Study supporting the impact assessment on the revision of EU legislation on food contact materials

Draft Final Report

Written by EY Consulting
For the European Health and Digital Executive Agency (HaDEA)
February 2024

HaDEA

EUROPEAN COMMISSION

European Health and Digital Executive Agency (HaDEA)
Unit A2: EU4Health/SMP Food

Contact: Konstantinos SOFIANIDIS
E-mail: konstantinos.sofianidis@ec.europa.eu

European Commission
B-1049 Brussel

PROJECT TEAM

LEGAL NOTICE

PDF ISBN: doi: EW:

Manuscript completed in … month / year

Luxembourg: Publications Office of the European Union, 202x

How to cite this report: […]

Contents

1 Abstract 5
2 Introduction 6
2.1 Context 6
2.2 The Impact Assessment on the revision of the FCM legislation 8
3 Methodological approach 9
3.1 Development of Policy Options to support an IT infrastructure for information exchange and verification of compliance 10
3.2 Assessment of the most significant impacts of Policy Options to support an IT infrastructure for information exchange and verification of compliance 11
3.3 Identification of implementation and development pathways for Policy Options to support an IT infrastructure for information exchange and verification of compliance 11
3.4 Methodological tools 11
4 Policy Options 13
4.1 Policy Options to support an IT infrastructure for information exchange and verification of compliance 13
4.1.1 Policy Options 1: Centralized IT system with an EU body principally responsible for management and decision-making 14
4.1.2 Policy Options 2: Decentralized IT system where Member States are principally responsible for local management and decision-making 17
4.1.3 Policy Option 3: Decentralized IT system where businesses are principally responsible for management and decision making 21
4.2 Impacts of Policy Options 23
4.2.1 Assessment of effectiveness 23
4.2.2 Assessment of impacts 25
4.2.3 Costs Assessment 31
4.3 Implementation pathways 32
4.3.1 Pre-conditions for implementing an FCM related IT system 32
4.3.2 Implementation phases for the FCM IT system 34
4.3.3 Technical steps of the Implementation Pathways 39
4.3.4 Implementation challenges: 44
5 Conclusions 44

1 Abstract

This study compares three Policy Options to support the establishment of an IT infrastructure for information exchange and verification of compliance in Food Contact Materials (FCM). Policy Option 1 proposes a centralized EU IT system, Policy Option 2 (2a and 2b) proposes decentralized national IT systems, Policy Option 3 suggests decentralized industry-managed IT systems. The assessment of such options shows that Policy Option 1 demonstrates strengths in cost efficiency and data management, while Options 2 and 3 show complexities and potential inequalities. Decision-makers can use this analysis to select an efficient FCM IT system. The study contributes insights for establishing an effective, compliant IT system for FCMs.

2 Introduction

2.1 Context

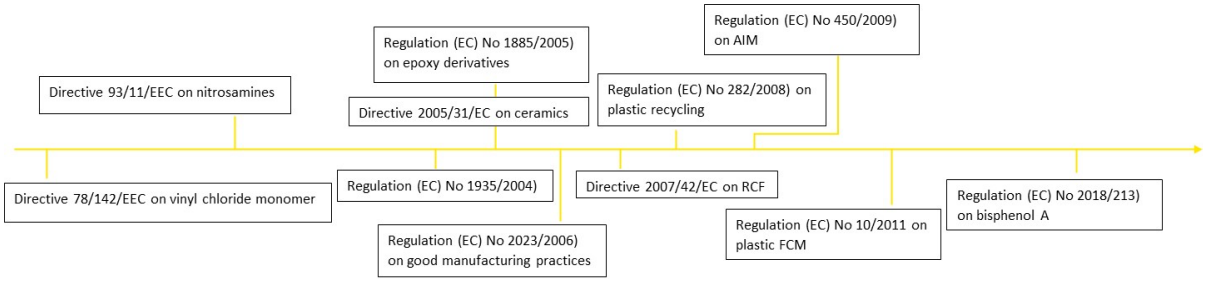
Importance of ensuring FCM safety

The term Food Contact Material (FCM) refers to any material or article that "is either intended to be brought into contact with food, is already in contact with food and was intended for that purpose or can reasonably be expected to be brought into contact with food or to transfer its constituents to food under normal or foreseeable conditions of use"[1]. This may occur during the food's production, processing, storage, preparation and serving before its final consumption. FCMs are made from a variety of materials, including those such as plastics, paper, rubber and other natural and plant-based materials and they directly contribute to the safe production, processing, transport, sale, and final consumption of food on the EU market. FCMs are not inert and final articles contain constituent substances that may transfer into food and result in human contact and/or consumption of those materials. Since the transfer of the constituents of FCMs may affect the chemical safety of the food and affect human health, it is vital to ensure the safety of Food Contact Materials.

Evolution of EU FCM legislation

The European Union began legislating on FCMs in 1976 and has since pursued the general objectives of: i) providing the basis for securing a high level of protection of human health and the interests of consumers; and ii) ensuring the functioning of the internal market. The original Council Directive 76/893/EEC on FCM[2] has since been revised twice, resulting in the final main EU legislation on FCM, Regulation (EC) No 1935/2004[3], hereafter referred to as the FCM Regulation. This sets out the rules on the authorization of substances, labelling, compliance documentation, and traceability as well as provisions on inspections and controls of FCMs along their production and supply chain. To ensure a high level of food safety, all food contact materials when placed on the European market must comply with this Regulation and be manufactured in accordance with the Commission Regulation (EC) No 2023/2006[4]. These two Regulations form the basis of EU FCM legislation, on top of which further material-specific EU legislation has been introduced, such as for ceramics (Directive 84/500/EEC)[5], plastics (Regulation (EC) No 10/2011)[6], and active and intelligent materials (Regulation (EC) No 450/2009)[7]. Where EU-specific legislation does not exist, Member States may adopt their own national provisions on FCMs (Article 6 of the FCM Regulation). Furthermore, the current Regulation does not contain any requirements concerning hygiene, environmental concerns, or waste management.

Figure 1. EU FCM legislation timeline



Source: EY illustration

Regulation (EC) No 1935/2004 on Food Contact Materials

The FCM Regulation provides a detailed framework that governs the operations of FCM producers and businesses handling these materials. Article 1 establishes the scope, outlining the types of materials covered by the regulation. Article 2 defines key terms used throughout the regulation, ensuring clarity and consistency. Article 3 of the FCM Regulation lays down general requirements for the manufacturing of FCMs. It mandates that under normal or

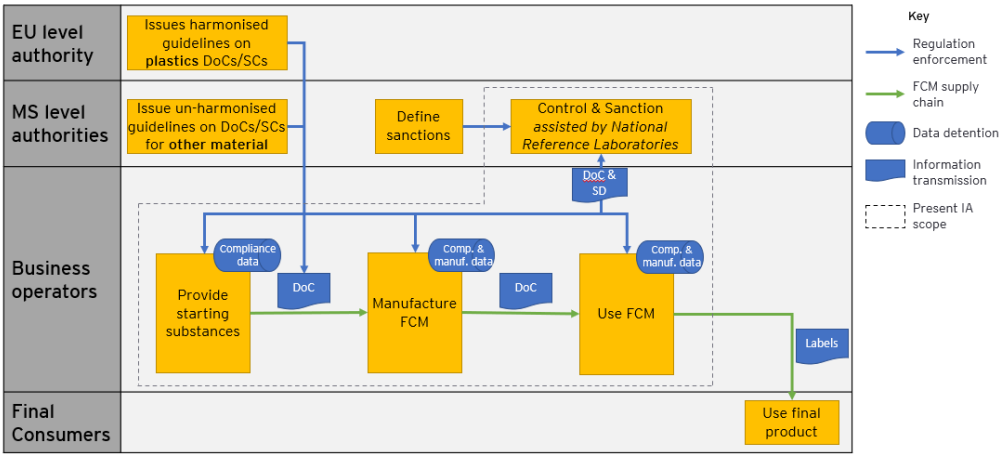
[1] Article 1 of Regulation (EC) No 1935/2004 of the European Parliament and of the Council of 27 October 2004 on materials and articles intended to come into contact with food
[2] Council Directive 76/893/EEC of 23 November 1976 on the approximation of laws of the Member States relating to materials and articles intended to come into contact with foodstuffs
[3] Regulation (EC) No 1935/2004 of the European Parliament and of the Council of 27 October 2014 on materials and articles intended to come into contact with food and repealing Directives 89/590/EEC and 89/109/EEC
[4] Commission Regulation (EC) No 2023/2006 of 22 December 2006 on good manufacturing practice for materials and articles intended to come into contact with food
[5] Council Directive 84/500/EEC of 15 October 1984 on the approximation of the laws of the Member States relating to ceramic articles intended to come into contact with foodstuffs
[6] Commission Regulation (EU) No 10/2011 of 14 January 2011 on plastic materials and articles intended to come into contact with food
[7] Commission Regulation (EC) No 450/2009 of 29 May 2009 on active and intelligent materials and articles intended to come into contact with food

foreseeable conditions of use, these materials should not transfer their constituents to food in amounts that could: a) pose a risk to human health; b) lead to unacceptable changes in food composition; or c) cause deterioration in the organoleptic properties of the food. A crucial aspect of compliance with the FCM Regulation is the requirement for a Declaration of Compliance (DoC) for all FCMs subject to EU-specific measures. This DoC serves as a formal statement indicating that the FCMs meet the applicable regulations. Additionally, businesses must provide Supporting Documentation (SD) to demonstrate compliance. The SD includes detailed information such as the identity of the business operator, materials and substances used, limitations on material use (e.g., temperature thresholds), and test results or other evidence of safety.

The issue of information exchange in the FCM supply chain

Effective information exchange is vital for ensuring the safety and compliance of FCMs throughout the supply chain. When seeking authorization for new substances, businesses must submit a technical dossier to the European Food Safety Authority (EFSA) for review. This dossier contains detailed information specified in EFSA guidelines for safety assessments. Throughout the supply chain, the FCM Regulation mandates that businesses produce DoCs, which may be passed along to downstream businesses. These declarations help ensure that all entities in the supply chain are aware of the safety status of the materials and articles they handle. However, the completeness and consistency of DoCs can vary, leading to potential gaps in information transmission, especially in terms of compliance tests performed by the business operator. This additional data, detained by each business operator performing compliance tests, is part of supporting documentation for which it is not certain that the business operators transmit it throughout the supply chain (see problem driver three, further elaborated below). The quality and quantity of information provided in the declarations of compliance and supporting documentation can be variable and depend on the Member State of the business operator and on the type of material (problem driver two, further elaborated below)[8].

Figure 2. Roles and responsibilities of actors of the FCM supply chain regarding the transmission of information



Source: Joint Research Centre[9], Union Guidelines on Regulation (EU) No 10/2011[10]

The evaluation of the FCM legislation

An evaluation of the EU FCM legislation[11] has been carried out and provides the basis for its revision, which was announced in the Farm to Fork Strategy[12] in May 2020. This includes commitments to improve food safety and public health, support the use of innovative and sustainable packaging solutions using re-usable and recyclable materials, and contribute to food waste reduction. The recent evaluation constitutes the first time that EU FCM legislation has been formally evaluated.

The evaluation aimed to address key objectives, including: (i) Ensuring FCMs are manufactured to high-quality standards, including the application of Good Manufacturing Practices (GMP), (ii) Addressing consumer needs for information on correct and safe use through labeling requirements, such as the wine glass and fork symbol, and prohibiting misleading labeling, (iii) Enhancing enforceability, including the removal of non-compliant products from

[8] C. Simoneau et al, Non-harmonised food contact materials in the EU: Regulatory and market situation, 2016, EUR 28357 EN; doi:10.2788/234276.
[9] C. Simoneau et al, Non-harmonised food contact materials in the EU: Regulatory and market situation, 2016, EUR 28357 EN; doi:10.2788/234276.
[10] Chapter IV of Union Guidelines on Regulation (EU) No 10/2011 on plastic materials and articles intended to come into contact with food; Part 4 of Union Guidance on Regulation (EU) No 10/2011 on plastic materials and articles intended to come into contact with food as regards information in the supply chain
[11] SWD (2022) 163 final Commission Staff Working Document – Evaluation of the legislation on food contact materials – Regulation (EC) No 1935/2004
[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Farm to Fork Strategy for a fair, healthy and environmentally friendly food system

the market through official controls and improved traceability, (iv) Promoting transparency in safety assessment procedures for FCMs and ensuring accountability in the authorization processes, (v) Considering technological advancements by establishing rules for materials that intentionally change food in accordance with food law.

The evaluation highlighted challenges such as limited availability and adequacy of DoCs and SD throughout the supply chain. Traceability was identified as a key concern, with difficulties in tracking FCMs from raw materials to finished products. Additionally, businesses reported challenges in obtaining comprehensive supporting documentation, particularly regarding Good Manufacturing Practices and clear substance identification. The evaluation also noted shortcomings in Member State performance, particularly in identifying businesses involved in the FCM chain. Small and Medium-sized Enterprises (SMEs) faced challenges due to limited internal resources and reliance on external sources for information.

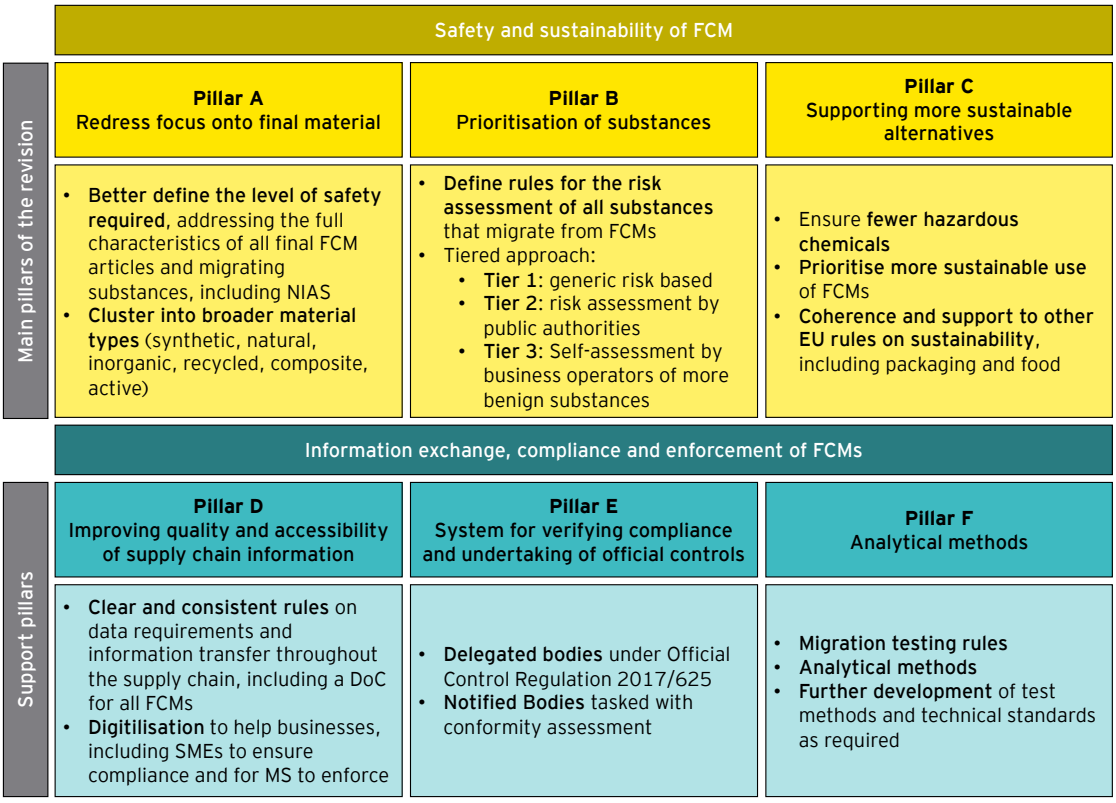
In conclusion, the evaluation recommended modernizing and digitalizing FCM systems to enhance accountability, improve information flow, and streamline compliance efforts. These efforts align with broader initiatives such as the Circular Economy Action Plan and the EU's Chemicals Strategy for Sustainability, aiming to promote innovation, sustainability, and safety in the FCM sector.

2.2 The Impact Assessment on the revision of the FCM legislation

On the basis of the conclusions put forward by the evaluation, the Commission launched an impact assessment in 2020 to revise EU Food Contact Materials (FCM) legislation, following conclusions from an evaluation. This initiative, announced in the Farm to Fork Strategy, seeks to address key issues identified in the evaluation. The goal of the revision is to establish a comprehensive, future-proof, and enforceable regulatory system for FCMs in the EU. This system aims to ensure food safety, protect public health, maintain the internal market's effectiveness, and promote sustainability. Equal rules would apply to all businesses, including those importing FCMs from third countries.

Various measures are being considered to address identified problems. These options aim to enhance consumer safety, support market functionality, and encourage the development of safer, more sustainable alternatives in line with the Farm to Fork and Chemicals Strategies. The revision of the legislation is focused on two main themes: (i) safety and sustainability and (ii) information exchange, compliance and enforcement, declined in five main 'pillars', as in the figure below:

Figure 3. Five 'pillars' of the revision of the FCM legislation



Source: EY illustration based on Tender Specifications

The focus of this study: Pillars D and E

In the context of this impact assessment, the European Commission contracted this study to support the part of the impact assessment work concerning information exchange, compliance and enforcement. The study was tasked with tackling the difficulties in the transfer of information along the FCM production chain, resulting in difficulties for industry to ensure and demonstrate compliance and for Member States to undertake controls. To do so, the study's

objective was to develop and assess the impacts of 3 options to support an IT infrastructure required for information exchange and verification of compliance and controls of FCMs, including establishing the roles and responsibilities of the various FCM actors on the infrastructure.

The team was proposed three Policy Options in the Tender Specifications to work on:

- Option 1 - Centralized IT Infrastructure System: The first option is to establish a centralized IT infrastructure system. In this setup, a principal EU body would be responsible for system management and decision-making processes.
- Option 2 - Decentralized IT Infrastructure System - Member States: The second option involves a decentralized infrastructure system where Member States are predominantly responsible for local management and decision-making procedures.
- Option 3: Decentralized IT Infrastructure System – Businesses: The third option also suggests a decentralized system but assigns the primary responsibility of management and decision-making to businesses.

The development of the aforementioned IT infrastructure options could provide significant benefits by increasing the level of transparency regarding FCMs' safety throughout their production chain. With this transparency, producers of final FCMs would have in-depth knowledge about all substances in their products, including their identity, quantity, and migration possibilities, alongside ensuring the absence of 'tier 1' substances. On the other hand, official control bodies would have quick access to the information generated, enabling them to assess the safety of FCM articles swiftly during verification of compliance.

Problem definition

In the context of this support study, the problem at hand was defined in accordance with Tool #13 of the Better Regulation Guidelines. The verification of the existence of the problem and the actors that are affected by it, including the scale of the problem, its drivers and likelihood of persistence, are paramount to a successful identification of the appropriate policy responses.

The problem at hand concerns *non-compliance FCM products still entering the market*. Despite compliance assessments, some FCMs still pose health risks due to undetected substances. Cases include instances of excessive migration of plasticizers, non-compliant polyethylene, and polypropylene granulates. Accordingly, there is a significant gap between required safety assessments and actual compliance work. Verification challenges arise due to lacking compliance documentation, confidentiality, and poor information exchange.

