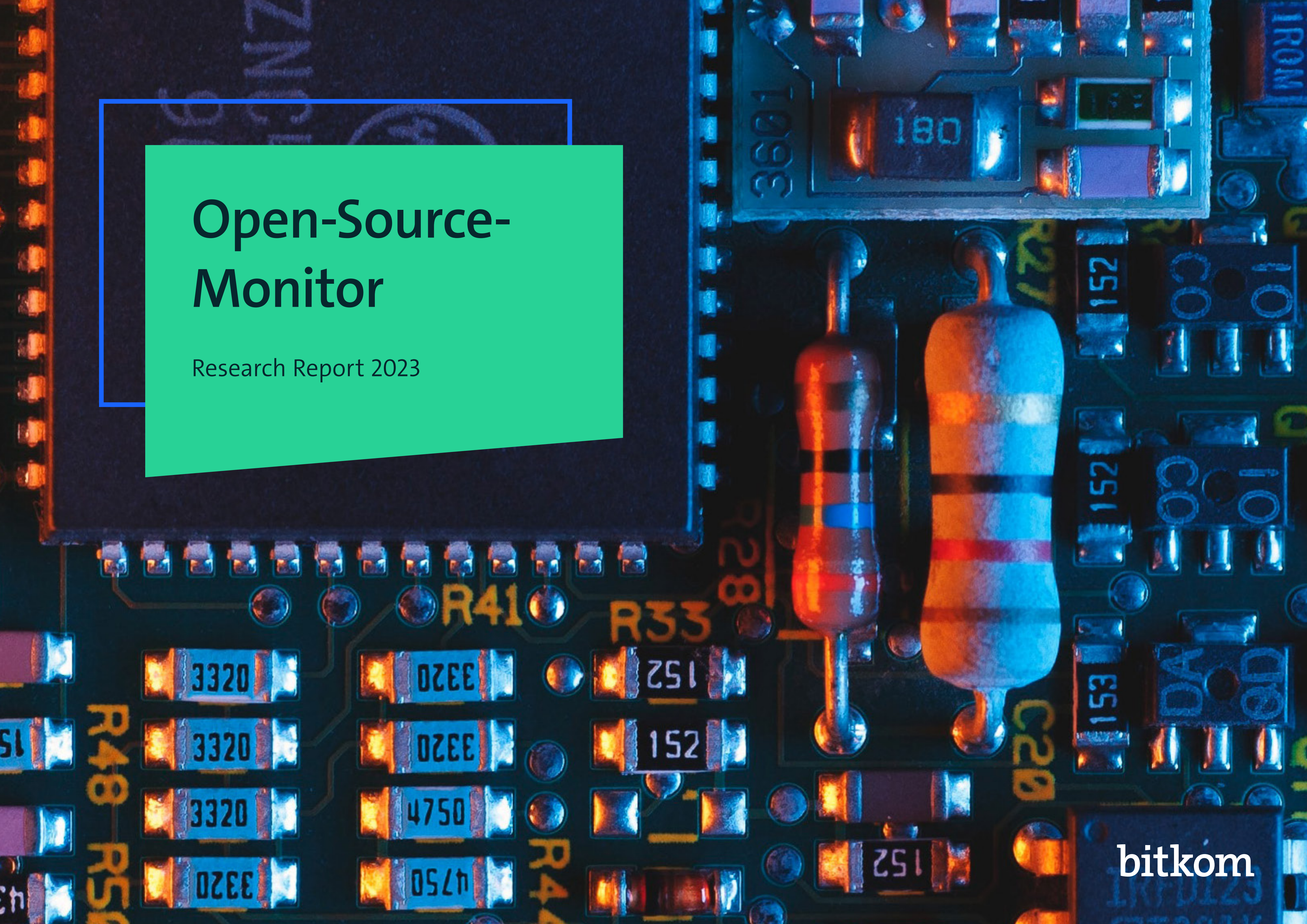


Open-Source-Monitor

Research Report 2023

bitkom

Content

Figures

With friendly support from:

bitsea.

bundesdruckerei.

dataport

DB

ECLIPSE FOUNDATION

Fraunhofer

ITDZ IT FÜR BERLIN

KERNKONZEPT

KPMG

Mercedes-Benz

{metæffekt}

NORDEMANN

Stay Open. OX

Osborne Clarke

publicplan.

pwc

Red Hat

SIEMENS

sonatype

SUSE

What impact will Open Source have in the years 2023 and beyond? If you are looking for an answer to this question, you simply have to take a look at one of the current hot topics: artificial intelligence and large language models. This trend was initially driven by companies like OpenAI, Microsoft, Google, and Meta. However, the Open Source community has since caught up and is sometimes even leading the way. Many predict that Open Source language models will eventually set the benchmark for quality. Open Source – a new niche in the digital world? Far from it.

There are plenty of examples in other fields. No software development team is complete without Open Source tools. Whether it's social networks or streaming services, all the major digital platforms we use daily are based on Open Source. Without it many of the services we take for granted would not exist. What about Internet traffic? Much of the Internet traffic depends on Open Source protocols and software. However, the impact is not limited to computers and servers. The smartphone revolution that radically transformed communication was only possible with Open Source components. Not only do they ensure that the devices work, but they also facilitate the rapid innovation seen in recent years.

Open Source Software has become widely used across the entire German economy: seven out of ten companies deliberately use such solutions, and half of all companies participate in further developing Open Source Software, usually by purchasing support services or corresponding enterprise solutions. We surveyed more than 1,100 companies for the third edition of the »Open-Source-Monitor 2023«, which aims to highlight the role of Open Source in today's economy and identify vital trends. Once again, we surveyed around 100 public sector organisations to understand public sector sentiment. The results confirm that Open Source Software has also become an integral part of government agencies: 59 percent are currently using such solutions.

Open Source offers a wide range of advantages since it allows access to the source code and the possibility to make improvements, make them available to the public, and create custom software using the Open Source components.
It translates into lower costs for the company, customised solutions and the possibility to perform in-house security audits. Moreover, Open Source also offers opportunities for the whole of the economy and society:

> Open Source can be instrumental in achieving digital sovereignty by allowing us to retain or regain control over the software we use.

However, that means we must increase the focus on Open Source and approach it more strategically. After all, only about one in three companies (32 percent) say they have an Open Source strategy.

There is still much room for improvement and much work to be done by the Open Source community, to which we would like to contribute with this »Open-Source-Monitor 2023«.

Dr. Ralf Wintergerst
President of Bitkom

Methodology

The third edition of the »Open-Source-Monitor 2023« provides insightful answers to questions on the status quo and the possible uses and challenges of Open Source Software in Germany. As in the previous 2019 and 2021 studies, this year, the focus will once again be on the German economy and the following questions:

- What is the general position of companies towards Open Source Software, and what advantages and disadvantages do they see for their companies?
- Do companies have a strategy for using or participating in Open Source Software?
- To what extent do companies use Open Source Software, and what criteria do they use to select it?
- What resources do they use for Open Source Software management? Has an Open Source Program Office been set up, and do they have analytic tools to perform security audits of their Open Source Software components?
- To what extent are companies actively involved in the (further) development of Open Source Software?
- Do companies have written policies for Open Source Software?
- How do companies address the issue of compliance with Open Source Software?
- Is there a strategy for establishing and standardising compliance processes?

To answer these and other questions, we surveyed companies to examine the strategic use of Open Source Software in German companies.

The digital association Bitkom and Bitkom Research developed the study design with the 20 partners Bitsea GmbH, Bundesdruckerei GmbH, Dataport AöR, DB Systel GmbH, Eclipse Foundation Europe GmbH, Fraunhofer-Gesellschaft, ITDZ Berlin AöR, Kernkonzept GmbH, KPMG AG Wirtschaftsprüfungsgesellschaft, Mercedes-Benz Group AG, {metæffekt} GmbH, NORDEMANN, Open-XChange, Osborne Clarke, publicplan GmbH, PwC GmbH, Red Hat GmbH, Siemens AG, Sonatype and SUSE Software Solutions Germany GmbH. The aim was to continue to gain a representative picture of the German economy. First, a standardised questionnaire was developed with the specialist expertise of the project consortium. Next, trained telephone interviewers conducted computer-assisted telephone interviews (CATI) between the end of March and mid-May 2023.

The company survey included 1,155 German companies with at least 20 employees, selected by size category and industry to provide a representative sample. The stratification of these random samples ensured that companies from different size categories and industries were represented in sufficient numbers for statistical evaluation.

The statements of participants were weighted during analysis to ensure that the results provide a representative picture of all German companies with at least 20 employees (see Figure 1). The selected sampling structure makes it possible to identify specific characteristics within selected size categories and industries.

Size categories	Absolute Unweighted	Percentage Unweighted	Absolute Weighted	Percentage Weighted
20 – 99 EE	353	30,6 %	926	80,2 %
100 – 199 EE	302	26,1 %	119	10,3 %
200 – 499 EE	249	21,6 %	72	6,2 %
500 – 1.999 EE	152	13,2 %	32	2,8 %
2.000+ EE	99	8,6 %	6	0,5 %

Sectors	Absolute Unweighted	Percentage Unweighted	Absolute Weighted	Percentage Weighted
Automobile sector	150	13,0 %	6	0,5 %
Banking & Insurance	151	13,1 %	15	1,3 %
Transport & Logistics	150	13,0 %	74	6,4 %
IT & Telecommunications	151	13,1 %	43	3,7 %
Commerce	151	13,1 %	207	17,9 %
Other industries	202	17,5 %	316	27,4 %
Other service providers	200	17,3 %	494	42,7 %

Sample: All companies with at least 20 employees (n = 1,155) | Source: Bitkom Research 2023

Figure 1 – Composition of the company sample by size category and industry (unweighted and weighted)

As in the »Open-Source-Monitor 2021«, most German companies in this year's survey have at least 20 employees. In contrast to 2019, when most German companies had 100 employees, this allows us to measure the use of Open Source Software in smaller companies with 20 to 99 employees once again. The sample was expanded in 2021 and 2023 from approximately 800 companies to over 1,150 companies to highlight the changes from 2019 to 2023. The expansion of the entire sample has made it possible to directly compare year-on-year results of companies with at least 100 employees (↗ Chapter 2).

First introduced in 2021, in addition to the representative company sample, we surveyed a subsample of 100 public administration organisations to better understand the use of Open Source Software in public administration (↗ Chapter 3). Included are organisations in public administration, including general public administration, public administration related to healthcare, education, cultural services and other social services, business support services, economic regulations, and economic governance. Foreign affairs, defence, administration of justice, public order and safety and social security are not included.

The final sample breaks down as follows: 41 percent local government, 42 percent state government and 17 percent federal government (see Figure 2).

Size categories	Absolute Unweighted	Percentage Unweighted
20 – 99 EE	26	25 %
100 – 199 EE	26	25 %
200 – 499 EE	27	26 %
500+ EE	23	23 %

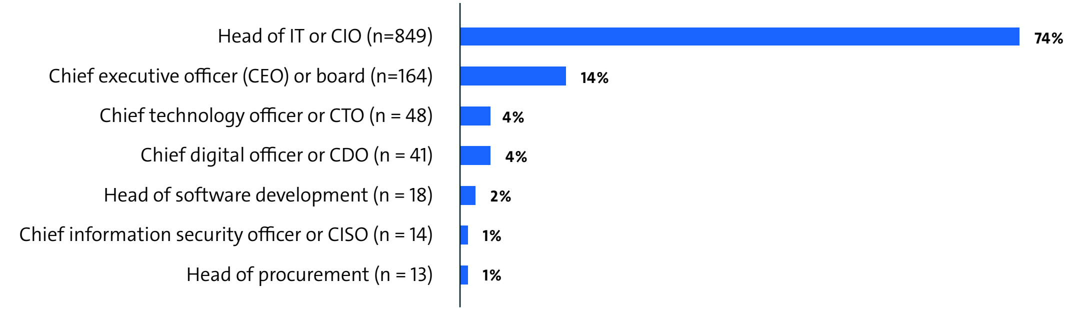
Administrative level	Absolute Unweighted	Percentage Unweighted
Federal government	17	17 %
State government	43	42 %
Local government	42	41 %

Sample: All respondents in public administration (n = 102)
Source: Bitkom Research 2023

Figure 2 – Composition of the administration sample by size category and administrative level (unweighted)

The standardised company survey was adapted for public administration and, like the company survey, was also conducted using computer-assisted telephone interviews (CATI) between the end of March 2023 and mid-May 2023. The public administration results were neither weighted nor included in the overall result of the representative company survey. Although the size and distribution of the sample are not representative of the use of Open Source Software in public administration, it does provide a valuable picture of public sector sentiment.

The interviews were conducted with executives responsible for Open Source Software within their companies. Around half of the companies (49 percent) have designated this role to one person, formally or informally. One person is generally assigned an informal role, such as the Head of IT or Digitisation. Only twelve of the companies surveyed have created a formal position for Open Source Software management (1 percent).

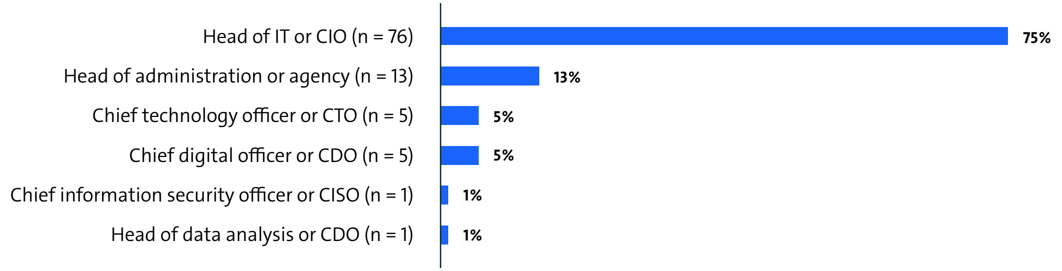


Sample: All companies with at least 20 employees (n=1,155) | Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

Figure 3 – Composition of the company sample by respondents' position in the company (unweighted)

In companies with no designated person for Open Source Software (47 percent), we surveyed their executives responsible for software deployment or development. The composition of the sample by respondents' position is shown in Figure 3.

Three-quarters of the company surveys (74 percent) were conducted with the executive in charge of IT. Similarly, 75 percent of the public administration surveys were conducted with the head of IT (see Figure 4).



Sample: All respondents in public administration (n = 102) | Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

Figure 4 – Composition of the administration sample by respondents' position in the company (unweighted)

At the beginning of the surveys, we established a uniform understanding of what defines Open Source Software for all participants. It was the following description, which also forms the basis for this research report:

> Open Source Software refers to software, such as program modules, source code and libraries, programming tools, as well as complete operating systems or software solutions, with Open Source codes and a licence that allows licensees to run the software for free, analyse it, adapt it and distribute it in unmodified or modified form. It requires the source code to be openly accessible and royalty-free.

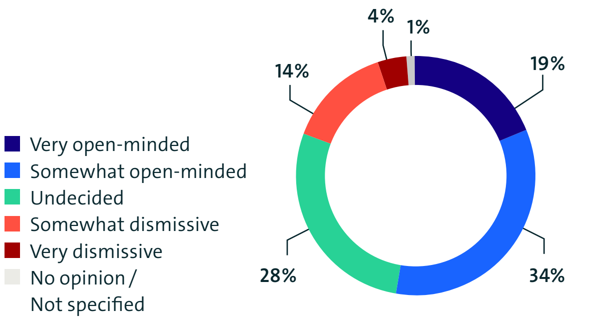
In keeping with the survey, we will mainly use the abbreviation OSS for Open Source Software in this report.

1 Use of Open Source Software in companies

1.1 Attitude towards Open Source Software

Almost half of all companies with at least 20 employees (53 percent) are generally open to OSS (see Figure 5). As many as 34 percent of the companies are somewhat open, while one-fifth (19 percent) are even very open. Only 18 percent of the companies are dismissive of OSS. About one-quarter (28 percent) are undecided about OSS.

What is the general position of your company towards OSS?

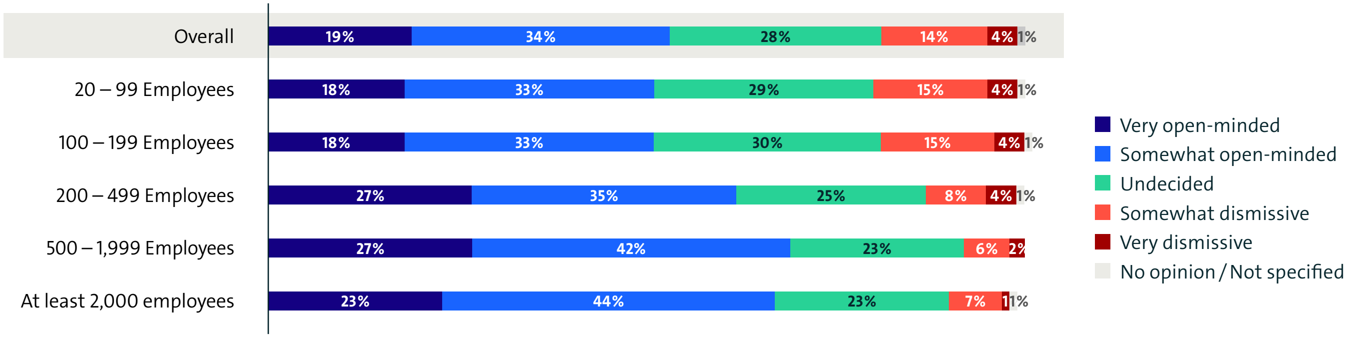


Sample: All companies with at least 20 employees (n=1,155) | Not all percentages add up to 100 due to rounding
Source: Bitkom Research 2023

Figure 5 – Attitude towards Open Source Software

Looking at the different company sizes, we can see a linear correlation between the attitude towards OSS and company size (see Figure 6). While 51 percent of small and medium-sized companies (20 to 199 employees) are open to OSS, this figure increases to six out of ten companies (62 percent) in the 200 to 499 employee size category. This trend continues, with large companies showing the most interest in OSS (500 to 1,999 employees: 69 percent, at least 2,000 employees: 67 percent).

