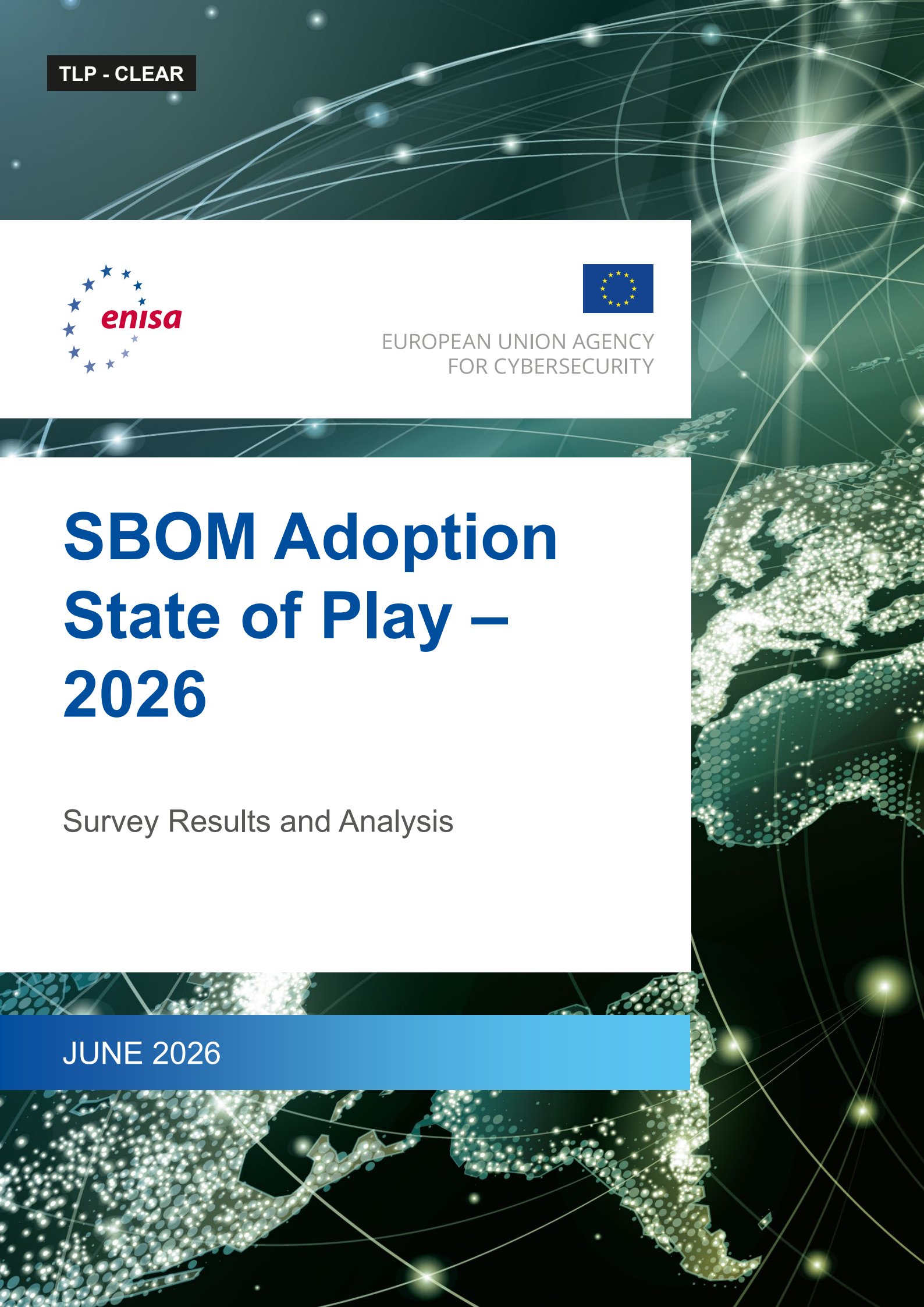
TLP - CLEAR



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SBOM Adoption State of Play – 2026

Survey Results and Analysis

JUNE 2026

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors, please use product_security@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

European Union Agency for Cybersecurity (ENISA)

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2026

COPYRIGHT NOTICE

ISBN 978-92-9204-791-7, DOI 10.2824/0741767

Table of Contents

About ENISA 1

Executive Summary 3

1. Introduction 6

1.1 The Background 6
1.2 The Concept of SBOM 6
1.3 The Survey 7

2. Analysis of the SBOM State of the Art Survey 8

2.1 Survey Cohort 8
2.2 CRA Applicability, Awareness, Exposure and Investments 9
2.3 Supply Chain Security 12
2.4 SBOM Specifics 14
2.4.1 Adoption Readiness 14
2.4.2 Formats, Tools and Lifecycle Integration 17
2.4.3 Usage Patterns and Gaps 20
2.4.4 Barriers, Needs and External Supports 23
2.4.5 Vulnerability Management 25
2.4.6 Interoperability Requirements 26
2.4.7 Supplier Requirements (for SBOM consumers) 27
2.4.1 Guidance 29

3. Conclusions 30

Executive Summary

The **EU Cyber Resilience Act** (CRA) becoming fully applicable in December 2027, transforms the supply chain security landscape by making **security-by-design** and **security-by-default**, a legal obligation for all digital products entering the EU market. Software supply chain transparency thus becomes a **required cybersecurity capability**, positioning the **Software Bill of Materials** (SBOM) as an **enabler and key mechanism** for operational efficiency, vulnerability management, third-party risk management, and regulatory compliance.

SBOM is defined as a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements. It provides visibility of the components, libraries, dependencies and licencing requirements in a software product.

The European Union Agency for Cybersecurity launched a survey at the end of 2025 to gain **factual data** on how organisations across industries and of varying sizes are approaching **SBOM adoption in response to the CRA**. This report analyses the results of the SBOM state of the art survey, by discussing:

- → CRA awareness, perceived applicability and organisational impact;
- → supply chain security concerns and investment plans for the identified risks;
- → SBOM familiarity and adoption levels;
- → SBOM formats, tooling ecosystem, integration patterns, depth and vendor supply;
- → SBOM implementation barriers, needs and external support;
- → SBOM interoperability requirements;
- → the guidance required to support SBOM adoption at scale.

The analysis confirms that the **CRA acts as an accelerator** for SBOM adoption as organisations broadly invest in SBOM generation and automation to integrate SBOM in the Software Development Lifecycle (SDLC), while expediting their implementation timeline to meet expected maturity levels. Based on the respondents' estimations, **79% of the organisations will reach the necessary SBOM maturity level** by the time that the CRA will be fully applicable.

Organisations acknowledged the **value** of continuously generating and consuming SBOM **in risk reduction** and **cost avoidance** (37 %), in **operational efficiency** (29 %) and in **meeting contractual requirements** and gaining a competitive edge in bids (26 %).

78 % of the respondents reported that their organisations **have already initiated their SBOM adoption journey**, with 44 % currently being in the pilot or limited adoption phase. 9 % have already reached a **mature level of implementation, fully supported by automation**, while 25 % have stated that SBOMs are **broadly adopted in their products**.

The selected SBOM formats appear to align with the CRA requirement regarding using a format that is commonly used and machine-readable: 44 % of the respondents reported using **CycloneDX** and 29 % **Software Package Data Exchange** (SPDX). However, 11 % of the respondents indicated that they do not use a standard format and the remaining 17 % still use a proprietary format.

The survey indicates that SBOM will be used for **the identification and patching of vulnerabilities** by 29 % of the organisations, for **ensuring open-source licences** (OSS) are correctly used/declared by 22 %, for **meeting regulatory requirements** by 19 %, for **evaluating third-party software risks** by 14 % and for **maintaining an up-to-date inventory** of all components by 13 % of the organisations.

The main barriers that prevent organisations from adopting SBOMs at scale, as identified by the respondents in different parts of the survey, are:

- → the technical challenge of achieving a high degree of **SBOM completeness** (62 %);
- → the lack of internal **skills** or dedicated staff (28 %);
- → SBOM data **quality** (37 %); and
- → **vulnerability matching** (35 % quite a lot and 23 % extremely challenging).

The means that are going to facilitate this process have also been assessed by the respondents in different parts of the survey. It is clearly stated that external support is needed. The main needs can be summarised:

- → a **reference implementation** providing the pipelines in a public repository;
- → a **guide** navigating the process of tool selection based on evaluations and benchmarking;
- → **conformance tests** with check point and validators;
- → **industry consensus** on best practices to integrate producing/consuming SBOMs:
  - into software development practices, deemed the most critical (23 %),
  - into risk and compliance processes (19 %),
  - how to produce/consume SBOMs and how these methods will evolve/improve over time (19 %);
- → development of a **profile** defining what constitutes a **'good enough' SBOM**;
- → call for the **standardisation of SBOM** formats and their required fields;
- → development of **a risk assessment framework** that leverages SBOM data.

Overall, the survey findings indicate that SBOM adoption across organisations is progressing and is strongly influenced by the regulatory requirements introduced by the CRA. However, they also demonstrate that SBOM adoption fluctuates and further progress will depend on the development of **shared implementation practices**, **improvements in supplier transparency**, **continued investment in workforce capabilities**, and definition of the **role of SBOMs within operational risk** management frameworks.

334
responses across the world

65%
EU based

80%
directly impacted by the CRA

33%
never heard about SBOM before

72%
increased their investment in SBOM tooling and automation

79%
will reach the envisioned SBOM maturity level by the end of 2027

73%
are already using a commonly used and machine-readable format

39%
generate SBOM on software builds

20%
do not know where to consume SBOM

36%
need all primary components and direct dependencies with known unknowns

41%
aim to fully automate the SBOM generation per release/build

26%
request a reference implementation providing the pipelines in a public repository

62%
highlight the technical challenge of achieving SBOM completeness

29%
call for the standardisation of SBOM formats and their required fields

31%
call for the development of a profile defining a "good enough" SBOM

1. Introduction

1.1 The Background

The EU Cyber Resilience Act (CRA) ([1]), recognising the exponentially increasing cybersecurity challenges faced by the European Union, aims to enhance cybersecurity culture and strengthen cyber resilience across the EU market. These goals are fulfilled via a legal framework which lays out the essential requirements for the development of secure products with digital elements, ensuring security and transparency in the digital supply chain. It is a methodological and structured approach to target the low levels of built-in cybersecurity in many products, address the insufficient provision of security updates and help end users assess cybersecurity in the products that they consume.

Along with other horizontal rules which address different aspects of cybersecurity, the CRA introduces for the first time the legal requirement for manufactures to create, maintain and, where necessary, share with market surveillance authorities Software Bill of Materials (SBOM) for all products with digital elements. This change transforms SBOMs from a best practice and optional implementation for supply chain security into a mandatory security measure upholding security, transparency and conformity with the regulation. SBOMs now play a multifaceted role in building market trust by facilitating informed, risk-based decision-making, providing traceability of products and components, supporting compliance and securing the supply chain.

1.2 The Concept of SBOM

Under the CRA, the SBOM is defined as a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements. The SBOM obligations for manufacturers, outlined in the CRA, can be summarised as follows.

- Manufacturers must generate SBOM for every product with digital elements they place on the EU market.
- The SBOM must be in a commonly used and machine-readable format.
- The SBOM must cover at least the top-level dependencies of the product.
- The SBOM must be kept up to date throughout the product's life cycle.
- The SBOM must be included in the product's technical documentation and provided to market surveillance authorities upon request. There is no obligation to make it public.
- The SBOM must be included in the vulnerability handling process put in place by the manufacturer and support the identification and recording of vulnerabilities and components contained in products with digital elements.

([1]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

1.3 The Survey

Given the significant role of SBOM in software supply chain transparency and security, along with its now mandatory nature as defined by the CRA, the European Union Agency for Cybersecurity (ENISA), with this survey, sought to examine SBOM readiness and the current state of SBOM adoption across various organisations and industries. The results provided meaningful insights on:

- the level of SBOM adoption and maturity;
- the most common formats, tooling and usage scenarios;
- perceived value, challenges, and the gap between SBOM generation and consumption.