This problem is constituted of four main drivers:

- *Problem Driver 1 - Missing or inadequate information at manufacturing stage*: industry lacks or cannot produce necessary compliance information to then fill in compliance documentation. In particular, Non-Intentionally Added Substances (NIAS) pose a challenge due to inadequate assessment and lack of guidance. The responsibility for assessing NIAS often falls on downstream users, hindering compliance.
- *Problem Driver 2 - Incorrect or incomplete compliance documentation*: compliance documents often lack essential details such as substance identification, upstream suppliers and complete risk assessment. There is lack of trust with regards to documentation, which leads to repeated compliance assessments and doubling of work. Business operators and, in particular, SMEs face difficulties obtaining comprehensive documentation from suppliers.
- *Problem Driver 3 - Insufficient exchange of compliance information in the supply chain*: information transfer along the supply chain is often inadequate. Confidentiality issues, lack of knowledge and long supply chains hinder information exchange. Lack of DoCs for non-harmonized sectors and imported FCMs pose additional challenges.
- *Problem Driver 4 - Limited capacity of Member States to enforce legislation*: national control systems are weak, lacking expertise and effective enforcement. Official controls primarily focus on formal documentation checks, without verifying content or assessing compliance adequately.

3 Methodological approach

The methodology applied to this study was designed systematically and strategically to address the study questions outlined in the Tender Specifications. These questions served as pillars, guiding us to effectively accomplish the three-fold phases of the study:

- Developing Policy Options aimed at supporting an IT infrastructure for information exchange and verification of compliance,
- Assessing the most significant impacts arising from these Policy Options,
- Identifying the appropriate pathways for implementing and developing these Policy Options.

To inform these phases and the responses to the study questions, we leveraged an array of methodological tools. This diverse approach ensured comprehensive data collection and interpretation, contributing substantially to the quality and accuracy of our conclusions.

The methodological toolbox includes extensive desk research that provided the initial insights and helped us establish a firm foundation for our study. Feedback on the preliminary impact assessment was gathered, enabling us to identify the initial areas of potential impact. Written questionnaires were distributed among Member States' National Competent Authorities (NCAs) and National Reference Laboratories (NRLs), collecting preliminary ideas and testing positions on the Policy Options. Industries were provided with an online survey, drawing on their professional insights and experiences, while individual interviews added a further layer of depth to defining the Policy Options. A second round of interviews was carried out to confirm the Policy Options and get additional stakeholders' feedback. Case studies offered a practical perspective, shedding light on certain processes and procedures in real-world settings, and an open public consultation encouraged inclusive participation, providing valuable input from a range of stakeholders.

Altogether, this methodological approach ensured an accurate, comprehensive, and balanced analysis informed by a diverse set of data sources, which were triangulated to respond to the study questions and inform the main pillars of this study.

3.1 Development of Policy Options to support an IT infrastructure for information exchange and verification of compliance

Based on the principles of the Better Regulation Guidelines, the first phase of our study aimed to developing adequate Policy Options to remedy the existing issues in the spheres of information exchange and verification of compliance in the FCM supply chain. This implied the development of two main system options: a centralized IT infrastructure (Policy Option 1) and a decentralized one (Policy Option 2-3). Each system presents unique organizational governance scenarios, and thus roles and responsibilities may vary.

Approach to developing options for IT systems

The approach to developing Policy Options for an IT infrastructure facilitating information exchange and compliance verification primarily included establishing the strategy and vision, determining the target state architecture, anticipating change management, refining functional capabilities, and constructing a multi-phase planning.

The strategy and vision were primarily driven by the European Commission and aimed at facilitating information exchange throughout the supply chain and with National Competent Authorities, enhancing compliance, and reinforcing enforcement. We gathered information on this strategy and vision through interviews with the Commission and Agency representatives.

To determine the target state architecture, we divided it into business and technological components. The business architecture identified and modelled processes that serve the strategy. These processes were scrutinized and juxtaposed with supply chain actors' roles and were broken down either by state or by industry, depending upon the existing processes. This step led to the listing of necessary IT system actions, actors, and content access in the system. The technological architecture broke down these processes into technological blocks, defining services, database model, interactions, quality and security, and system workflows.

In the anticipation of change management, we considered both organizational and governance aspects in defining the target state architecture. The deep dive into the functionalities and capabilities ensured the technical design complied with functional and security aspects. This stage expanded the technological architecture study, refined functionalities, managed the marginal user stories and developed the implementation roadmap.

The construction of the target IT system was then developed. The architecture was divided into the business strategy, actors and processes; application architecture; data architecture; and IT infrastructure layers. The business layer consisted of identifying the personas, their journeys, and user stories, based on consultations with industry stakeholders and NCAs. This led to the recommendation of the most suitable technology, i.e., online platform, and the architectural components, for the second layer; designed modules, business functional services, and the end-to-end security for the third layer; and worked on setting up the infrastructure and spin-up environments for the fourth layer.

Finally, we established a macro-process for information exchange and compliance enforcement, which served as the basis for stakeholder consultation and the comparison of centralized and decentralized IT scenarios. We considered approaches that include intermediate assessments of products and holding manufacturers accountable for migration of all substances in their products. A simple and effective IT system would require specific guidelines per industry due to varying requirements across industries and national authorities.

3.2 Assessment of the most significant impacts of Policy Options to support an IT infrastructure for information exchange and verification of compliance

The second phase of the study aimed at assessing the most significant impacts of the identified Policy Options. The methodology mainly relied on a qualitative analysis of the options and their impacts following the completion of data collection; to some extent, some quantification of the impacts has been carried out where sufficient data allowed.

Approach to assessing Policy Options

The initial step consisted in the elaboration of assessment criteria required to evaluate the Policy Options. In accordance with the Better Regulation Guidelines, the first assessment criterion has centered around effectiveness. This include assessing how the adoption of the Policy Options contribute to achieving the policy objectives set forth in the amendment to the FCM legislation.

The assessment of impacts was then focused on the technical impacts specific to IT systems associated with the options. In conclusion, a comparative analysis of the impacts of different options was conducted to identify the strengths and weaknesses of each approach.

3.3 Identification of implementation and development pathways for Policy Options to support an IT infrastructure for information exchange and verification of compliance

The third phase of the study addresses the identification of implementation and development pathways of the options. This phase is crucial due to the absence of an existing IT infrastructure for FCMs and the foreseen significant changes brough about by a possible IT system in how FCMs will be analyzed and controlled. In this phase, we lay down the preconditions required to implement the options and chart out the steps needed to ensure these preconditions are in place, as well as the steps towards the implementation of the options themselves. This includes considering the systems that need to be in place, the investments required, the actors involved, the preconditions, and estimates of timeline. The resulting pathways are described and, where possible, visualized using diagrams.

3.4 Methodological tools

To inform the different phases of the study, several methodological tools have been utilized, including desk research, an Open Public Consultation (OPC), as well as survey questionnaires, interviews and case studies. The combination of these tools ensured a full coverage of stakeholder categories involved in FCMs, as well as the collection of the evidence needed to inform the development of the three Policy Options, identify and assess their possible impacts.

Desk research

Two round of desk research were carried out in the context of this study: preliminary and in-depth desk research. Preliminary desk research included an analysis of the legal basis for FCMs as well as examining the evolution of legislation and policy in this area. This enabled the Study Team to examine the past Evaluation of the FCM Regulation with a view to presenting an initial context as well as an updated Problem Tree, as presented in the Annex X. While elaborating a problem definition was not a key task for this Study, it was necessary for the Study Team to undertake this work as understanding and analyzing the problem is the first step to then be in a position to develop the Policy Options and assess the manner in which the Policy Options shall provide advantages and disadvantages to the current context.

In-depth desk research was undertaken for the Study, with the list of sources presented in the Annex 8. The aim of this activity was to mainly identify and select relevant documentary sources and analyze them. This activity further contributed to inform the problem definition and to detail the analytical approach to the Study Questions. Desk research has continued over the consultation phase, as documentary evidence was identified during e.g., interviews with stakeholders. The evidence extracted from these documents was utilized to inform the definition of Policy Options as well as for their assessment.

Analysis of responses of stakeholders to the Inception Impact Assessment

The Study Team assessed the feedback on the Inception Impact Assessment (IIA) provided by 302 respondents between 18 December 2020 and 29 January 2021. These responses have been used to (i) further identify the points made by stakeholders in relation to information exchange and compliance of FCM rules and (ii) identify further potential stakeholders to be consulted for the Study. The analysis of responses can be found in the Annex 7.

Open Public Consultation (OPC)

An open public consultation (OPC) aimed at collecting views of citizens and stakeholders, in order to support the impact assessment of the legislative revision of EU rules on FCMs, has taken place from 05 October 2022 to 11 January 2023. The Study Team analyzed the responses to the Open Public Consultation, where 609 responses were received, in relation to information exchange within the FCM supply chain and enforcement of FCM rules on safety and compliance. The analysis of OPC responses can be found in the Annex 5.

Written questionnaire

The methodology of this study heavily relies on gaining insights from a variety of stakeholders, with one of the central tools being the deployment of written questionnaires for Member States. The Study Team has undertaken an initial mapping of key entities to be consulted and worked with the Commission to finalize the list. This includes National Competent Authorities in EU Member States, including Norway and Iceland, as well as at National Reference Laboratories.

Written questionnaires were disseminated by EY with an initial response period of one month. However, this period was extended by an additional month upon request from Member States to accommodate the collection of information across different entities during the summer period.

The Study Team has received responses from 21 National Competent Authorities (Belgium, Germany, Estonia, Austria, Finland, Slovenia, Greece, Bulgaria, Lithuania, Spain, Italy, Denmark, Malta, Poland, Norway, Portugal, Hungary, Cyprus, Latvia, Slovakia) and 6 National Reference Laboratories (Spain, Germany, Greece, Denmark, Austria, Hungary). Two Member States, Sweden and Luxembourg, responded via email. Sweden informed the Study Team that it has not had a functioning FCM control in the past but is developing one since 2021. In their email, Luxembourg shared their general position on the revision of the legislation without answering the questionnaire.

The responses gathered from the written questionnaires were utilized to complement the study question responses and to inform the set-up of Policy Options.

Online survey

The Study Team implemented an online survey questionnaire to gather views from industries throughout the entire supply chain, with an emphasis on including SMEs. The survey was disseminated to EU Professional Associations concerning Food Contact Materials, as highlighted in the European Commission's list from February 2021 (detailed in the Annex).

The survey was launched on 13 June 2023, using the EY Qualtrics Survey tool and remained open for six weeks, including a two-week extension to accommodate stakeholders during the summer period. The approach involved sending an open link to the survey to EU organizations representing relevant industry in Brussels. These organizations were then able to further distribute the survey to relevant stakeholders within each Member State. The use of an open link facilitated wide-scale dissemination by industry members, ensuring a thorough reach.

Out of 355 responses collected, 170 respondents who completed more than 10% of the questionnaire were considered for the study analysis, as completing less than 10% did not provide sufficient information for the study's relevance. The responses to the online survey greatly informed the setup of Policy Options, by complementing the responses to the study question with views from the industry. The analysis of responses to the online survey can be found in the Annex 5.

Targeted interviews

To gather comprehensive data for the study, the Study Team undertook a two-part interview process. In total, 51 interviews have been conducted, supplementing the data collected from online surveys and written questionnaires. 22 interviews were held with EU industry associations or their members, 6 with EU Member State authorities, and 9 with the European Commission and its agencies. These were performed to elaborate on the study question responses and initially formulate Policy Options.

After the initial formulation of three Policy Options, which were developed and agreed with the Commission, a second round of interviews was held for feedback. 8 additional interviews were conducted with NCAs from Member States and Norway. Further, 3 additional interviews each were held with industries involved in supply chain case studies (metal packaging - MPE, plastics – Plastics Europe, wood – CEI-Bois) and 3 with representatives of similar IT systems (IMDS, EMVO and Digital Product Passport). The full list of interviews carried out in the context of this study can be found in the Annex 5. These latter interviews were instrumental in gathering detailed information about the functioning of parallel IT systems, providing initial insights into implementation pathways and costs.

Interviews took place via videoconference using Microsoft Teams, with a diverse range of stakeholders selected based on criteria such as current legislation beyond EU requirements, type of organization in relation to FCM regulations and enforcement, and weight on the FCM supply chain. The interviews were organized using a common mailbox, with personalized emails sent to each stakeholder. An interview topic guide was provided in advance to help interviewees prepare.

Case studies

The Study Team implemented case studies to map the current process of information exchange in relation to FCM and existing IT systems. Three of these case studies exemplify the current state of information exchange, focusing on the plastics, metal packaging, and wood industries, thereby covering diverse substances. These case studies reconstruct the supply chain and the involved information exchange. In addition, "use case" scenarios have been

developed to illustrate potential application of different Policy Options for these industries. These use cases explain in practice how the application of policy options, and hence of the related IT systems, would shape the process of exchanging information across each supply chain. Feedback on these hypothetical scenarios was collected through additional interviews with industry representatives. The analysis of case studies can be found in the Annex 6.

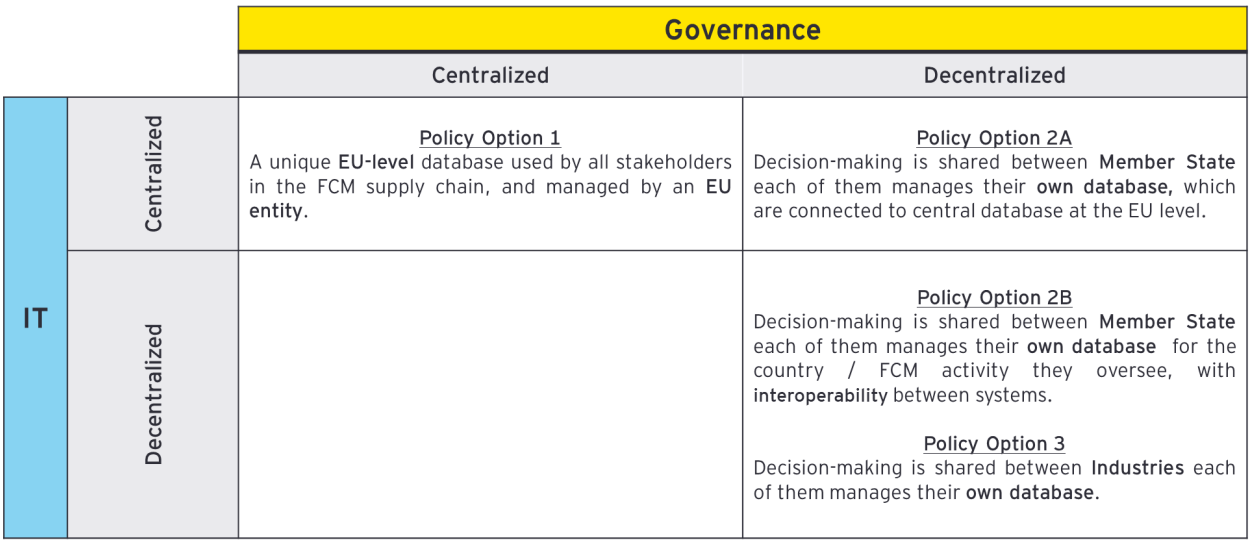
Moreover, five case studies analyzed existing IT infrastructures for information exchange, detecting best practices and potential impacts (cf. annex 1.1.1.2). These studies supplemented interviews with relevant IT systems, providing early insights into the consequences of applying Policy Options to these practical examples.

4 Policy Options

4.1 Policy Options to support an IT infrastructure for information exchange and verification of compliance

The following sections describe each of the three Policy Options that have been conceived to support an IT infrastructure for information exchange and verification of compliance. In the context of this study, as requested by the European Commission, the three policy options presented in the figure below were developed.

Figure 4. Overview of Policy Options supporting an IT infrastructure for information exchange and verification of compliance



In this section, we present an introduction of each the option and the feedback received by stakeholders during consultations, an overview of the related IT system, an explanation of the governance of the same, as well as the role of the actors using the system for information exchange and verification of compliance. The IT system architecture, which will be detailed in sub-section 4.6.2. on Implementation Pathways, is common for all Policy Options, which will all function the same through the four layers (Business and processes, Application, Platform and Data, and Infrastructure).

The draft version of the options has been presented to the Commission and confirmed by the latter in a dedicated meeting on 13 November 2023. We present the refined options, which take into account the comments provided by the Commission, as well as the additional inputs collected from stakeholders during the consultation activities conducted throughout December 2023. The options were approved, together with the Initial Report on Options, on 19 January 2024.

The table below details the structure of the Policy Options developed over the course of this study:

Figure 5. Detail on Policy Options to support an IT system for information exchange and verification of compliance

		PO1	PO2A	PO2B	PO3
Governance	Supervision	European Commission	European Commission	European Commission	European Commission
	Management	EU Body	NCAs	NCAs	Clusters of industries/ EU industry associations
IT architecture	Database	Central EU Database	Decentralized databases at MS-level managed by NCAs	Decentralized databases at MS-level managed by NCAs	Separate databases per clusters of industries/EU industry associations
	Interoperability	N/A	Central EU-Hub	Interoperability between MS databases	N/A – NCAs have access to each industry database

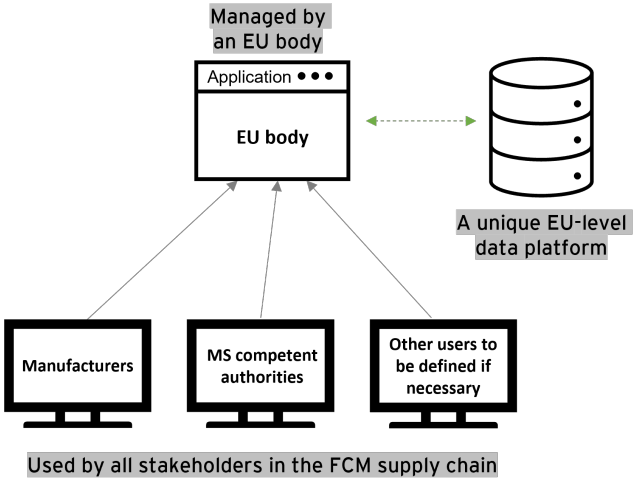
4.1.1 Policy Options 1: Centralized IT system with an EU body principally responsible for management and decision-making

4.1.1.1 Overview

This option proposes the establishment of an IT infrastructure where the management and decision making for the latter are responsibility of an EU body. This centralized IT system managed by an EU body consists of having a central data platform linked to a centralized application at the EU level. Each stakeholder, either an actor of the FCM supply chain or a national competent authority (NCA), will access the system through an end user interface. This system would be based on an online platform. Such system enables the data to be stored in one place under the responsibility and control of an EU body, which makes it easier to apply guidelines and updates when necessary. The development of this system has been inspired by the TRACES system.