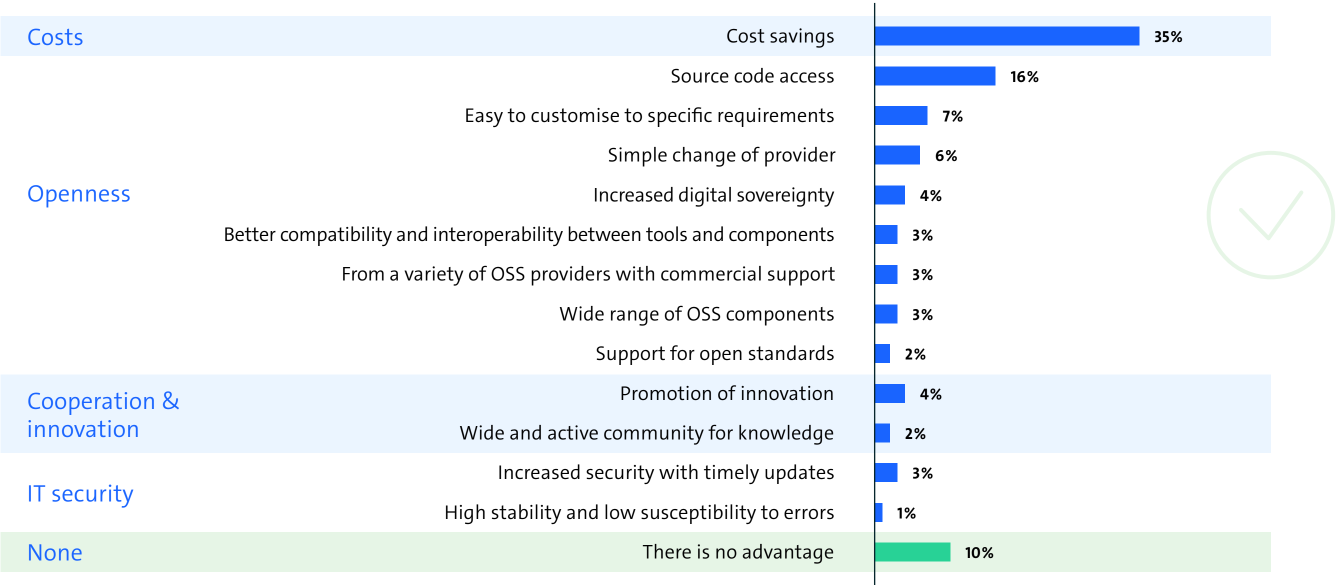
What is the general position of your company towards OSS?



Sample: All companies with at least 20 employees (n=1,155) | Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

Figure 6 – Attitude towards Open Source Software by company size classes

Only one-tenth of companies (10 percent) think that OSS has no advantages in response to the open-ended question (i.e., a question that provides no predefined answers) about the most significant advantage that speaks for the use of OSS (see Figure 7). All companies that use, integrate, (further) develop, or contribute to OSS in some other way believe that using OSS offers considerable advantages (no advantages: 0 percent).



In your opinion, what is the most significant advantage of using OSS in your company?

Sample: All companies with at least 20 employees (n=1,155) | Open-ended question, only one possible answer | Missing values: »No opinion / Not specified«
Source: Bitkom Research 2023

Figure 7 – Advantages of Open Source Software

Considering all the companies surveyed, one-third (35 percent) cite cost savings as the most significant advantage of using OSS. It makes the fact that OSS is royalty-free the most commonly cited advantage. Using open-ended questions allows us to identify various reasons for using OSS based on the many other advantages mentioned.

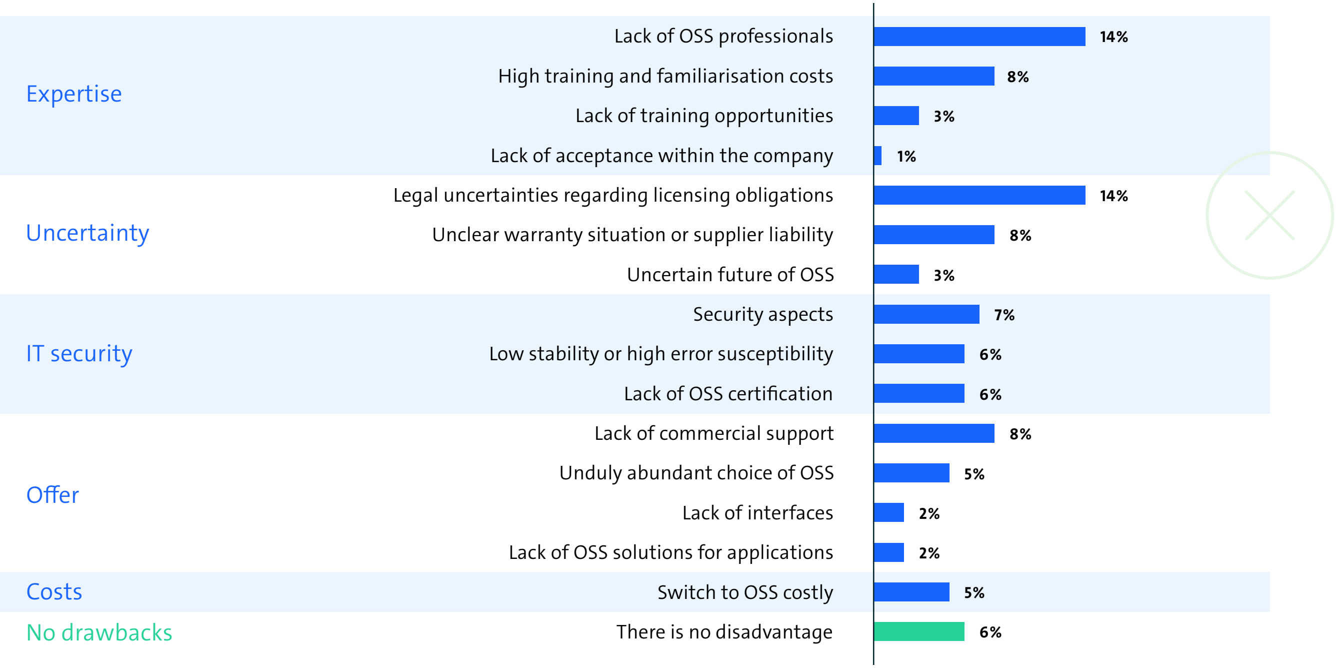
If we look at the categorisation of advantages, most of the responses refer to the accessibility of OSS (44 percent). 16 percent of the companies cite access to the source code as the most significant advantage. The ease of customising OSS to specific requirements is cited as the next most important advantage, accounting for 7 percent. It is followed by the compatibility and interoperability between tools and components (3 percent), the variety of OSS providers with commercial support (3 percent), the wide range of OSS components (3 percent) and support for open standards (2 percent).

A total of 6 percent of companies regard promoting cooperation and innovation as the most significant advantage. 4 percent of those companies cite promoting innovation as a specific advantage. An additional 2 percent rate the broad and active OSS community as beneficial for knowledge exchange.

Only 4 percent cite IT security aspects as the most significant advantage of using OSS. 3 percent of companies believe the main advantage derives from improved security due to timely updates. Only 1 percent mention the low susceptibility to errors of OSS.

This study was not only interested in the advantages but also in the disadvantages that companies see concerning OSS. Accordingly, we included an additional open-ended question that addresses increased digital sovereignty (4 percent), the most significant disadvantage that stands in the way of using OSS. In contrast to the advantages, no single reason is at the top of the list. The lack of OSS professionals and the legal uncertainties regarding licensing obligations are the most commonly reported disadvantages from a company perspective, accounting for 14 percent (see Figure 8).

In your opinion, what is the most significant disadvantage that stands in the way of using OSS in your company?



Sample: All companies with at least 20 employees (n=1,155) | Open-ended question, only one possible answer
Missing values: »No opinion / Not specified« | Source: Bitkom Research 2023

Figure 8 – Disadvantages of Open Source Software

The picture then becomes more nuanced again, in many cases with only a few percentage points difference between reasons. Those reasons can also be grouped into general categories, as shown in Figure 8. A quarter of companies (26 percent) name disadvantages related to expertise. Apart from the lack of OSS professionals already mentioned, they also cite the high training or familiarisation costs (8 percent), the lack of training opportunities (3 percent), and the lack of acceptance within the company (1 percent).

An additional quarter (25 percent) generally associate the use of OSS with uncertainties. Eight percent are not only concerned about licensing uncertainties but also about the unclear warranty situation or supplier liability for OSS. Another 3 percent of companies are worried about the uncertain future of OSS.

Almost one in five (19 percent) companies consider IT security a disadvantage. Looking at the advantages, where only 4 percent of companies mentioned IT security, it is evident that the concerns in this area outweigh the benefits. At this point, the results of the 2021 study were even more ambivalent in this regard. Two years ago, only 9 percent of companies cited IT security as a disadvantage.
At the same time, 9 percent also listed these aspects as the most significant advantages. The uncertainties about IT security have thus increased in 2023. This year, 7 percent of companies list security aspects as the most significant general disadvantage. 6 percent of companies cited the high susceptibility to errors and the lack of OSS certification as critical factors.

Another 17 percent of companies stated disadvantages related to the available OSS products. The lack of commercial support for OSS (8 percent) is the most frequently cited disadvantage, followed by too much choice (5 percent), lack of interfaces (2 percent) and lack of OSS solutions for enterprise applications (2 percent).

Lastly, a further 5 percent of companies cite the costs required to switch to OSS as the most significant disadvantage that stands in the way of using OSS.

Overall, nine out of ten companies (92 percent) cite disadvantages related to using OSS. If we have another look at the companies that use, integrate, further develop or contribute to OSS in some other way, this view is primarily the same. 89 percent of those companies mention a disadvantage related to using OSS. On the other hand, 6 percent of all companies surveyed do not see any disadvantages that stand in the way of using OSS.

Open Source – the key to resilience, sovereignty and progress

Marcel Scholze
Director, Head of OSS
Management Services
PwC

Regulators recognise the importance of Open Source
The draft of the EU Cyber Resilience Act (CRA), the Executive Order on Cybersecurity in the US, the Digital Operational Resilience Act (DORA) or the ENISA Guidelines for the IoT Supply Chain are just a few examples of laws and regulations that directly or indirectly deal with Open Source Software (OSS) and the importance of software bills of materials (SBOM). Regulators have recognised the central importance of Open Source for digital transformation and are promoting the secure, legally compliant use of OSS. This creates great opportunities, but also challenges for the Open Source community and for companies. For this reason, it is essential to establish appropriate OSS management.

Using regulation as an opportunity
It is of central importance for companies not only to implement the above-mentioned requirements of the market and regulatory authorities as a minimum, but to actively use them as an opportunity to strategically utilise the known advantages of Open Source and to firmly anchor them in the corporate culture. This is not only about the opportunity for accelerated innovation, cost reduction or transparency, but also about promoting one's own resilience and sovereignty. The strategic use of Open Source enables organisations to react flexibly to a dynamic market environment, strengthen their technological independence and gain long-term competitive advantages.

Strengthen your organisation through an optimised OSS management system
As an international standard, the new OpenChain ISO 18974 provides important guidance on how security management processes for Open Source should be designed. As with Open Source compliance processes (ISO 5230), these are complex workflows that usually involve multiple company departments and tools. A central inventory of OSS in use is an important linchpin here.

Even though the two ISO standards are each independent of each other, a harmonised set-up can help realise synergy effects. The implementation of OSS security and compliance structures requires the design of individual solutions along established standards and their cyclical optimisation. Know-how in the fields of IT, business processes, Open Source, and legal are essential.

An external view of the organisation can be valuable here, e.g. in identifying regulatory gaps, optimising latency times or neutrally evaluating the toolchain used. As in 2021, the participants in the Bitkom Monitor see a challenge in the area of Open Source Software in the lack of qualified Open Source specialists. This makes it all the more important to equip the available resources with an efficient process and tool environment.

Independence and interdisciplinary expertise for your Open Source management
The strategic implementation of ISO 5230 and 18974, including the integration of a reliable SBOM, requires individual measures and comprehensive technical as well as legal expertise.

PwC advises and implements or audits and certifies Open Source management systems and offers professional managed services for code scanning, SBOM creation and curation, and supplier audits.

↗ www.pwc.de/en/opensource

The respective company is responsible for the content of the page.

Open Source Compliance as a service

The challenge

As Open Source Software compliance is becoming more important, it is also becoming more challenging: Software development cycles are shortening, and automated continuous delivery is becoming more common. At the same time, software is getting bigger and more complex. Even relatively simple projects often contain hundreds, if not thousands, of third-party components. From a legal point of view, it is necessary to ensure that all licensing obligations are met.

Many companies merely look up the licence text of the respective third-party component. Frequently, they then compile copyright notices and ship both with the software. From a factual standpoint, this task alone is anything but trivial – however, from a legal perspective, it is only the first step. It is because, in addition to the requirement to disclose license texts and copyright notices, many licences contain other obligations, limitations and conditions that must be met. It requires an in-depth review of the license texts, ultimately representing a significant investment. Moreover, many obligations arise from the specific use case of the licensed software. Thus, more is needed to review and assess licences legally – the specific use case of the software components must always be considered.

Our solution

Drawing on more than a decade of experience with legal issues of Open Source compliance, we have developed FOSS-matrix. This solution can be made available as a web service. It makes it possible to automatically evaluate almost 200 licences – broken down by 75 characteristics – focusing on the defined use cases. Detailed descriptions of possible licensing issues with references to the underlying licences and other sources then provide a quick overview of the potential problems and allow subsequent steps to be taken to resolve them.

Complex legal issues were broken down into several parts and given different scores and assessment criteria. A detailed written report of all the different steps and results was compiled where necessary. As a result, it is also possible to record, evaluate and visualise controversial legal issues, cases of doubt and grey areas.

The solution is highly flexible: It can be run stand-alone using a web interface or integrated into an existing tool infrastructure utilising an API.

Your advantage

The solution we have developed makes it possible to quickly and transparently perform an automated legal assessment of many licences and to check whether they meet the requirements of the company's intended use.

Osborne Clarke has extensive experience providing comprehensive legal and technical advice on Open Source. He offers Open Source Software (OSS) Compliance and Contributions solutions.

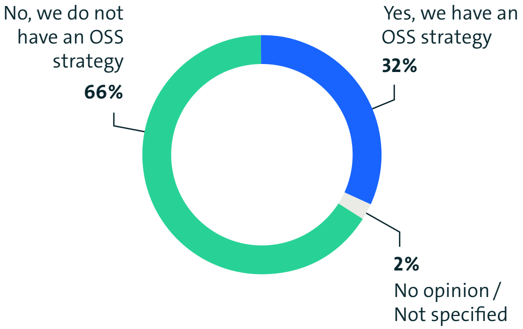
Dr. Hendrik Schöttle
Lawyer, partner, specialised in IT law

↗ osborneclarke.com/oss

1.2 Open Source Software Strategy

Another significant aspect surveyed companies with at least 20 employees must consider is how they approach Open Source strategically. The study asked companies whether they had a strategy for using or participating in OSS. A strategy was defined as a document with written goals and plans.

Does your company have a strategy for using or participating in OSS?



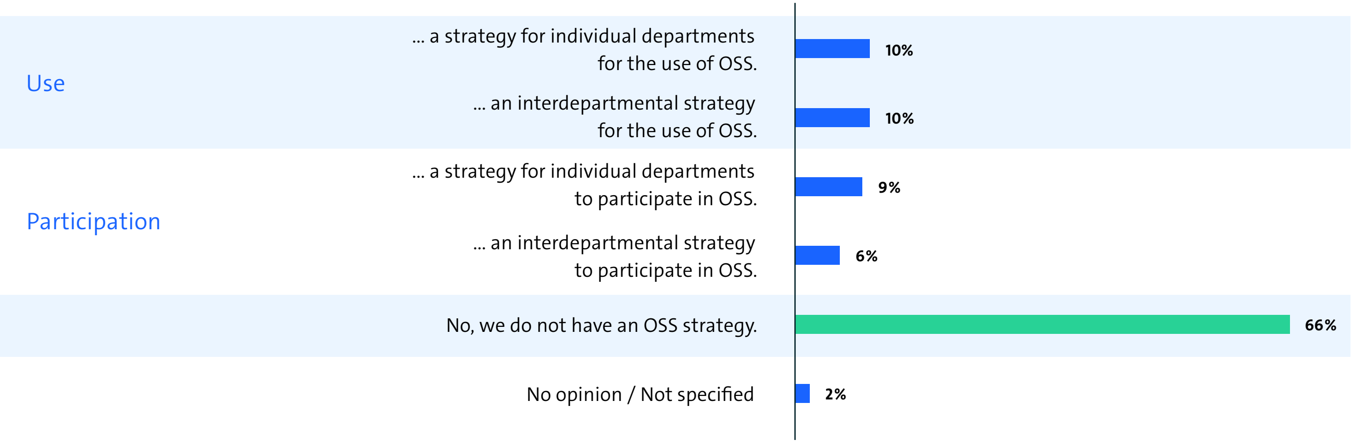
Sample: All companies with at least 20 employees (n=1,155)
Source: Bitkom Research 2023

Figure 9 – Open Source Software strategy

Figure 9 shows that one-third (32 percent) of the companies have already put in place an OSS strategy. The strategic importance of Open Source for German companies was also evident in the ↗Chapter on methodology. Accordingly, about half of the companies (48 percent) have informally designated one person for the OSS role. Only 1 percent of companies have established a formal position for OSS management.