The survey was divided into seven sections to gain targeted understanding on each subject area, from demographics to CRA awareness, SBOM predominant trends, adoption and maturity. Most questions were presented in multiple-choice format to facilitate pattern identification and the analysis of the results, while a few open-ended questions were included to gather specific insights. All responses were confidential and used only in aggregate.

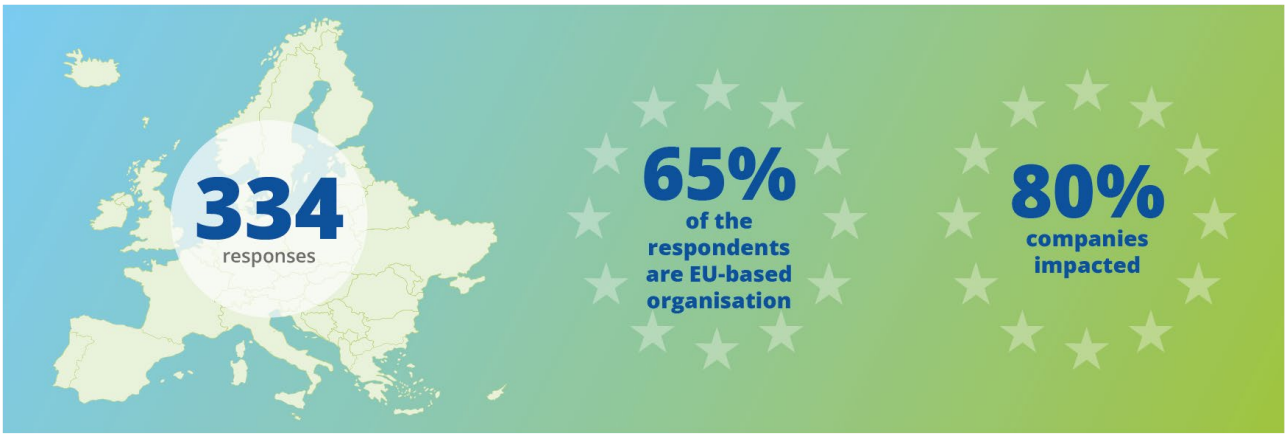


Figure 1: Survey infographic

The survey received **334** responses from organisations across the EU and, in some cases, beyond; almost **65 %** of the respondents are EU-based organisations and **more than 80 %** are companies that are directly impacted by the CRA.

This report presents the analysis of the SBOM state of the art survey results conducted at the end of 2025 and has the following structure:

- **Executive Summary**
- **Section 1.** Introduction
- **Section 2.** Analysis of the SBOM State of the Art Survey
- **Section 3.** Conclusions

2. Analysis of the SBOM State of the Art Survey

2.1 Survey Cohort

The survey received mainly responses from private-sector companies (87.72 %). This was expected due to the CRA's focus on manufacturers and importers of products with digital elements. Public authorities, trade associations and non-governmental organisations account collectively for approximately 8 % of the responses received.

Organisations with over 250 employees are heavily represented in the survey with more than 65 % of the responses. Medium-sized enterprises represent 18 % while microenterprises and small enterprises collectively represent 16 % of the respondents. This distribution potentially reflects the capacity and tendency of big organisations to be proactive and explore compliance elements of EU policy and law ahead of time. This approach can also be explained by their involvement in both the legislative consultation process and the CRA Expert Group established by the European Commission.

Large enterprises: 65 % of respondents

Large enterprises have the means and capacity to be proactive and prioritise innovation, automation and regulatory compliance.

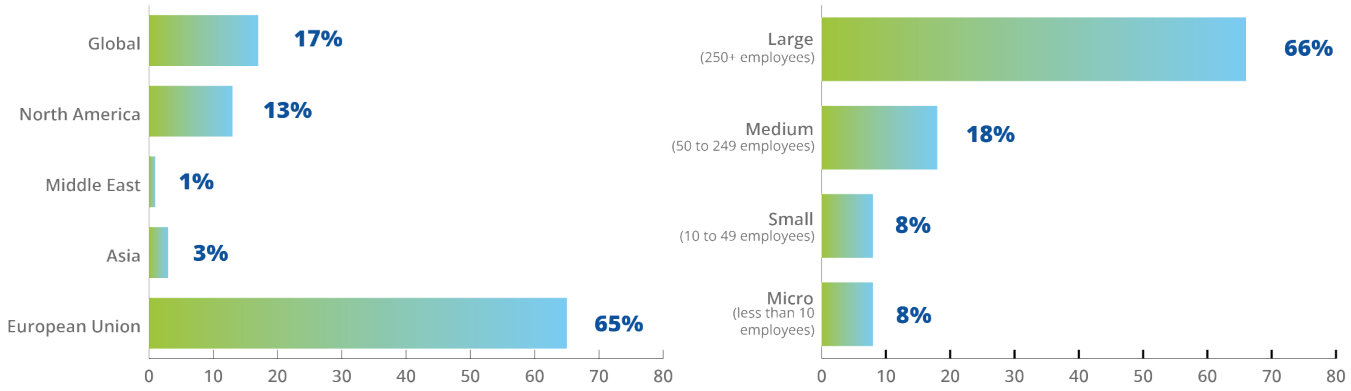


Figure 2: Geographical spread and organisation size

Regarding geographical representation, 65 % of the respondents operate mainly within the EU, while 17 % are global operators, 13 % are North American and only 4 % are from Asia and the Middle East.

Regarding sector representation, the IT and manufacturing sector represents 54 % of the responses, while more specific sectors (automotive, healthcare, financial, energy and telecommunications) represent lower percentages that do not exceed 35 % collectively.

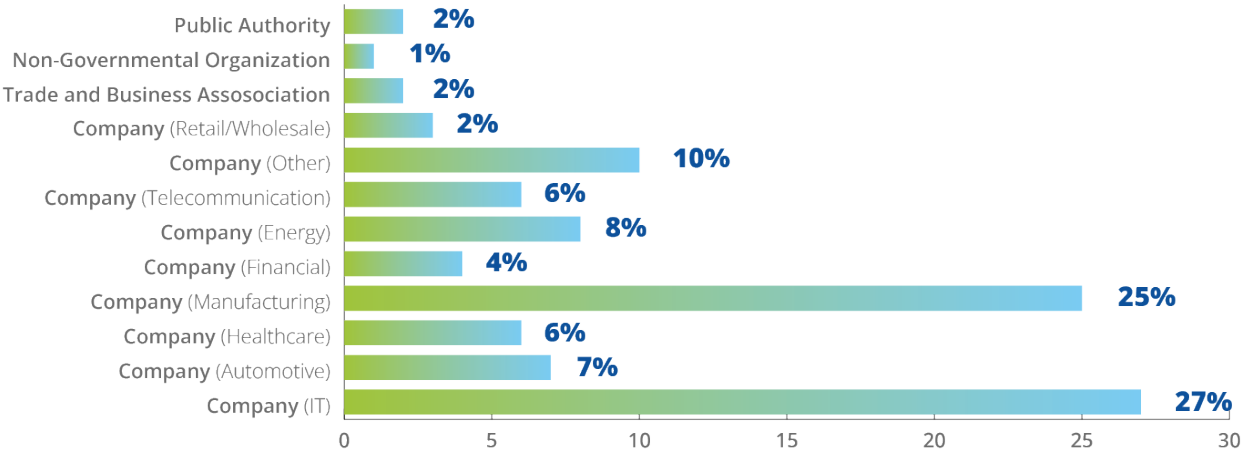


Figure 3: Type of organisation

2.2 CRA Applicability, Awareness, Exposure and Investments

To establish a baseline understanding of how the CRA influences organisations across the EU ecosystem, we asked the respondents if and how the regulation is impacting their organisations. This question serves as an indicator of awareness and perceived applicability which can determine future activities to support the organisations based on their needs. By grouping the responses based on organisation size, we can identify the scope and target audience of the CRA while also obtaining an initial indication of anticipated maturity levels.

An interesting finding is that 80 % of small enterprises were directly impacted by the CRA either because they place products on the EU market or because they supply components to manufacturers. However, the focus mainly shifts towards the readiness journey of microenterprises, as 23 % of the respondents were either unsure if the CRA impacts their organisation or are currently exploring.

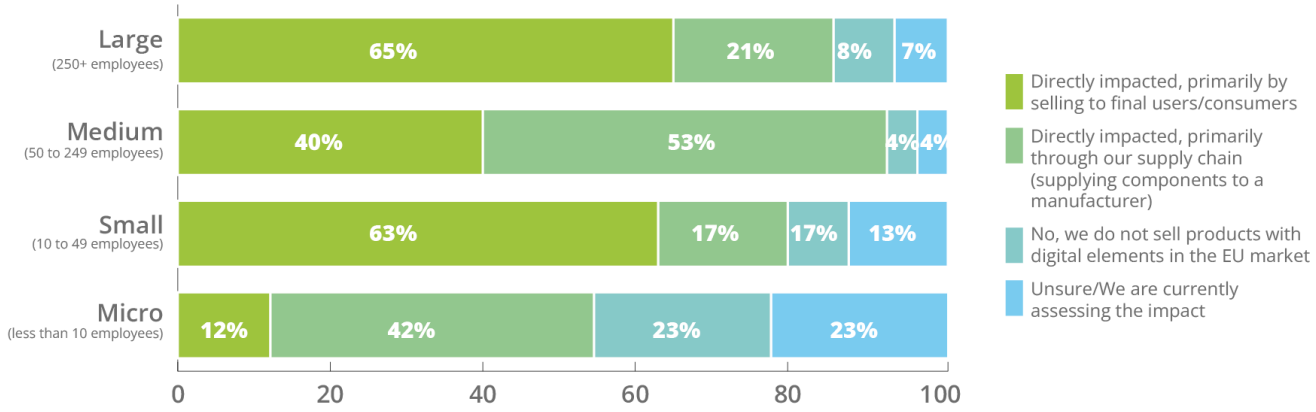


Figure 4: Envisioned CRA impact based on organisation size

In assessing organisations' awareness of the CRA obligations related to SBOM, 87 % of the large enterprises provided a positive answer, while 13 % remain unaware. Nearly all medium-sized enterprises confirmed their awareness, whereas for 26 % of small enterprises still unclear.

Even though the results indicate a high level of awareness, it is important to acknowledge that there is still room for improvement for organisations of all sizes.

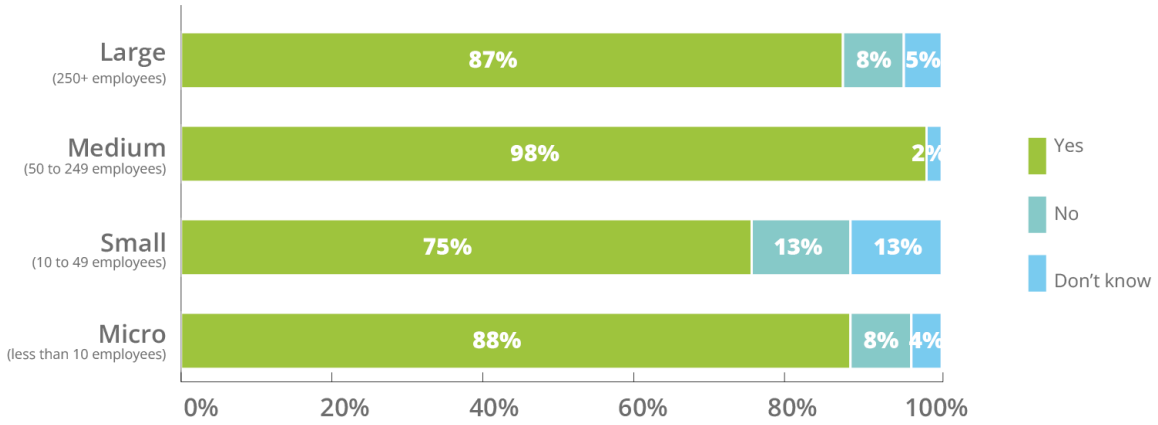


Figure 5: Awareness of CRA obligations related to SBOMs

To better understand the relationship between organisational awareness and regulatory exposure, the survey examined how the respondents' familiarity with SBOMs correlates with their perception of the CRA's applicability to their organisation. This comparison provides insight into whether organisations that fall within the CRA's anticipated scope are also developing the foundational awareness needed to operationalise these practices. The following results illustrate how SBOM familiarity varies depending on perceived CRA applicability, highlighting potential readiness gaps across the ecosystem.