The system is established based on the following architecture:

Figure 6. Overview of IT architecture for PO1



4.1.1.2 Roles & Responsibilities

Administrator - EU body responsible for management and decision-making: It is considered that the centralized IT system features an EU body responsible for its management and decision making, complying with the European Commission's guidelines set for this system. During the consultations, it was discussed with the European Commission (DG SANTE and DG GROW) and its agencies (EFSA and ECHA) which EU body should oversee such a system. It was identified that the former should take on this role, as it is in the capacity to ensure harmonization and coordination across Member States. DG SANTE proposed a governance system where a policy unit and an IT unit work together. In specific, the former would oversee the adherence of the IT system with the legislation and the latter would oversee the technical running of the infrastructure. This governance structure is in effect being

applied in other IT infrastructure currently being run by DG SANTE (e.g., the E-submission food chain platform). Accordingly, Member States and industry associations should be involved in the setup of the IT system to discuss how to integrate individual and specific needs in terms of requirements and workflows. In addition, exchanges with these actors should happen on a regular basis to make sure that the platform is being kept up to date. In the interview with ECHA, the Study Team learned that the agency is putting in place an IT infrastructure for the submission of applications under the Drinking Water Directive. The system, that will be operational from 2026, will be governed by an EU body (ECHA) for decision making and management. Member States and industry will be involved in its development and upkeep by being regularly consulted. Considering these different elements, such system can be managed by an EU body. The latter can be under different forms, either the European Commission itself or one of its agencies or a newly dedicated entity (e.g., consortium of Member States). This can be discussed further and determined considering the resources available.

Other actors in the supply chain responsible for providing the compliance data of their product or substance (manufacturers, raw material and intermediate suppliers, non-EU suppliers, food business operators): FCM supply chain actors (manufacturers, raw material and intermediate suppliers, non-EU suppliers, food business operators) will have access to the system and be able to input data about their substances or products, as well as consult data about the substances and product they purchased to carry out their compliance work. Business operators and FCM manufacturers shall be able to request additional or missing information to upstream actors in the supply chain on the IT system. In turn, upstream actors shall be able to request information on the utilization of their FCM products or materials to downstream actors to perform their risk assessments.

NCAs shall be able to access data on FCMs and substances immediately and at every step of the way, to perform verifications of compliance, as well as any supporting and additional documentation proving the compliance and safety of their products on the IT system. Competent authorities shall have access to compliance and supporting documentation at all stages of the supply chain, as well as being able to request additional information when performing compliance controls and upon/during physical inspections.

Regarding the integration of non-EU suppliers in the future centralized IT system, there was an agreement during consultations between industry and national authorities that these actors should be fully integrated in the system. This is because non-EU suppliers are bound to the same legislation on FCM and participate in the same market, hence the same conditions should apply as for EU actors on the IT infrastructure (Silicones Europe, CEFIC, Flexible Packaging Europe, EUPIA). Interviewed NCAs pointed out that their integration is central to overcome the issue of the lack of information coming from non-EU suppliers, as well as allowing competent authorities to get access to full compliance information more easily (France, Hungary, Germany, Poland, Austria, Denmark). As it was learned in the cases studies, non-EU suppliers rely on their local EU subsidiaries or importers to provide compliance information in the supply chain. Therefore, this option considers that non-EU actors are represented in the system either by their local subsidiaries or by the importer of the substance or product who would have the responsibility to provide the compliance information on the platform.

4.1.1.3 Stakeholders' feedback

In the open public consultation (OPC), most respondents (n=205, 63%) agreed with the proposal of a digital or electronic system to contain and transfer supporting compliance documentation as opposed to a paper-based system. According to the position paper of Verbraucherzentrale Bundesverband e.V., such a system would be beneficial to facilitate the work of competent authorities. Similarly, a majority of respondents to the online survey (n=66, 60%), confirmed that DoCs and documentation supporting compliance should be contained and transferred along the supply chain and to competent authorities in a digital or electronic system.

Concerning the governance of the proposed digital and electronic system, respondents to the OPC generally tended to favor the establishment of a centralized digital system to exchange compliance information, which was supported by more respondents (n=143, 44%), as opposed to 86 of them (26%) who either disagreed (n=46) or strongly disagreed (n=40). This finding is corroborated by the fact that, on the other hand, more respondents (n=129, 39%) did not agree with the establishment of a decentralized digital system for the exchange of compliance information, whereas only 48 respondents (15%) agreed (n=34) or strongly agreed (n=14). The finding was further confirmed in the online survey, where a majority of respondents (n=63, 58%) indicated the introduction of a centralized digital system as the preferred solution vis-a-vis the proposal of a decentralized system for information exchange and verification of compliance.

Many NCAs indicated, both in the written questionnaires and during the interviews, that a common European IT platform/system accessible by competent authorities would further improve collaboration, the exchange of information and ensure coherence of control activities (Austria, Belgium, Estonia, France, Germany, Italy, Lithuania, Poland and Slovakia). Based on the views of the NCAs of those Member States, the role of this EU IT platform would be to collect DoCs and supporting documents from Business Operators and would allow to exchange information in the EU and facilitate direct requests for information among Member States.

During the second phase of consultations, when presented with the finalized Policy Option, all interviewed Member States (including Norway) and two industry representatives (metal packaging, plastics), confirmed their strong support for this Policy Option.

Accordingly, a centralized EU IT system would guarantee the highest degree of uniformity, quality and harmonization across the EU in terms of data collection. This system would be the most effective option to collect all information needed from business actors. According to Member States, an EU IT system would pose a more "serious" obligation to FCM actors to provide the correct information to the supply chain, compared to the situation in which single Member States or industries set up their own databases. The centralized IT system would also be more straightforward to understand and easier to use for both business operators and Member State authorities, as both would need to use only one database to input, exchange and retrieve information, compared to decentralized IT options. The system would accordingly be less costly for business actors and competent authorities compared to the other two options, as they would rely on a joint effort at the EU level. Also, having only one database, the centralized system would not need to set up and maintain interlinks, as it would instead be needed in the decentralized options, leading to considerable savings. This would be especially beneficial to Member States with less financial power and for those with small FCM industries, which would struggle to "sell" the idea of setting up a national database to their administrators, both for financial and political reasons. According to Member States, implementing an EU database would be quicker as compared to the situation in which each Member States sets up their own database. In the latter case, in fact, Member States would require considerable time to get the proposal for a national database accepted, to finance it and to implement it.

4.1.1.4 Use case application

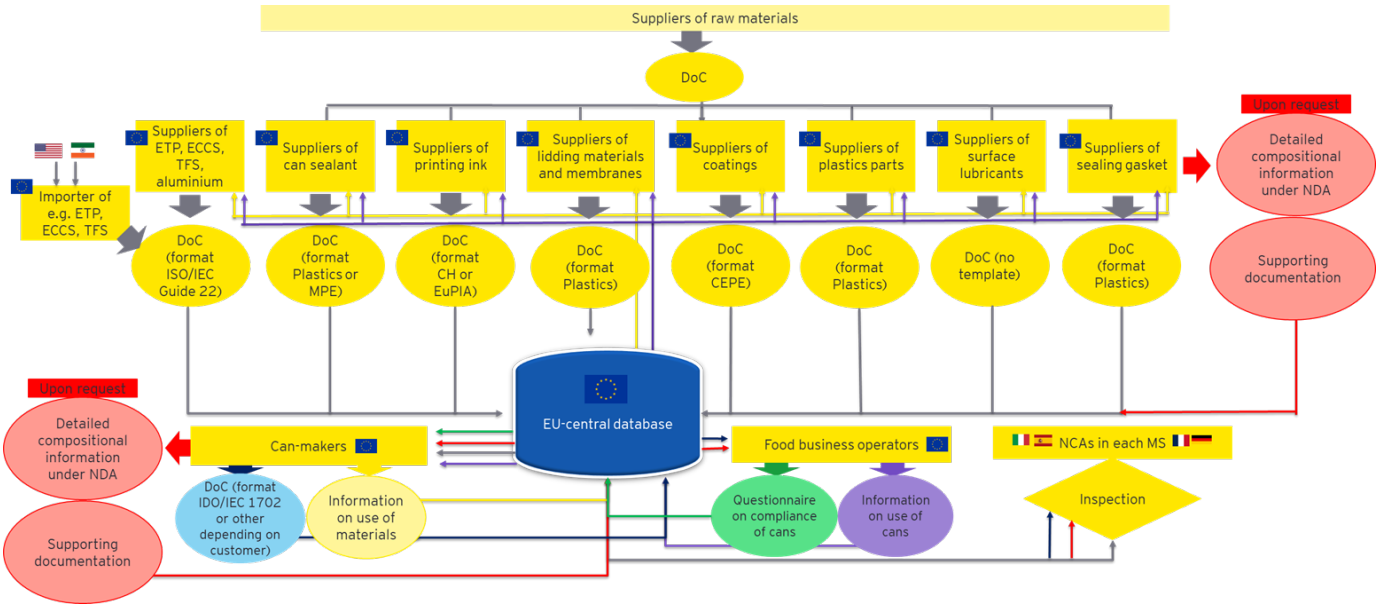
To understand how such system can adapt to FCMs, a case study about metal packaging industry (can-making supply chain) has been elaborated. Other two case studies (plastics and wooden FCM) have been elaborated and can be found in Annex 4. Case studies focused on the reconstruction of the supply chains for the three industries, as well as on the identification of the chain of information. Use case applications were developed to apply the policy options to the specific supply chains and have an overview of how information would be exchanged in the case of the establishment of IT infrastructures.

The metal packaging industry is a very complex one due to the multitude of suppliers, which makes the can-making use case a very good example of the application of the IT system's architecture.

The figure below shows that in this centralized IT system the data flow will follow a tree structure. Information about raw materials will feed the data about each component used to make e.g., cans, which will feed the central data base. This information will be available to e.g., the can-makers who will add data about their final products. Afterwards, part of this data shall be available to the food business operators who will add information about the use of the purchased products (in this case, cans). The NCAs will be able to access data on FCMs as collected throughout the whole supply chain and do their verification of compliance without any delay.

As for supporting information, that is mainly confidential, it would be possible to request it to the data owner who can open the access to it. NCAs will have access to this data without needing to request it.

Figure 7. Use case of Policy Option 1 for the can-making supply chain



4.1.2 Policy Options 2: Decentralized IT system where Member States are principally responsible for local management and decision-making

4.1.2.1 Overview

This option proposes the establishment of an IT infrastructure where the management and decision making for the latter are responsibility of Member States. In the case of this Policy Option, the governance of the system is decentralized and distributed across Member States who would set up their own IT systems. The exchange of information across these IT systems will differ in the case of sub-options 2a or 2b, as reported in the sections below. For this Policy Option, the same online platform technology considered for Policy Option 1 would be applied. However, since each Member State would have their own IT system, we can consider two possible architectures.

Policy Option 2a: EU level datahub

In this sub-option, the FCM IT system is set up by each Member State. However, since FCM supply chains spans across Europe, an EU level data hub is set up to collect the data from each MS database and ensure exchange of information across Member States.

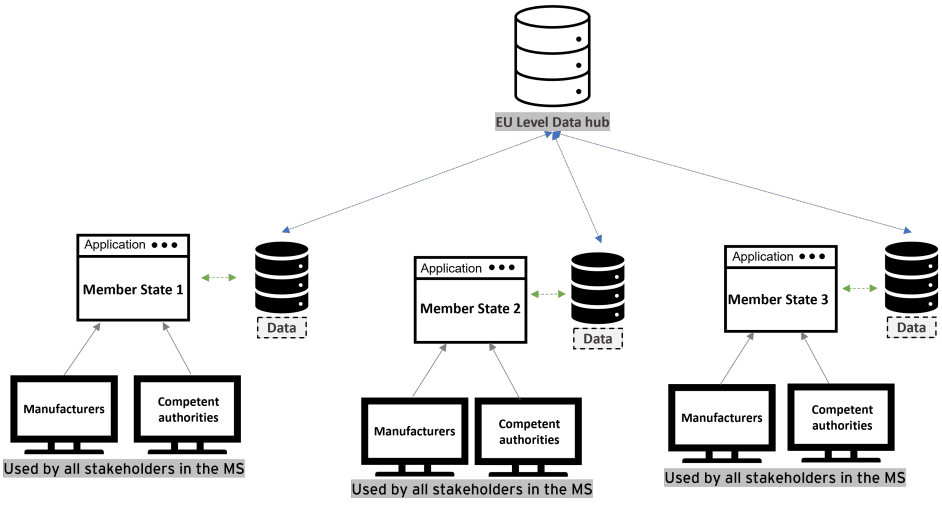
This architecture was inspired by EMVO's system. During an interview, EMVO representatives explained that their system is based on an (i) EU hub (EMVS) that is accessible by manufacturers and (ii) national systems (NMVS) that are accessible by pharmacies and wholesalers. There is a blueprint link between NMVS and the EMVS (EU hub) which makes it easier to exchange data between national systems. In this Policy Option, a version adapted to FCM is elaborated, as explained below.

A data hub is a modern, data-centric storage architecture that can allow the FCM supply chain actors and NCAs to access, store, and analyze data from various MS databases in a centralized location. It can facilitate data sharing and consolidation, enhance data analytics, and securely host data while also maintaining high-quality data governance. Unlike traditional means of storing data, a data hub places data at the center and uses metadata to create relationships between diverse data sets resulting in a more integrated and holistic view of an organization's data landscape. This means that all the data will be available in real-time at one place which is easily accessible, thus saving time and energy required in searching for up-to-date data. Having an EU level data hub can most importantly guarantee data integration from various sources, creating a seamless flow of information that would otherwise be disconnected.

It is however important to note that such set up will have additional costs for implementation and maintenance, either for technical matters or human resources. Moreover, there can be too much dependence on the data hub: if it goes down for maintenance or experiences a failure, the ability to access data and process information can be severely affected, which will limit access to data from other Members States either for NCAs or supply chain actors.

The system is established based on the following architecture:

Figure 8. Overview of IT architecture for PO2a



Policy Option 2b: Interoperable MS-managed systems

On the other hand, it is possible to bypass having an EU level data hub by creating connections between each Member States database based on interoperability.

Interoperability refers to the ability of different information systems, in this case the Member States IT systems. This involves the sharing of information and data, seamlessly without any loss, distortion, or alteration. It involves hardware, software, processes, and human interaction. There are three levels of interoperability that must be considered:

- Technical: connecting systems and services
- Semantic: making sure that the exact meaning of exchanged information is understandable by any other system or service not initially developed for this purpose
- Organizational: coordinating and management processes in which all different organizations having to act jointly.

Such system would enable FCM MS IT systems to have an automated data exchange and processing, saving time and resources, which responds to the need for information to flow cross-MS. Additionally, interoperability can lead to the development of shared standards and protocols, ensuring consistency and quality of data.

Nevertheless, aligning different systems across Member States may be a complex and time-consuming process, considering the differences in languages, protocols, and standards. Therefore, it is important to provide specific and strict guidelines to have a better data quality and functioning of the system.

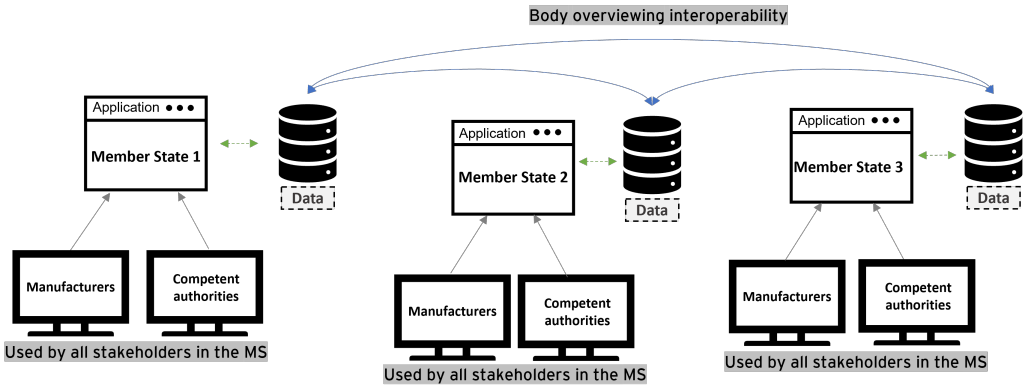
Establishing and maintaining interoperability can require significant financial investment, comprising the development and implementation of common technical standards, interfaces, protocols, and data structures to facilitate smooth communication across diverse systems and platforms. Moreover, ensuring all systems remain updated and compatible with these standards can entail further expenses. Continuous system testing, handling exceptions, data mapping, and system modifications for interoperability could also add to the costs.

Legal challenges may also exist in relation to data ownership, especially when multiple parties are involved: determining who has the rights to use, modify, distribute, and delete the data can become complex.

Data sovereignty matters could appear, pertaining to the National laws and regulations of Member States where FCM data is created and how it must be stored, protected, and processed under that jurisdiction. Therefore, for a system spanning multiple countries, each with its own data regulations, managing data sovereignty can be challenging.

Compliance with national data regulations also poses legal obstacles as data laws can significantly vary among different countries. For a European system involving 27 nations, integrating data effectively while also respecting each country's data laws is a considerable challenge. The system must remain vigilant and adaptive to each nation’s evolving data privacy regulations and requirements to avoid legal penalties and safeguard stakeholders' trust.

Figure 9. Overview of IT architecture for PO2b



Both alternatives (2a and 2b) have the same result: data flow between each MS IT system. However, there are some notable differences that must be considered:

- Interoperability between databases means that different databases can communicate with each other and share data. The databases themselves can be distinct and separate, each one maintained and operated independently, but they can exchange and make use of data from each other. This often involves the use of standard protocols and data formats to ensure the data can be understood across different systems.

- On the other hand, a data hub centralizes data from different databases. The collected data is stored in a single location or repository, and it can be analyzed and reported on from that central point. The purpose of a data hub is to provide a unified view of data from various sources.

While both interoperability and data hubs are about sharing and integrating data, they differ mainly in where and how the data is aggregated and accessed. With interoperability, data might still be housed separately but is shared and used across systems, whereas a data hub collects data and brings it into a central location.

4.1.2.2 Roles & Responsibilities

Administrators - Member States responsible for management and decision-making shall comply with the European Commission's guidelines and would be responsible for the daily management of the system (access, application of guidelines, alerts, etc.). Each Member State will be tasked with administrating its own data platform. Another body would have to overview and manage either the EU-level data hub or the interoperability between national systems.
These National administrators will have to meet several needs:

- Setting up a system that meets the European Commission's requirements in terms of both functionality and infrastructure for interoperability.
- Setting up the appropriate technical and functional organization to maintain the system and carry out day-to-day operations.
- Collaborate with the European organization in charge of setting up guidelines, as well as with other member countries, for feedback and upgrades.
- Ensure compliance responsibilities by enabling their national authorities to use the information system.
- Ensure accessibility, performance, and security for all users.
- Operate to decision-making on the system regarding the issues faced.

Other actors in the supply chain responsible for providing the compliance data of their product or substance (manufacturers, raw material and intermediate suppliers, non-EU suppliers, food business operators): business operators and FCM manufacturers shall be able to access the system, input and consult data about their substances or products manufactured/purchased, request additional or missing information to upstream actors in the supply chain on the IT system. In turn, upstream actors shall be able to request information on the utilization of their FCM products or materials to downstream actors to perform their risk assessments.

NCAs shall be able to access data about FCMs and substances immediately and at every step of the way, to perform verifications of compliance, as well as any supporting and additional documentation proving the compliance and safety of their products on the IT system. Competent authorities shall have access to compliance and supporting documentation at all stages of the supply chain, as well as being able to request additional information when performing compliance controls and upon/during physical inspections.

