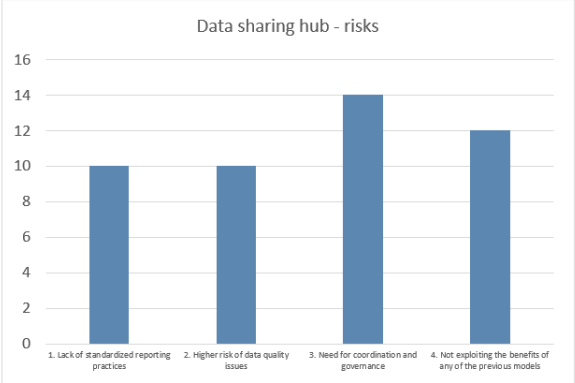


- Alignment with the current legal framework, no changes in notification channel and limited exposure to data concentration risks were identified as main benefits
- Other benefits include low risk of SPOF, potential for faster responses times, NCAs as main POC for technical issues, secure data sharing mechanisms as other benefits of the approach

- Responses identified lack of standardized reporting practices, lack of efficiency in the reporting process (duplication of flows), greater need for coordination and dissemination as the critical risks for the baseline scenario. Higher risk of data quality issue was also identified.

FIGURE 34 BENEFITS– RISKS - BASELINE

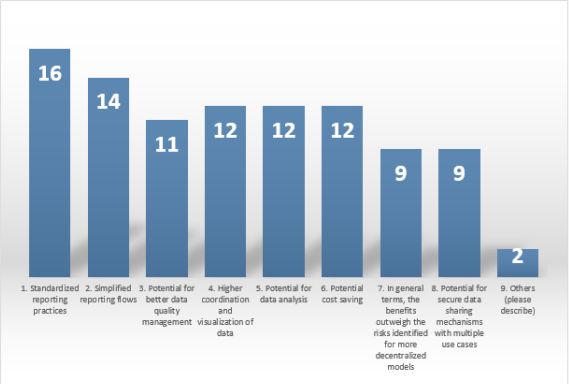


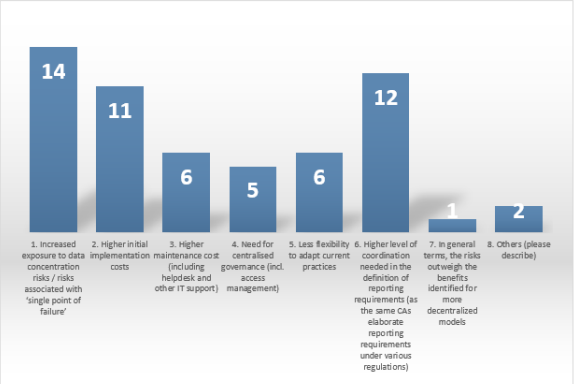


- Respondents see the data sharing hub as a solution of balance between the other two options. Benefits mentioned often include the NCAs as POC for technical questions, the potential for faster response times from CAs, and that no changes in the notification channels are required for this solution.
- Other benefits include reduced exposure to data concentration risk, and the potential for secure data sharing mechanisms.

- The main risk emphasized by respondents is the need for coordination and governance. Also, they see that this model will lack in exploring the benefits of any of the previous models.
- Also, the lack of standardized reporting practices, and higher risk of data quality issues are raised in the questionnaire.

FIGURE 35 BENEFITS – RISKS – DATA SHARING

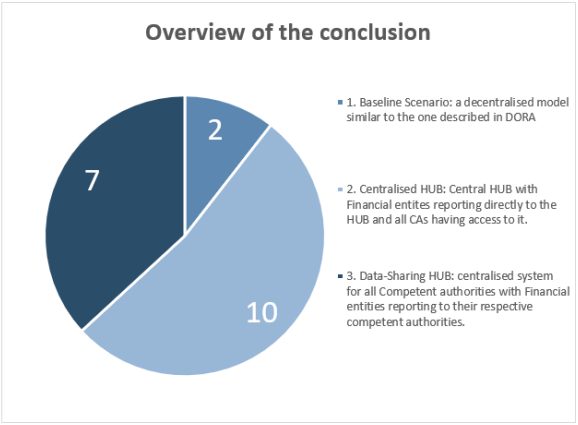




- Respondents value in this scenario the standardized reporting practices, the simplified reporting flows. Also, higher coordination and visualisation of data is mentioned, the potential for data and see the potential cost saving benefits.
- Other benefits include better data quality management, and secure data sharing mechanisms.