Figure 10 provides a deeper insight into the existing strategies or sub-strategies. It shows that one-fifth of companies (20 percent) have a strategy that focuses on the use of OSS. The scope of strategies around use is distributed evenly between individual and interdepartmental strategies (10 percent each). An additional 15 percent of companies have a strategy for participating in OSS. At 9 percent, strategies for individual departments are slightly ahead of interdepartmental strategies (6 percent).

Does your company have a strategy for using or participating in OSS?



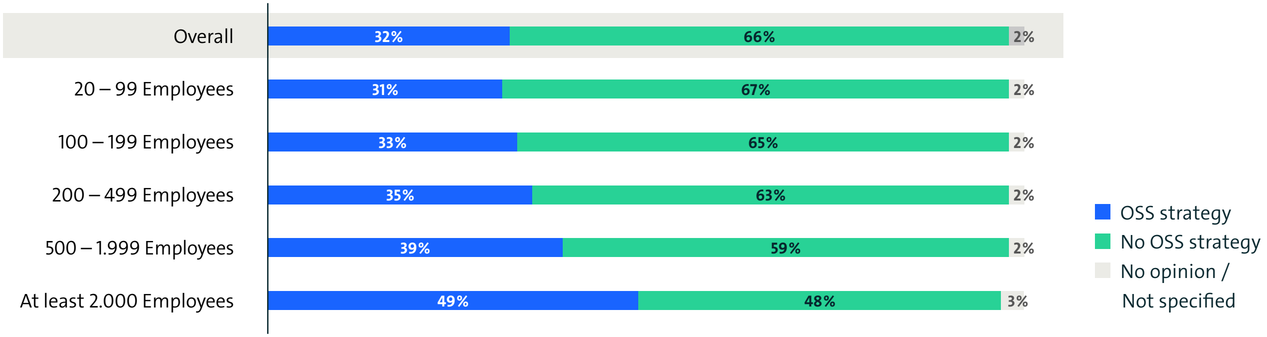
Sample: All companies with at least 20 employees (n=1,155) | Multiple answers possible | Source: Bitkom Research 2023

Figure 10 – Open Source Software strategy by type

Once again, as with the attitude towards OSS (↗ Chapter 1.1, Figure 6), we see a linear correlation with company size classes (see Figure 11). 31 percent of small companies with 20 to 99 employees have an OSS strategy. Likewise, about one-third of small-and-medium-sized businesses (100 to 199 employees: 33 percent; 200 to 499 employees: 35 percent) have an OSS strategy.

Four out of ten large companies with 500 to 1,999 employees (39 percent) have an OSS strategy. The figure increases to approximately half (49 percent) among large companies with at least 2,000 employees.

Does your company have a strategy for using or participating in OSS?



Sample: All companies with at least 20 employees (n = 1,155) | Source: Bitkom Research 2023

Figure 11 – Open Source Software strategy by company size class

Invisible support: How Open Source Software strengthens digital sovereignty

Studies have long shown that Open Source solutions are becoming more widespread and practical. Yet this growth is all too often overlooked by the public.

Study
A 2020 survey by Open Email indicated that 76.93 per cent of all accessible email systems in Germany rely on Open Source technologies such as Open-Xchange.

Thus, millions of users in Germany unknowingly use Open Source solutions every day. Namely, whenever they log in to their private e-mail account.

Exploiting the advantages in public administration

Open Source solutions are crucial for public administration in achieving true digital sovereignty.

As a result, the **political support** for Open Source solutions is growing continuously. Several federal states have already passed resolutions to promote digital sovereignty, and the national Centre for Digital Sovereignty (ZenDis) has also started its work.

Particular attention is paid to the **stable and secure operation** of email and collaboration platforms. Many government agencies prefer to use specialised service providers for this purpose and rely on best-practice Open Source solutions. These providers deliver adequate protection against spam, malware and botnets.

Furthermore, Open Source solutions have become much more user-friendly, and standards have also been established. It is worth noting that **seven out of 16 federal states have already opted** to set up state-wide email and collaboration platforms in education and administration using solutions such as Open-Xchange and Univention.

Four digital-sovereignty principles

The advantages can be leveraged most effectively if the software is genuinely Open Source. The following four simple principles help identify whether any software or cloud solution is Open Source.

1. **The availability of more than one provider**
   ensures independence from the manufacturer.
2. **The flexible operation of the software**
   guarantees independence.
3. **Flexible data migration**
   facilitates flexible and free use.
4. **Transparency for accountability:** transparent software enables joint advancement and control.

Government agencies aiming to regain their digital sovereignty have no choice but to use proper Open Source Software. As a result, the public sector can technically implement its legal requirements without **relying on manufacturers**.

The respective company is responsible for the content of the page.

Open Source-based online workspace for the public sector

Digital sovereignty at work with the dPhoenixSuite

Digital transformation in the public sector increasingly requires government agencies to collaborate digitally and to use flexible video conferencing. As a result, the administration is becoming more dependent on manufacturers of digital solutions. The state can only function with access to IT and data, as the processing of citizen and company data is only possible with digital solutions. Digital sovereignty of the administration, i.e., independent control of IT and data, is crucial for the digital state.

How can the administration utilise modern digital solutions without becoming dependent on technology companies? Dataport offers the answer: dPhoenixSuite, an Open Source-based online workspace for the public sector. The suite unites e-mail, calendar, contacts, word processing, chat, video conferences and collaboration in virtual spaces. It is modular and includes powerful Open Source applications from various German and European manufacturers.

Dataport and its partners from business and administration developed the dPhoenixSuite in the Phoenix project. This network delivers the online workspace with service-level agreements and support while continuously improving it.

Each Open Source dPhoenixSuite module is run in secure German clouds and on German servers, giving the state complete control over the data, subject to EU data protection rules.

The dPhoenixSuite offers a digital alternative to traditional office suites. It can be accessed through a web browser or mobile without needing installation. It features a user-friendly interface with a »single sign-on« mode. Users of classic office applications will find it easy to navigate.

Overview of the individual dPhoenixSuite modules:

dPhoenixMail
- Communicate via email
- Organise appointments
- Manage contacts
- Plan tasks

dPhoenixOffice & FileShare
- Create and edit texts, spreadsheets and presentations. Alone or together with colleagues. Compatible with Microsoft Office products and the Open Document Format
- Share files with ease and organise in folders

dOnlineZusammenarbeit 2.0
- Conduct audio and video conferences
- Chat
- Work simultaneously in small groups (breakout sessions)
- Collaborate on a whiteboard
- Take notes
- Conduct polls

dPhoenixSuite is now available in version 3.0. The upgrade to version 4.0, which will also allow the integration of electronic files, is planned for spring 2024.

© @freepik

Around 200,000 members of various administrations in Germany work with the dPhoenixSuite, using different modules of the suite or will do so shortly. These include, among others, the state government and the Ministry of Education of Schleswig-Holstein, the Ministry of Infrastructure and Digital Affairs of Saxony-Anhalt, the Ministry of Justice of North Rhine-Westphalia and the Robert Koch Institute.

↗ dPhoenixSuite.de

The respective company is responsible for the content of the page.

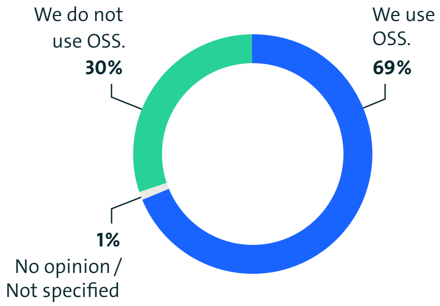
1.3 Use of Open Source Software

The previous two chapters show that almost every second company (53 percent) is generally open to OSS (↗Chapter 1.1, Figure 5). In contrast, one-third of companies (32 percent) have a formal strategy for using or participating in OSS (↗Chapter 1.2, Figure 9). The overwhelmingly positive attitude of German companies still needs to be fully reflected in the strategic integration of OSS. It raises two additional questions that play a central role in this study:

- To what extent is OSS currently used in companies?
- What factors significantly impact the selection of OSS used in companies?

The use of OSS is much more widespread in German companies with at least 20 employees compared to the general attitude and OSS strategies. Some seven out of ten companies (69 percent) use OSS in their company (see Figure 12). 30 percent of companies state that they do not use OSS.

Does your company use OSS?



Sample: All companies with at least 20 employees (n=1,155)
Source: Bitkom Research 2023

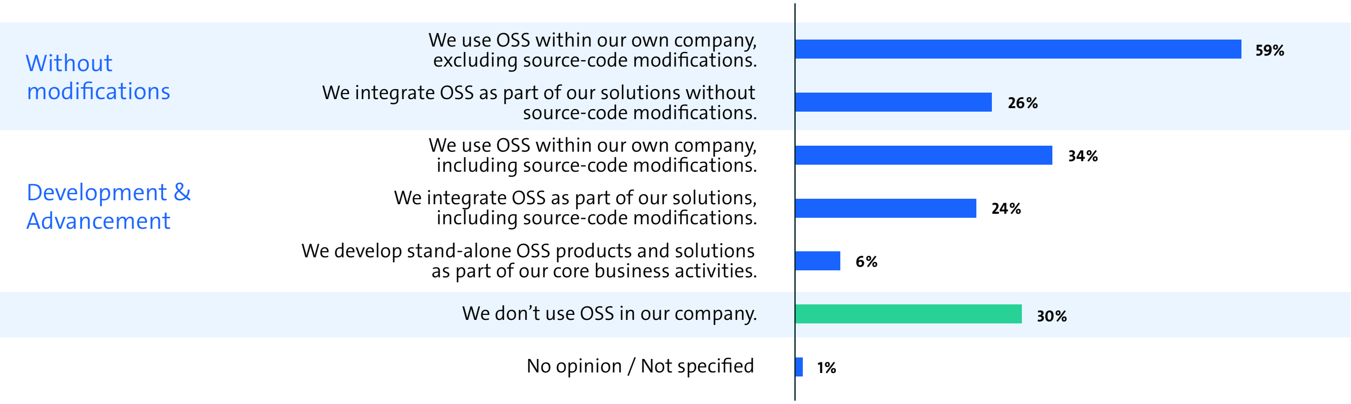
Figure 12 – Use of Open Source Software

If we look at the type of use, we can see that most companies (59 percent) use OSS for a user group within their company without modifying the source code (see Figure 13). The 2021 survey also supported this finding. However, the specific type of use has increased by 7 percentage points in the last two years (2021: 51 percent use in the company, without modification). Moreover, a quarter of companies (26 percent) integrate OSS into their products and solutions for their customers without modifying the source code.

One-third of companies (34 percent) state that they use OSS within the company and modify the source code for that purpose. A quarter (24 percent) modify the source code, integrating OSS as a component of their customer solutions. Just 6 percent of companies develop stand-alone OSS products and solutions as part of their core business activities.

A look at the company size classes again shows an increase in the use of OSS depending on the number of employees (see Figure 14). While about seven out of ten small companies (20 to 99 employees: 68 percent) use OSS, this figure rises to 85 percent among large companies (at least 2,000 employees). 73 percent of companies with 100 to 199 employees use OSS. While eight out of ten companies with 200 to 1,999 employees (78 percent) use OSS.

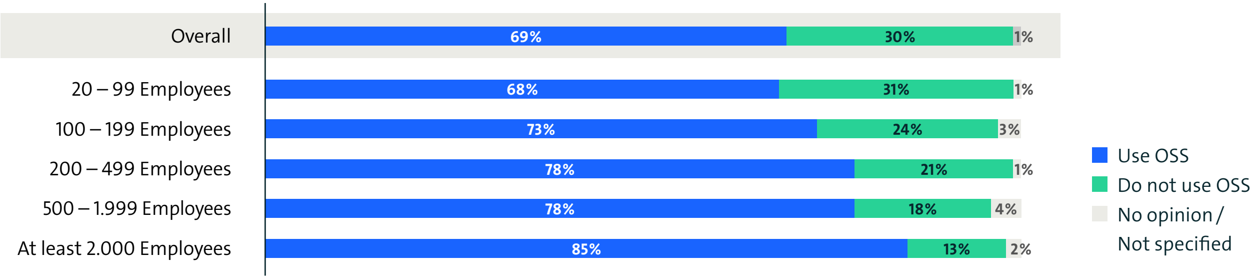
Which of the following statements apply to using OSS within your company?



Sample: All companies with at least 20 employees (n=1,155) | Multiple answers possible | Source: Bitkom Research 2023

Figure 13 – Use of Open Source Software by type

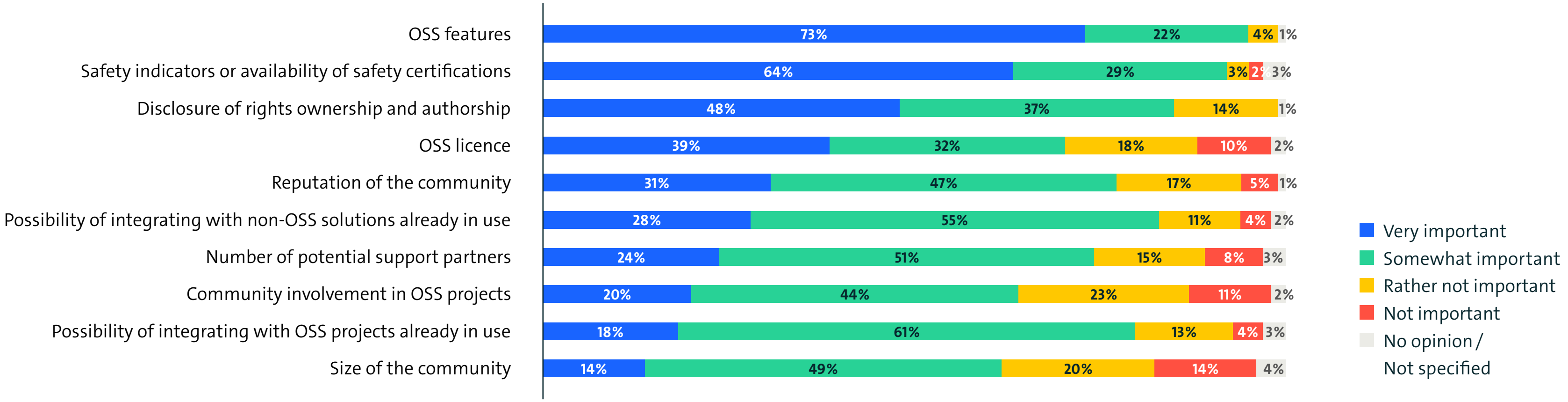
Does your company use OSS?



Sample: All companies with at least 20 employees (n = 1,155) | Source: Bitkom Research 2023

Figure 14 – Use of Open Source Software by company size classes

How vital are the following criteria for selecting OSS projects in your company?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

Figure 15 – Criteria for the selection of Open Source Software projects

Now that we have looked at the use of OSS, we want to explore the factors that companies using (i.e. deploying, integrating or (further) developing) OSS take into account in the selection of OSS. Figure 15 shows that companies consider the features of OSS the most essential criterion, with 73 percent rating it as »very important«.

An additional 22 percent of companies consider features »somewhat important«. In addition to this fundamental requirement, it becomes evident that the features of OSS are not the only factor necessary to companies. Nine out of ten companies (93 percent) regard security indicators, such as the number of reported CVEs, or the availability of safety certifications, like NIST certifications or Common Criteria, as essential criteria. Two-thirds (64 percent) rate this aspect as »very important« and 29 percent as »somewhat important«.

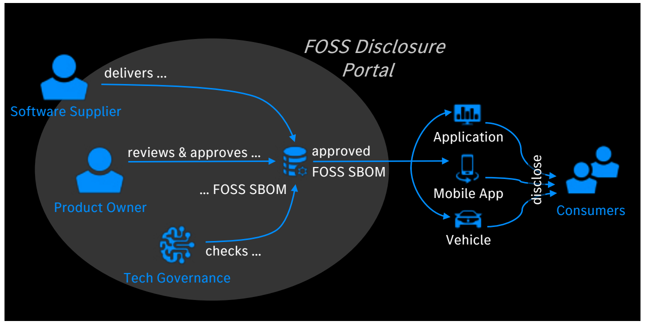
Companies not only attach great importance to features and security aspects but also to the regulatory environment. Accordingly, at 85 percent, the disclosure of OSS rights ownership and authorship comes in third on the list of selection criteria. Nearly half of companies (48 percent) consider this factor »very important«, and 37 percent regard it as »somewhat important«.

SBOM management at Mercedes-Benz

With our published **Mercedes-Benz Free & Open Source Software (FOSS) Manifesto**, we demonstrate that we want to facilitate the cultural change in Mercedes-Benz and our subsidiaries towards Inner Source and FOSS. While **FOSS** brings innovation, efficiency, and speed, we need to make sure to play it safe. Therefore, opening to the worldwide FOSS community must also go along with the responsibility in a highly regulated industry to have clear internal rules and processes for FOSS. Furthermore, **digital standards** need to be established within the supply chain. We envision this and can already demonstrate it with several company activities. Overall, we strive to foster a secure and standardized data exchange for all **participants in our automotive value chain**.