4.1.2.3 Stakeholders' feedback

More respondents to the OPC (n=129, 39%) did not agree with the establishment of a decentralized digital system for the exchange of compliance information. Similarly in the online survey, most respondents (n=63, 58%) indicated the introduction of a centralized digital system as the preferred solution vis-a-vis the proposal of a decentralized system for information exchange and verification of compliance. During the interviews and written questionnaire with Member States, the Study Team identified that Member States may be appealed by a decentralized IT system as they value the autonomy, customization, local skills development, efficient decision-making, compliance with local regulations, and adaptability it offers. These advantages align with their desire to maintain control, foster innovation, and address their specific needs effectively at the local level.

At the same time, during the second round of interviews, all consulted Member States did not find it reasonable to build up a system with 27 national databases (or even more, as EEA Member States applying the same rules as EU Member States would also need to set up their own databases), as the idea would be difficult to "sell" in their Member States, both financially and politically. This is especially the case of Member States with small FCM industries, which would find themselves building up a database for a few (small) actors. It was commonly agreed among interviewed Member States' representatives that getting to a uniform system, where all Member States set up their own databases, may take several years. This would be due to possible lengthy political negotiations, difficulties to get funding, differing levels of knowledge of IT systems and understanding of FCM across Member States and few resources in Member States' competent authorities that would be able to work on the set up of such a system (for instance, in Slovakia, only 2 people from the NCA would be involved). Such differences among Member States, and notably financial availability of one Member State compared to another, would lead to a situation in which some Member States are able to build and maintain their database and others do not. The differing level of investment on

national databases would, accordingly, also have an impact on the quality of each national database and may create inequalities across the EU.

In our industry case studies, we found that only the wood industry had a preference for this Policy Option. During interviews, wood industry representatives explained that the wooden FCM industry relies on different practices to analyze wood for food applications and to demonstrate compliance depending on different Member States. National wood industry association have developed different templates to demonstrate compliance. The industry does not foresee a harmonization of the latter at the EU level anytime soon. Accordingly, national databases would be able to capture specific practices in each Member State.

Belgium and Slovakia reported their experience in setting up similar national databases. Both representatives explained that such systems have taken several years to be put in place and have proved to be unnecessarily expensive. In both cases, full implementation has yet to be reached (both systems are in a stand-still due to lack of financial resources).

This decentralized IT system is perceived as more costly by both Member State representatives and the interviewed industries. Member States fear having to bear the costs of setting up and operating databases, as well as the interoperability between them. Accordingly, the latter would further delay the full implementation of the system and would take additional resources resulting in extra financial burden for Member States, compared to a centralized IT option. In addition, both representatives recognize that this system would add an extra layer of complexity for business operators, that would be confronted with the difficulty of having to use different databases instead of one (as for the centralized option). Portugal suggested that, if Policy Option 2 were to be selected for implementation, the sub-option 2A would be more effective as the central EU hub would guarantee higher levels of implementation, would be less costly for Member States to set up and maintain and its implementation would be quicker.

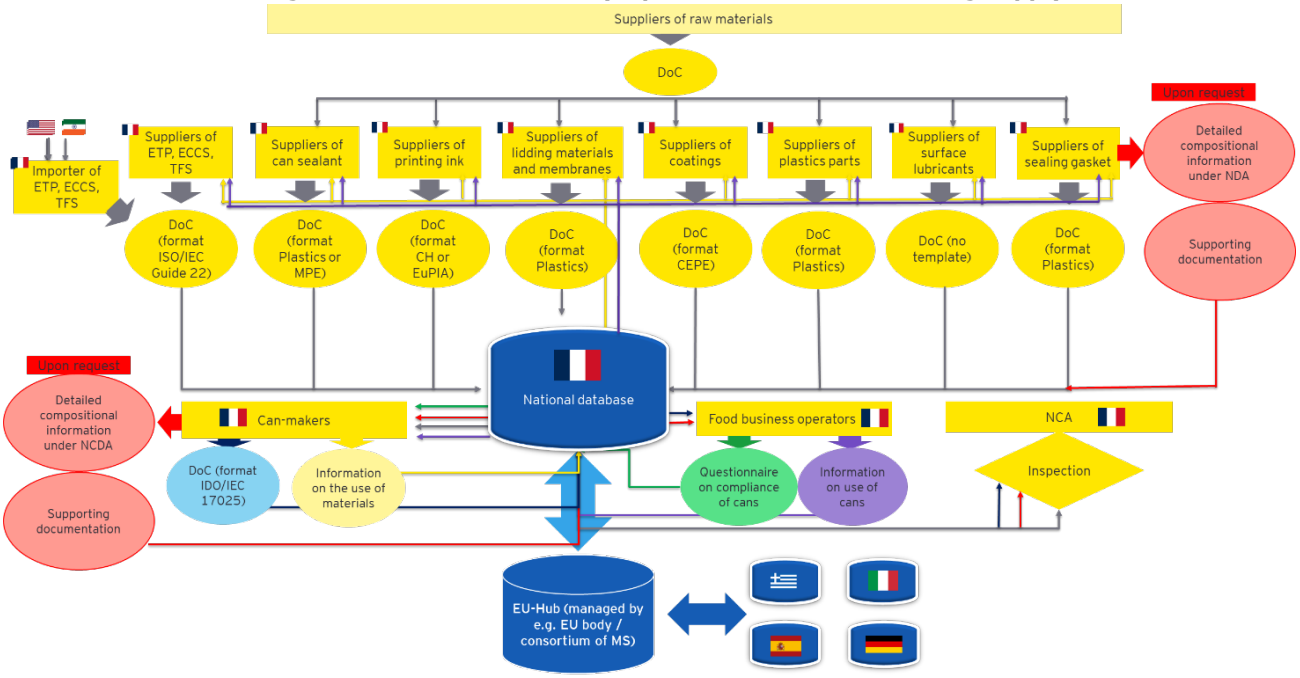
4.1.2.4 Use case application

As explained in Policy Option 1, the case of can-making industry is used to illustrate the functioning of the system.

For this Policy Option, as previously explained, we shall have two alternatives for the system's architecture, both following a tree structure.

For Policy Option 2A, the system will be based on national systems in addition to an EU-level data hub. Information about raw materials will feed the data about each component used to make cans from suppliers within the Member State – in this example, France – which will feed the national data base. This information will be available to the can-makers established in the Member State, who will add data about their final products. Afterwards, part of this data shall be available to the food business operators in France, who will add information about the use of the cans. The NCA shall be able to access information at any time to conduct verifications of compliance within their national scope. The data will be available in the EU data hub for the other NCAs to consult if needed for their verification of compliance.

Figure 10. Use case of Policy Option 2A for the can-making supply chain



For Policy Option 2b, the system will be based on having national systems with interoperability between each one of them. The flow of data will be alike to Policy Option 2a, with the exception that instead of having data go through an EU-level data hub to be accessible to other NCAs, the national systems will be interoperable. This means that NCAs will be able to access data of FCM actors in other Member States by interrogating the information system.

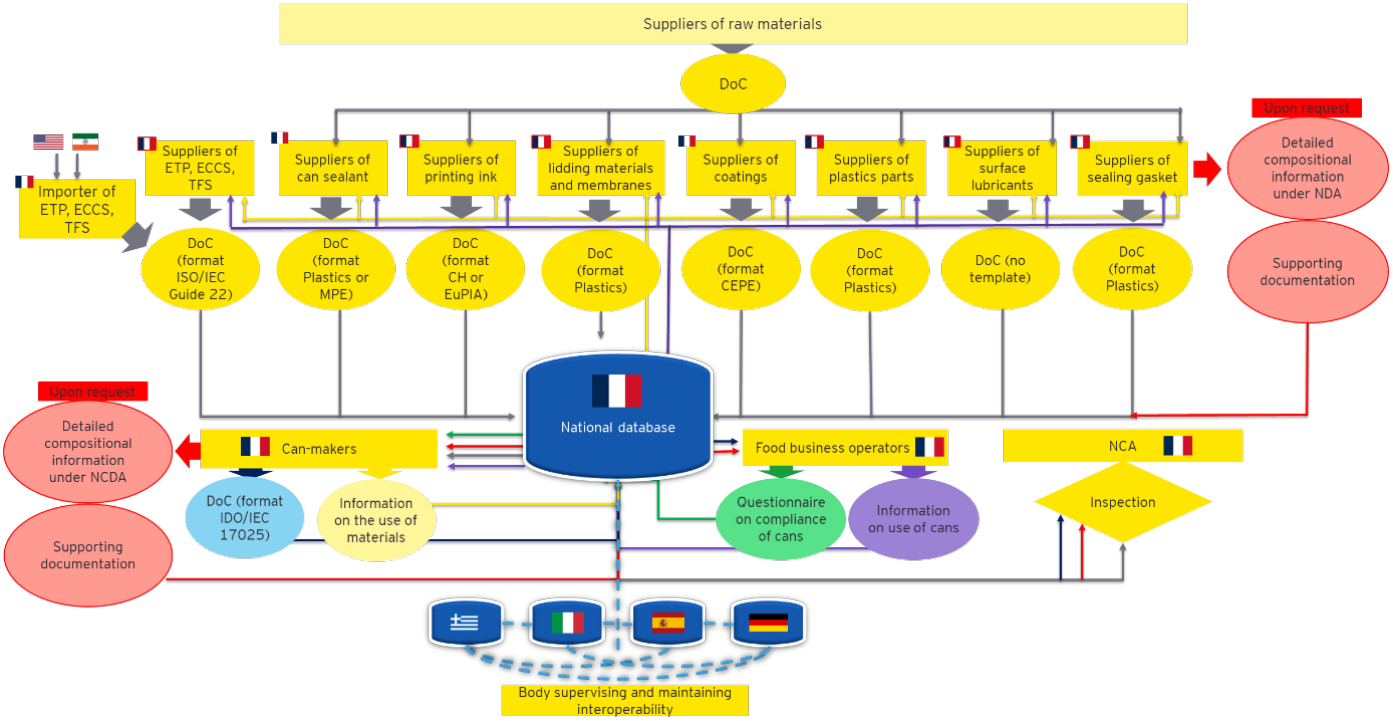


Figure 11. Use case of Policy Option 2B for the can-making supply chain

4.1.3 Policy Option 3: Decentralized IT system where businesses are principally responsible for management and decision making

4.1.3.1 Overview

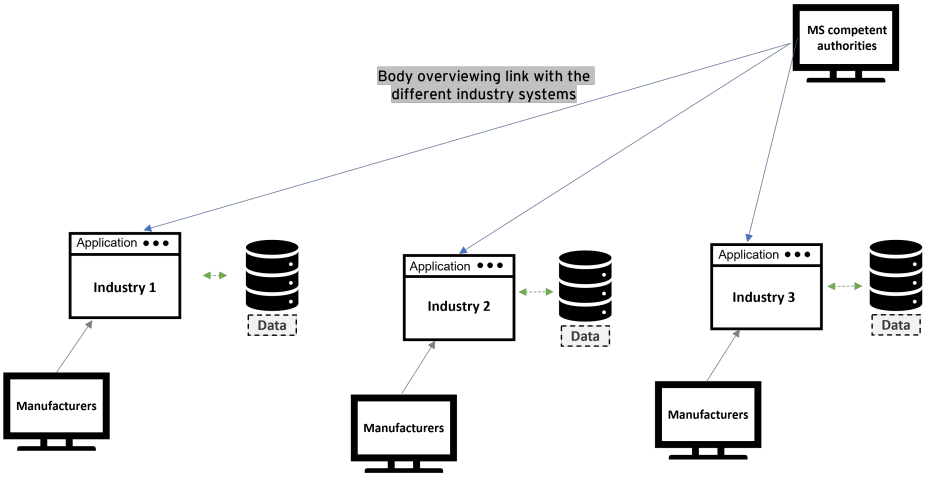
This option proposes the establishment of an IT infrastructure where the management and decision making for the latter are responsibility of businesses. In the case of this Policy Option, the governance of the system is decentralized and distributed across industries (either at the level of industry associations or industry clusters) who would set up their own IT systems. For this Policy Option, the same online platform technology proposed for Policy Option 1 is considered; however, the management of the system would be in the hand of the industries at an EU level.

This system is inspired by the IMDS, which is set up by the automotive industry for information exchange throughout the supply chain. The difference is that for the IMDS, national authorities do not access the system nor set up guidelines. Which must be the case for FCMs.

The following figure shows an overview of the architecture of the system. Each industry shall have its system with its own database and user interface. These different systems will not need to be interconnected. NCAs shall have access to each system.

A prerequisite for such system would be to define an exhaustive list of industries. What is recommended is to split them into final FCM categories.

Figure 12. Overview of IT architecture for PO3



4.1.3.2 Roles & Responsibilities

The role of the different actors and enforcement authorities in accessing the data and providing information in a decentralized IT system will be similar to Policy Option 2, with the system being administrated by Industries instead of Member States.

Administrators - Industry responsible for management and decision-making - Administrators of each system shall be embodied by representatives of each industry, either industry associations or a consortium to be defined. They would comply with the European Commission's guidelines and would be responsible for the daily management of the system (access, application of guidelines, alerts, etc.).
They will have the same roles and duties in the system as Member States do in Policy Option 2:

- Setting up a system that meets the European Commission's requirements in terms of both functionality and infrastructure for interoperability.
- Setting up the appropriate technical and functional organization to maintain the system and carry out day-to-day operations.
- Collaborate with the European organization in charge, as well as with other member states and other industries, for feedback and upgrades.
- Ensure compliance responsibilities by sending all essential information for compliance and enforcement to EU database.
- Ensure accessibility, performance, and security for all users.
- Operate to decision-making on the system regarding the issues faced.

Actors in the supply chain responsible for providing the compliance data of their product or substance (manufacturers, raw material and intermediate suppliers, non-EU suppliers, food business operators): shall access the system, input the data about their substances or products, consult data about the substances and product they purchased.

NCAs shall be able to access the system, consult the data about FCMs and their components immediately and at every step of the way, and verify the compliance of FCMs.

4.1.3.3 Stakeholders' feedback

As already discussed for Policy Option 2, more respondents to the OPC (n=129, 39%) did not agree with the establishment of a decentralized digital system for the exchange of compliance information.

In the second round of interviews, when confronted with policy option 3, Member State representatives as well as industry representatives questioned that all industries working on FCM would be able or willing to handle all the necessary information and manage large amount of data. Industry associations or clusters of industries do not have the enforcement power to demand the provision of information in their databases, especially if compared to the situation in which databases are set up by Member States or even by the EU. There may also be complications arising from seeking to create organized industry groups (either industry associations or clusters of industries) to set up and manage databases, as most FCM products are made of several materials. There may be therefore

difficulties and high costs related to the need to manage multiple databases, especially for industries supplying several sectors.

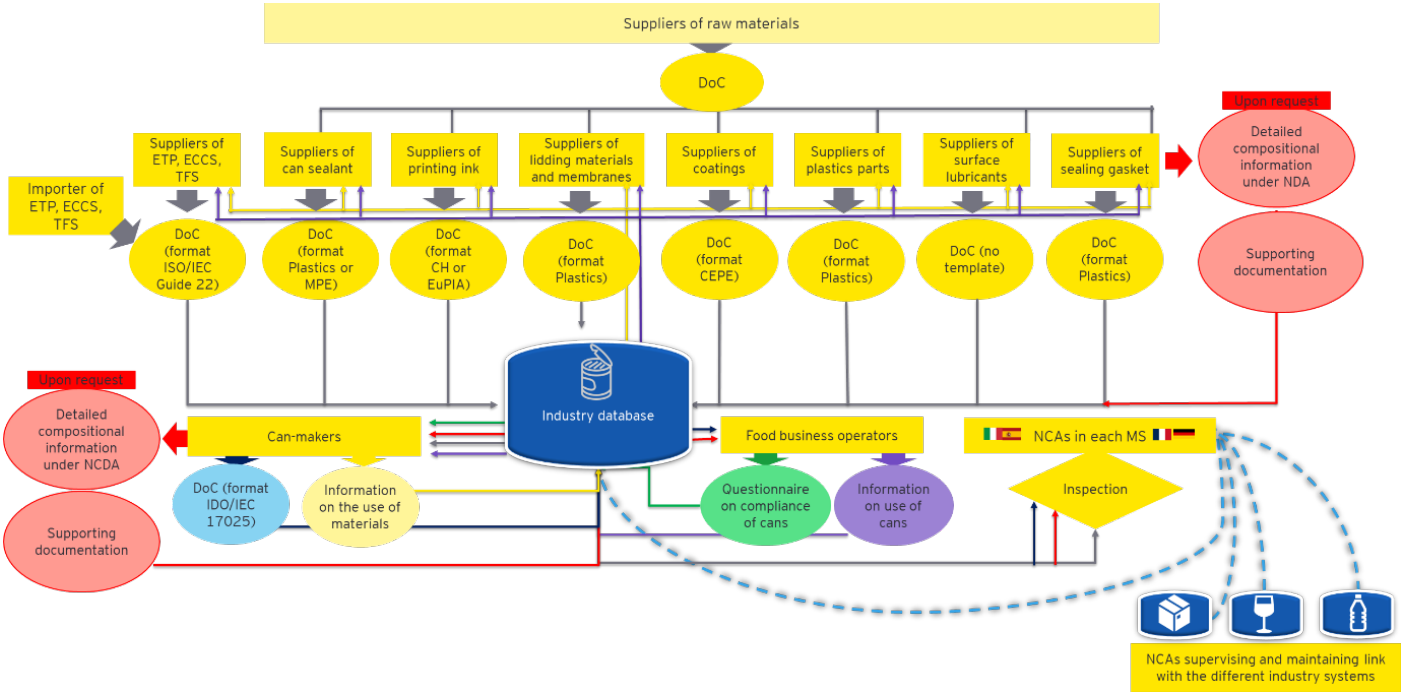
Varied levels of investment on the databases across industries may also create an imbalance in the system and could unfairly benefit larger associated industries, leaving smaller companies at a disadvantage. Small businesses, especially the non-associated ones, may be left unaware of the system and therefore may struggle to adapt to it. There is a concern related to the fact that both business operators and Member State authorities would find it hard to understand which database to enter to input and retrieve information, due to the complex composition of FCM products. This would in turn create extra financial burden on both these actors as this would make them lose time.

4.1.3.4 Use case application

As explained in Policy Options 1 and 2, the case of can-making industry is used to illustrate the functioning of the system.

For this policy option, the system will be set up and managed by industries. Information about raw materials will feed the data about each component used to make cans from suppliers within the industry all over the EU, which will feed the industry data base. This information will be available to the can-makers, who will add data about their final products. Afterwards, part of this data shall be available to the food business operators purchasing products from the metal industry, who will add information about the use of the cans. The NCA shall be able to conduct verifications of compliance within their national scope by having access to the industry database, in addition to other industries' databased. Supporting information can be disclosed upon justified request, except for NCAs, whom shall be able to access it without providing justification.