- Respondents emphasize the risks of increased exposure to data concentration, and higher level of coordination needed in defining the reporting requirements. The initial implementation costs is also mentioned often.
- Other risks emphasized by responses include the maintenance costs, the governance arrangements costs, as well as the lack of flexibility to implement the practices used today.

FIGURE 36 BENEFITS – RISKS - CENTRALISED



Baseline scenario

- Least favourite option, only supported by two members of the OPSG

Centralized HUB

- Centralized HUB option is supported by 9 different members, while a respondent opt for either the Centralized HUB or the Data-sharing HUB
- Members who support this option are part of 3 different stakeholder groups, OPSG, IRSG, and BSG

Data-Sharing HUB

- This is seen as the ideal option by 6 different members, which are part of the 3 different stakeholder groups, SMSG, BSG, and OPSG.

FIGURE 37 CONCLUSIONS

Annex VII: Stakeholders Questionnaire: BSG joint response.

Executive summary

The BSG is supportive the proposed centralisation of major ICT-related incident reporting (Art. 21 DORA) and is looking forward to engaging with the European Supervisory Authorities (ESAs) in further discussions based on the forthcoming feasibility report, which the BSG is looking forward to with great interest.

At this point in time, and without wishing to pre-empt the findings of the feasibility report, the BSG is of the view that a Centralised Hub, which collects incident reports directly from financial entities in all EU member states, would likely yield greater benefits than the Data Sharing model, both in terms of facilitating the timely and comprehensive collection and distribution of incident-related information and in terms of cost-efficiency. In order to further refine this initial assessment, the feasibility report should provide sufficient detail on the proposed technical and procedural arrangements for each of the two scenarios, as well as a preliminary consideration of the expected cost of implementation.

The BSG currently does not have a distinct preference as to which authority should be responsible for hosting the single EU Hub. The BSG recognises, however, that the Joint Committee of the ESAs (JC) has established a dedicated Sub-Committee on Digital Operational Resilience, which is tasked specifically with the implementation of DORA and would therefore appear well placed to host the single EU Hub.

The BSG is mindful that the establishment of a single EU Hub could potentially create a ‘single point of failure’ but is confident that this risk could be contained if the authority hosting the single EU Hub is provided with appropriate technical infrastructure and expert personnel. Adequate security arrangements, risk management policies, and recovery and back-up arrangements would have to be put in place. The feasibility report should therefore comprise an assessment of the relevant requirements for each of the two options.

The BSG would expect the feasibility report to include, in particular, an initial consideration of necessary and appropriate updates to procedural aspects of major ICT incident reporting, e.g. templates and data formats, and to highlight any potential for further streamlining and harmonisation. The feasibility report should examine, in some depth, how to achieve interoperability of the new single EU Hub with existing systems and, going forward, explore pathways for the integration of other ICT incident reporting schemes, e.g. under Directive (EU) 2022/2555 (NIS 2) and Regulation (EU) 2016/679 (GDPR), into the Hub.

In this context, the BSG would like to emphasise that the feasibility report should incorporate a long-term view and envisage a scenario where the single EU Hub could serve as a future focal point of convergence for currently separate incident reporting schemes, especially DORA and NIS 2. This long-term perspective could provide a useful frame of reference, especially for the design of technological and processual arrangements for the single EU Hub. The BSG is aware that the creation of a legal basis for the single EU Hub, let alone the potential integration of other operational and ICT incident reporting frameworks across sectors, would require further intervention by the co-legislators to amend the relevant legislative acts.

The BSG believes that the proposed EU Hub would be an important first step towards a long-term plan for convergence and would be in keeping with the EU's wider strategic priorities of harnessing the benefits of digitalisation, improving the efficiency of supervisory processes, and promoting the creation of common European 'data spaces.