With the development of a **FOSS Disclosure Portal**, we are continuing to build a more efficient, transparent, and digital supply chain. By digitizing and automating our FOSS disclosure process with our internal and external partners, we want to further increase transparency regarding the FOSS components we use, for better licence compliance and security. FOSS information is handled in **Software Bills of Materials (SBOM) with SPDX from the OpenChain Project** (ISO / IEC standard for Open Source licence compliance programs) as the defined format for our SBOM exchange.

We recognized the need to introduce a FOSS Disclosure Portal to manage our FOSS SBOMs at scale, together with our partners.



FOSS SBOM in the Software Supply Chain

The purpose is to facilitate the exchange FOSS information directly & frequently from the CI/CD pipeline for developers, product & application owners, and suppliers. That way, our software guidelines, especially for FOSS compliance and security, can be followed. We want to provide more automated guidance with respect to checking licence conformance (e. g. allow and deny list information for licences defined in respective software development use case policies) and obligation management (quality checks on relevant SBOM details based on our licence database).

As a result, a central worldwide inventory of FOSS SBOMs from all companies within the Mercedes-Benz Group AG will be created. This inventory can be analysed e. g. for identified security issues.

Our partners and suppliers in the supply chain should benefit from the introduction of the FOSS Disclosure Portal in the following ways: By connecting to the portal's API, FOSS information can be submitted directly instead of filling out specific disclosure documents. The resulting information in the portal provides transparency and allows for earlier and more frequent alignments between all parties in the development process in order to meet our defined FOSS quality standards.

The development of our FOSS Disclosure Portal is based on current technologies. Our vision is to drive the development of this product together with the Open Source Community and our partners. To allow the optimization to exchange FOSS information on both sides, an initial component of the FOSS Disclosure Portal (our Command Line Interface, CLI) has already been published under Open Source. Based on these learnings we would like to plan further steps in driving this initiative together with motivated FOSS experts.

References

↗ Mercedes-Benz FOSS Manifesto
↗ Disclosure CLI on Github

Sonatype

As vital as we know open source is to building software in today's world, there is significant room for error, when not properly managed. Open source has and will continue to change how the world innovates, but simply put not all parts are created equal. Sonatype's 8th annual State of the Software Supply Chain Report found that in the last year alone organizations downloaded more than 3.5 Trillion open source components from just the top 4 programming languages. These components are then comprising 80-90% of an average application.

Further, we know that around 1 in 10 components downloaded contain a **known** security vulnerability. This doesn't include malicious attacks on open source (which has grown over 700% each year in the past three years). This is just known security issues. And, these truths are not unknown by the market. Look no further than 2021's infamous Log4j project that contained the now-famous Log4Shell security vulnerability.

This is all important to understand as we look at the very interesting data from the current 2023 BITKOM Study Open-Source-Monitor around securing open source. The report says 40% of commercial and 33% of public companies are attempting to manage all of this manually. While it's encouraging to see nearly a third of companies are using an analysis tool, the percentage of those monitoring their security of open source components manually or not at all is concerning. Further, another third of respondents, both private and public, noted that they trust the open source supplier to let them know if there is a security issue within a component.

Recognizing the sheer magnitude of open source adoption unveils a harsh reality: relying solely on manual reviews is comparable to futilely emptying the ocean with a teaspoon, rendering it practically fruitless. We wholeheartedly acknowledge and appreciate the efforts of open source maintainers as security allies, but it is crucial to acknowledge their imperfections and not rely solely on them for a primary open source cybersecurity strategy.

Delving deeper into this year's findings, it becomes apparent that merely 21% of users of analysis tools are leveraging them as intended within development build tools. The prevailing majority of both private companies (63%) and public companies (53%) rely on these tools in a manual capacity, namely, whenever the need presents itself. Unfortunately, the harsh reality is that if one opts to run an analysis only »as needed,« they are likely already lagging behind.

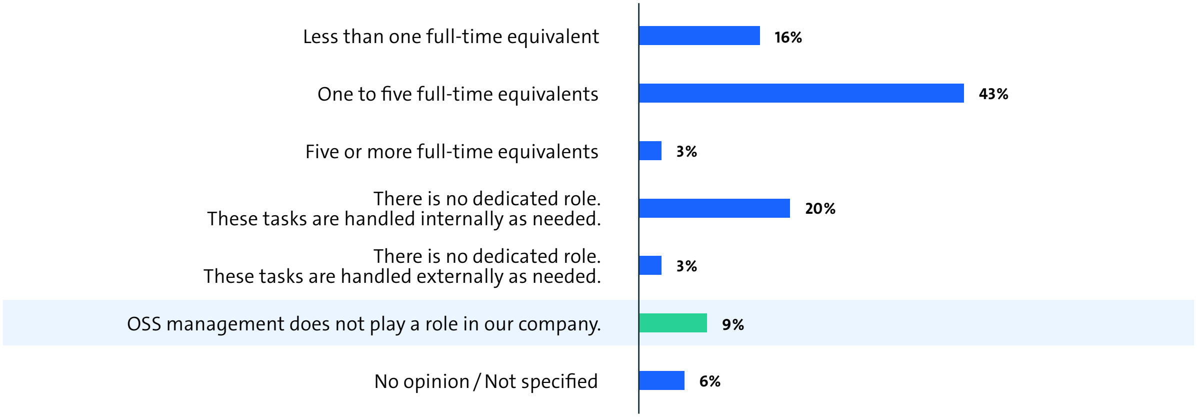
With the recent enactment of the Cyber Resilience Act (CRA), the data becomes even more alarming and warrants thorough analysis, for European Union member countries. The CRA is designed to address the growing threats surrounding digital products, by bolstering development and delivery standards. It places liability squarely on product creators, ensuring a serious focus on security throughout the product's lifecycle. Complying with the CRA will require German companies to establish a scalable operation. However, the responses to the BITKOM study indicate that there is still a considerable distance to cover.

1.4 Open Source Software management and security checks

The previous chapter shows that most German companies with at least 20 employees report using OSS (69 percent). This chapter deals with questions about OSS management to get a more detailed insight into the use and handling of OSS within companies. OSS management in this context has been defined as follows: Practices and processes used to manage and coordinate the development and deployment OSS within organisations. We will be looking at the number of employees companies assign to OSS management, whether they have a dedicated OSS department, and how they conduct security audits in the context of OSS management.

Around six in ten (62 percent) companies that use OSS say that a dedicated number of people focus on managing OSS in the company (see Figure 16). One-fifth (20 percent) of the companies handle the tasks internally if required, and 3 percent commission external service providers for OSS management if needed. Only one-tenth (9 percent) of companies state that OSS management plays no role.

How many employees focus on OSS management?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801)
Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

Figure 16 – Open Source Software management

How many employees focus on OSS management?

Size categories	Ø employees
20 – 99 EE	1,2
100 – 199 EE	2,9
200 – 499 EE	2,8
500 – 1.999 EE	6,1
2.000+ EE	6,7
Overall	1,7

Deployment level	Ø employees
Usage without advancement	1,7
Integration without advancement	1,8
Development and Advancement	1,8
Overall	1,7

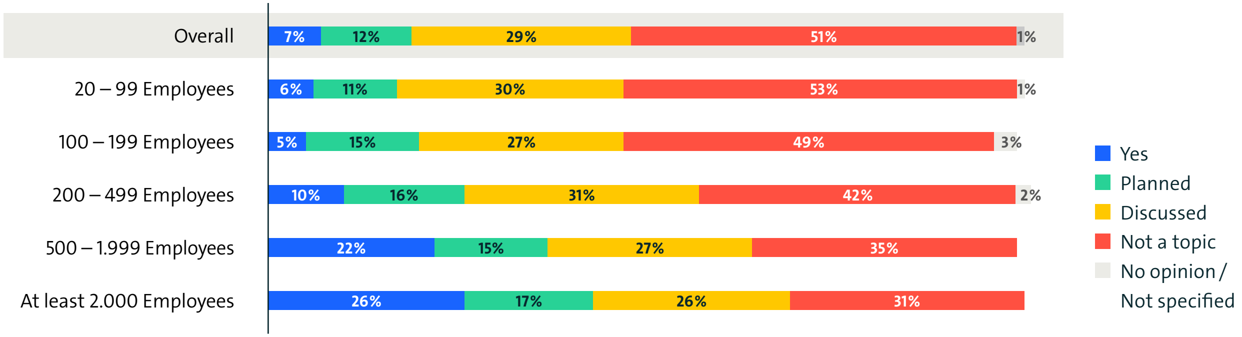
Sample: All companies with at least 20 employees that have a dedicated role for OSS management (n = 504) | Source: Bitkom Research 2023

Figure 17 – Employees Open Source Software management

Figure 17 shows that companies that create a dedicated role for OSS management allocate an average of 1.7 full-time equivalents to this task. As expected, the number of employees increases with the size of the companies. Looking at the deployment levels of OSS (use, integration, and (further) development)), there are no differences in the average number of employees.

When asked about an Open Source Program Office (OSPO), i.e., a central organisational unit that takes care of Open Source Software issues across the board, 7 percent of the companies that use, integrate, or (further) develop OSS say they have set up such an organisational unit (see Figure 18). Around one-tenth (12 percent) say they have specific plans to set it up. Just under a third (30 percent) are discussing the establishment of such an organisational unit.
This consideration is currently not an issue for half (51 percent) of the companies.

Have you set up an Open Source Program Office?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

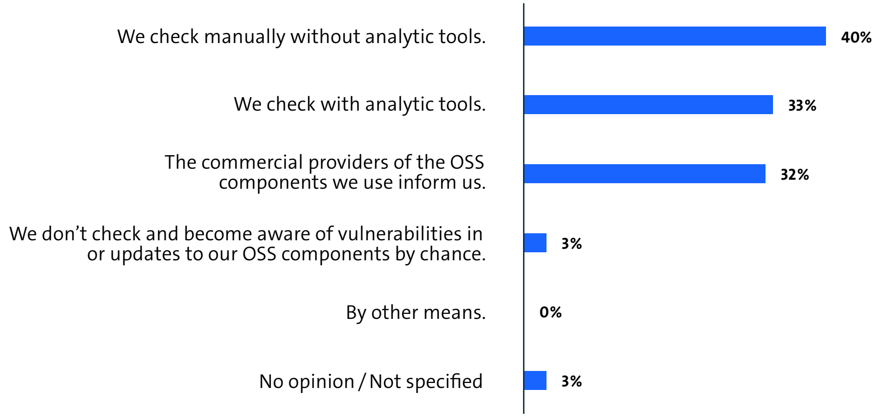
Figure 18 – Open Source Program Office deployment by company size classes

A look at establishing an OSPO along the company size classes shows a more significant jump for companies with 500 or more employees. One-fifth of companies with 500 to 1,999 employees (22 percent) have already set up an OSPO. Among companies with 2,000 or more employees, that figure is as high as a quarter (26 percent). Accordingly, the proportion of larger companies for which an OSPO facility is currently not an issue is also lower (500 to 1,999 employees: 35 percent; 2,000 and more employees: 31 percent).

↗Chapter 1.1 showed that aspects of OSS's IT security, compared to the most significant advantages, were predominantly mentioned as a disadvantage of OSS (disadvantage: 19 percent, advantage: 4 percent). Thus, this chapter's central aspect deals with the security testing of OSS components that companies use, integrate, or (further) develop.

While 40 percent of companies say they audit manually without analytic tools, one-third (33 percent) state they audit with analytical tools (see Figure 19). Another third (32 percent) are also informed about vulnerabilities by the commercial providers of their OSS components.

What approach do you take to check the security of your OSS components in your company?



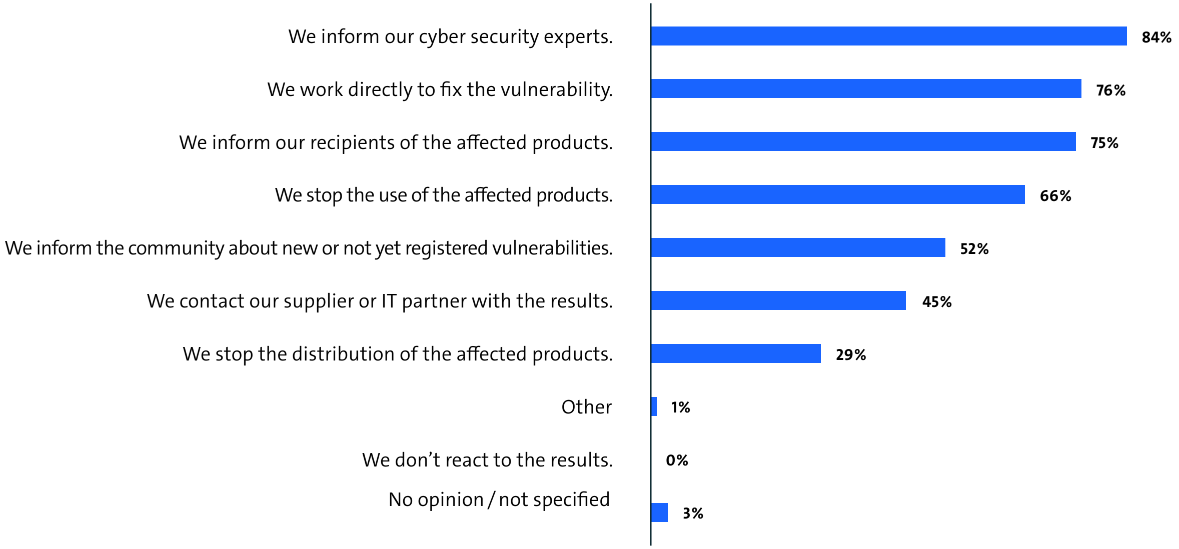
Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Multiple answers possible
Source: Bitkom Research 2023

Figure 19 – Open Source Software security audit

Only 3 percent of companies say they do not specifically check for vulnerabilities or security updates, compared to 23 percent in 2021. The decline by 20 percentage points shows that the security of the OSS used has become much more critical in the last two years.

Among the companies with a process for auditing the security of deployed OSS components, no one (0 percent) reports not acting on the results (see Figure 20), which was expected. Eight out of ten (84 percent) companies inform their cyber security experts about security vulnerabilities. Three-quarters (76 percent) of the companies work directly on fixing vulnerabilities and let the people who use affected OSS products know (75 percent). Two-thirds (66 percent) of the companies also stop using the affected products. Half (52 percent) of the companies say they will inform the OSS community if the vulnerabilities still need to be registered. 45 percent of the companies turn to suppliers or IT partners with the findings. Three out of ten (29 percent) companies say they stop selling the affected products.

How do you deal with findings from the analysis about security vulnerabilities?



Sample: All companies with at least 20 employees that generally perform security vulnerability testing (n = 753) | Multiple answers possible
Source: Bitkom Research 2023

Figure 20 – Open Source Software Vulnerability management

NORDEMANN

Open Source Software and patent portfolios

Legal and organisational challenge of Open Source contributions

The welcome development of increasing Open Source contributions raises the question of patent clauses and how they constitute a »threat« to the IP portfolio. Many Open Source licences contain provisions on patent licensing, and even without such requirements, implicit licensing can be assumed. We have already encountered cases where patent owners have potentially licensed a patent family almost entirely free of charge to anyone through ill-considered and insufficiently organised Open Source out-licensing.

This topic is particularly relevant in larger technology companies that regularly manage patent portfolios. A functioning coordination between Open Source teams (OSPOs), which tend to be »IT-oriented« and traditionally patent-centred IP departments, is required. Here, Open Source contributions give rise to new central legal questions and a corresponding need for organisational design.

From a legal point of view, the first question to be examined is which patents could be covered by out-licensing as part of an Open Source contribution. This approach requires interpreting the relevant patent clause. From our experience, this can be a first challenge for legal departments and Open Source teams. For the patent department, it is then a matter of examining the IP portfolio, which can also be a challenge. In particular, the »subsumption« of a specific software component as part of a patent application clause and the subsequent identification of the corresponding IP rights can become complex as this has to be examined in detail.

This question, initially a legal issue, is also reflected in the company's organisational aspects and processes. First, care must be taken to ensure that appropriate regulations for Open Source contributions exist in the company and that Open Source contributions can be made under the supervision of the Open Source team. Furthermore, the Open Source team and the IP department must specify the relevant IP rights, assess any risk, and identify risk-minimising design options, if necessary.

NORDEMANN offers comprehensive advice in IP/IT and Open Source law. Christian Czychowski and Sebastian Dworschak are available for enquiries.

Prof. Dr. Christian Czychowski

Sebastian Dworschak

↗ www.nordemann.de
↗ info@nordemann.de

The respective company is responsible for the content of the page.

Secure Open Source

From the university project over EAL4+ certified Separation Kernel to SECRET-approved products platform – the Open Source Operating system L4Re example

Katrin Kahle
Head of Product, Kernkonzept GmbH

Emergence of the FOSS Operating system core at TU Dresden

The L4Re Operating System Framework results from the development of a group of operating system scientists at TU Dresden, who have been researching real-time capable and secure L4 microkernels since the mid-1990s. At that time, the conditions were such that today's safety or certification requirements did not yet play a role.

Thanks to the group's high standards for qualitative software development, the foundation of L4Re was laid.
L4Re is used as an operating system or hypervisor in many products approved up to a SECRET level.