Figure 14. Use case of Policy Option 3 for the can-making supply chain



4.2 Impacts of Policy Options

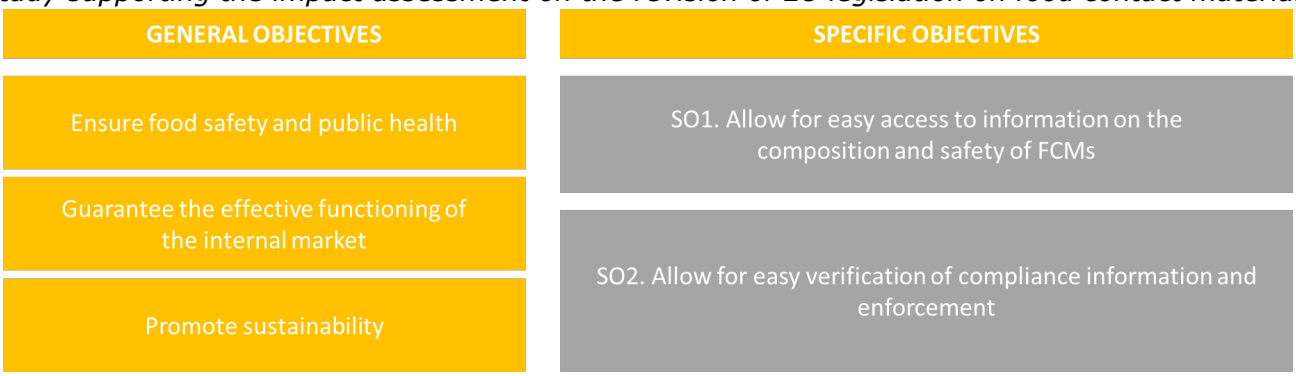
Assessing the impact of each Policy Option detailed in this report is critical, since this assessment will provide insight into the advantages and disadvantages of each Policy Option according to different criteria.

4.2.1 Assessment of effectiveness

In accordance with the Better Regulation Guidelines, the first assessment criterion focuses on effectiveness, hence examining how the adoption of the Policy Options shall contribute to the policy objectives to be achieved through the amendment of the FCM legislation.

In elaborating the context and problem definition for this Study, we have considered the General and Specific Policy Objectives that have been set. The former refers to Commission's policy priorities and strategic goals to which the FCM legislation aims to contribute, whereas the latter aim at practically guiding the setup of policy interventions for the revision of the FCM legislation. The figure below illustrates the objective tree.

Figure 15 Description of general and specific objectives



Source: EY illustration based on Tender Specifications

The following table provides an assessment of the effectiveness of each proposed option to achieve the specific objectives set.

Based on this analysis, Policy Option 1 (Centralized EU Database) appears to be the most effective in achieving both Specific Objective 1 (Easy Access to Information) and Specific Objective 2 (Easy Verification and Enforcement). It provides the most streamlined and centralized approach, addressing the identified problem drivers and offering a clear path for improved access to information and compliance verification. On the other hand, Policy Option 2 (Decentralized National Databases) is less effective because it introduces potential interoperability issues between national databases, increased costs for Member States, and the likelihood of disparities in fundings and IT system development, possibly hindering easy and harmonized access and verification of FCM information across the EU. Policy Option 3 (Decentralized industry-managed databases) is assessed to be the least effective because it relies heavily on industry collaboration, which may not ensure comprehensive compliance data, could complicate access for enforcement authorities, and poses challenges in ensuring complete and accurate information on FCM composition and safety.

Table 1. Assessment of effectiveness

Policy Options	Specific Objective 1	Specific Objective 2
Policy Option 1: Centralized EU Database	Generally effective to achieve the specific objectives	
	Simplifies access to information: By creating a single database at the EU level, all stakeholders can easily access information on the composition and safety of FCM articles.	Provides a centralized source for compliance information: Control bodies and enforcement authorities in Member States have a single, reliable source for compliance documentation, aiding in verification and enforcement.
	Improves harmonization across the EU: Ensures consistency in the data available, reducing discrepancies and confusion among Member States.	Simplifies access for control bodies and enforcement authorities: These entities can easily retrieve necessary compliance information, enhancing their ability to enforce regulations.
	Enhances quality of compliance documentation: Standardized templates and centralized management lead to better quality and completeness of compliance documents.	
Policy Option 2: Decentralized National Databases	Less effective to achieve the specific objectives	
	Potential issues related to exchange of information across countries: Multiple national databases may struggle to communicate and share data effectively, creating challenges in data exchange. However, this can be ensured thanks to an EU datahub or interoperable links between national databases.	Complicates verification due to potential interoperability issues: Control bodies and enforcement authorities may face difficulties in verifying compliance across different databases.
	Costly and time-consuming for Member States: Each Member State must develop and maintain its own database, leading to duplication of effort and potential disparities in data quality.	
	Could create disparities in terms of implementation across Member States:	

	Some Member States may experience extended times to get the proposal for a national database approved as well as difficulties in financing it, creating possible disparities among countries.	
Policy Option 3: Decentralized industry-managed databases	Least effective to achieve the specific objectives	
	Challenges in data ownership and compliance: Industries may not be willing to provide all necessary information, posing challenges in ensuring comprehensive compliance data.	May not effectively address problem driver 4: Relies on industry willingness to comply and share information, which may not sufficiently strengthen Member States' enforcement capacity.
	May not effectively address problem drivers 1, 2, and 3: If industries are reluctant to provide information, problem drivers such as missing or incorrect compliance data may persist.	Complicates management of compliance information: Each industry managing its own database may lead to inconsistencies and difficulties in accessing and verifying compliance data.
	Could hinder information exchange: Industries not collaborating may lead to incomplete information in the supply chain, hindering easy access to comprehensive data.	

4.2.2 Assessment of impacts

Through the following assessment of impacts, decision-makers and stakeholders will have a more thorough understanding of the Potential Risks and challenges that may occur during the implementation and run phase of the new system, how stakeholders will be affected, how resources will be allocated, how change will be managed without disrupting business operations, how success should be measured and how to strategize the development of this system.

Table 2. Assessment of impacts

		Policy Option 1	Policy Option 2a	Policy Option 2b	Policy Option 3
		Centralized: unique EU-level data platform used by all stakeholders, managed by an EU entity	*Decentralized: decision-making shared between Member State, each manages its own data platform, which are connected to central data-hub at the EU level*	*Decentralized: decision-making shared between Member State, each manages its own data platform, which are connected through interoperability*	*Decentralized: decision-making shared between Industries, each manages its own data platform*
Implementation	**Coordination effort**	**Low coordination efforts**: the governing EU entity will have overall control and responsibility for the system, with a clear hierarchy of stakeholders. It can easily maintain contact and coordinate with stakeholders in each country, including NCAs, industry representatives, and technology service providers.	**Moderate coordination efforts**: since national entities will manage their own data platform at the national level and coordinate with local stakeholders, governance will be more complex and require stronger coordination to ensure the integration with the centralized hub (which could nonetheless be a common ground for coordination).	**Moderate coordination efforts**: since national entities will manage data platforms at the country levels and connection will be achieved through interoperability standards, more efforts will be needed to achieve the coordination required to ensure that interoperability standards and guidelines are met.	**High coordination efforts:** since individual industries will be responsible for their data platform's development and management, and decision-making, this option can and will lead to significant variations in systems and require tight oversight and important efforts to ensure coordination, cohesion and meaningful data exchange.
	Cost efficiency	**Highly cost-efficient** upfront: a single, centralized data platform would be developed, thus reducing costs associated with maintaining separate data platforms for each country/industry. However, costs could arise due to customization and adaptation needed for certain countries/ industries.	**Moderately cost-efficient**: costs associated with developing each individual country's data platform, ensuring they can connect with a central hub, and maintaining both the hub and the individual data platforms	**Not cost-efficient**: costs associated with developing each individual data platform and ensuring interoperability, which can be complex and costly due to varying standards, technologies, and data formats across countries.	**Moderately cost-efficient**: quickly compounding costs due to the development and maintenance of several data platforms managed by different industries. Ensuring interoperability or centralized access could also add to the cost, as well as the potentially high costs associated with ensuring data uniformity, security, and compliance across different data platforms.
	Consolidation	**Highly efficient data consolidation** due to highly streamlined and consistent processes, as all data is stored and managed within one system. However, this system will need to support a complex data structure that fits all country and industry-specific requirements in addition to central guidelines.	**Moderately efficient data consolidation**: complexity will arise from the consolidation process needed between the individual data platforms, even though there's a centralized hub. Lesser standardization compared to PO1.	**Moderately efficient data consolidation**: each data platform might use different structures, standards, and languages. Ensuring interoperability between different systems can be complex.	**Inefficient data consolidation**: risk of significant discrepancies in data standards, quality, and structure across industries. Creating a unified view from disparate systems would require substantial data harmonization work, possibly more resource intensive.
	Data management	**Simple and efficient:** a centralized architecture improves coherence, makes cross-referencing	**Complex**: each Member State manages its data platform and maintains	**Highly complex:** requires aggregating the countries' data platforms with different data formats and standards,	**Highly complex:** heterogeneous data formats and structures, with possible discrepancies in data management

	easier, and reduces the complexity of managing multiple data platforms. Requires robust structures and protocols to handle data variations. Centralization will simplify the coordination of the data checking/ cleansing activities that will need to be conducted by users to ensure that the data input in the system respects the established guidelines. However, it may also represent an additional workload for the administrator, if they chose to conduct this activity themselves.	compatibility with the central hub. Complexities arise from structuring data, ensuring interoperability, coordinating and performing data validation and cleansing, and managing access rights.	making data consolidation and reporting a complex task. Interoperability needs to be strongly enforced to ensure data consistency and accuracy across the entire union. Coordination of the data checking/ cleansing activities will be complex.	practices. Requires robust data standardization and cleansing efforts. Coordination of the data checking/ cleansing activities will be complex.
Governance complexity	**Complex governance:** centralization will simplify decision-making and data management. Complexities arise from ensuring that the system caters to the diverse needs of all countries and stakeholders.	**Complex governance:** need to coordinate and manage data across different systems, complex decision making as Member States will balance sovereignty and control. Potentially faster implantation.	**Complex governance:** challenge of ensuring interoperability between different systems across Member States. Coordinating policies, protocols, and standards to allow interoperability could add to the complexity of governance.	**Highly complex governance:** shared amongst industries, each with their specific needs, standards, and systems. Decision-making may be complex due to conflicts and diverging interests.
Inequalities	**Low inequality:** a unique EU-level data platform managed centrally is more equally accessible to all Member States and industries. Decision-making will not rely on the varied capacities of individual countries or industries, which ensures a more balanced distribution of resources and decision-making power. Some inequalities could arise between countries/ industries due to their lack of direct control or influence over the system.	**Moderate inequalities** between countries based on their wealth, level of technological development and infrastructures: some might achieve a more effective data platform implementation than those with fewer resources, potentially leading to unequal representation or access to the benefits of the system. Or in the case where those countries with less resources were assisted by the more resourceful countries in setting up the FCM IT system, this *free riding* could be considered inequal.	**Moderate inequalities** due to disparate technological capabilities and resources among the countries (similar to PO2a). Additionally, countries with more influence on the interoperability standards could potentially shape them to their advantage and impose their decisions over the smaller and less experienced countries on these matters.	**Inequalities:** as for PO2a and PO2b, inequalities could arise between industries based on their size, influence, and resources. Larger or more technologically advanced industries might be able to implement and manage their data platforms more effectively, potentially leading to unequal opportunities to influence the system's evolution. Moreover, within an industry, the larger and more resourceful companies might influence the system in a way that may not benefit to smaller businesses.
Glo bal Ada	**High global adaptability**: the	**Moderate global adaptability:** member states can	**Low global adaptability:**	**Low global adaptability:**

		central and unique governing entity can swiftly implement adaptations and changes.	set their individual data platforms to adapt them more easily to local needs, requirements, and regulations.	complexity can arise from the need to ensure that no adaptations could negatively impact interoperability across data platforms.	coordinating changes across and within industries can be challenging, particularly in ensuring that adaptations maintain integrity, comparability, and reliability of data across different systems.
	Local Adaptability	**Low local adaptability**: the central and unique governing entity will lack flexibility to accommodate diverse requirements and preferences across the different countries/ industries.	**High local adaptability**: coordinating adaptations and changes that affect the entire system or the centralized hub could be complex and time-consuming.	**High local adaptability**: each country has maximum flexibility and autonomy to adopt solutions suited to its needs, possibly resulting in high adaptability at the local level.	**High local adaptability**: high level of customizability and adaptability for individual industries, which will better account for the diversity of situations of businesses of various sizes.
Run	**Consolidation**	**Highly efficient data consolidation** since all the system's data will be funneled into a unique central data platform. The consolidation process will be simplified since it will not require any interoperability testing or data translation. Stringent data quality control at the point of data capture will be needed to ensure uniformity across all Member States and Industries.	**Moderately efficient data consolidation** due to the need to collect and store data from each Member State's data platform into the centralized hub. Over time and as the data volume increases, harmonizing data structures and formats across different data platforms may put a strain on the performance of the centralized hub.	**Moderately efficient data consolidation** requiring significant resources to ensure data consistency and compatibility for effective consolidation of the data that each Member State will store in their individual data platform.	**Inefficient data consolidation**, due to the potential discrepancies in data standards, formats, structures, capture methods across industries, which will require extensive efforts in data harmonization.
	Scalability	**Highly scalable** technically since it requires scaling only one data platform. However, the monolithic nature of the system under this Option could make it a bottleneck that would slow the scaling process (every change would require modifying the entire system)	**Moderately scalable**: each country's data platform can be scaled independently based on local needs, and the central hub can be scaled separately. However, ensuring the consistent performance of the entire system during scaling, given varying capacities of individual data platforms, could be complex.	**Moderately scalable**: individual scaling per country would be swift and easy, and suitable for localized demands. However, scaling while maintaining the systems' interoperability could be complex.	**Moderately scalable**: each industry's data platform can easily be scaled as needed. However, scalability at the overall system level would be complex because of the differences in capacities, standards, and technologies across the various industries and companies.
	Data management	**Simple data management** since the centralized data platform would enable simple day-to-day operations, and the streamlined control would facilitate the	**Complex data management** due to the need for continuous synchronization and data validation of the centralized data hub to ensure data	**Complex data management** due to the non-uniformity of the datasets. Rigorous controls and highly standardized protocols will be needed to ensure data	**Complex data management** due to varying standards, formats, and quality across industries, that will require a high level of coordination and sophisticated data

	handling of large amounts of data. The administrator will need to ensure data accuracy, consistency, and security across all member states and industries, perform or coordinate data checking/ cleansing and monitor performance given the large volumes of data expected.	consistency, compatibility, and interoperability; since each Member State would manage their data.	compatibility and interoperability across National systems.	management tools and practices.
Service delivery	**Uniform and limited service delivery** since the centralized admin will oversee all updates, fixes, and improvements. However, the admin would be dealing with all requests and issues from the countries and industries; resulting in responsiveness being slower and less tailored to national/ industry needs.	**Specific and unequal service delivery** as services will be more tailored to each Member State, but uniformity of overall service will require National authorities to coordinate to ensure that changes in one country's data platform do not disrupt the centralized hub or other countries' datasets.	**Specific and unequal service delivery** with greater flexibility and customization of service delivery per country. However, overall service reliability and consistency could be a challenge, as changes in one country's system would need to be compatible with others to maintain the high interoperability required.	**Specific and unequal service delivery** with flexible, industry-specific service delivery. However, the heterogeneity of industries could lead to significant disparities in service quality, and maintaining the system's overall coherence could be complex.
Resilience	**Moderate resilience** with the risk of presenting a single point of failure, which could halt the entire system. However, resilience is improved by having one central admin responsible for the system with full control and the ability to implement a wide-ranging recovery plan.	**High resilience** since each country's data platform is independent of the others, thus localizing potential problems. However, any disturbance at the centralized hub level could still affect the overall system significantly.	**High resilience** since the decentralization increases flexibility and allows problems to be more localized. Strong agreed-upon recovery plans will be needed to solve any problems, due to the need for compatibility values among different data platforms.	**High resilience** due to each industry's system functioning independently. However, coordinating resilience strategies and standards across different industries might be complex.
Data protection	**High control over data protection**, since centralization brings robust, consistent data protection measures. The central administration enables a streamlined, uniform approach to data protection, making the system potentially less vulnerable to data breaches.	**Moderate control over data protection:** inconsistent between countries, as all Member States need to maintain high data protection standards to avoid propagation of any threat. However, the centralized hub allows for stronger oversight and coordination of data protection.	**Moderate control over data protection** due to the complexity of coordinating different systems, leading to vulnerabilities. Strong and consistent data protection measures will be needed, since individual countries' standards must be aligned, as consistent data protection measures may be complex to enforce.	**Low control over date protection** due to variations in the different industry players' data protection capabilities and resources. The lack of centralized oversight and potential inconsistency in standards could introduce vulnerabilities in an Industry's system, that could spread to other Industries' systems.
Governance complexit	**Simple governance:** authority and decision-making are concentrated in a single entity. All operations, including	**Complex governance**, as the coordination among different countries and management of a	**Complex governance**: each country's regulations and practices need to be aligned for interoperability.	**Very complex governance** since each industry would operate according to its own standards and practices.

		maintenance, system upgrades, and resolving conflicts would be managed centrally, simplifying governance.	centralized hub will pose considerable complexity. The centralized hub would act as a regulator.	Converging and maintaining the system to accommodate changes could be time-consuming and require continuous negotiation.	Coordination, consensus-building, the harmonization of standards, and the resolving of sector disputes could be challenging.
	Cost efficiency	**Highly cost-efficient**: one entity managing the data platform, software and infrastructure costs could be reduced compared to multiple smaller data platforms, thanks to economies of scale. Moreover, streamlined efforts and centralized control help reduce redundancy in tasks and operations which, in essence, can save costs.	**Moderately cost-efficient:** although resources may be optimized, costs associated with maintaining multiple data platforms and the centralized data hub could be less efficient. Implementing any evolutions in the system will require undertaking several identical projects across each data platform, which, although smaller and less costly in individual scope, will be more costly, once aggregated, than a single large-scope evolution of a centralized system. Lack of economies of scale. Shared responsibility across nations could potentially help distribute the costs.	**Cost inefficient** due to the need for a complex technical set-up to ensure interoperability, and continuous updates to maintain it. These costs could potentially be shared between nations, but the overhead cost of managing and maintaining interoperability can high. As for PO2A, implementing any evolutions across all data platforms will be less cost-efficient than a single large-scope evolution of a centralized system. Lack of economies of scale.	**Cost inefficient** since each industry manages its data platform, with a significant amount of resource duplication. Additionally, coordination costs could be high and individual industry's might have differing abilities to absorb and manage these costs efficiently. As for PO2A and PO2B, implementing any evolutions across all data platforms will be less cost-efficient than a single large-scope evolution of a centralized system. Lack of economies of scale.
	Innovation	**Difficult transformation but equal innovation:** the high level of centralization could result in limited opportunities for localized innovation but enable a uniform application and execution of centralized and equal innovation with potentially wide-reaching impacts.	**Moderate transformation and moderately equal innovation:** consistency brought by the centralized data hub reduces the innovative potential, as it might limit the variety of experimental approaches.	**Easy transformation and moderately equal innovation**: combining a distributed data platform system with local control while maintaining system-wide cohesion through interoperability encourages the exchange of innovative practices and solutions between countries. However, more technologically advanced countries could be more innovative than less advanced countries, making innovation unequal.	**Easy transformation but unequal innovation:** the diversity from multiple industries might spur innovation, as each industry would likely have unique insights and approaches to contribute. However, this innovation may be unequal among industries and companies, based on their resources and technological advancement.