General observations

As set out in the BSG's own initiative paper (BSG/2023/03, 05 May 2023), the BSG endorses the proposed centralisation of major ICT-related incident reporting (Art. 21 DORA). The establishment of a single EU Hub would facilitate information-sharing among authorities, prevent redundancies in reporting and improve effectiveness of technical and regulatory responses to cyber-risks.

The BSG is of the view that a single EU Hub could, in due course, serve as a common platform for financial entities to file and share, and for competent authorities to access incident-related supervisory information. The Centralised Hub model appears best suited to take full advantage of the potential benefits of centralisation, namely further standardisation of reporting formats and practices, faster and more reliable dissemination of critical information, and operational efficiency gains for both financial entities and public authorities.

Some members of the BSG emphasise that it would be appropriate and necessary to consider well in advance how each of the proposed scenarios, the Centralised and the Data Sharing Solution, would require updates and modifications to the templates and processes as set out – for the Baseline scenario – in the JC's draft RTS[29] and ITS for reporting major incidents (JC/2024/33). Centralisation should yield demonstrable benefits, for example by simplifying and standardising reporting templates, data structures and formats, which could in turn shorten response times.

The BSG is mindful that the concentration of sensitive information, such as incident reports, in a single Centralised Hub may pose new risks, e.g. from technical failure or cyberattack. These risks could be addressed, however, by providing the single EU Hub with the appropriate technical infrastructure and security measures, robust governance arrangements and strict operational policies.

The BSG does not have a clear preference as to which authority should be responsible for hosting the single EU Hub as long as it is provided with adequate resources, especially in terms of technical infrastructure and expert personnel, to deliver its tasks with the requisite high levels of security and operational efficiency. The BSG recognises that the Joint Committee of the ESAs (JC) has established a dedicated Sub-Committee on Digital Operational Resilience, which is tasked specifically with the implementation of DORA and would appear well placed to host the single EU Hub.

[29] It is noted that on 23 October 2024 the European Commission adopted the RTS supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and time limits for the initial notification of, and intermediate and final report on, major ICT-related incidents, and the content of the voluntary notification for significant cyber threats.

The BSG also notes that financial entities are subject to additional obligations besides DORA, notably under Directives (EU) 2022/2555 (NIS 2) and 2022/2557 (CER), which are not sector specific. The creation of a single EU Hub under DORA should be undertaken with a view to its potential future expansion, which could, in due course incorporate centralised incident-reporting for other frameworks, such as NIS 2. The BSG is of the view that it is important for the single EU Hub to promote convergence between different legal acts which require ICT incident reporting, so as to further harmonise and streamline the legal framework, lighten the regulatory burden and reduce the fragmentation of reporting lines. In the long run, the aim of establishing the single EU Hub should be cross-sectoral convergence and harmonisation of the regulatory frameworks for ICT and security risk management towards a single reporting obligation.

The BSG is conscious that the proposed centralisation of ICT incident reporting, regardless under which scenario, will require a revision of DORA and the provision of funds and staff resources for the technical implementation. The BSG believes that the single EU Hub could make an important contribution towards maintaining a high level of cybersecurity across the EU financial sector and should therefore be treated as a matter of priority.

Some members of the BSG suggest that the feasibility report should comprise an outline for developing a Risk Management Policy for the single EU Hub, which should set out policies to guarantee data security and prevent unexpected data leakage situations. This Policy should inform the operating management of the single EU Hub where it is planned to concentrate sensitive information.

The BSG points out that effective enforcement will be essential for the usefulness and credibility of the single EU Hub. Harmonised procedures would have to be put into place to identify violations of incident reporting requirements and impose sanctions. This aspect should also be explored in the feasibility report.

Detailed comments

Q.2. Incident reporting awareness and use

For the most part, financial entities represented on the BSG are well aware of the incident reporting process under DORA. Many of them already have experience with other incident reporting frameworks, including Directives (EU) 2015/2366 (PSD 2), 2016/1148 (NIS), 2014/65 (MiFID II), and relevant national regulations. Some of the larger entities, in particular, already operate centralised incident reporting systems across multiple jurisdictions, including harmonised processes for internal and external notifications.