While there is a **broad familiarity** with the concept of SBOM, varying from somewhat familiar to very familiar, most organisations which are unsure or currently assessing the impact of the CRA **have never heard about SBOM before.**

Noticeably, 33 % of those who answered that they have never heard about SBOM before also responded that their organisation is directly impacted by the CRA because it places products with digital elements on the EU market. This finding aligns with the high percentage (80 %) of organisations that report only recently hearing about SBOM yet also fall into the category of directly impacted organisations because they sell products with digital elements to end users.

Another finding is that among organisations which are still unsure or actively assessing if they are impacted by the CRA, a vast majority (67 %) reported never having heard about SBOM before, while 13 % had only recently become aware of it.

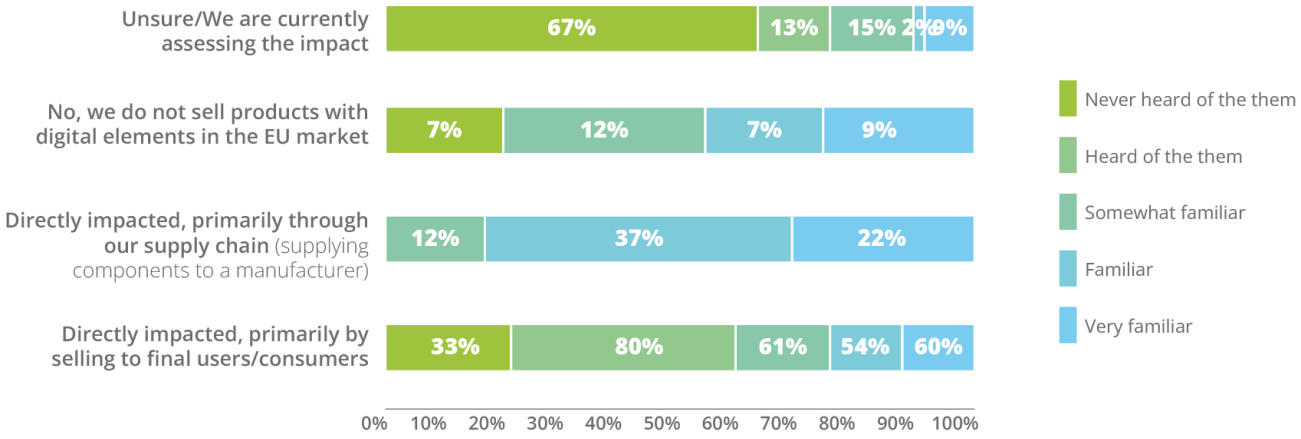


Figure 6: SBOM familiarity based on envisioned CRA impact

In another effort to fully understand the impact of the CRA on organisations that fall under its scope, it is important to assess the financial impact and investment trends related to the implementation of its requirements. Using the SBOM requirement as a focal point, we asked the respondents to indicate if their organisation's decision to invest in SBOM tooling and automation was influenced by the CRA.

Almost half of the respondents (43 %) indicated that the CRA has **'significantly accelerated' their investment in SBOM tooling and automation**, while an additional 29 % indicated a 'moderate influence'.

While, as depicted in Figure 7, almost 20 % indicated that the CRA itself did not play a role in the investment, it is worth highlighting the impact that the regulation has had on software development security.

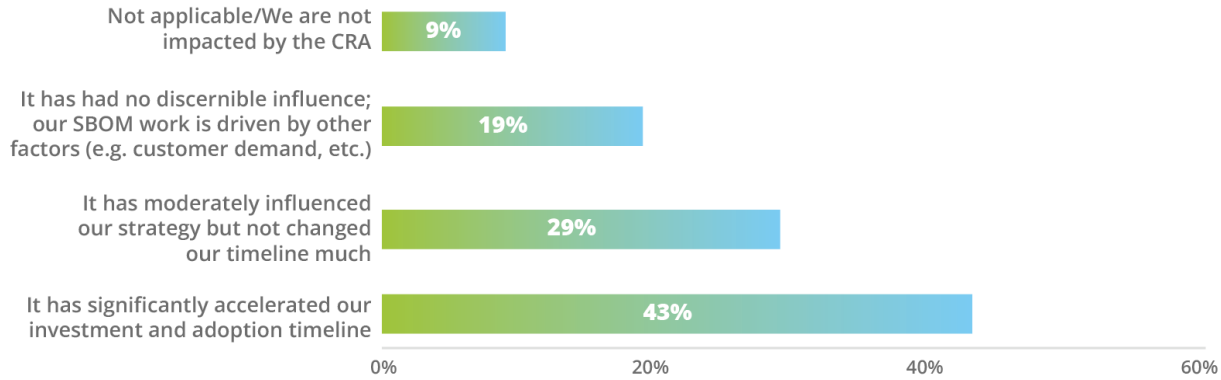


Figure 7: CRA influence on SBOM tooling and automation investments

This increase in investment seems to also have an impact on the expected timeline to meet the target SBOM maturity level required by the CRA, as reported by the respondents. As illustrated in Figure 8, 33 % of the respondents estimate they will reach the envisioned maturity level within 12 months (end of 2026), while 24 % anticipate requiring an additional six months. Meanwhile, 30 % indicated that they will require two years or more to reach this level, and 12 % were unable to provide an estimate.

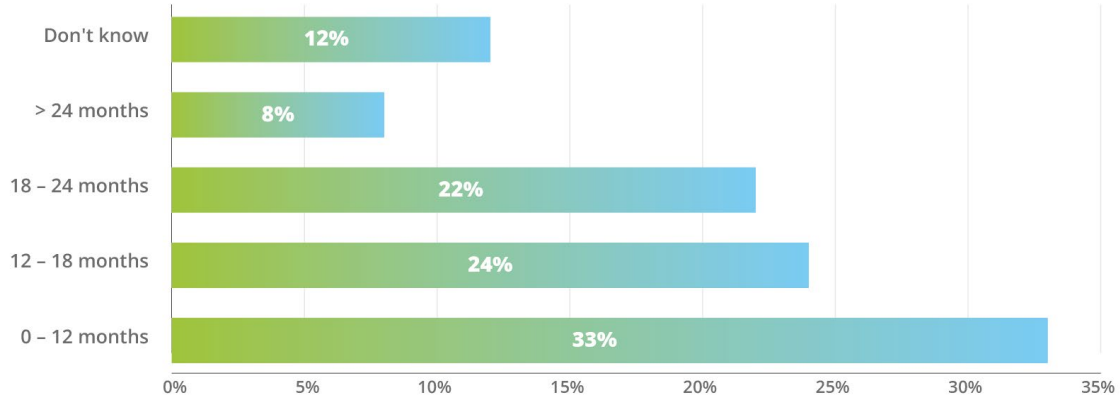


Figure 8: Estimated time required to meet the target SBOM maturity level required by the CRA

Investment decisions cannot only be supported by regulatory requirements if the end goal is to increase maturity and strengthen cyber resilience across the EU market. Implementors need to identify the value of these requirements. SBOMs could provide significant value in various use cases, security-related processes and business activities, but where do organisations obtain the greatest measurable value using SBOM?

Almost 37 % of the respondents acknowledged quite a lot of added value in **risk reduction and cost avoidance**, 29 % believed that SBOM adds quite a lot of value in **operational efficiency**, 26 % believed that SBOM will slightly add value to meeting **contractual requirements** and gaining a competitive edge in bids, while almost 26 % believed that SBOM will add quite a lot of value in making **compliance and audit processes** easier.

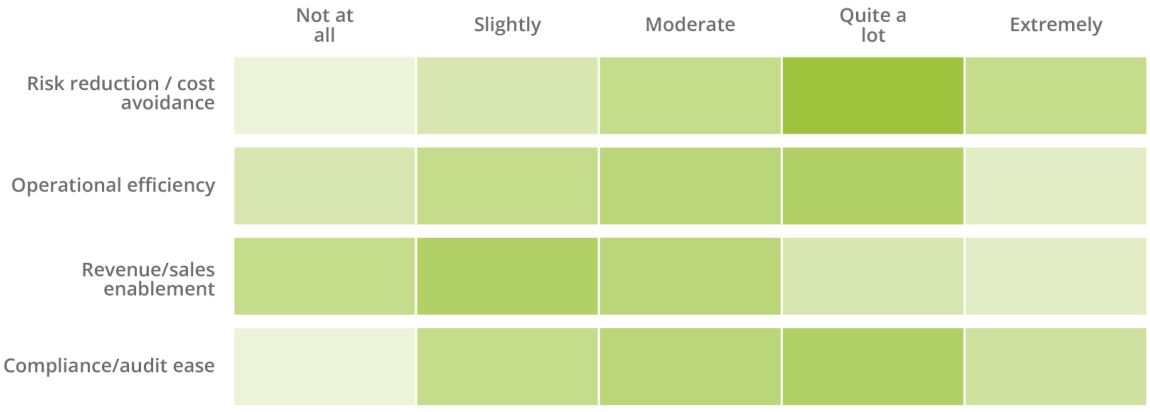


Figure 9: Envisioned value of using SBOMs

2.3 Supply Chain Security

Exploring the key concerns about supply chain security and its impact on the financial decision-making of the organisations, the survey included questions on how concerned the organisations are about supply chain security and how they allocate resources (budget, staff or tooling) to manage the security of the software that they use.

While there is broad acknowledgement that **supply chain security matters**, there is a gap in **how this risk is addressed in terms of allocated budget**. Noticeably, respondents with minimal to no concern dominate the limited investment space.

More than 90 % of respondents indicated they are concerned about the security of their supply chain; almost 60 % of them were very or extremely concerned. However, only 34 % of the respondents allocated significant or extensive resources to manage the security of the software they use.

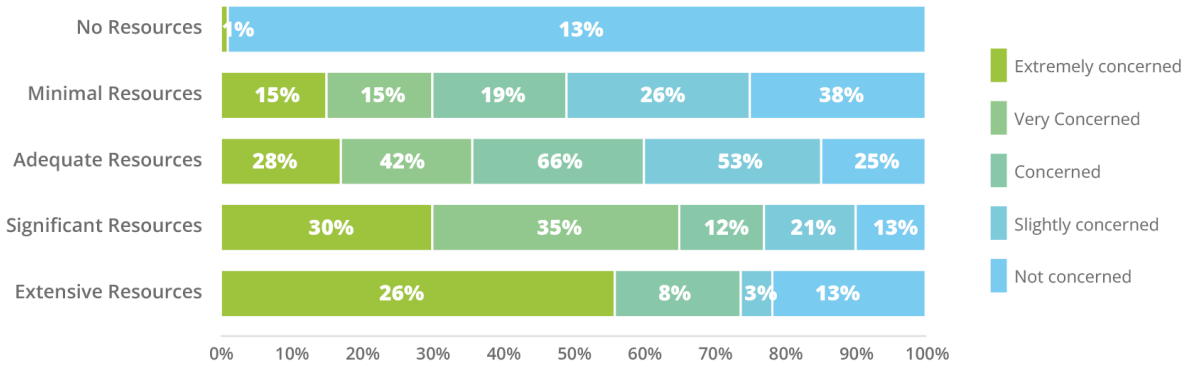


Figure 10: Cybersecurity resources allocated to address concerns about supply chain security

To establish a better understanding of how organisations address supply chain security, we asked respondents to prioritise the most important activities for their organisations. The following heat map shows that the 1st priority with the most votes is **secure development practices**, with **vulnerability reporting** coming second and **SBOM** third. The prioritisation of the activities based on their importance can be easily interpreted based on the current practices of the industry and the regulatory requirements that have accelerated the standardisation of such activities.

It is important to highlight that 53 % of the respondents placed **SBOM in their top three most important activities**. SBOM is directly connected with both of the other two activities as it enables visibility of the software components, libraries and dependencies as well as monitoring license compliance, thus promoting secure software development practices while also providing targeted input for vulnerability reporting. This constitutes a major enabler for the broad adoption of SBOM generation and consumption.