Implementation with Shift-Left since the 90s

The high standard was implemented early through a pronounced Shift-Left orientation to detect errors as early as possible. A process was established with six quality gates to be passed before a release.

Quality Gate 1: Integrated development environment of the developer: Choosing a good IDE helps navigate the code, provide documentation, and code completions.

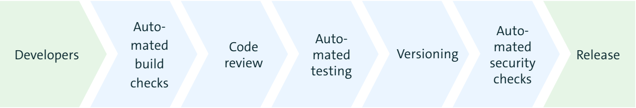
Quality Gate 2:Automated build checks after each change across all processor architectures and for all relevant configurations.

Quality Gate 3: Four-eyes code review, with audit logs for documenting difficult design decisions, allows high traceability and prevents the introduction of backdoors.

Quality Gate 4: Automated testing with low-level API tests, integration testing, and regression testing.

Quality Gate 5: Versioning for high traceability, integrity protection, availability, and joint development.

Quality Gate 6: Automated security checks using formal methods, advanced testing and focus testing.



Shift-Left Quality Gates at Kernkonzept

Additional steps for security according to CC EAL4+

Founding of Kernkonzept GmbH in 2012 as sole consultant to ensure the quality requirements of clientele and certification

Evaluierung and testing by an independent assessment office

Massive expansion of documentation: Process documentation and life cycle, creation of security advisories

Introduction of SBOM in SPDX format 2017
(Open Chain Project)

Result

A certified secure Open Source Operating system for safely connected devices and a digitally sovereign Europe

↗ contact@kernkonzept.com / kernkonzept.com

The respective company is responsible for the content of the page.

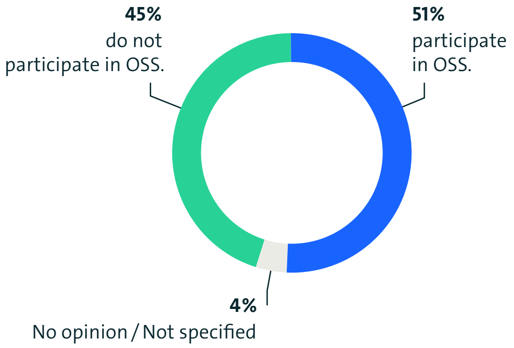
1.5 Participation in Open Source Software

The strength of Open Source Software lies in the commitment of users to the continuous improvement of the software. An active OSS community with high levels of participation in software development or advancement is the foundation of a successful OSS project. Half (51 percent) of German companies with at least 20 employees are actively involved in OSS's development or advancement (see Figure 21).

Participation in OSS projects is as follows: Four out of ten (41 percent) companies support purchasing support services or subscriptions for corresponding OSS enterprise editions (see Figure 22). A quarter (25 percent) of companies give individual employees or teams permission to participate in OSS projects as part of their work.

One-seventh (15 percent) participates by providing enhanced OSS source code. 12 percent initiate and participate in projects as part of their business activities. Another 8 percent say they are paying members of OSS foundations.
In comparison, only 3 percent of companies participate in OSS by sponsoring OSS events.

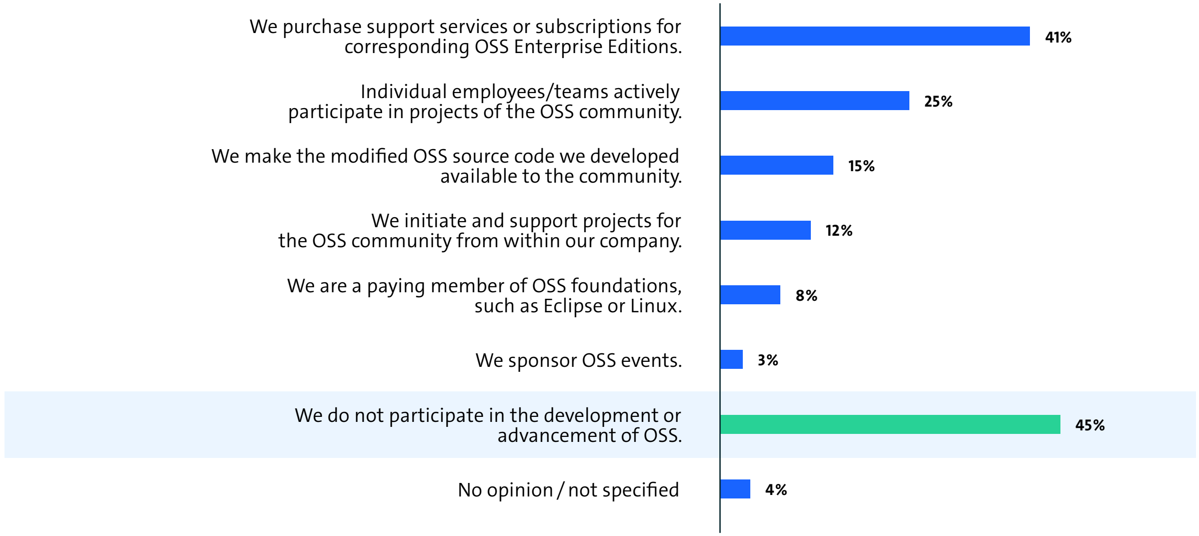
Do you participate in the development or advancement of OSS?



Sample: All companies with at least 20 employees (n=1,155)
Source: Bitkom Research 2023

Figure 21 – Participation in Open Source Software

To what extent is your company involved in the development or advancement of OSS?

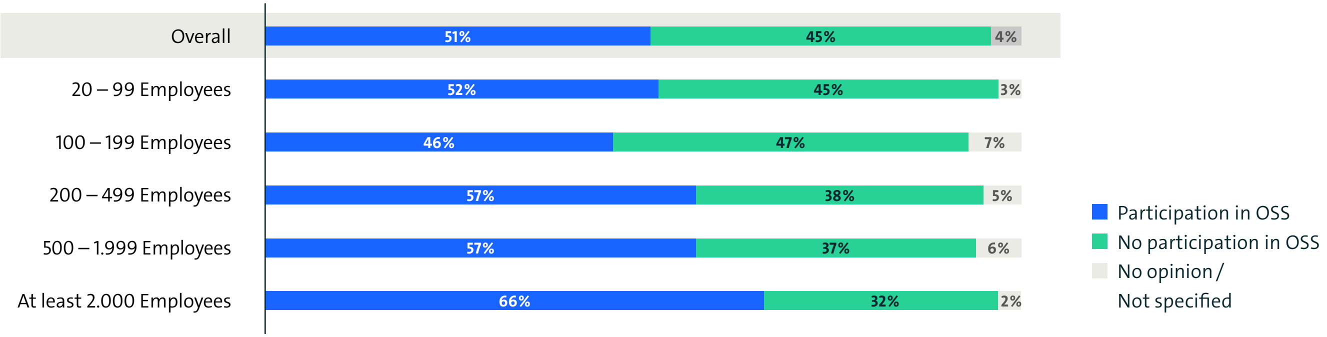


Sample: All companies with at least 20 employees (n=1,155) | Multiple answers possible | Source: Bitkom Research 2023

Figure 22 – Participation in Open Source Software by type

Participation in OSS's development or advancement depends on the company size classes (see Figure 23) and increases with company size. Half (52 percent) of companies with 20 to 99 employees participate in OSS. Among companies with 100 to 199 employees, participation decreases slightly (46 percent). Participation increases among companies with 200 to 1,999 employees: around six out of ten companies participate (57 percent). At 66 percent, the most pronounced participation is among large companies with 2,000 or more employees. There are parallels with the number of people who focus on OSS, which also grows with increasing company size (↗Chapter 1.4., Figure 17).

Do you participate in the development or advancement of OSS?



Sample: All companies with at least 20 employees (n = 1,155) | Source: Bitkom Research 2023

Figure 23 – Participation in Open Source Software by company size classes

Open Source Compliance? More efficient, please!

Open Source Software (OSS) has become pervasive and indispensable for modern software development. A typical software product often contains over 90 percent Open Source.

Alarmed by spectacular cyber-attacks on the software supply chain, the US has issued regulations such as the »Executive Order on Improving the Nation's Cybersecurity«. The EU is currently drafting the European Cyber Resilience Act (CRA). All Open Source components must be designated and identified for legally compliant use.

However, creating a complete Software Bill of Materials (SBOM) with a correct designation of components and copyrights can be time-consuming and costly. For example, a complete analysis of a product based on Android can quickly run into six-figure sums for the audit. Especially for medium-sized companies, these costs are often unexpected and usually an immense challenge.

Thus, all market participants mostly agree that efficiency in preparing a legally compliant SBOM must be increased. Various approaches are being pursued here: The OpenChain ISO/IEC 5230 standard marked a crucial step in the **standardisation** of the compliance process. Furthermore, the introduction of SPDX and CycloneDX unified the description of the relevant data, enabling a more efficient exchange within the supply chain.

Since most **scanners** still work with text recognition or curated databases, research projects attempt to increase the efficiency of SBOM creation utilising AI. However, initial tests suggest that considerable development and research is still required.

Another idea is to provide already **curated licence information**. Repositories such as »GitHub« and »Maven« have recently made these available. Tools track dependencies to facilitate licence compilation. However, the reliability of the information provided does not always meet the legal requirements. Projects such as »OSSelot« or »ClearlyDefined« allow the recycling of SBOMs of already audited Open Source packages and claim to offer better curated data.

The SW360 and SBOM Insight approach allows the creation of a **catalogue** of audited components along the supply chain. Both enable the reuse of trusted (proprietary) data between projects. Some projects take the approach of **restructuring** the code and adding more information to facilitate detection.

»REUSESOFTWARE« provides information on how complete licence information can be automatically anchored directly in the code. The 2017 Linux clean-up activity also aimed to provide all files in the kernel with a unique SPDX identifier.

Often it is attempted to integrate licence recognition directly into the development process in a CI/CD pipeline and to keep the SBOM up to date **continuously**.

Right now, several approaches are being pursued to make the preparation of an SBOM more economically efficient. However, the question of liability in the event of errors in the lists still needs to be clarified.

Bitsea advises on the sustainable use and compliance of Open Source Software. Our customers include well-known corporations from all industries. Bitsea is an OpenChain partner.

↗ www.bitsea.de

{metæffekt}

Expert-Statement: Positioning of the EU Cyber Resilience Act to the OSM#23

Context

With the Cyber Resilience Act (CRA) [1], the EU aims to harmonize the security requirements of products with digital elements in the European Market. The CRA intends to increase the level of cyber security of these products and to consequently counter vulnerabilities. The current draft contains basic and comprehensive requirements on the following topics:

- Creation of Software Bill of Materials (SBOM)
- Evaluation and management of security aspects
- Conformity of manufacturers in the supply chain
- Verification and validation of SBOM content

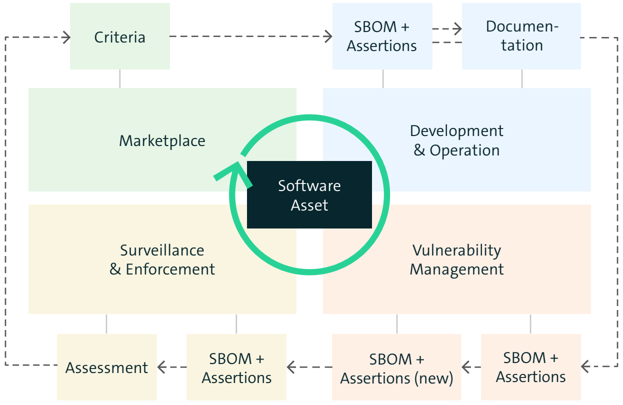
Open Source Software (OSS), if used in a commercial context, will be included in the future regulation.

Status Quo

To a certain extend central aspects of the CRA are already reflected in the Bitkom Open Source Monitor (OSM#23). Given measures and requirements formulated in the CRA are known practices in industry and administration. This can be observed in key figures of the OSM#23. For example, 38.5 percent in administration and 31.7 percent of the companies surveyed create an SBOM. When using OSS, 64.3 percent in administration and 72.8 percent in industry check the security of the components used. However, only 13.7 percent in industry and 23.5 percent in administration carry out automated checks at defined intervals.

Deduction from the CRA

In the following, the software asset as substantial part of a product with digital elements is depicted in the context of the four main regulatory areas of the CRA:



Software asset lifecycle

For such a software asset, various criteria are concluded from the demands of the market and emphasized by the CRA. These criteria must be recognized in development and operation. An SBOM is required to describe a software asset and to assert individual characteristics of its components. The CRA details specific requirements for the frequency of vulnerability analyses and the communication to the recipients of the software asset. The SBOM with its assertions is used to assess and monitor the market-specific criteria and enables due response to vulnerabilities or other issues affecting the software asset.

Open Source in Industry and Administration

OSS is essential for modern software development and encourages a collaborative ecosystem. The OSM#23 illustrates central arguments of industry and administration with respect to OSS. To stimulate the advanced application of OSS in this environment, it is necessary to ensure liability in the development and use of OSS. The CRA can suffice to promote the OSS ecosystem to a new standard of security and professionalism. However, this requires the cooperation of all participants, volunteers and companies involved.

Conclusion

From the OSM#23, it can be perceived that administration is formally better prepared than the industry in the supplier role. To meet the demands of the CRA, the current level of automation is not sufficient to provide immediate response to vulnerabilities in both sectors. The quality of the underlying SBOMs is yet out of question.

{metæffekt} GmbH [2] offers concepts, tools, and services for implementing automated processes in the software asset lifecycle. {metæffekt} is a reliable partner supporting customised implementations and integration.

[1] ↗ https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[2] ↗ https://metaeffekt.com

The respective company is responsible for the content of the page.

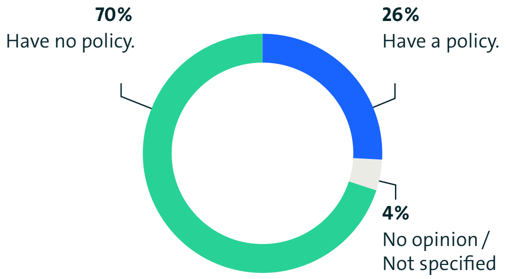
1.6 Open Source Software: Policy and Compliance

Open Source Software allows users to run it freely, view and adapt the source code, and pass it on in its original or modified form. However, it is essential to emphasise that Open Source Software does not exist in a legal vacuum. The freedoms offered by OSS are often tied to specific obligations or conditions set out in the relevant licences. Failure to comply with these licensing terms can lead to warnings, cease-and-desist obligations, or claims for damages, which can result in considerable costs for companies.

To avoid potential problems in this context, it is advisable that companies using OSS or participating in OSS projects also have adequate OSS compliance management in place. An OSS policy can be a first step in this management process. This written document sets out the company'cs guidelines and rules for dealing with OSS. A corresponding OSS policy should be required reading for employees working with OSS.

Figure 24 shows that only around one in four (26 percent) companies that use, integrate, (further) develop, or participate in OSS have an OSS policy. The vast majority (70 percent) state that they do not have a written OSS policy.

Does your company have an OSS policy, i.e., a document in which guidelines and rules concerning the use of OSS within your company are recorded?



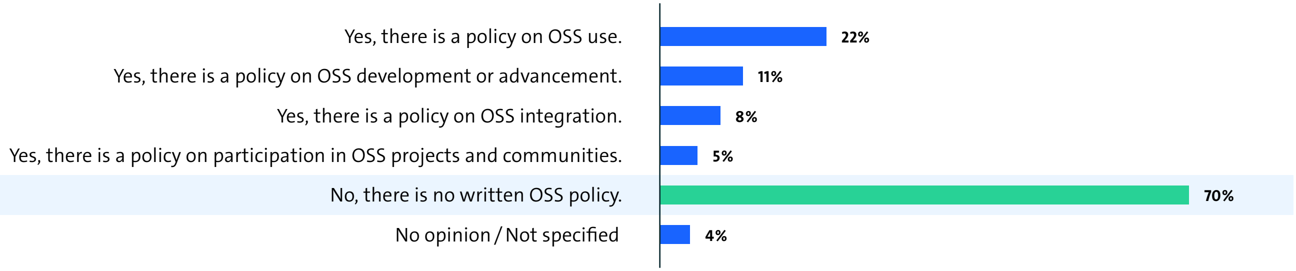
Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (n = 809)
Source: Bitkom Research 2023

Figure 24 – Open Source Software policy

The breakdown by type of OSS policy shows that most companies have a policy on OSS use (22 percent), followed by a policy on development or advancement (11 percent), a policy on OSS integration (8 percent), and a policy on participation in OSS (5 percent) (see Figure 25).

The breakdown by company size shows that smaller companies, in particular, often still need to define an OSS policy (25 percent with a policy for 20 to 99 employees and 26 percent for 100 to 199 employees) (see Figure 26).