Q.3. Elements for assessment in the feasibility report

Most financial entities represented on the BSG believe that a thorough analysis of technical requirements (standardisation of reporting formats and data structures, infrastructure and technology, interoperability and integration) and operational prerequisites (operational management) is essential for the successful creation of a single EU Hub. These aspects will also have a bearing on the overall cost of implementation, which is another significant concern. The analysis should also further expand on the conditions for membership.

Among the technical requirements, BSG members emphasise the need to ensure a high level of data security, both in transfer and at rest, e.g. through encryption, access control, data integrity checks and the use of secure transmission protocols, as well as the provision of adequate recovery and backup arrangements for the single EU Hub. BSG members also note that the technical specifications should provide for a high degree of standardisation and interoperability and, to the extent possible, facilitate a high degree of automation, e.g. machine-to-machine (M2M) communication.

The most critical elements of the operational management of the single EU Hub, from the perspective of BSG members, would be the governance structure of the Hub, data management procedures, and identity and access management. A detailed risk management policy should be developed for the single EU Hub, substantively in line with the JC's RTS on ICT risk management[30] and other relevant guidance by the ESAs.

With respect to the conditions of membership, members of the BSG generally agree that the criteria for eligibility (to access the single EU Hub) and measures to preserve confidentiality are the most critical aspects, which deserve particular consideration. The feasibility report should therefore outline potential criteria for membership of a single EU Hub, as well as conditions for granting and monitoring access rights.

Some members of the BSG also note that an analysis of the legal requirements, including potential revisions of DORA that may become necessary for the implementation of the single EU Hub, should be covered in the feasibility report. Other members of the BSG suggest that the feasibility report should provide further clarification on the purpose of the single EU Hub, the use of the reported data by public authorities, and the interaction between the authorities and financial entities regarding that data.

The BSG recommends that the feasibility study should take into consideration the integration, in due course, of related reporting obligations under other legal frameworks, such as Directives (EU) 2015/2366 ('major incident reporting', Art. 96 PSD 2), and 2022/2555 ('significant incident notification' Art. 23 NIS 2), and Regulation (EU) 2016/679 ('personal data breach', Art. 33 GDPR) and should assess whether overlapping or duplicate reporting could be removed.

There is no clear preference among BSG members as to which authority should be given responsibility for the single EU Hub. Some members of the BSG are of the view that this role should be assigned to the ESAs as they already have the primary responsibility for the application of DORA and are currently building relevant capabilities. This would be aligned with the wider supervisory convergence mandate of the ESAs of and would enhance cooperation between the NCAs and ESAs, as well as the between the NCAs themselves.

Other members suggest that ENISA would be best suited to host the single EU Hub given its technical expertise and cross-sectoral mandate for cybersecurity Members are mindful, however, that the nature and scope of incident reporting under DORA and NIS 2, the

[30] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework (OJ L, 2024/1774, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1774/oj).

framework currently administered by ENISA, differs and further alignment, as well as additional governance arrangements between the ESAs and ENISA may need to be established.

The BSG agrees, in any event, that the authority hosting the Hub must be provided with the necessary resources, including technical infrastructure and expert personnel, to ensure the requisite high levels of security and operational efficiency. Adequate cooperation arrangements would need to be put in place to ensure effective and fast coordination of responses between the authority hosting the Hub and the NCAs, and responsibilities, e.g. for the analysis and evaluation of incident data, would have to be clearly allocated.

Q.4. Relevant business requirements for the single EU Hub (two scenarios)

BSG members agree that the single most relevant function of the proposed single EU Hub would be data collection, i.e. data management should concentrate on the collection of incidents and their validation. They are of the view that the principal benefit of the EU Hub would be to aggregate information, accelerate the process of incident reporting and analysis, and eliminate redundancies. Altogether, the single EU Hub should enable supervisory authorities to better assess major ICT related vulnerabilities comprehensively and in a timely manner.