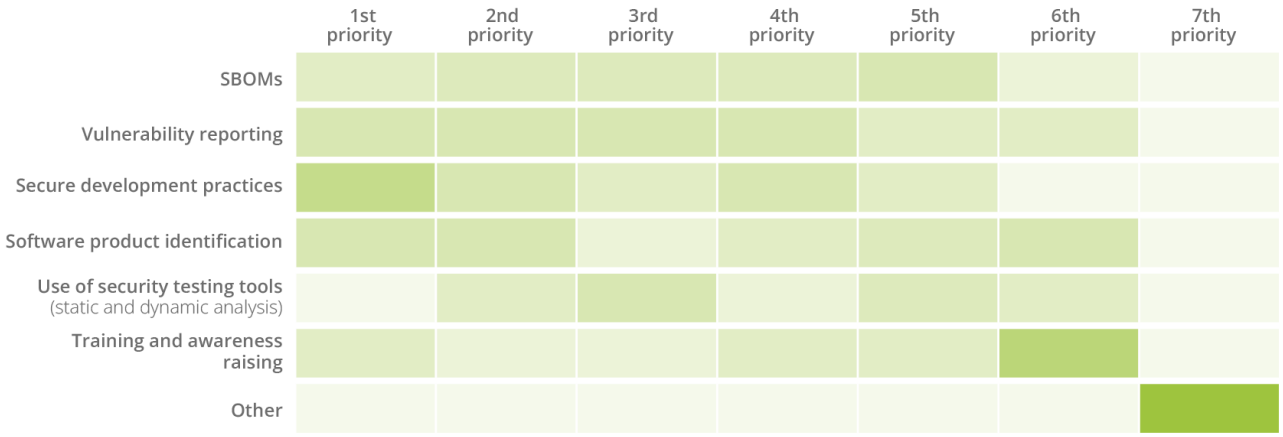


Figure 11: Elements envisioned to improve supply chain security

2.4 SBOM Specifics

2.4.1 Adoption Readiness

This section discusses organisational readiness in relation to the level of SBOM adoption, engagement and perception. The aim of this subject area is to understand the SBOM adoption journey of different types of organisations and how this is influenced by their size. The preliminary findings show how SBOMs are processed, highlighting the main barriers and the expected external support required to proceed with their implementation.

In Figure 12, based on the overall rating, we can identify that 78 % of the respondents reported that their organisations **have already initiated their SBOM adoption journey**, with 44 % currently being in the pilot or limited adoption phase. Only 9 % have reached **a mature level of implementation, supported fully by automation**, while 25 % stated that SBOMs are **broadly adopted in their products**.

An interesting finding has emerged at this point: microenterprises and small enterprises – representing 23 % and 25 %, respectively – have already reached a mature level of adoption. This contrasts sharply with medium-sized and large enterprises, which follow at much lower rates of 4 % and 6 %, respectively.

Assessing the overall outcome, medium-sized enterprises appear to lead the way, as the value for ‘Not yet started’ is 0 %.

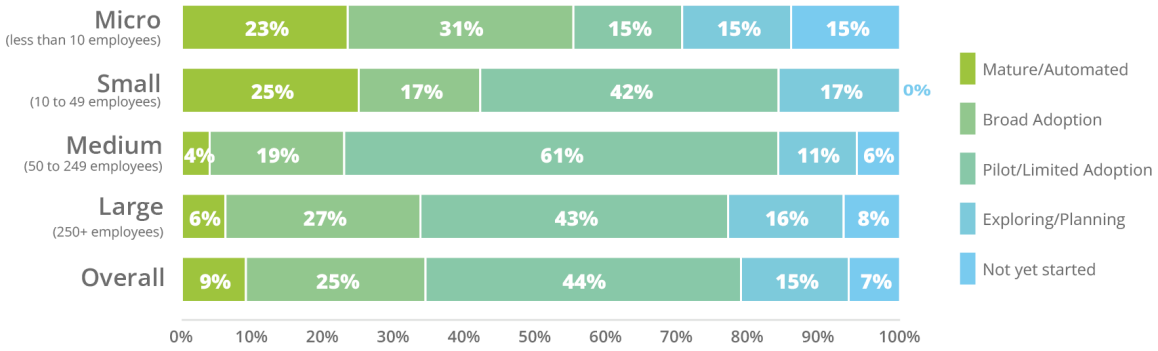


Figure 12: Level of SBOM adoption based on organisation size

To understand better how the SBOM journey translates into operational activities, the respondents were asked to indicate how their organisations engage with SBOMs. Across all organisation sizes, the most popular answer was **producing SBOMs for their own software**. For small, medium-sized and large organisations, the second most popular manner of engagement was consuming SBOMs from their vendors or partners, whereas for microenterprises it was providing SBOM tools, solutions and/or integration services.

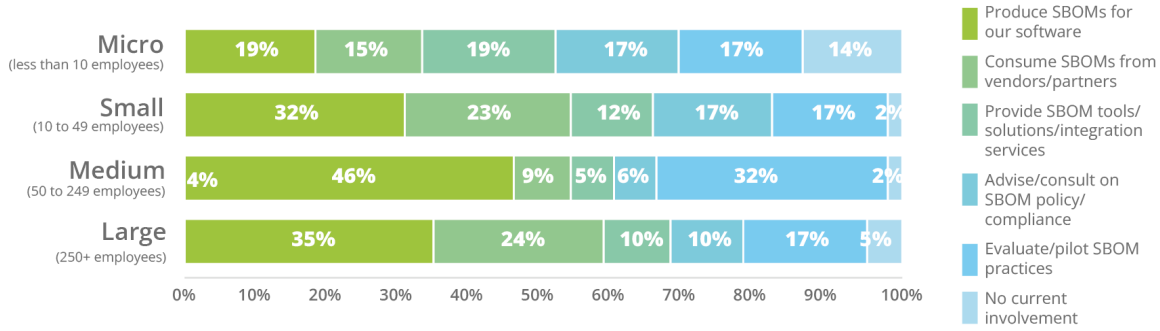


Figure 13: Engagement with SBOMs based on organisation size

Regarding the respondents' perception of SBOMs, the replies vary slightly depending on the size of the organisation. Overall, 28 % of respondents perceived SBOMs as a **mandatory burden**, which reveals a rather compliance-oriented approach, especially in large organisations where the percentage goes up to 36 %.

Regardless of the size of the organisation, SBOMs are prominently considered. Overall, by 42 % of respondents as a **'defensive necessity'** (i.e., a vulnerability management approach), by 20 % as a **'neutral inventory instrument'** and by 10 % as a **'competitive asset'.**

This dual perception highlights an important transition phase within the ecosystem; while organisations recognise the technical value of SBOMs, many still associate their implementation with compliance pressure.

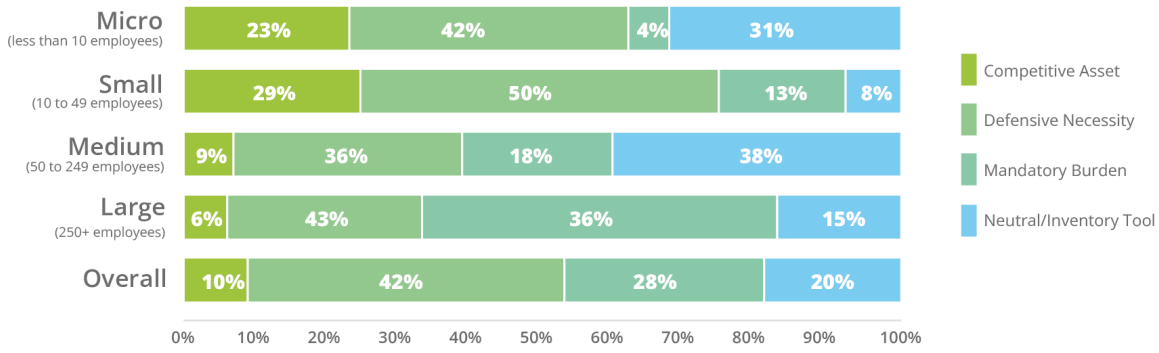


Figure 14: Perception of SBOMs based on organisation size

To have a more holistic perception of the status of SBOM adoption, it is crucial to understand the impediments that the organisations face throughout this process. The respondents were asked to assess the impacts of a variety of factors. The most commonly faced obstacle affecting them extremely is the **lack of supplier/third-party SBOM availability and/or quality**. Following closely is **vulnerability matching (CPE/PURL alignment, false positives)**, with almost two thirds of the organisations being affected extremely or quite a lot, and **data quality (incomplete components, identifiers, licences)**.

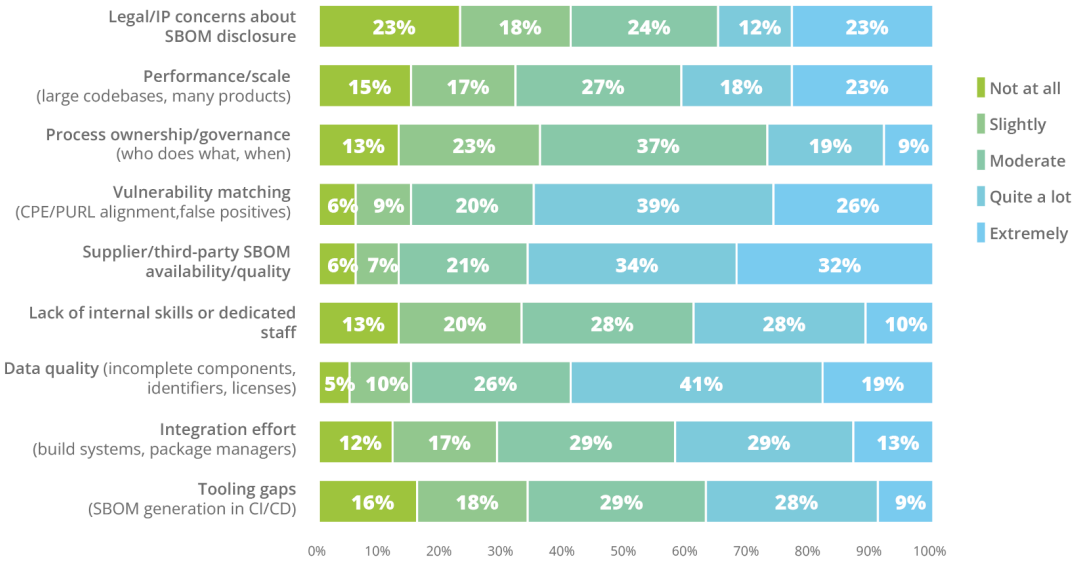


Figure 15: Main barriers to adopting SBOMs

To overcome these barriers and accelerate SBOM adoption, the respondents have indicated the type of external support they wish to receive.

26 % of the organisations suggested that a **reference implementation providing the pipelines in a public repository** would be beneficial. 22 % would find it helpful to have a **guide navigating the process of tool selection** based on evaluations and benchmarking, while 18 % would prefer a suite providing **conformance tests** with check points and validators.

All three activities indicated a need for **technical guidance and support**.

Figure 16 presents the respondents' preferences regarding all the activities defined as external support.

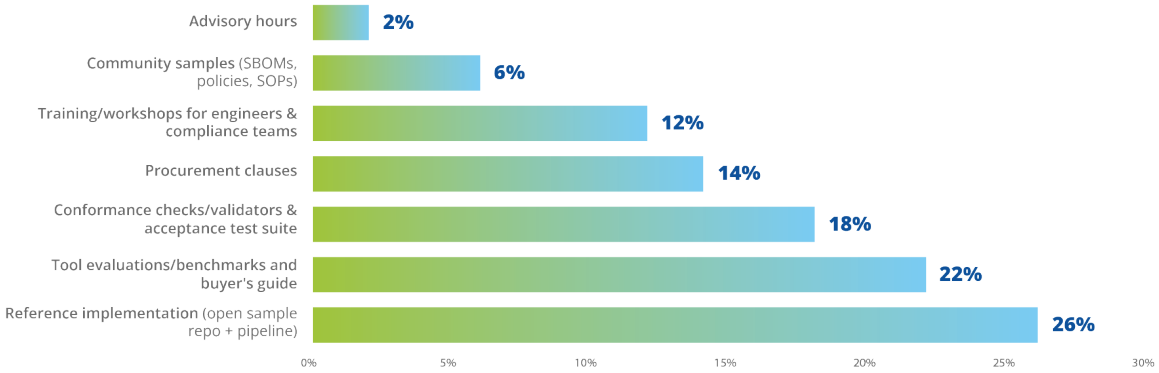


Figure 16: External support elements envisioned to accelerate SBOM adoption

2.4.2 Formats, Tools and Lifecycle Integration

CycloneDX is indicated as the predominant SBOM format, with 44 %, while **Software Package Data Exchange** follows with 29 %. Interestingly, 11 % of the respondents indicated that they do not use a standard format and the remaining 17 % still use a **proprietary format**.