	Global Adaptability	**High global adaptability**: the central and unique governing entity can easily implement any adaptations and changes due to evolving needs and regulations.	**Moderate global adaptability:** shared decision-making allows to adapt, and the centralized hub provides some uniformity of change. However, the data-hub may slow the pace of adaptations due to the need for centralized coordination.	**Low global adaptability:** complexity can arise from the need to ensure that no adaptations could negatively impact interoperability across data platforms.	**Low global adaptability:** the diversity and interests of the different industries could potentially make consensus and coordinated adaptation challenging.
	Local Adaptability	**Low local adaptability**: changes would have to be coordinated and implemented by the central entity, which could be slower and more difficult.	**High local adaptability** to local regulations & policies per Member State.	**High local adaptability**: the local control over data platforms combined with interoperability could enable individual countries to implement changes quicker and more easily. It also facilitates learning and adaptation from the experiences of other countries.	**High local adaptability**: high level of customizability and adaptability for individual industries, which will better account for the diversity of situations of businesses of various sizes.

4.2.3 Costs Assessment

The costs of implementing and managing the FCM IT System will vary according to the volume of data stored and transferred on the data platform(s). Thus, these costs will be distributed differently according to the chosen Policy Option, since they will impact data volumes:

- Policy Option 1: all FCM data will be stored in a unique data platform, which will have to process a significant volume of data, with no duplication.
- Policy Option 2A: FCM data will be stored in Member State-specific data platforms, reducing the data volume of individual platforms. However, this data will be duplicated in a data-hub, which will have to process a significant volume of data.
- Policy Option 2B: FCM data will be stored in Member State-specific data platforms, reducing the data volume of individual platforms, with no duplication.
- Policy Option 3: FCM data will be stored in Industry-specific data platforms. However, suppliers of FCM materials who supply different FCM product Industries will have their data duplicated across the data platforms of all the industries that they supply, which will increase the volume of data processed.

As mentioned in the Limits of the study, the inexistence of any IT system for tracking and compliance verification of Food Contact Materials, either at the EU level or at National/Industry level, means that we do not have any reliable source of real-world data from which we could derive a relevant quantitative assessment of costs. Moreover, the most similar IT systems are implemented (IMDS, EMVS, etc.) differ greatly from the FCM IT System in terms of scale and scope, making the use of any data about their costs potentially misleading.

Based on the content of this report, we propose to predict the potential costs of each Policy Option on 3 axes: the global cost (of the overall system, at the European scale), the local cost (for each Member State/Industry), and the coordination cost (of aggregating and harmonizing data):

Table 3. Cost assessment

	Policy Option 1	Policy Option 2A	Policy Option 2B	Policy Option 3
Global cost	**++++**	**+**	**+**	**+**
Local cost	**+** *Per MS/Industry*	**++** *Per Member State*	**+++** *Per Member State*	**+++** *Per Industry*
Coordination cost	**+**	**+++**	**++**	**++**

4.3 Implementation pathways

This section will specifically tackle the implementation of an IT system for FCM stakeholders (businesses and authorities) to exchange and verify compliance information. Before deep diving in the necessary pre-conditions and phases of implementing this system, many technologies were considered as a solution (cf. Analysis of the limits of technologies). However, the most suitable type of software appeared to be the online platform with data entry and withdrawal, for its simplicity of implementation and use, the availability of the software and competent resources in the market, and the fact that it is a widely tested solution at a large scale, including similar IT systems.

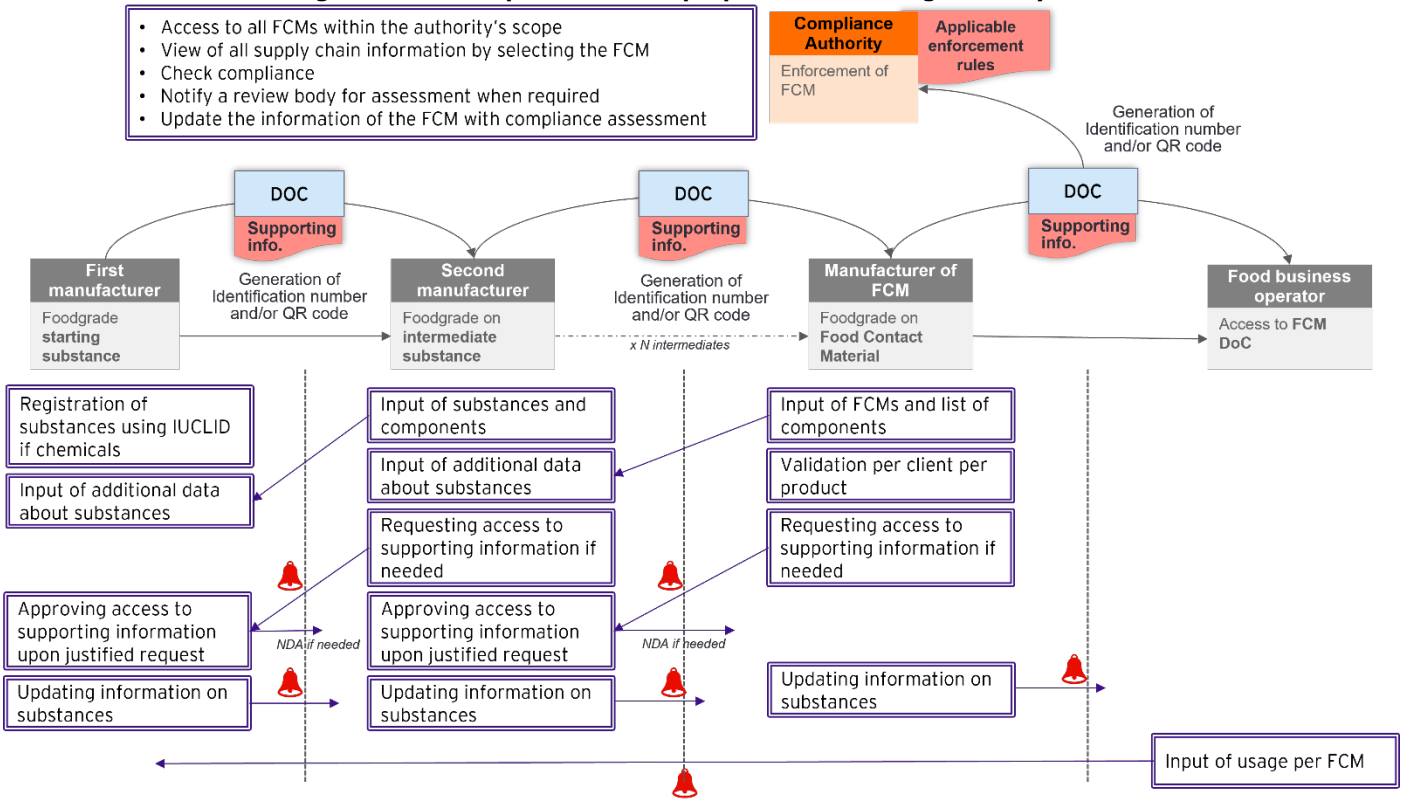
This means developing an online application accessible to all users, through a secure authorization and authentication process. The users would have specific permissions within the system based on their roles in the FCM sphere. These permissions will be managed by the system administrators.

A data management system will be included in the system, defining standardized data formats and terminology to ensure consistency. Templates of DoC must be created in the system for the users to complete for each substance, component and product. This will probably, depending on the evolution of the legislation, only concern harmonized industries at first, but must eventually be extended to all industries.

Interoperability with existing relevant IT systems, such as IUCLID, will be considered, making it easier to retrieve existing information and integrate it into the FCM IT system.

Confidentiality and security measures will be taken into account at all levels, through firewalls, encryption, and secure authentication methods. These measures will be detailed in section 4.3.3 of the report, on the technical steps of the Implementation Pathways.

Figure 16. Macro-process of the proposed functioning of the system



4.3.1 Pre-conditions for implementing an FCM related IT system

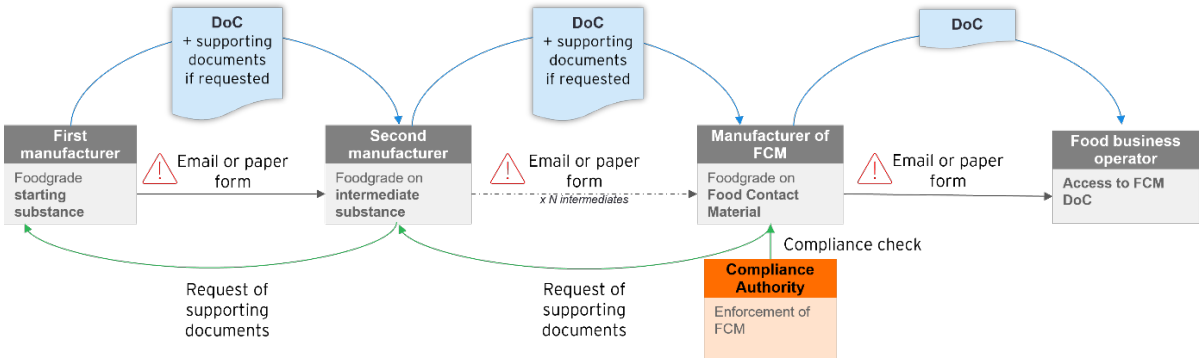
Understanding the challenges and the existing process

The FCM supply chain involves many players in each industry, for whom the production of components used for FCMs is neither the only nor the largest activity. During our consultations, we were able to delve deeper into the process of exchanging information and verifying compliance, both by industry and by country. The macro process described in the inception report is still relevant, with a few additional details: in some industries, intermediate and final products may comprise many components and therefore suppliers. Additionally, manufacturers of starting or intermediates substances sometimes use distributors who resell to several customers themselves. Distributors are usually not included in the data exchange process, which breaks the informational chain. Thus, the supply chain contains many intermediaries and distributors, making it difficult to know which material was transformed, by which intermediate FCM manufacturers, and by which food business operator it was used.

Today's FCM supply chain involves distributors, particularly upstream, making it difficult to identify customers. Moreover, manufacturers of substances or raw materials are the main suppliers of many industries and are not solely involved in the manufacturing of FCMs (for some, FCMs represent only 3% of their sales). Finally, suppliers have clients from different sectors and may even be operating from outside the EU. Even if some industries do not encounter major difficulties in exchanging information and fulfilling their duty of compliance, some key constraints are still pointed out by most industries: difficult access to DOCs, long lead times and a lack of traceability. Today, all exchanges of compliance declarations and supporting information between manufacturers take place by e-mail.

The macro-process illustrates the flow of information within the FCM supply chain. It is important to note that supporting documents are not always prepared and ready to be sent by manufacturers, which causes additional delay in case of manufacturers risk assessments and compliance checks. DoCs and supporting documents are mainly exchanged via email or sent in paper form, which may cause security issues, especially when exchanging confidential information.

Figure 17. Macro-process of the current exchange of information and verification of compliance for FCMs



Selecting the corresponding policy option

Implementing an FCM IT system would be disruptive for most of the stakeholders. However, the governance of the system must be clearly defined beforehand. As explained in the previous section, there are three policy options to support IT infrastructure for information exchange and verification of compliance. Based on interviews and consultations with stakeholders, desk research, and discussions with experts of similar IT system, the policy options were refined throughout this whole study resulting in an Impact Assessment. The latter will enable the European Commission and stakeholders to determine which of the policy option would be most relevant and adapted to the context and need of FCM actors.

The governance, management and decision-making of the system would be directly related to its financing. There are many possibilities to finance such system:

- Public funding: the system's development and maintenance can be fully funded by public authorities, either the European Commission or the National Authorities within Member States. These two options can be considered in the case of choosing policy option 1 or 2. This possibility would be similar to how the TRACES system is managed and funded.
- Private funding: the IT system can be entirely funded by suppliers, manufacturers and operators of FCMs across all industries. This funding possibility would be more relevant in case of implementing policy option 3, leaving it up to industries to manage and make decisions regarding the system. A good example for such funding would be the IMDS system, where automobile manufacturers support the governance and financing of the system. Maintenance costs are also covered via annual fees paid by OEMs; suppliers do not contribute financially. The financing of the system is based on usage which makes it fair for manufacturers of all sizes. Support programs must be considered to help SMEs cover part of the costs if needed.
- Public-Private Partnership: a hybrid financing solution could be a mixed funding by public authorities and private companies. For example, the creation and implementation of the system can be funded by the European Commission while licenses to use the system and maintenance costs can be covered by users, i.e., FCM supply chain actors and NCAs through annual fees. Support programs must be considered to help SMEs cover part of the costs if needed. As far as this study goes, there aren't any identified similar IT systems that follow this financing model. However, in many organizations, and especially for IT related projects, this business model is adopted. It allows the prescriber to finance the creation of the technical base, and the user to support the costs of maintaining and customizing the services.

Adapting the legislation and defining guidelines

Implementing an IT system for FCMs will be a highly consequent project to undertake, both technically and organizationally. As mentioned in the interviews and the existing macro-process, there is no standardized system nor governance currently in place.

During interviews with industry associations, nearly all of them deplored the lack of guidelines and reported that they would be in favor of European-level regulations precisely defining the elements to be investigated and verified for compliance.

It is important to note that, due to the multitude of industries and national authorities, establishing specific guidelines per industry would be a prerequisite for such system to be effective and simple to implement and use. Member states can also add guidelines, if necessary, to ensure compliance with national laws and regulations.

Practically, and within the IT system, establishing guidelines would make it easier to implement automated rules and processes, ensure the consistency of the data to be input in the system, increase the efficiency of the system, and most importantly, meet the need for clarity expressed by all stakeholders, either actors of the supply chain or NCAs.

Initiating the collection of data on substances

The system will need to contain pre-existing data on FCM substances, such as the name of the substance, their components, whether they are hazardous or not, etc. This data can be provided by REACH and other European and international organizations. Identification numbers specific to the FCM IT System would be associated with each substance for simplification reasons. Additional data about other non-chemical materials can also be relevant.

It is important to prepare this data at an early stage of the project, in order to save time, to guarantee interoperability with preexisting systems, but also to have a more accurate estimation on the data volumes and therefore adapt the planning of the implementation of the system consequently. Having this data would also improve the system's design, since this data can influence the design and functionalities of the IT system, by helping software engineers and system designers to customize the system accordingly.

Ensuring stakeholder engagement

It is critical to identify all stakeholders impacted by the new system, including all FCM supply chain actors (suppliers, intermediaries, FCM manufacturers, food business operators), NCAs in all member states, and the central administration (European Commission agencies). They need to be informed, engaged, and their feedback should be taken into account during the planning and design, whether they are identified as system administrators or not, following the chosen policy option.

For this matter, clear and regular communication is vital to manage stakeholder expectations. The team that will be responsible for implementing this IT system should consult with stakeholders and ask for their feedbacks and recommendations before engaging in the implementation, but also keep stakeholders informed about the progress all throughout the project.

Workshops and Q&As should be organized to ensure that stakeholders, who would be the main users of the system, are aligned with the design of the FCM IT system.

Anticipating resources availability

Resources are the backbone of any IT project. Their availability and effective allocation will play a critical role in the success of implementing this new IT system. When discussing resources in the context of IT system implementation, we refer to a broad range of elements, from human resources and financial support to technical requirements.

It is essential to thoroughly assess what resources are needed and available, identify any possible gaps, and plan accordingly to ensure a smooth process from planning, through to deployment, and beyond. Available resources will also influence the timeline and workflow of the project.

The chosen policy option would have a significant influence on resources allocation. Availability of resources depends on whether the system would be centralized or decentralized within a member state or industry.

It is important to note that proper resource allocation is necessary not just during the initial implementation, but also for the ongoing maintenance and future updates of the system.

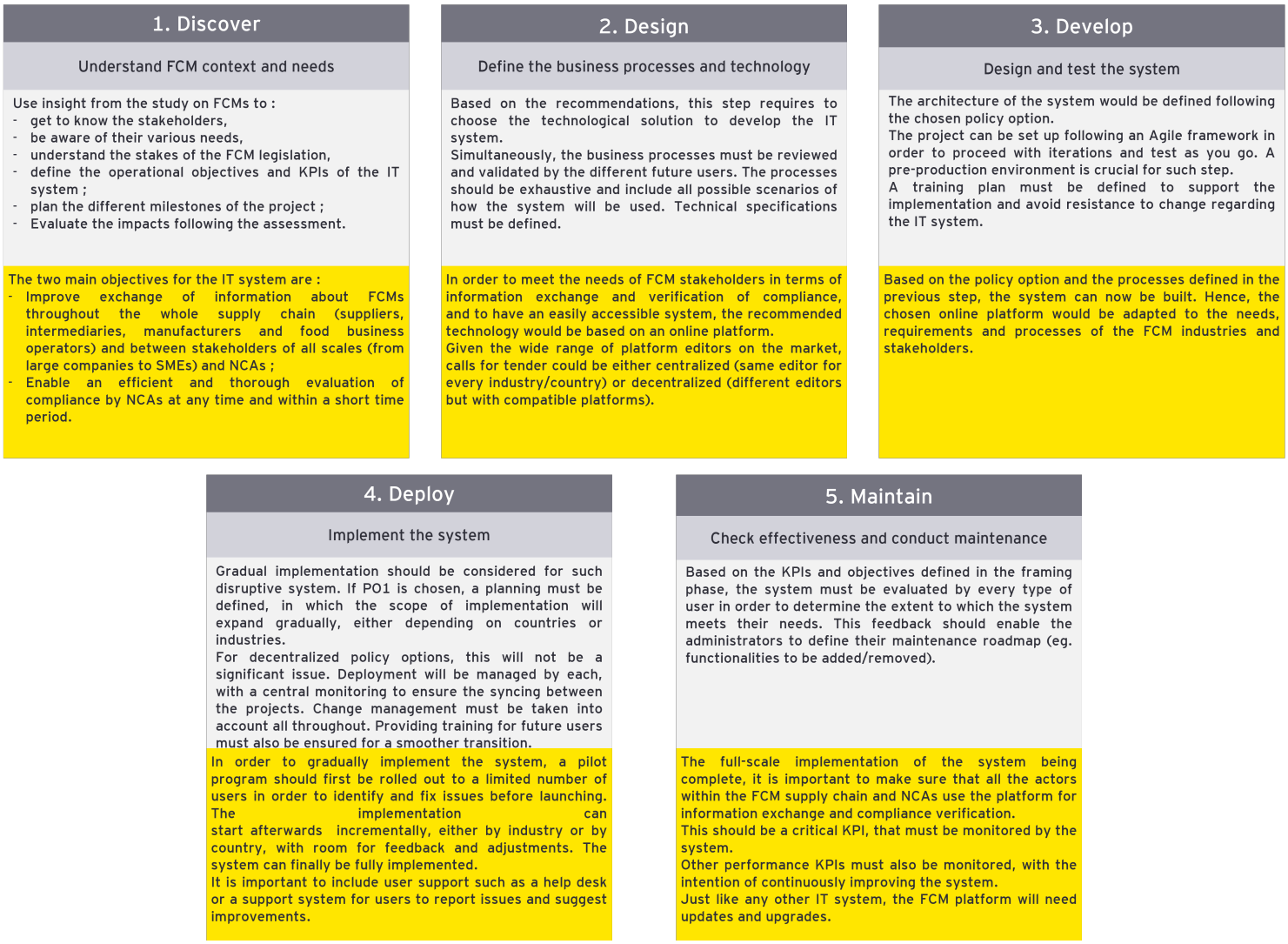
4.3.2 Implementation phases for the FCM IT system

Currently, there is no existing IT system for Food Contact Materials nor an infrastructure to be based on. For this matter, the following section will present a comprehensive overview on the implementation of such system.