The BSG believes that there could also be considerable benefit in enabling competent authorities to prepare supervisory analyses and statistics on the basis of aggregated incident data. Some members also expect that competent authorities could provide financial entities and the public with periodic alerts, analysis and/or trend reports. Such reports could be of considerable value to market participants as they would enable cross sectoral learning and sharing of intelligence on threats and vulnerabilities, which would, in turn, contribute towards the overall objective of strengthening digital operational resilience throughout the financial sector. Moreover, it would demonstrate the usefulness of centralised data collection and increase the acceptance of centralised incident reporting among the industry.

Q.5. Potential benefits and risks of a future EU Hub

Baseline scenario – Benefits and Risks

The BSG agrees that the Baseline scenario, due to its decentralised structure, does not rely on any critical nodes that could become ‘single points of failure’, unlike the more centralised alternative scenarios. It is therefore less exposed to data concentration / risks associated with “single point of failure” – due to the inherent redundancy incident data would still be available both at national MS level and EU level. Some BSG members are of the view that the direct contact with national competent authorities under the Baseline scenario could also shorten response times and allow financial entities to interact bilaterally with the competent authority, e.g. to clarify technical questions. There would also be no incremental investment needed for financial entities to establish new reporting channels.

The BSG is of the view, however, that the drawbacks of the Baseline scenario outweigh the potential benefits of the more centralised models. In particular, the BSG observes that the Baseline scenario contains significant redundancies on several levels: reporting obligations are duplicated across jurisdictions, reporting formats and practices are not standardised, the

flow of information between competent authorities and other recipients complicated, and data quality likely to be inconsistent.

Centralised Hub – Benefits and Risks

There is general agreement among BSG members that a Centralised Hub could provide significant benefits, in particular regarding the standardisation of reporting practices, the simplification of reporting flows, better quality management of data, better data analysis, and scalability (infrastructure could be used for other similar reporting frameworks). In addition, a Centralised Hub would not rely on intermediation by national competent authorities and could provide more timely and comprehensive visibility on the ICT related vulnerabilities and threats on the market. Moreover, a Centralised Hub could generate significant cost savings over time and improve the overall efficiency of the incident reporting process. In sum, taking into account the initial investment and continuous operating costs, a Centralised Hub would likely be the most cost-efficient option. A number of financial entities represented on the BSG are of the view that these benefits are seen to outweigh the potential risks. They point out that it is vastly more efficient to enter incident data once only, in a standardised format, instead of filing multiple reports with competent authorities. A Centralised Hub may also be more aligned with the EU data strategy in general, and the creation of a supervisory 'data space' for the EU financial sector, in particular, and draw useful inspiration from the 'once-only' principle as referenced in Regulation (EU) 2018/1724. Finally, it would also appear consistent with the objectives of the Capital Markets Union (CMU).

BSG members who favour a Centralised Hub scenario are conscious of the potential risks inherent in this approach, especially security risks associated with a 'single point of failure'. To address this concern a Centralised Hub would have to have a high level of security built into the system from the very beginning. Other concerns include the higher initial implementation cost and the need for appropriate (centralised) governance arrangements, including access management.

Data-Sharing Hub – Benefits and Risks

In the view of BSG members, the main benefit of the Data-Sharing Hub would be that it could potentially shorten response times from competent authorities. BSG members also believe that it could be simpler to implement as it would not require changes to the already established notification channels between financial entities and national competent authorities.

Some financial entities represented on the BSG consider the Data Sharing Solution as a viable compromise between the Baseline scenario and the more efficient, but potentially more expensive Centralised Hub scenario. They believe that the Data Sharing Solution could achieve a certain reduction of the reporting burden for financial entities, primarily vis à vis other public entities, without the need for substantial new investment. They recognise, however, that it would not significantly increase the efficiency of incident reporting overall.

Other members of the BSG believe that the Data Sharing Solution offers no improvement whatsoever over the Baseline scenario as it combines the weaknesses of the Baseline (lack of standardisation, data quality issues) with the drawbacks of the Centralised Hub (concentration risk, 'single point of failure').