This result comes even though the CRA stipulates the use of 'a commonly used and machine-readable format' under Annex I, Part II ('Vulnerability handling requirements') and the Technical guideline BSI TR-03183-2 ([2]) indicates that 'newly generated or updated SBOM must be in JSON- or XML-format and a valid SBOM according to CycloneDX, version 1.6 or higher [or] System Package Data Exchange (SPDX), version 3.0.1 or higher'.

It is worth highlighting that 28 % of the respondents represent a **possible interoperability barrier** at the EU market.

([2]) Technical guideline BSI TR-03183: Cyber resilience requirements for manufacturers and products – Part 2: Software bill of materials (SBOM), available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03183/BSI-TR-03183-2_v2_1_0.pdf?__blob=publicationFile&v=5.

Figure 17: Types of SBOM format currently in use

Despite 33 % of overall SBOM generation relying on **open-source tools**, large and medium organisations rely a lot on **commercial and proprietary tools** as well. Interestingly though, reliance on manual processes across all company sizes sits at around 11 % overall, however in microenterprises it goes up to 16 %, introducing an additional hurdle since the CRA aims to provide security throughout the lifetime of products. 10 % of the respondents do not generate SBOMs at all.

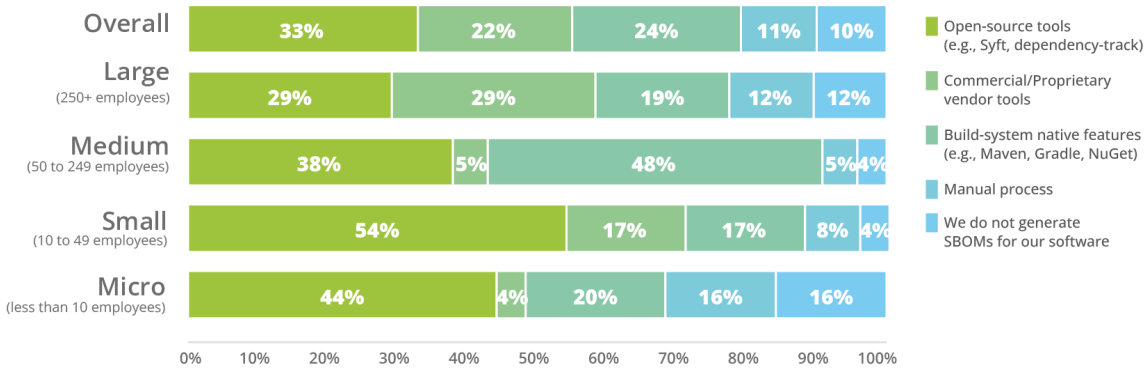


Figure 18: SBOM generation tooling based on organisation size

Knowing when organisations are producing SBOMs in the Software Development Lifecycle provides valuable insights on the accuracy, trustworthiness and usefulness of SBOM data for vulnerability management, incident response and regulatory assurance. 39 % of the organisations reported that they produce SBOMs during software builds, 16 % during software delivery to an artifact registry or repository and 14 % during software deployment.

As the majority of organisations opt for **build-time SBOM generation**, it is safe to assume that they use them as an operational benefit, which also supports software supply chain trust.

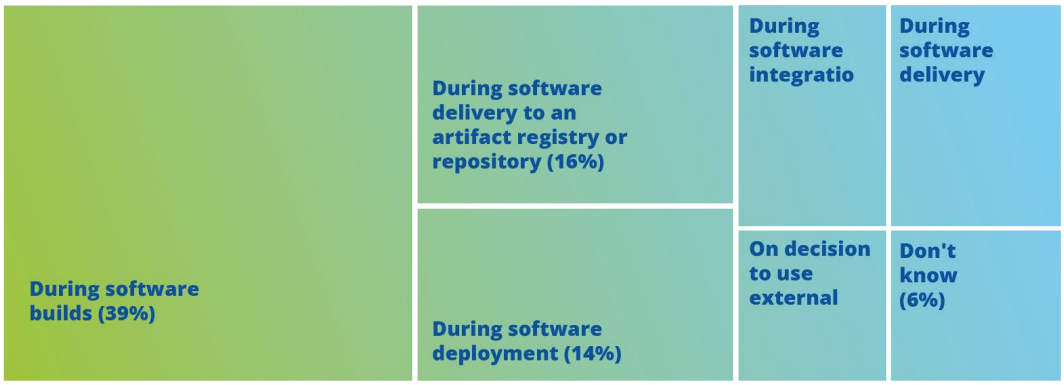


Figure 19: SBOM production in Software Development Lifecycle (SDLC)

Following the same notion, the timing of SBOM consumption indicates if they are used proactively to prevent risks or reactively to detect and manage them after integration or deployment. 16 % reported that they consume SBOMs **during software builds**, 15 % **during software integration** and 14 % during the **decision-making process** determining if an external software is going to be used. Noticeably, the majority of the respondents don't know if or how the SBOMs are consumed in their organisation.

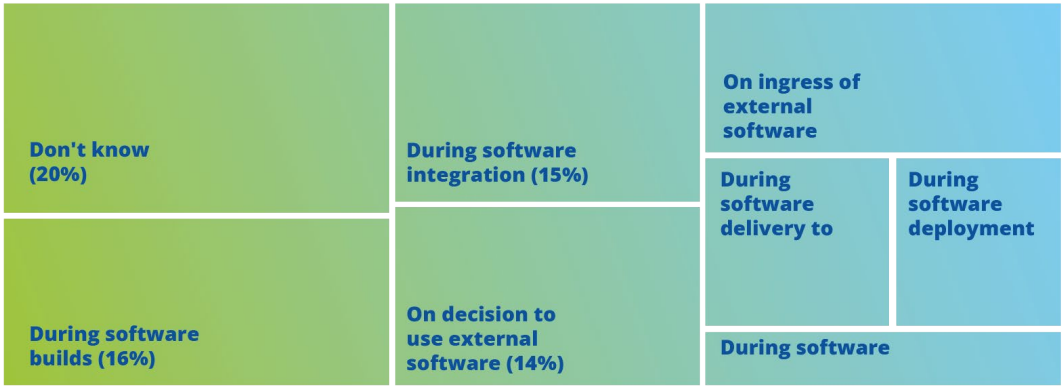


Figure 20: SBOM consumption during Software Development Lifecycle (SDLC)

Currently, SBOM generation and consumption spans all levels of organisational readiness. Fully automated implementation across each phase of the SBOM life cycle is the end goal for achieving maturity and reliability.

During this period of transition, **74 % of respondents reported that they have partially or fully automated SBOM generation for each release/build**, 59 % have partially or fully automated the SBOM minimum content (only top-level dependencies) in machine-readable format (SPDX/ CycloneDX), **51 % have partially or fully automated the vulnerability handling workflow tied to SBOM**, 52 % have partially or fully automated SBOM updates for the product support period and 39 % have partially or fully automated the inclusion of SBOM in their technical documentation.

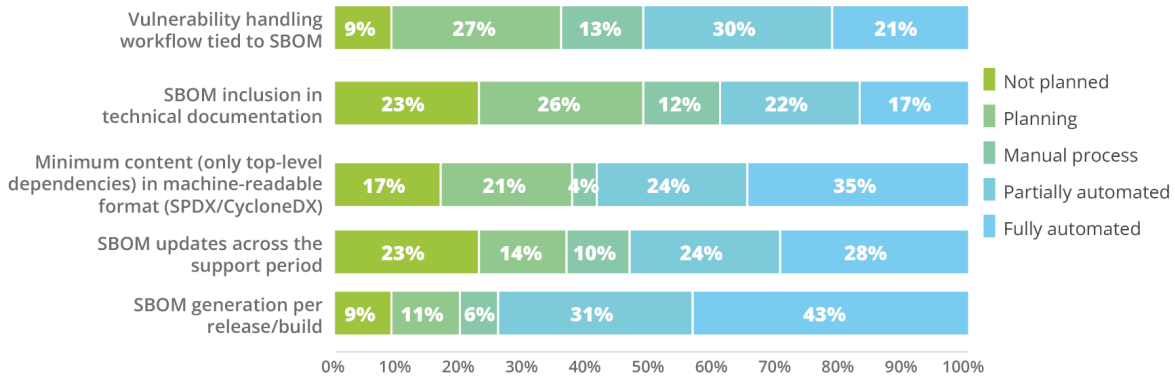


Figure 21: SBOM automation level across different stages

Regarding commercial off-the-self software (COTS) products purchased by organisations, we asked the respondents to indicate how often they receive SBOMs from the manufacturers that they collaborate with.

Overall, the vast majority of the responses were **'Rarely'** and **'Never'.** 39 % of all organisations responded 'Never', 39 % 'Rarely', whereas only 2 % answered 'Always', implying that they have standardised this practice as an official process.

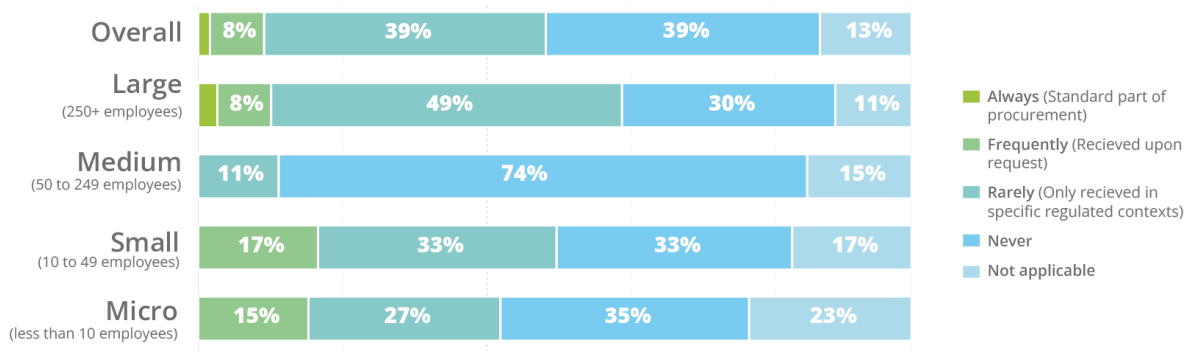


Figure 22: COTS and SBOM based on organisation size

2.4.3 Usage Patterns and Gaps

SBOM depth is crucial to determine if an organisation is effectively identifying risks in transitive dependencies, build components and runtime environments. Figure 23 presents the level of SBOM depth that organisations need versus what they receive.

A **big gap** between the need and actual result has been identified:
36 % of respondents stated that their organisations **need all primary components and direct dependencies with declared known unknowns** but only 29 % actually receive them, 24 % of the organisations **need SBOMs with full depth analysis** but only 14 % receive them, while 27 % require **SBOMs with depth analysis including declared known unknows** and only 12 % receive them.

Besides the gap between the organisational needs and how they are addressed, it is important to highlight the percentage of respondents who stated that they do not know what SBOM depth their organisation needs versus what they receive.