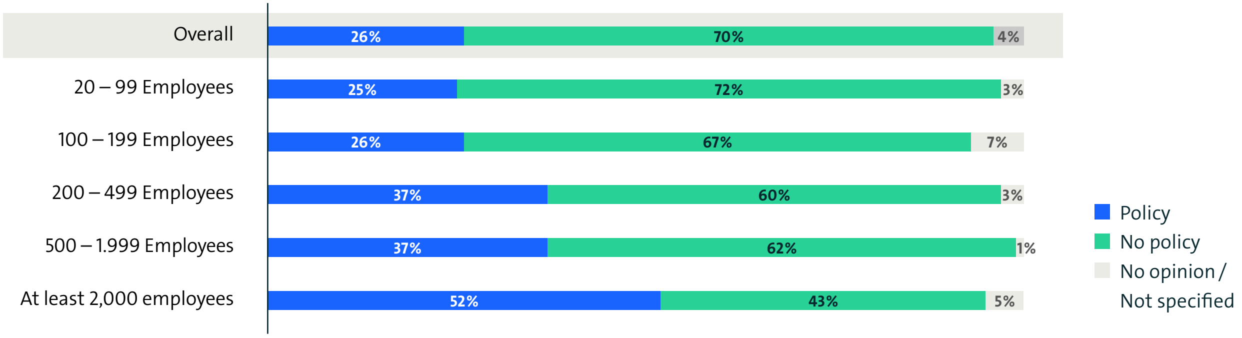
Does your company have an OSS policy, i.e., a document in which guidelines and rules concerning the use of OSS within your company are recorded?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (n = 809) | Multiple answers possible
Source: Bitkom Research 2023

Figure 25 – Open Source Software policy by type

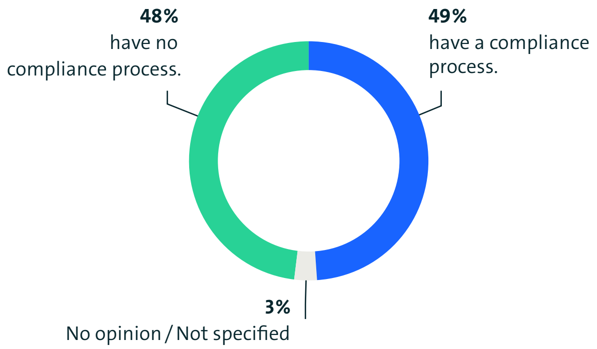
Does your company have an OSS policy, i.e., a document in which guidelines and rules concerning the use of OSS within your company are recorded?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (n = 809)
Source: Bitkom Research 2023

Figure 26 – Open Source Software policy by company size classes

Does your company have a formal compliance process for dealing with OSS?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (n = 809)
Source: Bitkom Research 2023

Figure 27 – Open Source Software compliance process

Almost four out of ten (37 percent) companies with 200 to 1,999 employees have an OSS policy. Over half (52 percent) of large companies with at least 2,000 employees already have an OSS policy in place.

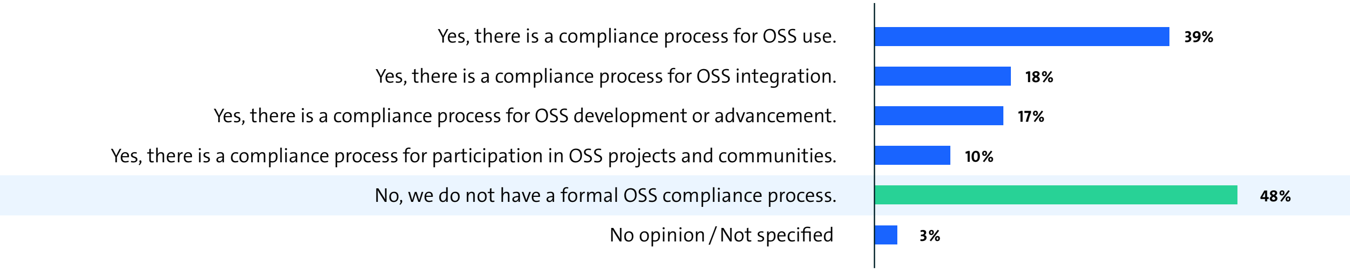
The results concerning compliance processes within the companies using OSS or participating in OSS projects differ from an OSS policy (see Figure 27).

Around half (49 percent) of the companies have a written compliance process. In other words, there are almost twice as many companies with compliance processes documented in a guideline – i.e. standardised procedures that provide a binding framework for the OSS strategy and the guidelines and rules for employees – than with an OSS policy. Deeper insights regarding an existing OSS strategy and compliance process are provided in ↗ Chapter 2. There, the two questions are considered across time, using the results from 2019 and 2021.

A look at the active areas in which compliance processes exist shows that two fifths (39 percent) of the companies have a compliance process for using OSS (Figure 28). 18 percent have a compliance process for integrating OSS. 17 percent for the development or advancement of OSS. Only one-tenth (10 percent) of companies have a compliance process for participating in OSS projects and communities.

Figure 29 shows no significant changes concerning the proportion of companies with a compliance process for business with up to 1,999 employees (20 to 99 employees: 49 percent; 100 to 199 employees: 52 percent; 200 to 499 employees: 46 percent; 500 to 1,999 employees: 51 percent). The share only increases significantly for large companies with 2,000 or more employees. In this company size class, two-thirds (67 percent) of companies have a standardised procedure using written compliance processes.

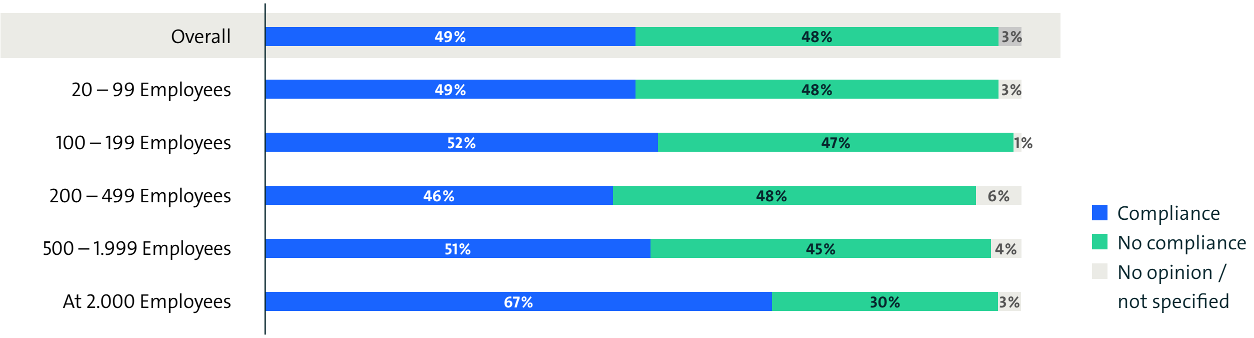
Does your company have a formal compliance process for dealing with OSS?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (n = 809) | Multiple answers possible
Source: Bitkom Research 2023

Figure 28 – Open Source Software compliance process by type

Does your company have a formal compliance process for dealing with OSS?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (n = 809)
Source: Bitkom Research 2023

Figure 29 – Open Source Software compliance process by company size classes

2 Company Use Key Topic: Policy and Compliance

The first chapters have provided a representative overview of how OSS is used in German companies with at least 20 employees. This chapter will focus on questions about the standardisation of processes in the field of Open Source. Although Open Source processes may be standardised to varying degrees depending on the project and the community, overall efforts are underway to establish a form of standardisation to improve the collaboration, interoperability and reusability of Open Source Software.

Period-related questions about a policy and a compliance process for OSS are shown first to contextualise this topic. After that, the focus is on compliance management of OSS in the supply chain. For this purpose, the following is examined:

- Are companies aware of the OpenChain standard for OSS compliance or ISO/IEC 5230?
- Do companies provide or request a document of all OSS components used and their licences, also known as a Software Bill of Materials (SBOM)?

The international standard ISO/IEC 5230 defines the requirements for an effective Open Source compliance program. At the same time, creating a document with licence texts is an essential part of this.

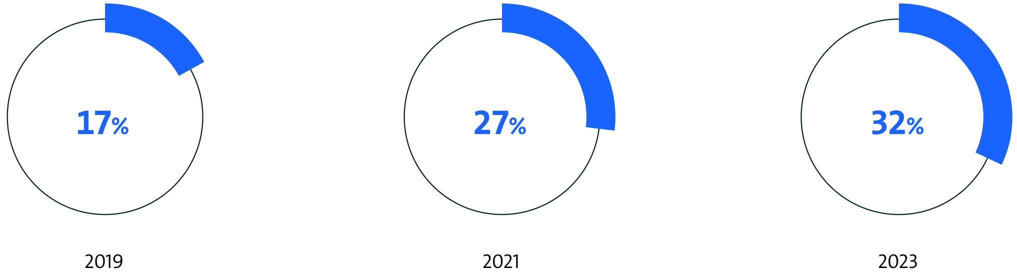
The results should help to understand to what extent companies that use, integrate or (further) develop OSS have standardised their OSS processes.

As mentioned in the methodology section, we only surveyed companies with at least 100 employees in 2019. The selected period from 2019 onwards was used to evaluate companies with at least 100 employees that use OSS or participate in OSS projects.

For companies with at least 20 employees, an annual comparison from 2021 to 2023 was also evaluated.

A look at the availability of an OSS policy shows an increase of 10 percentage points from 2019 (17 percent) to 2021 (27 percent) (see Figure 30). However, the increase levels from 2021 to 2023 for companies with 100 or more employees (2021: 27 percent; 2023: 32 percent; see Figure 30) and businesses with at least 20 employees (2021: 22 percent; 2023: 26 percent; see Figure 31).

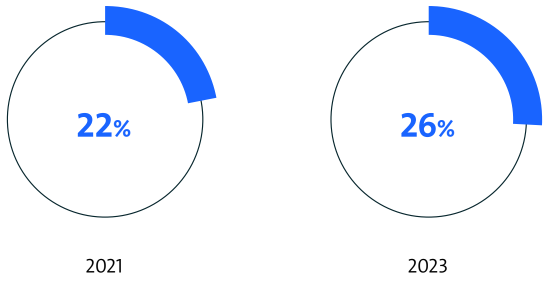
Does your company have an OSS policy, i.e., a document in which guidelines and rules concerning the use of OSS within your company are recorded?



Sample: All companies with at least 100 employees that use or integrate or (further) develop OSS or participate in OSS (2023: n = 616 | 2021: n = 629 | 2019: n = 593) | Source: Bitkom Research 2023

Figure 30 – Open Source Software policy year on year since 2019

Does your company have an OSS policy, i. e., a document in which guidelines and rules concerning the use of OSS within your company are recorded?

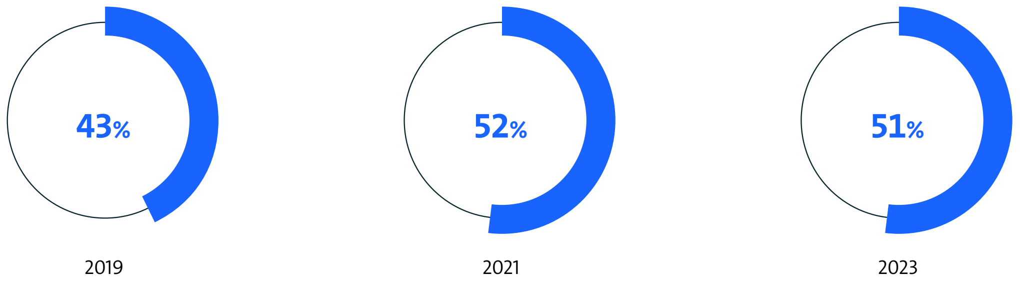


Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (2023: n = 809 | 2021: n = 843) | Source: Bitkom Research 2023

Figure 31 – Open Source Software policy year on year since 2021

A similar observation can be made with respect to the question of whether a compliance process is in place. The percentage of companies with a compliance process for OSS increased from 43 percent in 2019 to 52 percent in 2021 (see Figure 32). In 2023, no changes were observed for compliance processes. The shares stagnate for companies with 100 or more employees (2021: 52 percent; 2023: 51 percent; see Figure 32) and for companies with 20 or more employees (2021: 48 percent; 2023: 49 percent; see Figure 33).

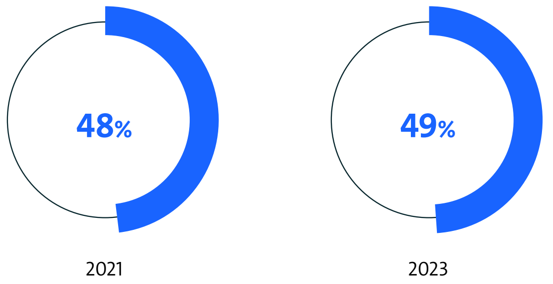
Does your company have a formal compliance process for dealing with OSS?



Sample: All companies with at least 100 employees that use or integrate or (further) develop OSS or participate in OSS (2023: n = 616 | 2021: n = 629 | 2019: n = 593) | Source: Bitkom Research 2023

Figure 32 – Open Source Software compliance process year on year since 2019

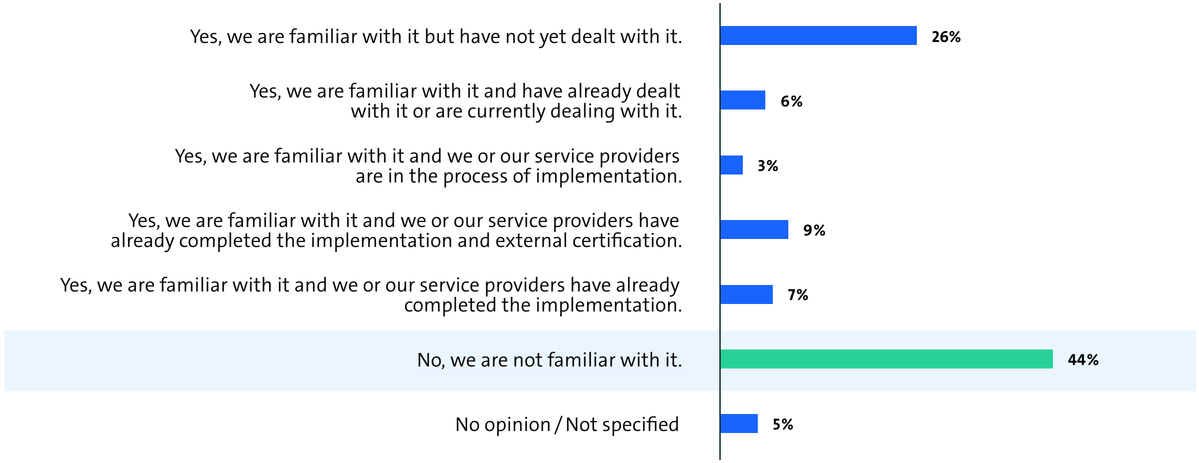
Does your company have a formal compliance process for dealing with OSS?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS or participate in OSS (2023: n = 809 | 2021: n = 843) | Source: Bitkom Research 2023

Figure 33 – Open Source Software compliance process year on year since 2021

Are you familiar with the OpenChain standard for OSS compliance or ISO/IEC 5230?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Source: Bitkom Research 2023

Figure 34 – Awareness of ISO/IEC 5230 OpenChain standard

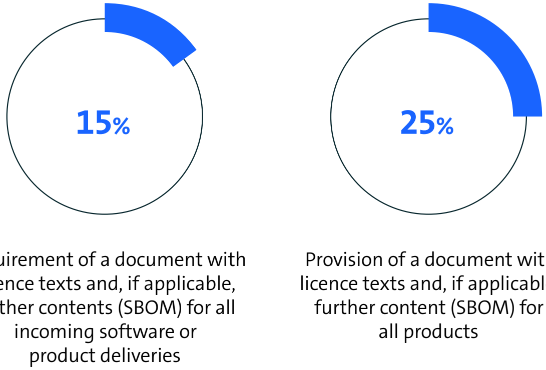
Thus, increased standardisation through increased written in-house OSS policies or OSS compliance processes has yet to be observed since 2021. To get a better picture of standardisation, the companies with at least 20 employees that use, integrate or (further) develop OSS were also asked about standardisation measures around compliance management of OSS in the supply chain.

The Linux Foundation's OpenChain project has developed an industry standard for Open Source licence compliance to promote best-practice compliance procedures for the use of Open Source Software in enterprises.
The standard was published at the end of 2020 and is called ISO/IEC 5230. Among the companies that use OSS, half (51 percent) are familiar with the OpenChain standard (see Figure 34). However, it should be noted that around a quarter (26 percent) of companies are aware of the standard but have yet to engage with it on a deeper level.

6 percent have already taken a closer look at it or are currently doing so. 3 percent state that they or their service providers are currently in the implementation phase of ISO/IEC 5230. About one-tenth (9 percent) have already completed the implementation of the standard. Only 7 percent of companies have completed external certification in addition to implementation.

An essential part of a compliance programme is the complete and correct identification of all OSS components and the corresponding creation of a Software Bill of Materials (SBOM). The SBOM lists all Open Source components used in a product or software and the associated licence information. Creating an SBOM is crucial to ensure transparency and traceability of the Open Source components used.

Which of the following measures and tools for OSS compliance management in the supply chain does your company use?



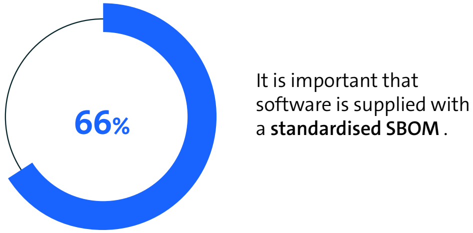
Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Source: Bitkom Research 2023

Figure 35 – Use of SBOM in OSS compliance management

As a result, companies have a much better understanding of the licences included in their software, the licence obligations they have to meet and whether the use of these licences complies with the company's internal policies and the licensing terms of the respective Open Source components. Among companies that use, integrate, or (further) develop OSS, only 15 percent require SBOM for incoming software or product deliveries (see Figure 35). A quarter (25 percent) of companies provide SBOM for all products.