There are many existing methodologies and frameworks for project management, especially for the implementation of an IT system. This section will be structured based on 5 major steps, mainly organizational, to understand the unfolding of such project, identify the actors involved in each step and designate its key results.

More technical aspects would be detailed in section 4.3.3.

Figure 18. Phases of implementation of an FCM IT system



In order to further understand what the outcomes of each of these steps would be and who would be the main actors, the tables below show in concrete terms functional details.

Table 4. Phase 1: Discover

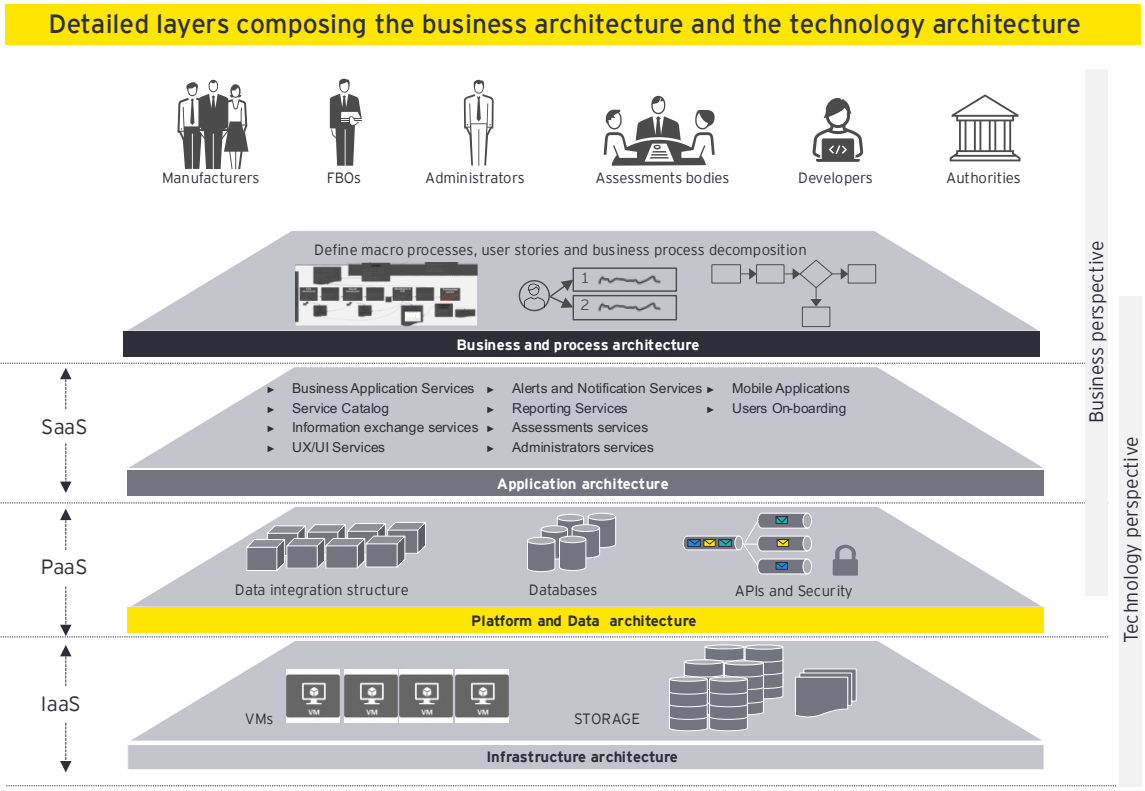
		Policy Option 1	Policy Option 2a	Policy Option 2b	Policy Option 3
Discover	**Actors**	• Project team: a European Body that would lead the project throughout all the phases. In the discover phase, they would determine with stakeholders the objectives and planning of the project. • Future users (industries & NCAs) would give insights and express their functional needs. • National and central FCM regulation authorities: overlook regulatory issues and give guidelines.	• Project team: one team per member state platform. • A team, either a central body or MS representatives, to overlook the EU-wide hub. • Future users (industries & NCAs). • National and central FCM regulation authorities.	• Project team: one team per member state platform. • A team overlooking interoperability between national IT systems. • Future users (industries & NCAs). • National and central FCM regulation authorities.	• Project team: one team per industry platform. • Future users (industries & NCAs). • National and central FCM regulation authorities.

	Outcomes	This phase would result in a project plan outlining the context and scope of the project, objectives of the IT system and implementation process including a timeline, training, resources required for each phase, allocated budget and change management approach. Other documents must be prepared such as a request for proposal addressed to a selection of online platform editors and integrators. Authorities would need to provide regulatory guidelines either specific to FCMs or to data security and confidentiality.
	Timeline	This phase could last from several weeks up to a few months. The project team would have to organize initial meetings with different stakeholders within their scope to evaluate their specific needs and define operational objectives. Consultations with FCM regulation authorities would be required to have the guidelines for the system. The project team would need to dedicate few weeks to analyze all insights and draft the complete project plan. A final meeting with relevant stakeholders and authorities should be conducted to approve the plan (timeline, resources, budget, etc.). It is important to note that the reports from this study on FCM, as well as the qualitative and quantitative analysis, are relevant to have insights, which would save time for the project team.

Table 5. Phase 2: Design

		Policy Option 1	**Policy Option 2a**	**Policy Option 2b**	**Policy Option 3**
Design	**Actors**	• Project team (cf. Phase 1: Discover) • Development team (either internal or external) would need to be present to give insight about what is possible to do in terms of technical architecture. • The selected editor of the online platform would need to provide the solution and the required licenses for the development on the software. • Future users would need to help the project team in refining the business processes that would be implemented in the platform.			
	Outcomes	The software editor would need to provide documentation and access to their platform for developers to work on. Technical and functional specifications for the IT system would need to be defined, such as business architecture and processes, technology architecture, security and compliance specifications. This includes the access to the system (authorization and authentication) and the use of the system (input of data, view of data, creation of DoC, verification of compliance, adding assessment rules, notifications, etc.). These specifications must include the system guidelines defined by authorities, in particular regarding the quality and coherence of data applicable to all users (language, structure, etc.).			
	Timeline	This step could take up to a few months depending on the chosen policy option and software editor. It would also depend on the availability of resources. It is important to note that for decentralized policy options, the duration of this phase would be different between each MS/Industry platform.			

Figure 19. Characteristics of business and technology layers



- The first *layer* concerns the business strategy, actors and processes. In this layer, we define and design user personas, journeys, and stories to enable consistent user experience. For this, we have consulted industry stakeholders in order to unpack the processes and describe the entire use of the future system. In addition, we performed functional and business decomposition that led to a set of fine-grained application services to later be used for the IT system.
- the second *layer* concerns the application architecture. In this layer, we define the foundational architecture components for the IT system, design an event-based architecture, and build software framework with cloud native principles, if needed.
- the third *layer* concerns the data architecture. At this stage, we design independent, interchangeable modules that are extensible, reusable, maintainable and adaptable, as well as Dev/Ops pipeline for streamline deployment. In this layer, we extend the framework to build autonomous, data driven business functional services and APIs, secure all digital channels, transactions, and APIs by realizing end to end security.
- the fourth concerns the IT infrastructure. It is aimed at setting up infrastructure and spin-up environments.

It is to be noted that although the business architecture concerns more the first layer, it will also provide us with preliminary information on application and data elements (layers 2 and 3). On the other hand, the technological architecture concerns mainly layer 2, 3 and 4, however the information collected for the first layer (on users' personas, journeys, and stories) will constitute the basis to build up such architecture.

As for business processes, they can be established based on each persona. The figures below represent an example of business processes for accessing and using the system by the different types of users:

Figure 20. User journey for an FCM Supplier

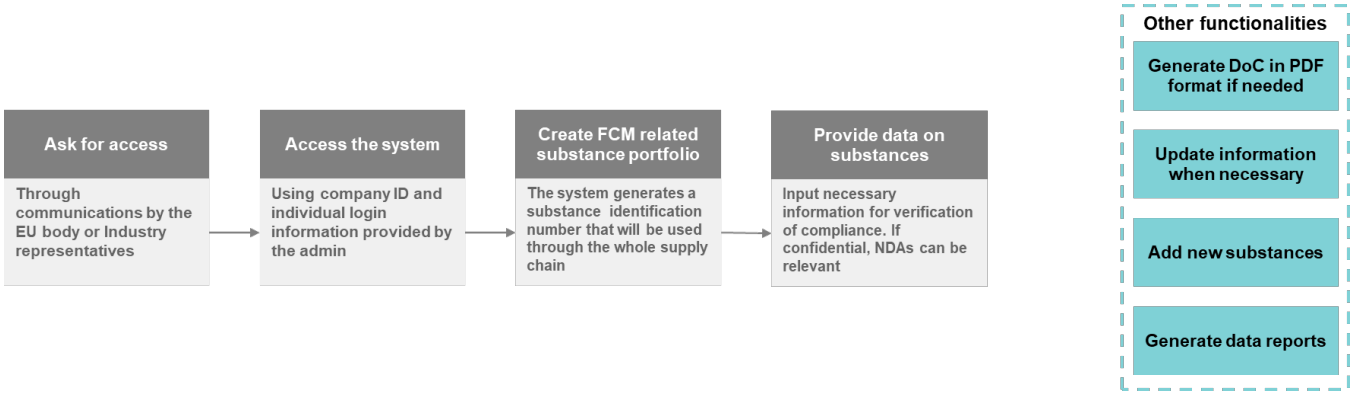


Figure 21. User journey for an FCM Manufacturer

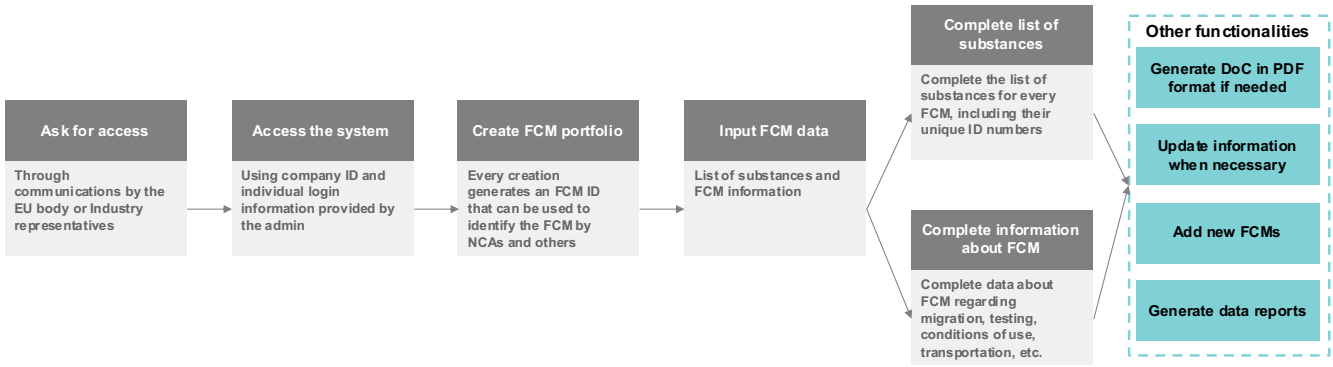


Figure 22. User journey for a Food Business Operator

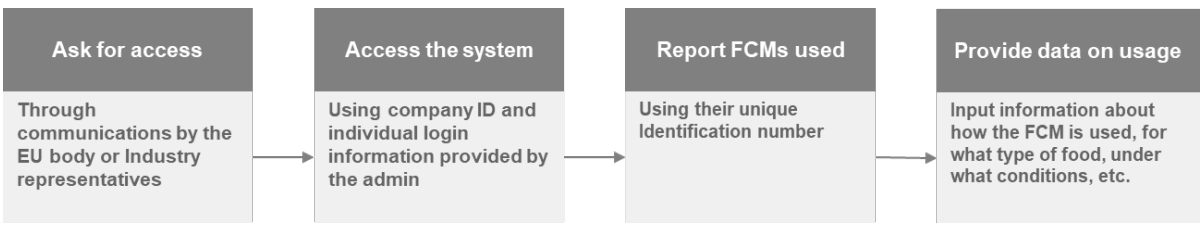


Figure 23. User journey for a National Competent Authority

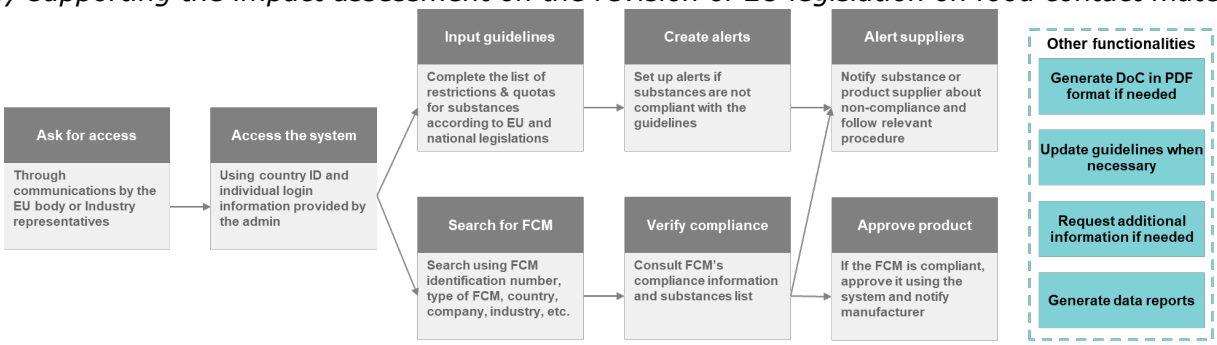


Figure 24. User journey for a system administrator

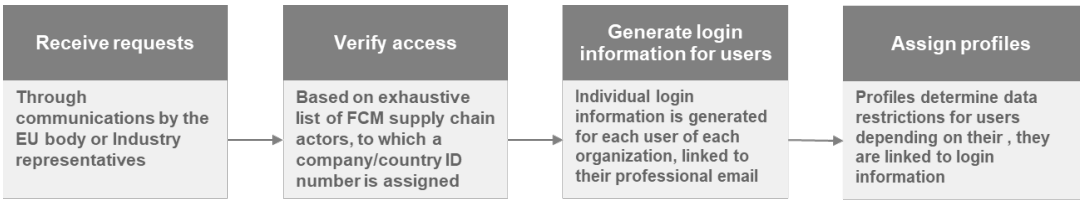


Table 6. Phase 3: Develop

		Policy Option 1	Policy Option 2a	Policy Option 2b	Policy Option 3
Develop	Actors	• Development team would need to develop the features and adapt them to FCM actors' needs. • Project team would need to assist the developers in translating business need into specifications and technical features. They must also ensure that the project timeline and objectives are met. • A group of testers should be constituted to help evaluating the developed features. • Authorities must follow the project to be able to communicate any changes in regulatory guidelines.			
	Outcomes	To conduct this phase, many documents and committees must be set up by the project team. First, a responsibility assignment matrix (RACI) can be created to specific assign roles to each actor. Depending on the chosen project framework, the deliverables can be different. For such project, the Scrum Agile framework would be the most suitable. For this matter, it is important to define the roles of each member of the project team and the length of the sprints (development cycle for a list of features), as well as the product backlog (features of the whole product), sprint planning (defining the features that would be developed for the specific sprint), review and retrospective to evaluate the features that were developed during the specific sprint. This framework is based on an iterative approach, which means that the solution can be tested as you go, and modifications can be considered early on the project. At this step, the system should be, as soon as the security requirement are sufficiently met, fed with available data on substances, collected before implementation (cf. pre-conditions). Simultaneously, a training plan must be prepared to train users on how to enroll in and use the system, to have a better understanding of the solution.			
	Timeline	The duration of this phase will depend on the chosen software, availability of resources, the number of features required for the system to be considered viable, etc.			

Table 7. Phase 4: Deploy

		Policy Option 1	Policy Option 2a	Policy Option 2b	Policy Option 3
Deploy	Actors	• The project team would need to organize and follow the different phases of deployment. • System users can at this phase access and use the system. • The development team would need to adapt the features following user feedbacks.			

		For this PO, an EU body would be responsible for management and decision-making of the IT system. For this matter, system administrators within this EU body must be appointed to grant access to the platform, monitor its performance, ensure its security, etc.	System administrators would need to be assigned to each MS IT system, in addition to an administrator for either the EU-wide hub or the interoperability of the IT systems.	Each industry platform would need its own administrator. They can be appointed by the industries or industry associations (following the governance chosen for this policy option).
	Outcomes	A pilot program can be rolled out to a limited number of end-users, that would identify and report issues to be fixed before official deployment. The project team together with the development team would have to create and look over a help desk and IT support, to receive user feedbacks and take the appropriate actions. Training sessions can also be organized to start embarking end-users on the use of the system.		
		Define the scopes of gradual deployment, either per member state or per industry (or both).	Since there would be one platform per member state (or a group of MS), the gradual deployment could be faster. For one platform the deployment could be done industry by industry.	Since there would be one platform per industry, the gradual deployment would be faster. For one platform the deployment could be done MS by MS.
		The deployment of the IT system can also begin with an implementation for harmonized industries, and gradually expand following the gradual harmonization of the rest of industries.		
	Timeline	The time needed for the deployment of an IT system for FCMs depends on several factors such as the chosen policy option, allocated budget and resources, the complexity of the system, training requirements, data migration needs, customizations, and more. A precise timeline could only be defined after consulting with the platform provider.		
		The gradual deployment can take much more time for this policy option.	Deployment of the platforms of different MS/Industries can be done simultaneously, which would make it much faster. However, this requires a lot of coordination and equal resources.	

Table 8. Phase 5: Maintain

		Policy Option 1	**Policy Option 2a**	**Policy Option 2b**	**Policy Option 3**
Maintain	**Actors**	• Project and development teams would need to switch to "run" mode and maintain the system (develop new feature, ameliorate existing ones, etc.) • System administrators would ensure access to the system by relevant users and contribute to maintenance of the system in terms of security, availability of resources, operations on databases, etc. • System users would need to input data efficiently and follow the guidelines defined by authorities. The system can only work if the quality of data and rules are respected by everyone.			
	Outcomes	At this phase, the outcomes of the deployment are analyzed. This can be done by monitoring key performance indicators of the system that were initially defined in the *Discover* phase and refined throughout the whole implementation. For this matter, dashboard for each actor within the project and administration team can be created to follow thoroughly and on a daily basis the previously defined KPIs. The results and analysis of KPIs would have to be reported to stakeholders and authorities, especially to the ones contributing to the financing of the system. A continuous improvement plan is then launched in order to refine the product. It relies on actions to encourage users to give feedback on the system, which would supply the project with insights on features to add and/or adapt in the system.			
	Timeline	This first phase can take up to a few months to collect relevant initial indicators. Afterwards, it should last as long as the system is used and maintained, with a modulation on the effort mobilized for these actions.			

4.3.3 Technical steps of the Implementation Pathways

You will find below a synthesized list of the different steps to follow in order to proceed with the implementation of the FCM IT System, with the precautions needed to ensure a smooth deployment.

A more detailed list can be found in Annex 2.