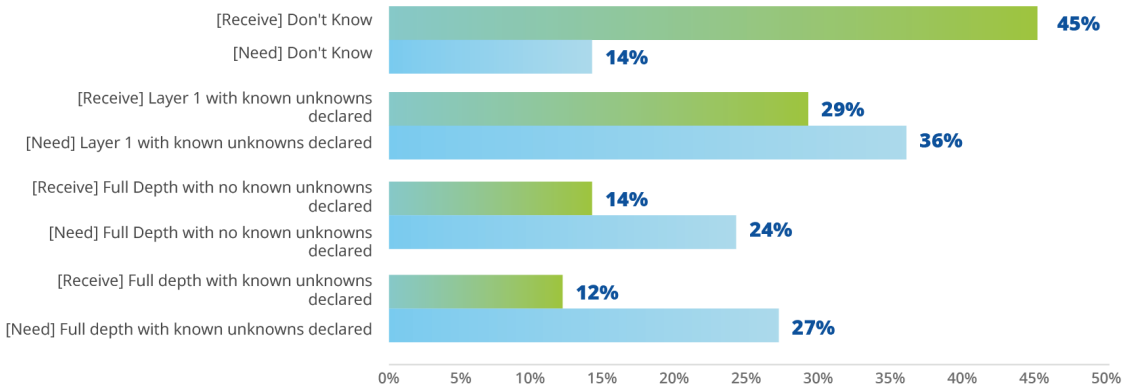


Figure 23: Level of SBOM depth needed and received

The information provided by the SBOMs based on their depth was primarily used for the **identification and patching of vulnerabilities** by 29 % of the organisations, for ensuring **open-source licences (OSS)** are correctly used/declared by 22 %, for meeting **regulatory requirements** by 19 %, for evaluating **third-party software risks** by 14 % and for maintaining an **up-to-date inventory** of all components by 13 %.

As depicted in the following figure, the respondents indicated that the primary stakeholders of SBOM consumption were the **security and application security teams** (34 %) and the **development and engineering teams** (34 %). The **legal/compliance teams** and **procurement teams** made limited use of SBOM information, with only 15 % and 5 % of the organisations, respectively, stating that these teams consume SBOM.

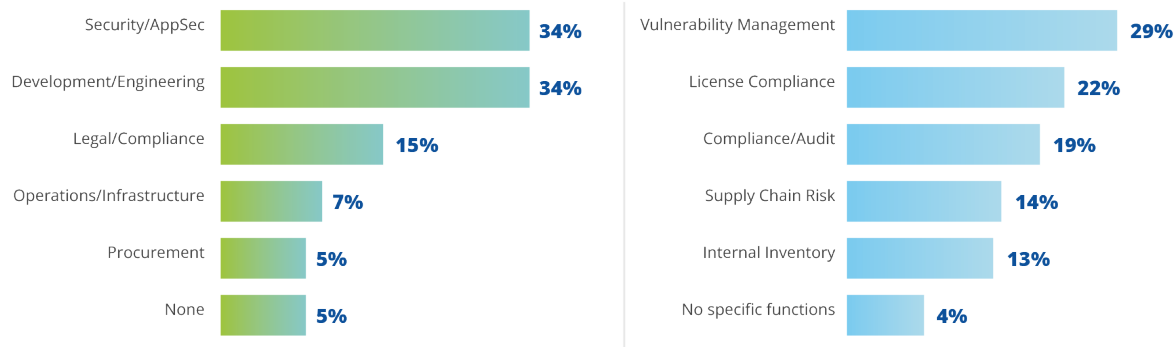


Figure 24: Primary use of SBOMs generated or received

As shown in Figure 25, 44 % of respondents reported a ‘moderate gap’ between generating SBOMs and utilising them while 23 % reported a ‘significant gap’. Only 7 % have closed the gap

entirely, which indicates that **SBOMs are not actively used to their full extent** for security but instead mainly for compliance purposes.

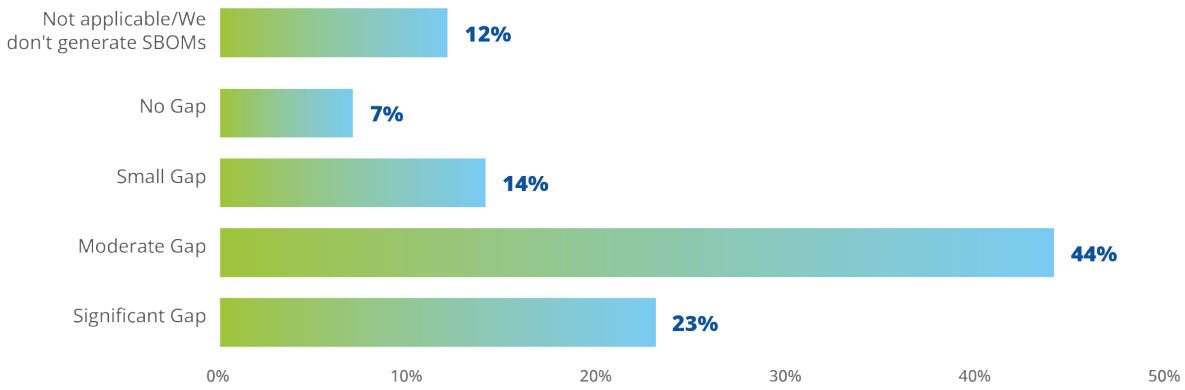


Figure 25: Gap in generating and consuming SBOMs

In an effort to close this gap, organisations are strategically investing in SBOM tooling and automation. The survey results show that 34 % of the organisations have invested in tools dedicated to **vulnerability handling via SBOM**, 21 % **in automating the inclusion of SBOM in the product's technical documentation** for market surveillance authorities, 19 % in tooling **generating SBOM** for all primary components with all transitive dependencies and their metadata (achieving full completeness) in a machine-readable format and another 19 % in **automating the continuous update of SBOMs** throughout the product's support period.

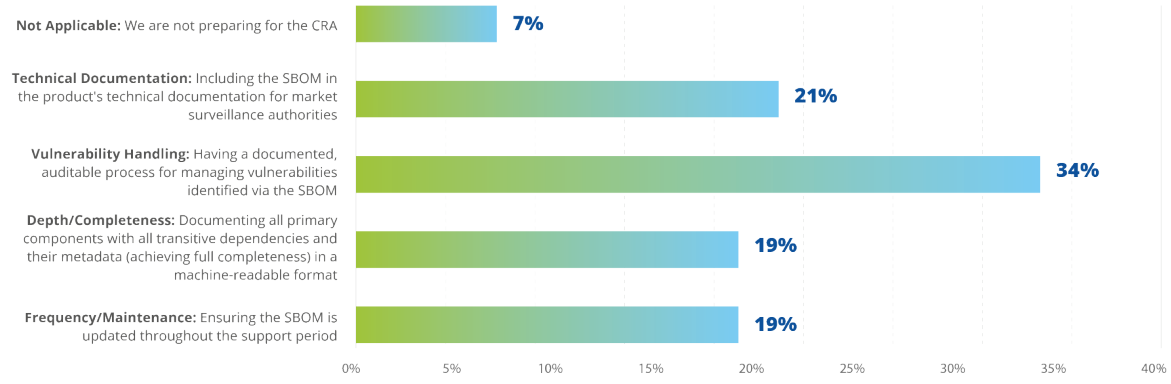


Figure 26: SBOM tooling and automation investment

Based on the identified gaps and investment strategies among the organisations, the envisioned approach to SBOM handling is depicted in Figure 27. 41 % of the organisations reported that they aim to **fully automate SBOM generation for each release/build**. Only 26 % of respondents believed that their organisations will **fully automate SBOM updates across the product support period** and almost 23 % believed that their organisations will **partially automate this process**. A concerning result is that almost 32 % believed that their organisations will automate the SBOM minimum content in machine-readable format while almost 22 % believed that their organisations will partially automate this process. This raises concerns about the quality, accuracy and usefulness of SBOMs. What comes as a surprise, though, is that most organisations are

planning to partially automate vulnerability handling workflows tied to SBOM, raising concerns about the ability to efficiently identify hidden risks in the software components.

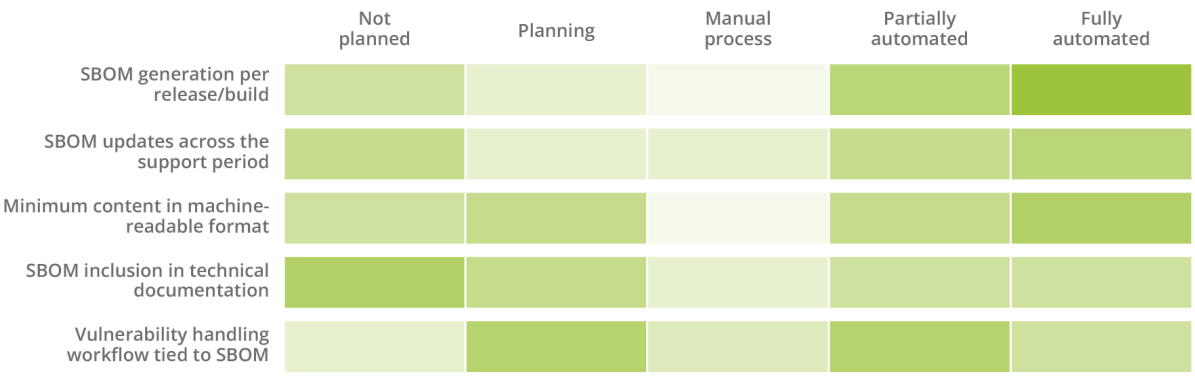


Figure 27: Envisioned approach to SBOM handling

To interpret the envisioned approach to SBOM handling, we need to understand the current challenges that organisations are facing.

Figure 28 presents the challenges in leveraging SBOMs today.

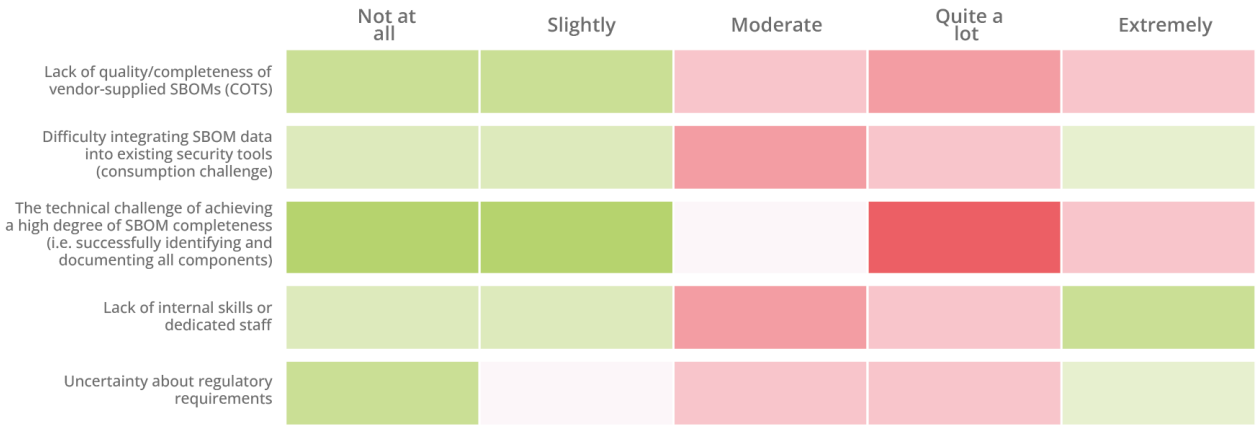


Figure 28: Current challenges in leveraging SBOMs

When asked about the technical challenge of achieving a high degree of **SBOM completeness**, 62 % of the respondents answered with quite a lot or extremely difficult. At the same time, when asked about the **lack of quality and complete vendor-supplied SBOMs**, 30 % of respondents answered with quite a lot and 27 % with extremely. When asked about the **lack of internal skills or dedicated staff**, respondents answered with moderate (29 %) or quite a lot (28 %).

2.4.4 Barriers, Needs and External Supports

Diving deeper into the main barriers that prevent organisations from adopting SBOMs at scale, the respondents were asked to rate the challenges presented in

Figure 29. As shown in the heat map, **data quality** (37 %), **supplier/third-party SBOM availability/quality** (31 % quite a lot and 30 % extremely), **vulnerability matching** (35 % quite a lot and 23 % extremely) and **process ownership/governance** (33 % moderate) were rated as the main barriers that could jeopardise the broad adoption of SBOM across organisations.