Q.6. Conclusions

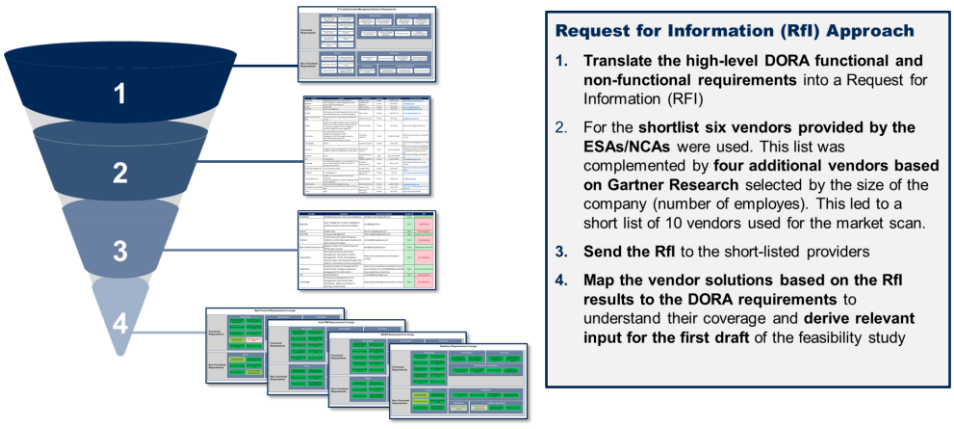
The BSG agrees, in principle, that further centralisation of major ICT incident reporting would be desirable and preferable to the current ('Baseline') scenario. On balance, there appears to be a preference among financial entities represented on the BSG for the Centralised Hub scenario where reports are sent directly to the Hub and made accessible to all competent authorities. BSG members who favour the Centralised Hub scenario argue that a single point of entry for all incident-related data would save time and provide more consistent data quality. They note also that competent authorities could access all relevant incident data in one place, and in a standardised format.

Some members of the BSG prefer the Data-Sharing Hub scenario where financial entities continue to report to their respective competent authorities and reports are subsequently forwarded to a central database. BSG members who prefer the Data Sharing Solution point out that this approach would produce some, albeit more limited, efficiency gains but reduce the investment required to transition from the Baseline scenario. This would allow more time for financial entities and national competent authorities, to some extent, to amortise their investment in 'Baseline-compatible' systems.

Annex VIII: Request for information (RfI)

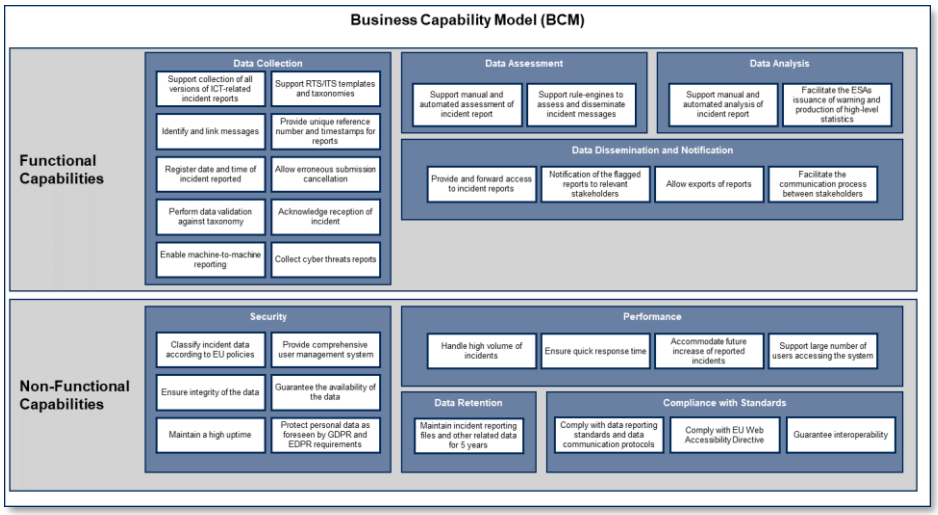
A request for information (RfI) was sent to selected software providers following the approach described below:

- A Business Capability Map (BCM) tailored to the specific DORA project scope was created and high-level functional and non-functional requirements were collected (see section 5 for details). This was the foundation for the market scan.
- A first list of vendors/solution providers was created on Gartner Research as well as a list provided by the ESAs/NCAs
- For the shortlist six vendors provided by the ESAs/NCAs were used. This list was complemented by four additional vendors based on Gartner Research selected by the size of the company (number of employees). This led to a short list of 10 relevant vendors invited to the Request for Information (RfI).
- The high-level DORA functional and non-functional requirements were translated into a Request for Information (RfI).
- The RfI was sent to the 10 short-listed vendors.
- The vendor solutions of the responding vendors were mapped based on the RfI results against the DORA functional and non-functional requirements to understand their degree of coverage.
- The results were summarised on an aggregated as well as on an individual level for each vendor solution.



–

The following Business Capability Model (BCM) was used covering functional and non-functional capabilities:



Business Capability	Specific Requirements
Data Collection	The HUB shall support the collection of all versions of ICT-related incident reports from the reporting entity in a timely manner (as defined in DORA and RTS/ITS on Incident reporting), and at any rate in a very short timeframe (to be agreed with CAs).
	Each reporting entity shall be able to submit incident reports to the HUB using the templates, taxonomy and respective data point model developed based on the RTS/ITS on Incidents reporting.
	The HUB shall identify and link the different messages related to every reported incident as per Art 19 (4) of DORA.
	The HUB shall provide unique reference number and timestamp for all submitted reports and link the reference numbers of subsequent reports (initial notification, intermediate and final report) in line with "The EU Hub shall identify and link the different messages related to every reported incident as per Art 19 (4) of DORA. "
	The Hub shall register the date and the time when the reporting agent reported the incident and tracking all actions taken on reports.
	The HUB shall allow unintentional or erroneous submissions to be cancelled, modified, or reversed by the submitting CAs or system administrators
	The HUB shall perform data validation checks against the taxonomy, technical specifications set by the ESAs when implementing technical package for RTS/ITS on Incident reporting or a predefined set of validations created ad hoc.

Business Capability	Specific Requirements
	The HUB shall acknowledge the reception of the incident to the reporting entity, following the reception of a report/notification file, in very short timeframe. The acknowledgement shall include the successful collection of the report or the need to revise/resubmit the report, where the validation and completeness checks have not been passed, (indicating the fields that didn't pass the validation). In relation to validation, this should happen immediately and in parallel to the process of uploading the information into the system (i.e. at the moment this information is available in the system, to avoid iteration loops as far as possible).
	The Hub shall support the ESAs in collecting significant cyber threats reports from the reporting entity. Although the notification of cyber threats is voluntary, it is considered that any HUB should be able to accommodate the reporting of these threats.
	The HUB shall enable machine to machine reporting (e.g. through APIs) from and to the systems of the reporting entity, as well as the possibility of manual reporting (as some reporting entities will have less sophisticated IT systems). At the same time the IR IT system shall support bulk file upload.
Data Assessment	The HUB shall support the manual and automated assessment of incident reports in order to identify whether the major ICT-related incident is relevant to stakeholders other than the reporting entity based on specific data fields from the incident report.
	The HUB shall support rule-engines that can be enabled and configured through pre-defined structured data fields to assess and disseminate incident messages/information to relevant users in a timely manner (very short timeframe to be agreed with CAs).
Data Dissemination and Notification	The HUB shall allow forwarding or providing access to incident reports to relevant stakeholders following the Data assessment phase.
	The HUB shall support the notification of the flagged reports to relevant stakeholders and shall provide the stakeholders with access to them, including all intermediate reports.
	The HUB shall allow the export of reports.
	The EU Hub shall facilitate the communication process between the different stakeholders through specific communication channels.
Data Analysis	The HUB shall support manual and automated analysis of the incident data in a way that allows using all reported data for the purposes of the preparation of the annual report or to be used in sectorial risk assessment by the ESAs, in accordance with Article 22.2 paragraph 1 of DORA.
	The HUB shall support the analysis of the incident data in a way that allows using all reported data for the purposes of the ESAs issuing of warnings (the IT system itself does not have to generate the warnings but support the process), and the production of high-level statistics, in accordance with Article 22.2 paragraph 2 of DORA (e.g. through data visualisation).