1. System Architecture Design:
    - **Design the overall architecture** of the information exchange system: cf. figures for data flow

- **Decide on the technology stack**, including databases, servers, and communication protocols: online platform based, databases will depend on PO.
- **Data flows:** design the overall architecture of the information exchange system and define the path that data will take from its initial entry point into the system, through the processes and transformations, all the way to its final output. This flow shall allow for systematic handling and tracking of data, making it useful in monitoring, quality control, and error detection.
- **Decide on the technology stack,** depending on the Policy Option and pre-existing technology stacks of administrator(s).

2. Security and Privacy:
   - **Implement robust security measures** to protect the exchanged information: firewalls, end to end encryption, etc.
   - **Address privacy concerns** and comply with relevant regulations: confidentiality measures.
   - **Select a robust encryption algorithm** that meets EU data protection standards that will immediately encrypt data once it is inputted in the system and set-up strong Access Attribution and Control, and encryption keys management. Define processes in place to rotate secured keys periodically to reduce the risk of compromission.
   - **Select a firewall solution** between the internal FCM IT network and any untrusted external networks to monitor and control incoming and outgoing network traffic.
   - **Define SSO and sign-in parameters** depending on the best practices for security, and profile assignation by the admin.
   - **Implement a security breach incident response plan**: identify an incident response team with clear roles and responsibilities (including IT, legal, and communications personnel from the various stakeholders) and define a plan outlining the steps to be taken in the event of a security breach.
3. Interoperability Standards:
   - Choose among several possible levels and types of interoperability standards for the FCM IT system to ensure seamless communication between different systems and platforms:
     1. Syntactic Interoperability: recommended for Policy Options 2b and 3: given their decentralized nature).
     2. Semantic Interoperability
     3. Structural Interoperability
     4. Process Interoperability
     5. Organizational Interoperability: recommended for all Policy Options by setting up the top-level guidelines, management, and policies that enable the different stakeholders to collaborate and exchange data.
4. Data Models:
   - Develop data models to represent the structure and format of the exchanged information.
     - ➔ Gather requirements from key stakeholders to gain a full understanding of the application's data requirements.
     - ➔ Conceptual Data Modeling.
     - ➔ Create a logical data model to provide more detail.
     - ➔ Physical Data Modeling.
     - ➔ Create Database and Implement Model.
     - ➔ Load or migrate data from existing sources.
     - ➔ Perform rigorous testing to ensure the database can handle expected tasks in real-world conditions.
     - ➔ Regularly review and adjust the data model as needed, when new requirements arise, or current ones change, and ensure the capacity of the data model and its implementation to evolve
   - Ensure compatibility with existing data standards.
     - ➔ Create a mapping of the existing data standards of the National and Industry databases to the new standards.
     - ➔ Adopt universally accepted data standards that can fit all the Countries'/Industries' existing databases.
     - ➔ Ensure that the data types used in the new data model align with the existing data types.
     - ➔ Ensure Data Structure Compatibility.
     - ➔ Ensure that the definitions, constraints, and rules for maintaining data quality align with the existing standards.
     - ➔ Create metadata specifications that align with existing standards in terms of content, format and detail level.
     - ➔ Define clear interfaces for data exchange between the new FCM System and existing National/Industry systems.
     - ➔ Test the model against the existing standards to ensure compatibility during all potential use cases and workflows.

➔ Review and update the data model to ensure continued compatibility as standards change and business needs evolve.

5. API Design:
   - Create well-defined Application Programming Interfaces (APIs) for communication between systems,
   - Consider several possible API solutions: RESTful API, Web APIs, SOAP APIs, JSON-RPC and XML-RPC, GraphQL APIs, gRPC APIs, OData (Open Data Protocol) APIs, Library-based APIs…

6. Authentication and Authorization:
   - Access Control: define roles for the system and assign access to the different stakeholders depending on their entities, and implement role-based access permissions, in accordance with the following table.

	PO1	PO2a	PO2b	PO3
Admin PO1: EU Body PO2a & b: MS/NCAs PO3: Industry consortium	**View & edit** unrestricted access to all the data			
NCA	**View & edit** unrestricted access to all the data			
Food business operator	**View** data about the FCM product used for their activity			
FCM Manufacturer and suppliers	**View & edit** data about their own FCM product			

   - Incentivize users to adopt strong security protocols.
   - Train employees on the importance of encryption and secure practices to limit the risk of a user compromising the system.

7. Data Exchange Protocols:
   - Choose appropriate data exchange protocols, depending on the nature of the information: HTTP/HTTPS, FTP/SFTP, MQTT, AMQP, SMTP, SOAP, REST…
   - Implement the protocols, in coordination with all the stakeholders.

8. Implement message queues or middleware to facilitate asynchronous communication and handle high volumes of data:
   - Identify System Requirements and the nature of messages transmitted:
   - Choose a Middleware/Message Queue Service (RabbitMQ, Apache Kafka, Amazon SQS, Google Cloud Pub/Sub)
   - Design Data Structures and Protocols to represent the information and establish a protocol for how messages are structured.
   - Implement the message queue service according to the specific guides for the chosen platform.
   - Modify the relevant components of the system to produce and consume messages.
   - Implement monitoring to ensure the health of the message queue and follow KPIs.

9. Error Handling and Logging to ensure uninterrupted service and to maintain data integrity:
   - Develop robust error handling mechanisms to manage failures efficiently.
     - ➔ Input Validation.
     - ➔ Structure exception handling.
     - ➔ Use and define error codes and messages.
     - ➔ Use built-in error handling features provided by the system's programming language, frameworks, or third-party libraries.
   - Implement logging for tracking and analyzing system behavior.
     - ➔ Define logging levels.
     - ➔ Implement a centralized logging system.
     - ➔ Maintain a consistent log format.
     - ➔ Use tools to monitor logs and generate alerts based on specific error events or when errors exceed a certain threshold.

10. Testing of the system must be conducted to ensure its effective and reliable functioning, and must be done within a pre-production environment made available by the developers:
    - Unit Testing
    - Integration Testing between different modules.
    - Functional Testing of the system.
    - Performance Testing to evaluate the system performance under load, test the speed, response time, reliability, resource usage, etc.
    - Security Testing of the system's preparedness against threats.
    - Compatibility and Interoperability Testing.
    - User Acceptance Testing (UAT) in collaboration with future end-users of the system.
    - Regression Testing whenever modifications are made in the system.
    - Automated Testing for repetitive and large-scale testing scenario.
    - Continuous Testing, as part of a Continuous Integration/Continuous Deployment (CI/CD).

Moreover, all test plans, test cases, and test results shall be documented for future reference and process transparency. Above all, a robust process for managing discovered defects must be set, involving the logging, prioritization, tracking, retesting, and validation of the fixes.

11. Deployment:
    - Deploy the information exchange system in a staged manner, ensuring minimal disruption to ongoing operations. This can be done in waves, either by country or by industry, depending on the Policy Option (cf. Implementation steps)
    - Decide on the system deployment strategy to follow, that will govern how the system is delivered into production: Blue/Green Deployment, Canary Deployment, Rolling Deployment, A/B Testing Deployment…
    - Monitor system performance and address any issues that arise during deployment.
    - Use Infrastructure as Code (IaC) tools to automate and manage the system's infrastructure.
    - Consider containerization for better deployment management and scalability.
    - Prepare the hardware and software for deployment and set up appropriate server monitoring tools.
    - Sync the IT System with the various stakeholders' existing systems and the proper syncing and compatibility during the deployment process.
12. Documentation:
    - Create comprehensive documentation for developers, administrators, and end-users.
    - Include information on APIs, data formats, security measures, and troubleshooting guides.
    - Gradually produce the necessary system documentation, that will serve as a roadmap for the system, and will assist in troubleshooting, system enhancements, training new team members, comply with audit requirements, and ensure overall system maintainability.
        - ➔ System Requirements Document.
        - ➔ Technical Architecture Documents.
        - ➔ Deployment Plan.
        - ➔ Documentation of the API methods, request/response examples, and any error statuses and their meaning.
        - ➔ User Manual with step-by-step instructions on how to use the system from a user's perspective as well as Frequently Asked Questions (FAQs) section.,
        - ➔ Test Reports.
        - ➔ Security Documentation.
        - ➔ Release Notes and Change Log.
13. Training and Support:
    - Provide training for users and administrators on how to use and maintain the system, that could include manuals, video tutorials, e-learning modules, or training workshops.
        - ➔ User Training.
        - ➔ Administrator Training for IT personnel or system administrators.
        - ➔ Continuous Training as system updates are rolled out.
    - Establish a support system to address user queries and issues.
        - ➔ System Support that users can contact for any assistance or to report issues.
        - ➔ Technical Support.
    - Implement change management to ensure the onboarding of the different stakeholders:
        - ➔ Develop a formal plan to help the stakeholders transition.
        - ➔ Regularly communicate with all stakeholders about the upcoming changes.
        - ➔ Identify "champions" in all the stakeholder entities involved in the system.
        - ➔ Get users involved in system testing or provide them with early access to the system.
        - ➔ Establish a feedback loop so users can report issues, suggest improvements, or voice concerns, and use this feedback to continually improve the system and its implementation.
        - ➔ Create a process for handling change requests after the system has been deployed.
14. Continuous Improvement will enable to streamline the FCM IT system's processes and enhance its effectiveness over the long run, by improving efficiency, reducing waste, and increasing productivity.
    - Establish mechanisms for continuous improvement based on user feedback and evolving requirements.
    - Regularly update the system to address security vulnerabilities and introduce new features.
        - ➔ Use metrics, user feedback, manual reviews, and automated tools to identify areas of improvement.
        - ➔ Define clear and achievable improvement goals based on identified issues.
        - ➔ Implement improvements in a controlled and manageable manner.
        - ➔ Implement robust Automated Testing.
        - ➔ Closely monitor the system after each improvement.
        - ➔ Regularly review the changes and their impacts. Gather feedback from users and stakeholders to understand how the changes are affecting them.
        - ➔ Implement Continuous Integration / Continuous Deployment (CI/CD) pipelines.
        - ➔ Continuously gather feedback from all stakeholders.

- ➔ Keep the development and operations team up to date with training on the latest technologies, tools, and best practices.

15. Compliance and Governance:
    - Ensure compliance with relevant National and industry regulations and standards.
    - Implement governance mechanisms to monitor and enforce policies.
        - ➔ Implement a Compliance Management System.
        - ➔ Make sure that the data protection measures respect the GDPR.
        - ➔ Conduct regular audits to ensure that the system is compliant.
        - ➔ Develop and document all policies and procedures for compliance.
        - ➔ Implement controls to protect sensitive information from being misused by employees, partners, or contractors (insider information).
        - ➔ Make sure that everyone involved in the project participates in training programs.
        - ➔ Establish processes to promptly report, manage, and mitigate any compliance-related incidents.
16. Implementing a comprehensive system for monitoring and analyzing the FCM IT System's deployment to ensure it is operating efficiently and to identify areas for potential improvement:
    - Implement monitoring tools to track system performance, identify bottlenecks, and ensure optimal operation. Implement a *data quality* approach, in order to check that users input all the required data into the system and that this data satisfies all the regulatory requirements (format, relevance, etc.).
    - Use analytics to gain insights into user behavior and system usage.
        - ➔ Determine the key performance indicators (KPIs) that are important for the system.
        - ➔ Implement system and network monitoring tools.
        - ➔ Enable comprehensive logging in the system and consider implementing a log management solution.
        - ➔ Application Performance Monitoring (APM) tools to monitor and manage the performance and availability of software applications.
        - ➔ Implement User Behavior Analysis tools to get insights into how users are interacting with the system.
        - ➔ Regularly monitor the data platforms for any performance or security issues.
        - ➔ Security Monitoring wit Security Information and Event Management for real-time analysis of security alerts.
        - ➔ Conduct regular reviews of the monitoring and analysis data.
        - ➔ Set up a notification system to immediately inform the admin team members about significant events, issues, or anomalies detected by the monitoring tools.
        - ➔ Provide a performance dashboard giving a comprehensive view of the different monitoring metrics in real time.
17. Scalability by design: the system should be able to adapt without major changes to the presentation or data access layers as the business logic evolves or the application load increase.
    - Design the system with scalability in mind to accommodate growing data volumes and user loads:
        - ➔ Design the system using microservices architecture.
        - ➔ Use database systems that support sharding, indexing, partitioning, and replication. These capabilities will allow the databases to handle increased demand.
        - ➔ Implement load balancing solutions to distribute network traffic across several servers, preventing any single server from becoming a bottleneck and ensuring reliability and redundancy.
        - ➔ Incorporate auto-scaling features that automatically scale the system up or down based on CPU utilization, or other defined metrics.
        - ➔ Employ caching techniques to temporarily store copies of data that's expensive to fetch or compute, to reduce the load on the databases and speeds up data retrieval times.
        - ➔ Content Delivery Networks (CDN) can be used to cache data closer to end users.
18. Backup and Recovery
    - Implement regular backup procedures to safeguard data.
    - Develop a robust recovery plan in case of system failures.
        - ➔ Identify Critical Systems and Data that must be prioritized for backup.
        - ➔ Decide what type of backup is needed.
        - ➔ Determine the frequency of backups needed (hourly, daily, or weekly, etc.)
        - ➔ Choose method of storage
        - ➔ Encrypt backups to protect them from unauthorized access.
        - ➔ Regularly monitor the backup processes and periodically verify that the backups are successful, and the data can be restored.
        - ➔ Create a detailed and tested disaster recovery plan.
        - ➔ Consider redundant systems in separate geographical locations.
        - ➔ Preserve multiple versions of the data to allow recovery from various points in time.

- ➔ Regularly test the recovery process to ensure the systems and data can be restored effectively and in a timely manner.
- ➔ Use backup software to automate the backups.

19. Operational maintenance
    - Monitoring protocols once the system is deployed online, to oversee system performance and utilization.
    - Deployment and tracking of batches to ensure the system updates don't affect or interrupt the system's functionality.
    - Error management (cf. point 10.) with the implementation of automated system checks to detect errors, which can then be categorized and assigned to relevant teams for resolution.
    - Status reports relating to system usage, uptime, performance against service level objectives, errors identified and resolved, scheduled updates or improvements, and ongoing risk factors.

4.3.4 Implementation challenges:

Human challenges:

- Lack of stakeholders and users' engagement: lack of insights, resistance to change, etc.
- Lack of competencies and resources;
- Unavailability of resources needed for each phase;
- Training difficulties.

Technical challenges:

- Complexity of interoperability between systems;
- Coordination between different MS/Industry systems' implementations;
- Scalability challenges.

Financial challenges:

- Underestimating the costs of implementing such system, however the policy option;
- Allocate a permanent budget to maintain and develop the solution on the long term.

Limits of other alternatives to the online platform:

Many technologies and systems were considered and delved into throughout this study, such as blockchain and Peer-to-Peer (cf. Annex 3). Another type of system has emerged during discussions with coated metal industry, which is a system based on tokens that can be used as an identification method, instead of QR codes for example. Another possibility would have been for actors to each host their products' DoCs in their own databases and give access path to these documents to NCAs. However, despite its much lower costs, this solution wouldn't be able to ensure a smooth exchange of information and a transparent version history.

5 Conclusions

The context of Food Contact Materials is particularly complex. The multitude of actors within the supply chain, involved authorities and third parties makes it harder to exchange information easily, efficiently and without any loss of data. With the advent of digital solutions, it is undoubtfully relevant to lean toward the implementation of an IT system, enabling actors to input and access data about FCM-related substances, components and products easily and immediately when needed.

To aid in the decision-making process, we have conducted an in-depth analysis of possible policy options, platform architectures, and corresponding business models. This comprehensive study equips stakeholders with a detailed understanding of each approach, presenting the advantages and potential shortcomings of each. This information affords decision-making stakeholders the means to select the option that best suits their specific needs.

As we gear towards organizing the stakeholder workshop, these options will form the basis of discussion, nurturing a collaborative decision-making environment. The varying IT scenarios, complex as they may be, all represent potential avenues for the effective regulation and management of FCM. However, it is worth stressing that no IT solution will be effective unless backed by concise policy directions and harmonized guidelines. Regardless of the complexity of the chosen platform architecture, a well-structured policy direction paired with precisely harmonized guidelines can ensure the effective functioning and efficiency of any chosen model.

While these IT scenarios generally aim to increase efficiency, transparency, and data protection in the FCM management, they also need to account for diverse needs and preferences across the supply chain actors. The best policy option should not only enable seamless data exchange and regulation enforcement but also ensure local

adaptability and resilience. In this sense, the Centralized EU Database seems to be the most effective model, considering its ease of governance, simple data management, robust data protection, and cost-efficiency. However, if local adaptability and system resilience are higher priorities, other decentralized options may need to be evaluated, despite the associated challenges.

The proactive involvement of every actor in the implementation process, the establishment of a harmonized regulatory environment, and the ability to adapt and be resilient in the face of unexpected challenges will be crucial factors that determine the ensuing success of the digital transformation. A robust IT system for managing FCM, chosen carefully and implemented astutely, holds great promise for revolutionizing the entire FCM supply chain, making it more efficient, transparent, and ultimately safer.

Limits of the study

However, there are several limitations to this study that readers must remain aware of, and that should be considered in the decision-making process and planning of the FCT IT-system to be created:

- The primary limitation of this study lies in the fact that there is currently no existing IT system that records and tracks data specific to Food Contact Materials at a scale as significant as the European Union. This unprecedented nature of the project implies that this system is experimental as no existing model could serve as a valuable source of inspiration or offer constructive feedback based on its operation. Although several other IT systems were studies, this posed a challenge in the conception of this system, which hence relies on theoretical frameworks and guidelines, and is only inspired to some general degree to other existing IT systems; however, it remains deprived of empirically tested models that could guide the developmental processes and validate presumptive strategies.

- Moreover, drawing comparisons to, or deriving insights from similar IT systems has proved problematic, since all these systems (IMDS, EMVS, REACH, TRACES NT, etc.) are industry-specific: designed and optimized for operations within a single-industry context. The FCM IT system detailed in this study is used seamlessly across more than 14 industries; this complexity, requiring the system to cater to a diverse range of industry-specific needs and regulatory stipulations, while still maintaining a unified, efficient and coherent functional structure, makes the comparison with these existing IT systems less relevant.

- Collecting data to gain insight from FCM stakeholders poses some challenges: as detailed above, the nature of this Study implies to assess the impacts in the future of three options in relation to a potential and experimental IT infrastructure for information exchange on FCMs among the different stakeholders. As no IT system has yet been defined at the EU level, it has proven challenging for the different stakeholders to respond to the questions on IT infrastructure and to imagine precisely what such a harmonized system could achieve. During the targeted interviews, it has proven especially difficult to get precise estimates of the costs of such an IT system from most of the stakeholders interviewed.

- The nature of exploring a new IT system development led to challenges in quantifying impacts due to the lack of existing data or previous performance metrics for reference. Additionally, gaining complete access to financial details for the IT systems under evaluation proved difficult. Lastly, the uniqueness of the envisaged IT systems, in terms of complexity, design and functionalities, compared to existing systems, posed another challenge, introducing a degree of uncertainty to the accuracy of estimates and projections. Therefore, while our findings provide a robust qualitative starting point to assess impacts of the proposed options, the precise details relating to costs may evolve as more information emerges and the system develops from idea to reality.

Publications Office
of the European Union

doi: [...]
ISBN [...]