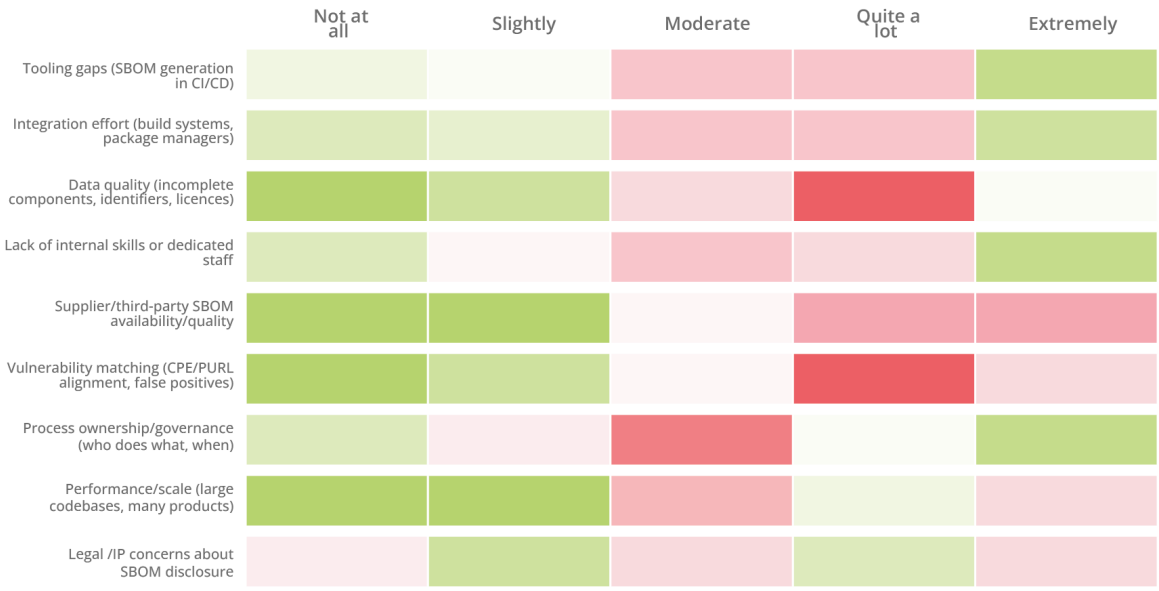


Figure 29: SBOM adoption barriers

Solely identifying the main barriers is not enough, so the respondents needed to provide their opinion on what would be useful to their organisations to improve their ability to produce and/or consume SBOMs.

Industry consensus on best practices to integrate producing/consuming SBOMs **into software development practices** was deemed the most critical (23 %), followed by industry consensus on best practices to integrate producing/consuming SBOMs into **risk and compliance processes** (19 %) and industry consensus on **how to produce/consume SBOMs** and how these methods will evolve /improve over time (19 %).

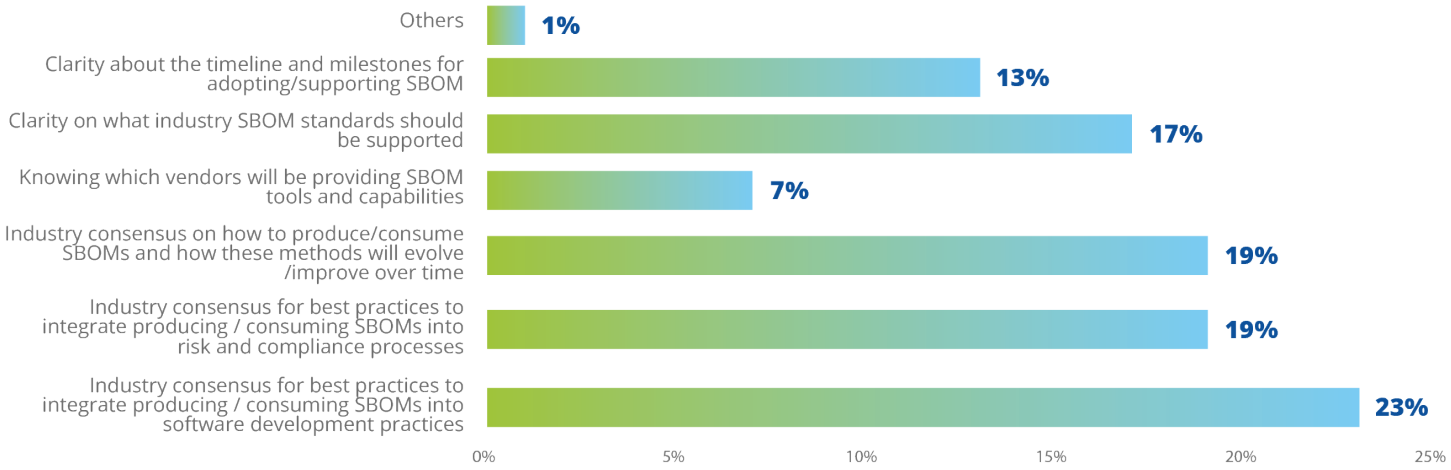


Figure 30: Elements improving the ability to produce or consume SBOMs

2.4.5 Vulnerability Management

Receiving vulnerability status or exploitability claims from suppliers was rated 'critical' by 39 % and 'important' by 37 % of respondents, as shown in Figure 31. Together, this accounts for 76 % of respondents, underscoring the significance of the coordinated vulnerability disclosure approach outlined in the CRA.

As depicted in Figure 32, their preferred options for receiving such claims were automatically (44 %) or via a standardised application programming interface (API) (40 %).

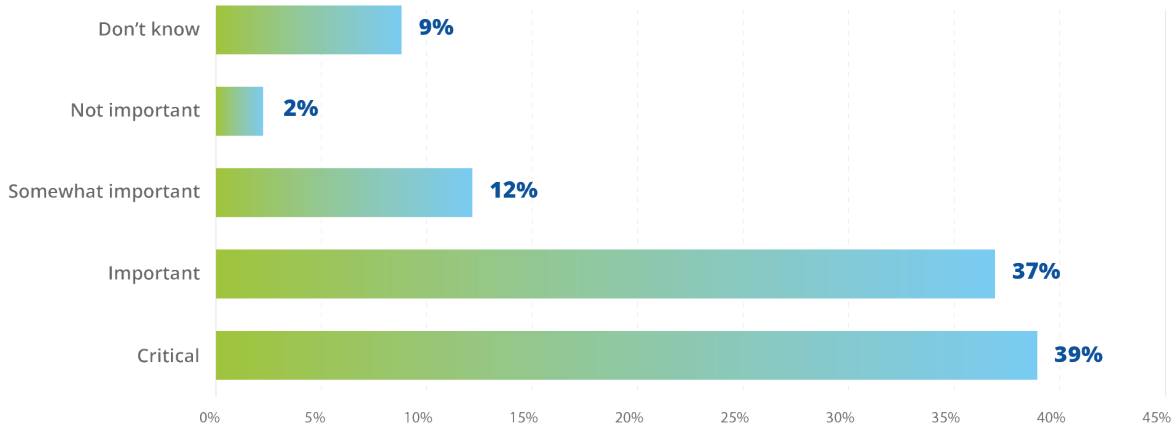


Figure 31: Importance of receiving vulnerability status from suppliers

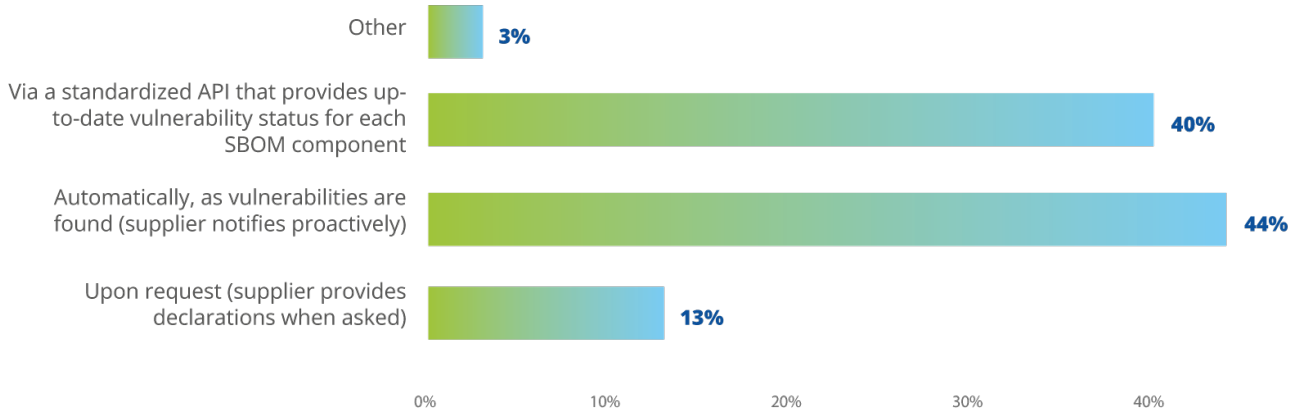


Figure 32: Preferred methods for receiving vulnerability claims from suppliers

2.4.6 Interoperability Requirements

SBOM interoperability was rated 'critical' by 30 % and 'important' by 39 % of the respondents.

As shown in Figure **34**, their preferred options to ensure delivery and interoperability were through **machine interfaces** (32 %) and by **supporting the conversion and compatibility between formats** (30 %).

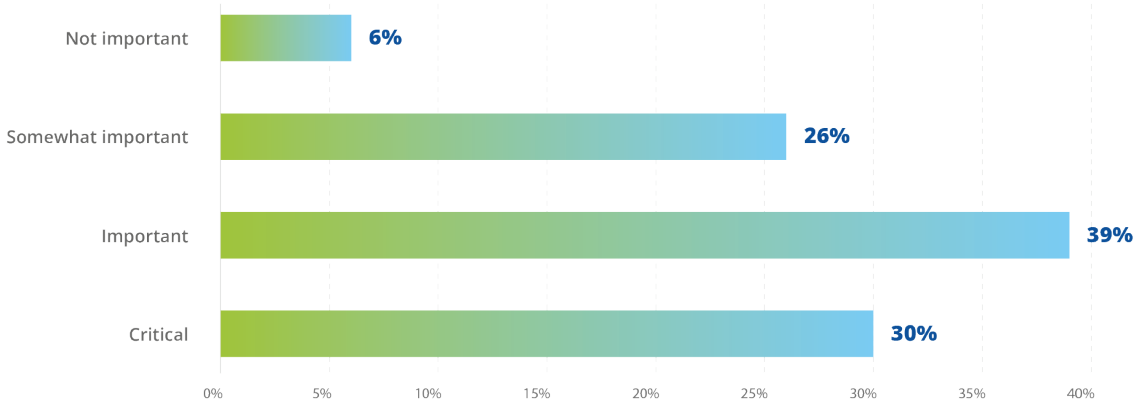


Figure 33: SBOM interoperability importance

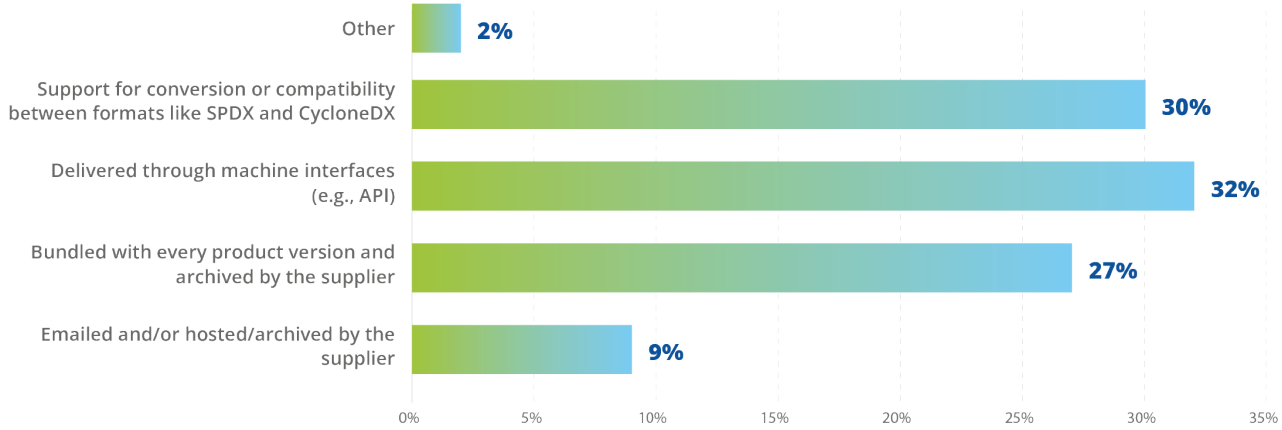


Figure 34: Preferred SBOM delivery or interoperability methods

2.4.7 Supplier Requirements (for SBOM consumers)

Only 10 % of respondents reported that their organisation had established **mandatory SBOM requirements within supplier contracts**. Assessing the overall responses, company size does not appear to significantly influence the adoption of this practice, as the reported percentages remain broadly consistent across organisation sizes, with the exception of medium-sized enterprises.

It is essential though to highlight that 55 % of the respondents were in the process of **including SBOM requirements in their supplier contracts** in a systematic and consistent manner. 37 % indicated that they already include them in an ad hoc manner, while 27 % were planning to include them.

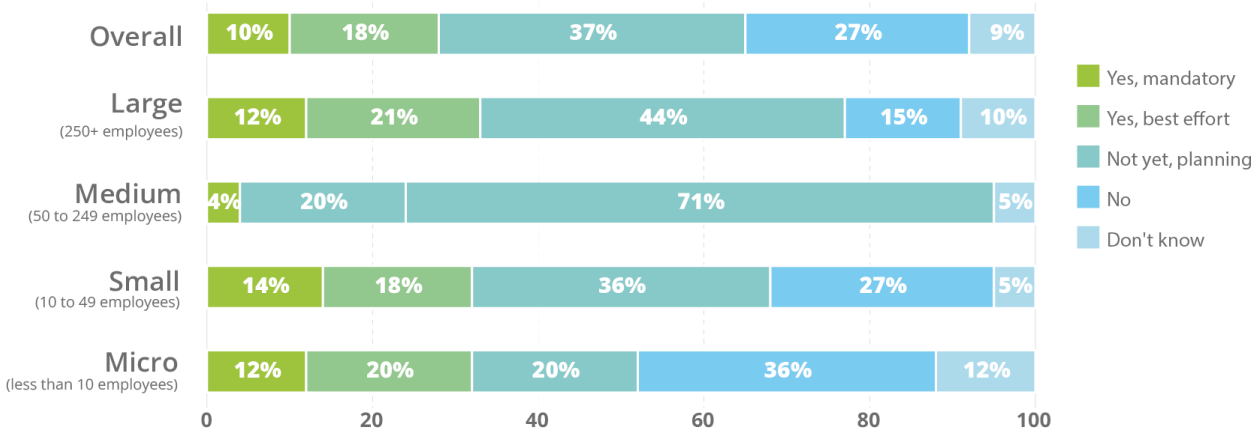


Figure 35: SBOM requirements in contracts

Incorporating SBOM requirements into contractual obligations can significantly **expand the pool of suppliers that align with the expectations of organisations**. 45 % of organisations reported that only 0 % to 25 % of their suppliers meet their requirements, while just 2 % indicated that 75 % to 100 % of their suppliers meet these expectations. This highlights a substantial gap in supplier readiness that contractual SBOM requirements could help improve.

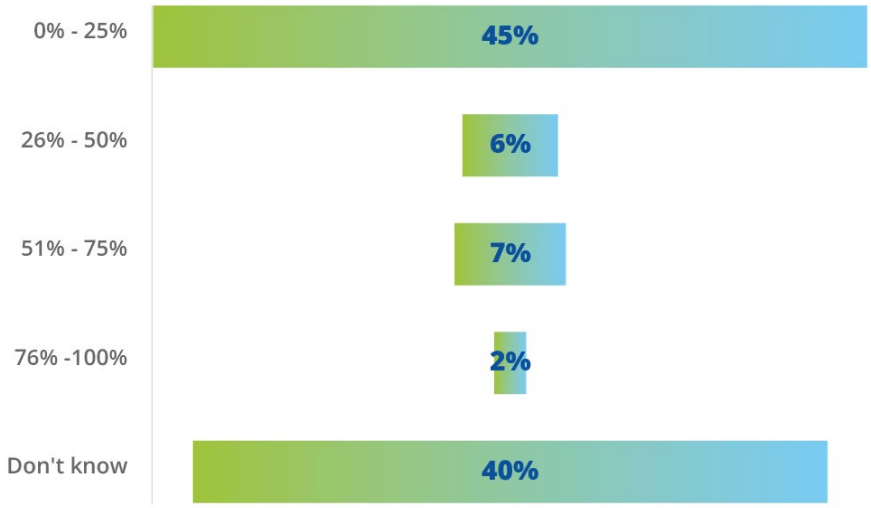


Figure 36: Suppliers providing adequate SBOMs

As depicted in Figure 37, supplier readiness gaps are primarily identified in three areas. Specifically, 27 % of respondents reported that supplier-provided SBOMs **do not meet completeness requirements**, 17 % indicated that **SBOM component identifiers lack sufficient accuracy** and 12 % highlighted issues related to the **quality or adequacy of vulnerability references**. These findings point out the quality challenges in supplier-generated SBOMs.

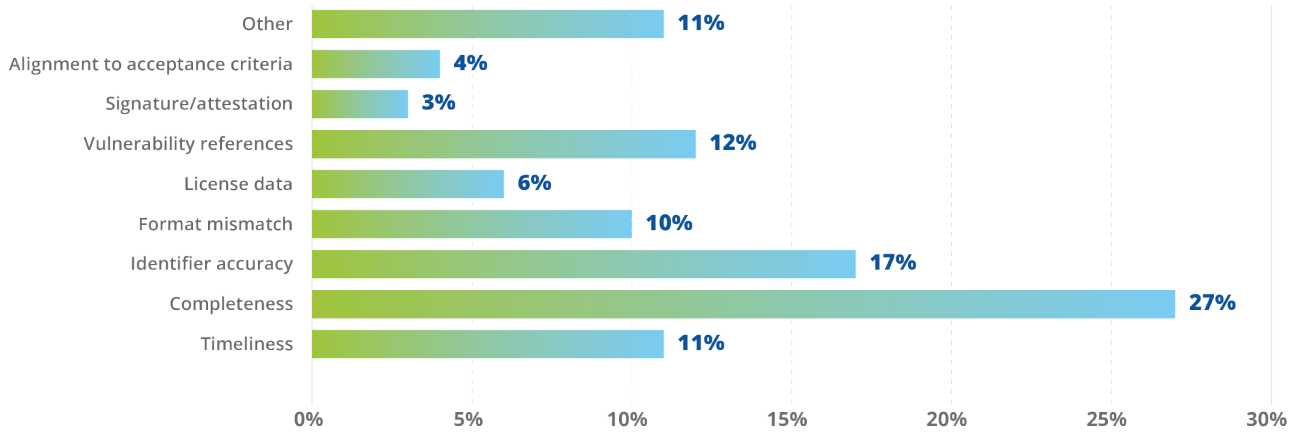


Figure 37: Main gaps in supplier's SBOMs

2.4.1 Guidance

Targeted external guidance is expected to support organisations across the EU market in overcoming barriers, responding to organisational needs and accelerating the SBOM adoption progress.

In particular, 31 % of respondents considered the **development of a profile** defining what constitutes a 'good enough' SBOM to be beneficial, 29 % **called for the standardisation of SBOM formats** and their required fields, and 20 % saw value in the development of a risk assessment framework that leverages SBOM data.

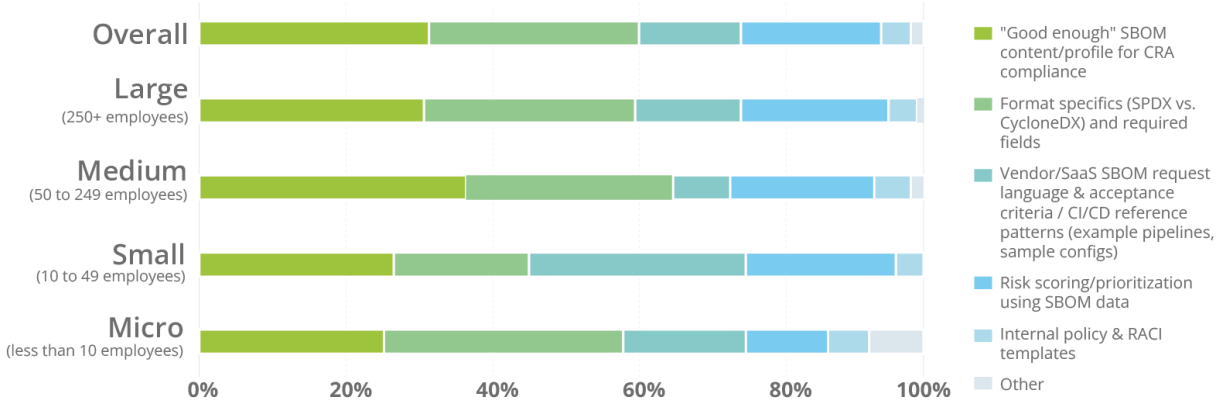


Figure 38: Areas that would benefit from guidance or templates

3. Conclusions

The SBOM SoA survey provides factual data on how organisations across industries and of varying sizes are approaching SBOM adoption in response to the CRA. Overall, the results demonstrate that the CRA is already acting as a **meaningful enabler for SBOM implementation**, while also revealing some maturity gaps, operational challenges, and areas where further ecosystem alignment is required to enable sustainable adoption at scale.

A central conclusion from the survey is that the CRA, while still in transitional period is already **shaping organisational investment priorities and capability development**. Respondents indicated that the regulation is acting as an **accelerator for SBOM adoption**. This demonstrates that the regulation is functioning as an early market signal influencing security engineering practices, supply-chain transparency, and compliance strategies.

Respondents reported that their organisations are progressing in their SBOM adoption journey, with **expectations to reach a level of maturity aligned with CRA expectations within planned timeframes**. Technical external support is needed to accelerate SBOM adoption at scale across all organisations, with the need for an **SBOM Reference Implementation ranking #1**.

The value of SBOMs is identified in **risk reduction**, **cost avoidance** and **operational efficiency**. SBOMs are primarily viewed as a **defensive cybersecurity mechanism**, particularly supporting vulnerability management, licence compliance and regulatory compliance activities. These use cases align closely with the expectations established under the CRA and broader secure-by-design frameworks.

There is a **strong alignment** across respondents regarding format-related requirements. Respondents broadly recognised that **SBOMs must be provided in commonly used and machine-readable formats** to support supply chain transparency at scale. This alignment is consistent with the expectations articulated in the CRA and reflects the fact that interoperability is not just a technical preference but a requirement for operationalising SBOM.

Respondents indicated that SBOMs are increasingly generated and consumed during **build-stage activities**, suggesting a **direct integration** into software development pipelines rather than a post-release documentation activity. Such integration represents an important step towards achieving **continuous transparency** across the software life cycle, supporting timely vulnerability analysis and facilitating more effective risk management.

While many respondents reported producing SBOMs with **full dependency depth**, others indicated that their current practices remain **limited to primary components and direct dependencies**. Deeper dependency visibility is essential for effective vulnerability management and supply-chain risk management, enabled by comprehensive SBOM coverage with full transparency across transitive dependencies.

Despite progress, respondents identified **several challenges** affecting implementation quality and scalability. Among the most frequently cited were **SBOM completeness**, **data quality** limitations, **and shortages of internal skills** and specialised staff. These challenges reflect that SBOM adoption is not just a tooling issue, but also an organisational capability issue requiring process adaptation and workforce development.

Respondents expressed concern about the **absence of widely accepted industry best practices** for integrating SBOM production and consumption into both software development workflows and organisational risk management processes. The **lack of consensus** in this area is one of the most significant challenges identified. These findings indicate that organisations are not only seeking technical specifications or standards but also **operational guidance**.

Respondents highlighted various priority areas where further support would accelerate adoption. These include the development of a profile defining what constitutes a **'good enough' SBOM** for practical use, the **standardisation of SBOM formats and required data fields** and the **establishment of a risk assessment framework** capable of leveraging SBOM information.

TP-01-26-008-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union