Because of these results, standardised compliance processes have not yet reached the majority in practice. However, it is exciting that two-thirds (66 percent) of companies that use OSS say it would be necessary for OSS to be delivered with a standardised SBOM (see Figure 36). It shows that the market recognises the need for action towards more standardisation, even if implementation still needs to catch up. This assumption is supported by the fact that just under half (47 percent) of the companies feel well-positioned to use OSS safely and consciously (see Figure 37).

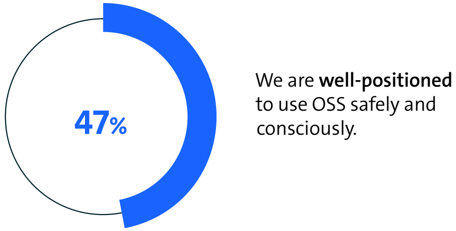
In your opinion, does the following statement apply to your company?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Percentages for »Strongly agree« and »Rather agree« | Source: Bitkom Research 2023

Figure 36 – Statement: SBOM

In your opinion, does the following statement apply to your company?



Sample: All companies with at least 20 employees that use or integrate or (further) develop OSS (n = 801) | Percentages for »Strongly agree« and »Rather agree« | Source: Bitkom Research 2023

Figure 37 – Statement: Intentional use of OSS

Cooperative competition instead of lone wolves

Red Hat

The added value of an ecosystem becomes even more evident when we consider the interaction of all components. The interests and needs of numerous actors are brought together, and innovative ideas are developed as if guided by an invisible hand. Open Source is an ecosystem that empowers developers, service providers, and consultants in their projects to work together on new solutions. It requires an open, transparent mindset that replaces lone wolves with collaborative performance. This approach does not dilute corporate success but rather accelerates cultural change, enabling companies to innovate disruptively.

One of the central advantages of Open Source is the efficient and cross-company use of resources. It undermines the basic assumption in production theory that all available company resources must be used to maximum output. Open Source means that internal resources are no longer the limiting factor, as companies can draw on an entire ecosystem of innovations and solutions.

Thus, it becomes possible to dissolve internal path dependencies, skip development steps, and dock onto the international status quo. It also makes sense from an ecological perspective to rely on Open Source, in addition to this economic added value: As a result, companies can more sustainably manage labour and environmental resources in times of resource scarcity and regulatory pressure.

In practice, despite limited budgets, a transparent and open system is often the fundamental prerequisite for companies to integrate complex and disruptive IT solutions into their processes. The example of artificial intelligence (AI) shows this clearly. The industry for automation and networking of plants already uses intelligent dialogue systems for customer communication. However, both examples require solutions to handle vast data and integrate with the inventory software and infrastructure. Open Source allows companies to benefit from high technology across company boundaries without a return on investment calculation or quick wins blowing up the bill. It enables a long-term approach to development that does not rely on short-term return on investment but takes a holistic approach.

Thus, resource efficiency and high technology contribute to a third success factor – innovation in day-to-day business. Developing and implementing innovative products or processes is increasingly difficult in the complex digital production that has become a reality in many markets. Only some people will succeed in establishing a new development from one day to the next. With Open Source, this innovation threshold can be lowered significantly: Those responsible can draw on a mature product and solution portfolio instead of having to develop it themselves. This way, no one has to reinvent the wheel that others have already perfected. Together, they benefit from a technological status quo that puts the next level within reach.

Dinko Eror
Vice President EMEA Central Europe, Red Hat

The respective company is responsible for the content of the page.

Open Source »end-to-end«

Digitisation with low code

publicplan GmbH, based in Düsseldorf, Berlin and Málaga, has implemented future-proof eGovernment for public administration since 2010. The service portfolio ranges from eGovernment consulting and project support to the (further) development of software solutions and long-term maintenance and support.
The team of more than 340 experts develops Open Source solutions to make the administration's services accessible to citizens. Anytime, anywhere and on any device.

The challenge
End-to-end digitisation continues to be one of the greatest challenges in the public sector. Many procedures do offer digital access from the citizen and business side. But if you think that everything will be seamlessly processed digitally once the application has been submitted, you are on the wrong track – literally. Many applications are printed on paper and end up in filing systems to be processed in the old and established ways. It costs the applicant, but especially the public sector institutions, time and resources. Digitisation looks different.

The solution
»formsflow.ai«, the Open Source solution used by publicplan, addresses precisely this issue, providing a single software product on a low-code basis, from the application to the issuing of the decision, but also queries about the applicant or even rejection.

This is made possible by the use and intelligent orchestration of standard Open Source Software components, which can be adapted quickly and modularly to the specific needs of government agencies (or business customers) – covering everything from online form creation and workflows to the integration of third-party systems.

In the sense of the low-code philosophy, simple changes and extensions can be implemented independently by desk officers in the institutions only after a brief introduction to the system.

The company publicplan is already successfully using the low-code software »formsflow.ai« for various federal-state projects, including internal digitisation, but also for funding application procedures and their processing.

The company »formsflow.ai« has a broad user base in public administration in Canada and other American countries. Some OSS components used are form.io, Camunda, reDash, Robo-corp, and Keycloack. The connection of third-party systems and the linking to interfaces is made easy and flexible by this modular structure of the publicplan low-code solution on an open-source basis, tailored to the individual use cases.

In Germany, Austria, and Switzerland, publicplan is partner of the formsflow.ai main contributor AOT.

↗ https://www.publicplan.de/loesungen/low-code-loesungen

Dr. Christian Knebel
Managing Director, publicplan GmbH

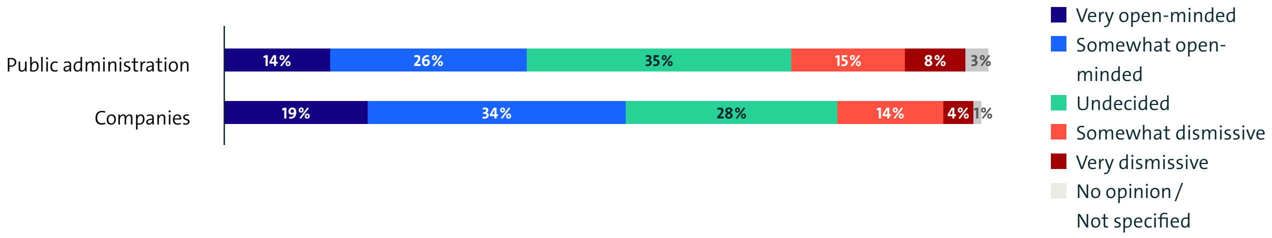
The respective company is responsible for the content of the page.

3 Open Source Software in public administration

In addition to companies in the business sector, we also surveyed public administration organisations in this study to find out how they use OSS. As mentioned in the methodology section, the public administration results are not representative but provide an insightful picture of public sector sentiment. Compared to the business community, public administration has less interest in OSS (see Figure 38).

Only two-fifths (40 percent) of administrative organisations are open to using OSS, and only half (53 percent) of companies are. One-third (35 percent) of administrative organisations are undecided, and just under one in four (23 percent) organisations are dismissive of OSS.

What is the general position of your organisation/company towards OSS?

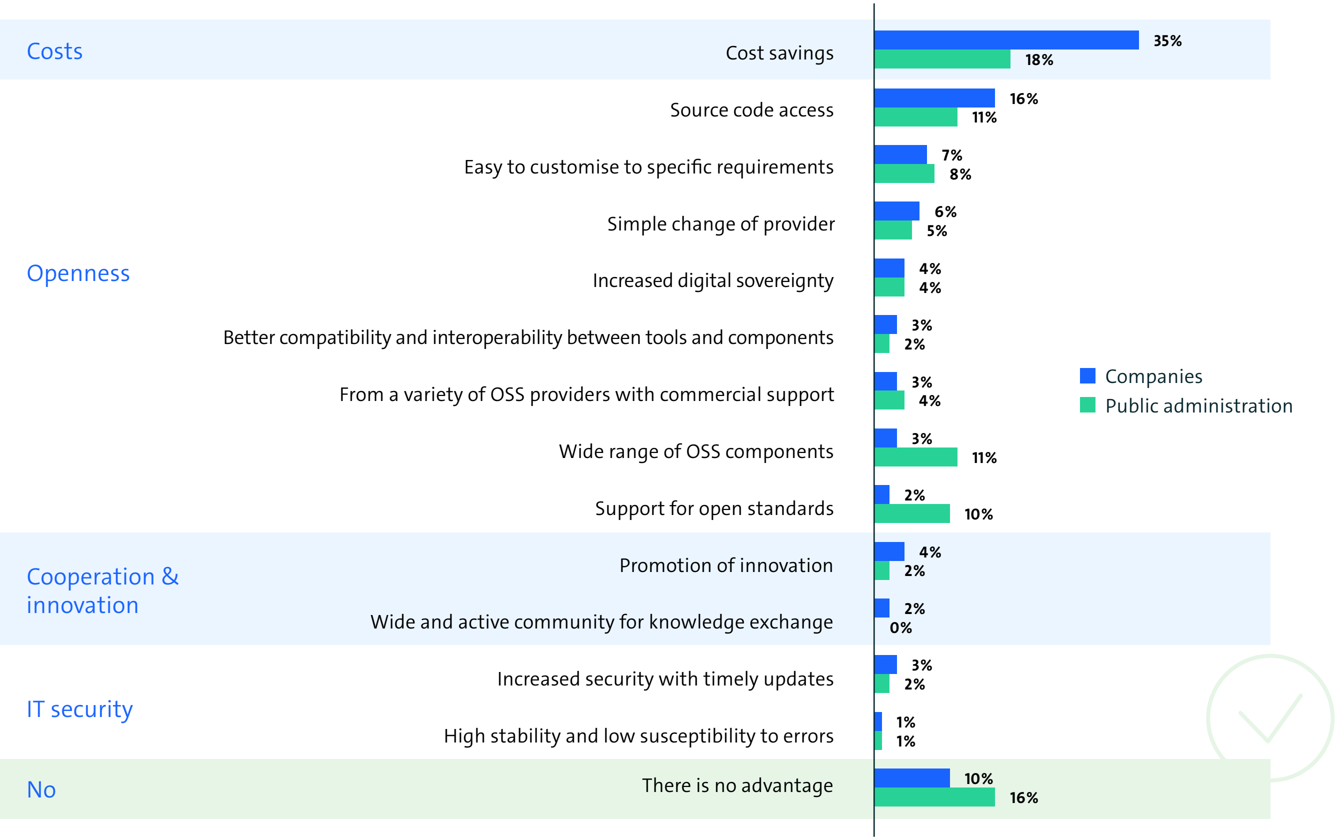


Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102)
Not all percentages add up to 100 due to rounding | Source: Bitkom Research 2023

Figure 38 – Attitude towards Open Source Software in public administration

When considering the open question about the most significant advantage of using OSS, the large selection of OSS components (11 percent) and the support of open standards (10 percent) stand out in comparison to the economy (see Figure 39). The costs saved using OSS are mentioned most often. However, the share among administrative organisations (18 percent) is significantly lower than that of the business community (35 percent). At the same time, a more significant proportion of public administration organisations (16 percent) see no advantage of OSS, unlike businesses (10 percent).

In your opinion, what is the most significant advantage that speaks for the use of OSS in your organisation/company?

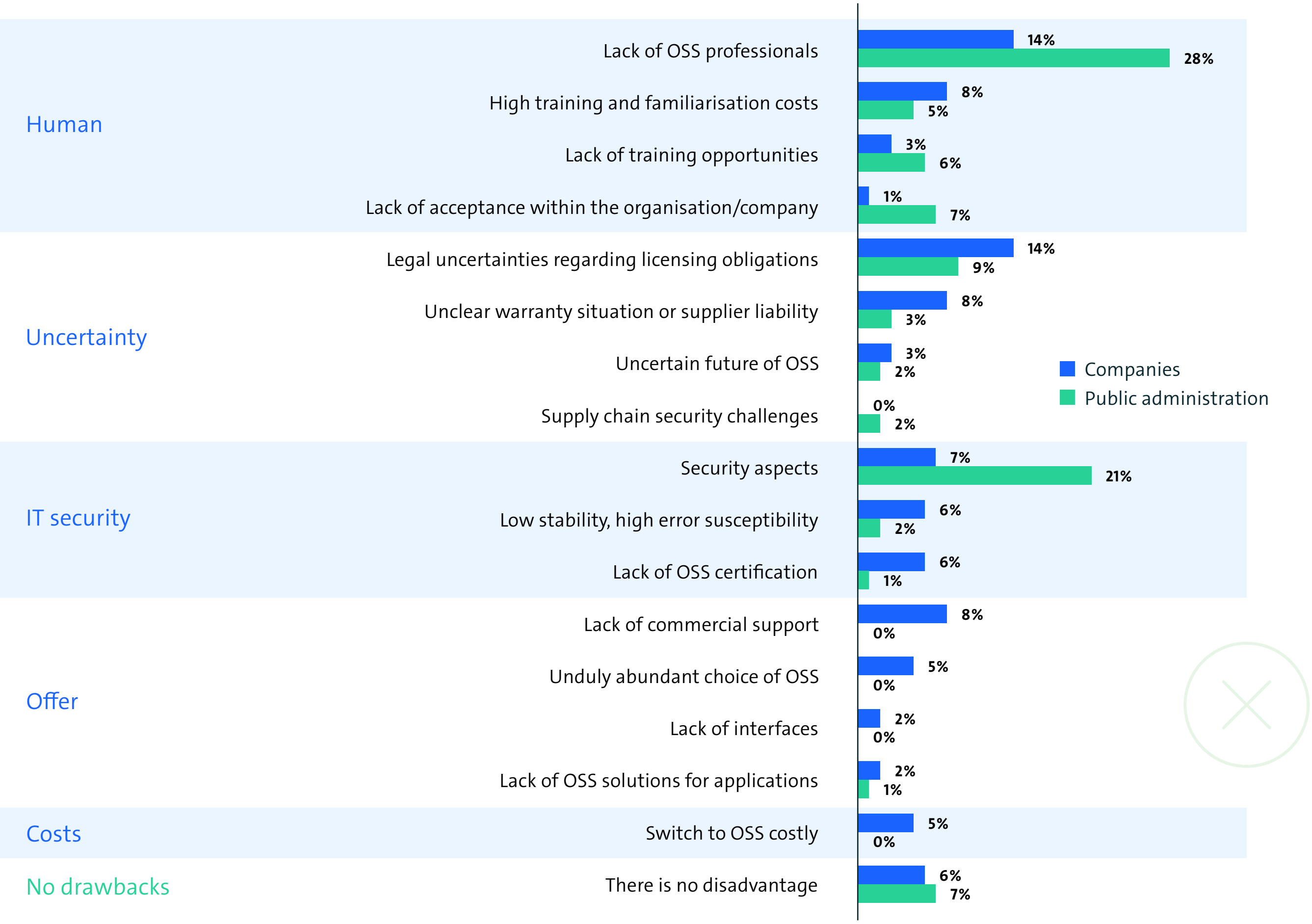


Sample: All companies with at least 20 employees (n=1,155) | Open-ended question, only one possible answer
Missing values: »No opinion/Not specified« | Source: Bitkom Research 2023

Figure 39 – Advantages of Open Source Software from the point of view of the public administration

Some differences between businesses and public administrations can also be seen with regard to the biggest disadvantage (see Figure 40). Public administration organisations cite the lack of OSS professionals (28 percent) as a disadvantage by a wide margin. Among companies, this disadvantage comes up only half as often (14 percent). Compared to companies in the business sector, the security aspects disadvantage is specifically evident. They apply to public administration organisations in particular. One-fifth (21 percent) of public administration organisations cite this disadvantage, in contrast to only 7 percent of business organisations.

In your opinion, what is the most significant disadvantage that stands in the way of using OSS in your organisation/company?



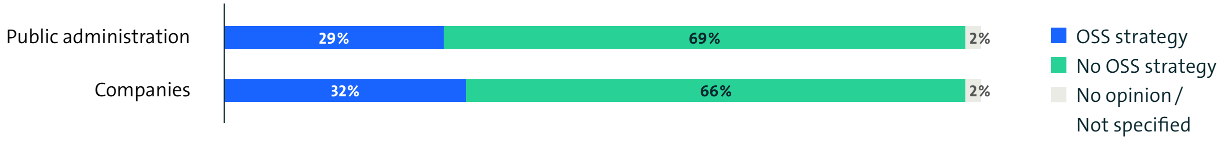
Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102)
Open-ended question, only one possible answer | Missing values: »No opinion / Not specified« | Source: Bitkom Research 2023

Figure 40 – Disadvantages of Open Source Software from the point of view of the public administration

Public administrations and businesses are at a similar stage in terms of OSS strategy (see Figure 41). 29 percent of public administrations have an OSS strategy, compared to 32 percent of companies.

When it comes to the use of OSS, this figure doubles. Around six in ten (59 percent) of administrative organisations use OSS (see Figure 42). Thus, the use of OSS by organisations is 10 percentage points lower than the ones by companies.

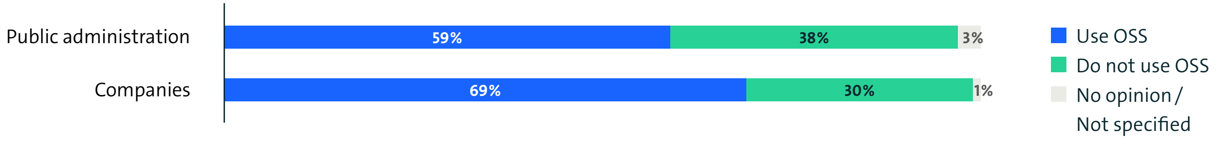
Does your organisation/company have a strategy for using or participating in OSS?



Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102) | Source: Bitkom Research 2023

Figure 41 – Open Source Software strategy in public administration

Does your organisation/company use OSS?



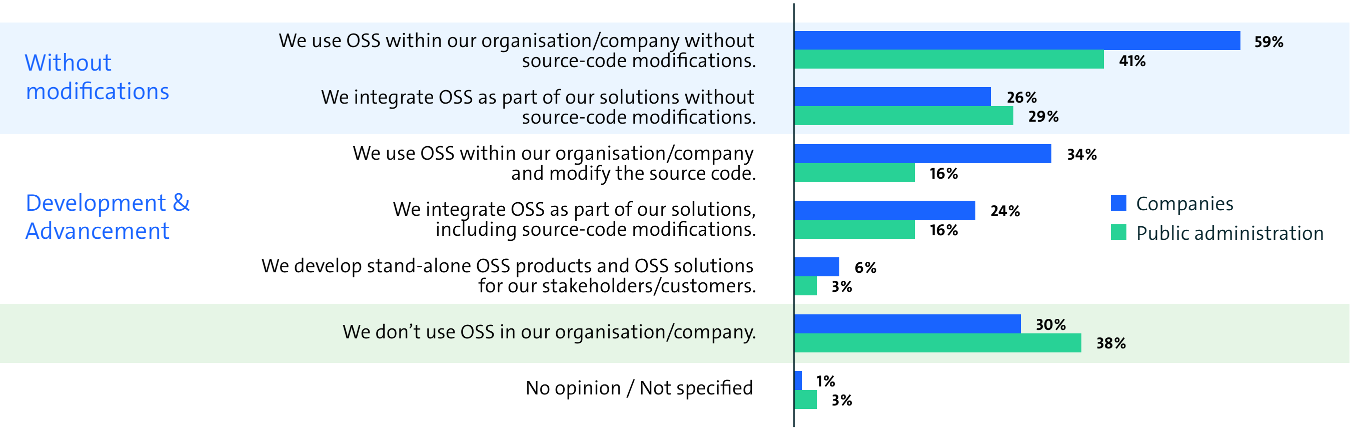
Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102) | Source: Bitkom Research 2023

Figure 42 – Use of Open Source Software in public administration

In most cases, OSS is used in public administration without source-code modifications (see Figure 43). About four out of ten (41 percent) organisations use OSS for internal use. Three out of ten (29 percent) integrate OSS into their solutions. In comparison, 16 percent of administrative organisations use OSS with modified source code for internal purposes and integrate it as part of their solutions. Only 3 percent of organisations develop stand-alone OSS products and solutions for their stakeholders.

Six out of ten (60 percent) organisations participate in OSS development or advancement (see Figure 44). Participation is somewhat higher compared to companies, where half (51 percent) participate in OSS projects.

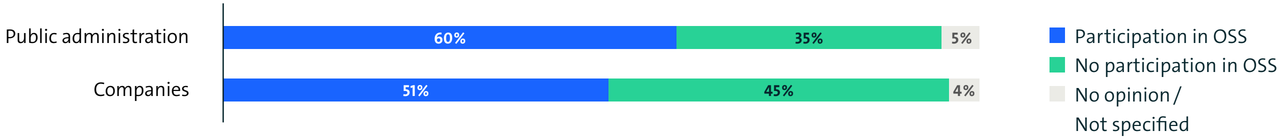
Which of the following statements apply to the use of OSS within your organisation/company?



Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102) | Multiple answers possible
Source: Bitkom Research 2023

Figure 43 – Use of Open Source Software by type in public administration

Do you participate in the development or advancement of OSS?

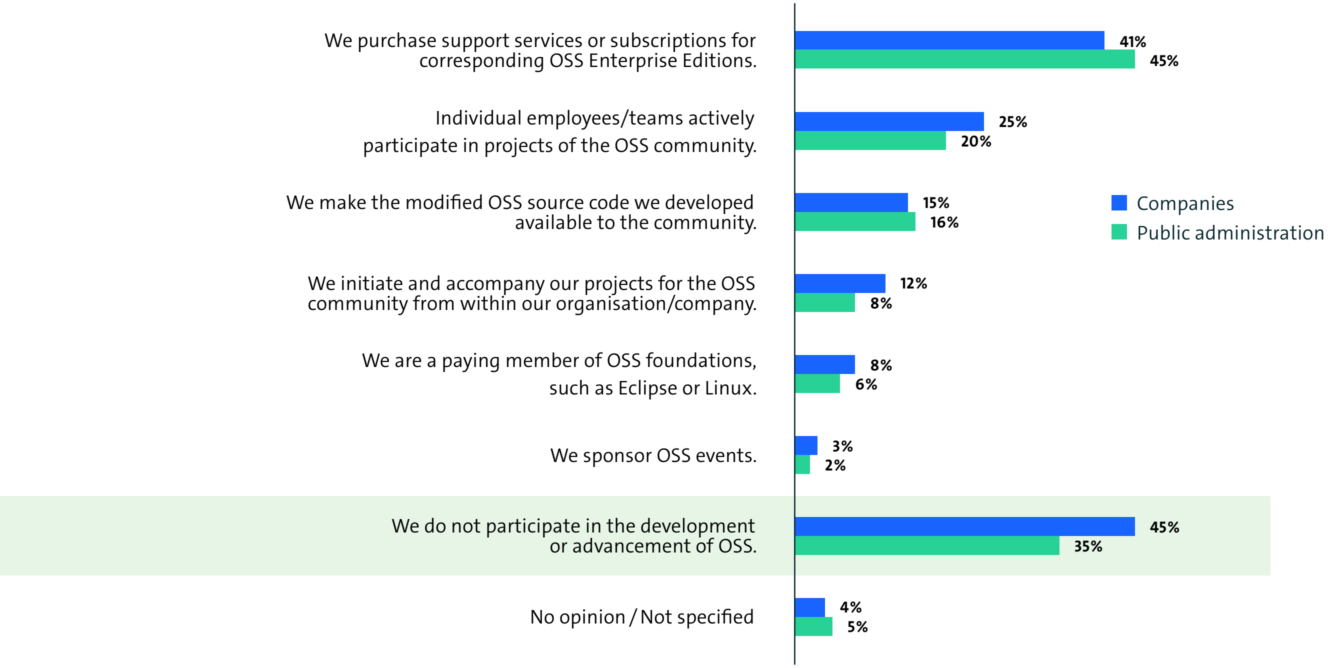


Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102) | Source: Bitkom Research 2023

Figure 44 – Participation in Open Source Software in public administration

Like businesses, public administrations primarily purchase support services or subscriptions for OSS (45 percent, see Figure 45).

To what extent is your organisation/company involved in the development or advancement of OSS?

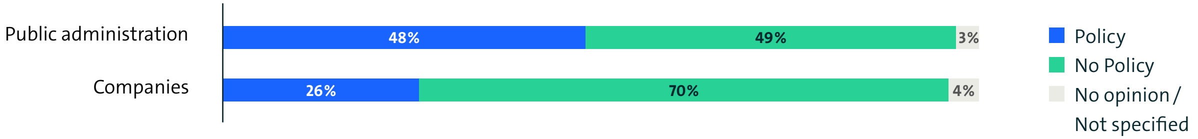


Sample: All companies with at least 20 employees (n = 1,155) and all respondents in public administration (n = 102) | Multiple answers possible
Source: Bitkom Research 2023

Figure 45 – Participation in Open Source Software by type in public administration

The questions on the existence of a written OSS policy and an OSS compliance process show that administrative organisations that use OSS or participate in OSS projects are a step ahead of the business community in this respect (see Figure 46 and Figure 47). While every fourth (26 percent) company has an OSS policy, less than half (48 percent) of public administration organisations do. The gap is not as significant for compliance processes. Nevertheless, with 56 percent, the administrations are 7 percentage points ahead of the business sector.

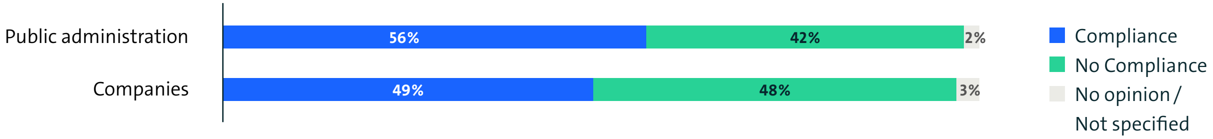
Does your organisation/company have an OSS policy, i.e., a document in which guidelines and rules concerning the use of OSS within your company are recorded?



Sample: All companies with at least 20 employees (n = 809) and all respondents in public administration (n = 65) that use or integrate or (further) develop OSS
Source: Bitkom Research 2023

Figure 46 – Open Source Software policy in public administration

Has your organisation/company have a formal compliance process for dealing with OSS?



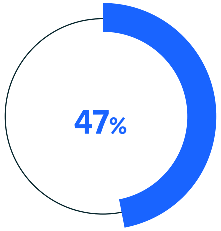
Sample: All companies with at least 20 employees (n = 809) and all respondents in public administration (n = 65) that use or integrate or (further) develop OSS
Source: Bitkom Research 2023

Figure 47 – Open Source Software compliance process in public administration

Among organisations that use, integrate, or (further) develop OSS, 47 percent (see Figure 48) of organisations feel well-positioned to use OSS safely and deliberately. It's the same number for the business community.

However, the statements show an apparent difference when it comes to compliance. Nine out of ten (90 percent) organisations think it essential that OSS comes with a standardised SBOM. Among businesses, the figure was only two-thirds (66 percent, see Figure 49).

In your opinion, which of the following statements apply to your organisation/company?



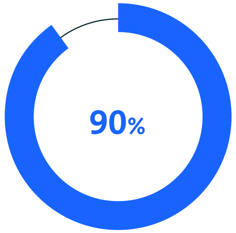
We are **well-positioned** to **use OSS** safely and consciously.

(Companies: 47%)

Sample: All companies with at least 20 employees (n = 801) and all respondents in public administration (n = 60) that use or integrate or (further) develop OSS | Percentages for »Strongly agree« and »Rather agree« | Source: Bitkom Research 2023

Figure 48 – Statements: Deliberate use of OSS public administration

In your opinion, which of the following statements apply to your organisation/company?



It is important that software is supplied with a **standardised SBOM** .

(Companies: 66%)

Sample: All companies with at least 20 employees (n = 801) and all respondents in public administration (n = 60) that use or integrate or (further) develop OSS | Percentages for »Strongly agree« and »Rather agree« | Source: Bitkom Research 2023

Figure 49 – Statements: SBOM in public administration

At the Forefront of Open Source

The IT Service Center Berlin (Berlin ITDZ) is the central IT service provider of the federal state of Berlin. It is pushing the use of Open Source Software (OSS). Three-quarters of the server and database infrastructure of the ITDZ Berlin is now Open Source. The strategic orientation towards OSS forms a vital basis for the secure and stable operation of the infrastructure. It enables modern information and communication technologies in the Berlin administration.

Dare to use more Open Source

OSS has the potential to fundamentally improve the way public administration works and interacts with citizens.

Open Source and open standards are indispensable for a digitally sovereign city. Thus, the federal state of Berlin is pursuing the »public money for public code« approach and placing Open Source at the heart of its IT solutions.

Because of the high adaptability of OSS, the administration's requirements can be implemented faster and more flexibly, leading to more efficient administrative work. At the same time, the Open Source approach is based on transparency and co-design. Thus, it strengthens citizens' trust in the state and administration.

- Digital sovereignty, thanks to open standards and interoperability
- Increasing transparency and trust in the state and administration
- Faster and more efficient creation of management applications

The future

According to the Open-Source-Monitor, not only do the majority of administrations in Germany already use OSS, but they also participate in its advancement. However, in many cases, there is still a need for more resources to fully exploit the existing potential and further increase the share of OSS use.

This is where ITDZ Berlin comes in: ITDZ Berlin is establishing an Open Source competence centre under its responsibility to bundle the expertise of economic, civil society, and scientific parties, making it centrally available to the Berlin administration. As part of an Open Source ecosystem, this enables the efficient use of resources, promotion of innovation, and effective re-use of existing solutions.

The provision of the source code on »Open CoDE«, the joint platform of public administration, promotes re-use and collaborations on public administration software solutions.

The respective company is responsible for the content of the page.

Shaping digitisation confidently and securely

Torsten Hallmann
Head of Public Affairs
SUSE

A few months ago, federal CIO Dr Markus Richter summarised it neatly during the founding of the Centre for Digital Sovereignty of Public Administration (ZenDiS): »The promotion of Open Source Software and the strengthening of digital sovereignty is more important than ever, especially against the backdrop of the current geopolitical situation.«

ZenDiS is a platform, impulse and innovation driver for a technologically independent administration in Germany. The results of the current Open-Source-Monitor show a need for a central contact point to support public administration in implementing Open Source strategies. For example, only 40 percent of respondents in administrative institutions are currently open to the topic of Open Source.

Education and raising awareness for Open Source should be among the most essential tasks of ZenDiS in the future.

However, the administration can only successfully promote Open Source strategies if there are clear internal responsibilities. Here, too, the Open-Source-Monitor shows a significant need to catch up: 70 percent of the organisations surveyed do not have a dedicated role for Open Source. In the remaining organisations, IT management often co-supervises Open Source initiatives rather informally.

The lack of competence is also reflected in the absence of a strategy: Almost 69 percent of public administration institutions follow no Open Source strategy. Only one in seven organisations (14 percent) have an interdepartmental strategy for using Open Source Software (OSS). However, Open Source solutions have become an integral part of everyday life in many administrative institutions: 59 percent of organisations surveyed say they already use Open Source Software. From the public administration's point of view, the biggest hurdles to a further expansion of Open Source initiatives are the need for more skilled staff (28 percent) and security aspects (21 percent).

Transparent and secure software supply chains are essential to address security concerns in the public sector and increase trust in OSS. The US government has required a Software Bill of Materials (SBOM) from suppliers since 2021. This inventory list indicates which components and libraries have been incorporated into the software. In Germany, SBOMs will soon be mandatory for all software products, especially critical infrastructures (KRITIS).

In addition, safety certifications issued by the Federal Office for Information Security (BSI), such as Common Criteria EAL4+, will also gain importance as compliance verification. Institutions should always ensure that the entire development process of a software product, including debugging, is considered during certification.

In the current Open-Source-Monitor, only four percent of respondents consider digital sovereignty the most significant advantage of OSS. However, the administration can reduce dependence on individual technology providers and regain more capacity to act only with Open Source initiatives such as Open CoDE and the Sovereign Workplace. The decisive factor here is that the institutions can rely on the security of OSS to use it flexibly and under their own control at any location.

The respective company is responsible for the content of the page.

4 The Future of Open Source Software

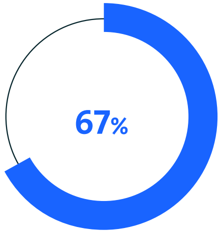
Dr. Frank Termer
Head of Software Division Bitkom

The future of OSS in Germany looks promising. More and more companies and organisations recognise the advantages of OSS solutions and know how to use them. In doing so, they do not act as mere »consumers« of OSS. They recognise their responsibility towards the Open Source ecosystem and contribute to the community by actively participating in content contributions. The public sector, in particular, has acknowledged its responsibility to be an active part of the OSS community to develop it further and realise its benefits. As European companies and institutions seek to retain or regain control over their digital infrastructures, OSS also strengthens digital sovereignty. It enables small and medium-sized enterprises to use cost-effective and robust solutions, strengthening their competitiveness.
This development will undoubtedly continue.

Europe is part of a global movement that sees Open Source Software as a digital innovation and collaboration catalyst. Cooperation between European and international actors in the domain of Open Source strengthens global networking. It also enables an efficient exchange of knowledge and resources.

Thus, Open Source and OSS will be essential building blocks for exploiting the promising transformative potential, e.g., in education, health, administration, and social innovations. Looking to the future, the Open-Source-Monitor shows that around two-thirds (67 percent) of OSS-using public sector organisations expect the importance of OSS to increase for their organisation. This figure drops to just under half (47 percent) (see Figure 50) for OSS-using companies.

In your opinion, which of the following statements apply to your organisation/company?



The **significance of OSS** will increase in our organisation/company.

(Companies: 47%)

Sample: All companies with at least 20 employees (n = 801) and all respondents in public administration (n = 60) that use or integrate or (further) develop OSS | Percentages for »Strongly agree» and »Rather agree« | Source: Bitkom Research 2023

Figure 50 – Statements: Significance of OSS in public administration

This discrepancy can likely be attributed to the fact that many companies already attach great importance to Open Source, which cannot be increased further. This level of maturity in the public sector has not yet been reached in terms of Open Source, and there is still a need to catch up. It will be exciting to observe future developments.

Although the future looks promising, the use and development of OSS still face many challenges. One of the most important is to ensure sufficient funding and support for Open Source projects. Initiatives like the Sovereign Tech Fund are a step in the right direction. However, more effort is needed to establish OSS as an integral part of our digital landscape. Europe must ensure it reduces existing dependencies on non-European technology providers and can develop, maintain, and protect its digital infrastructures. It requires targeted investment in Open Source solutions and close cooperation between the public sector, industry, and research.

The debates of the last few years have shown that we have reached a new point in the Open Source discussion. In the past, companies either made a conscious effort to distance themselves from Open Source or, vice versa, showed a strong commitment to Open Source. Today, the issue is no longer whether Open Source is better, more secure or more cost-effective than proprietary software but rather the role of OSS in the digital transformation and its potential impact. Consequently, all companies must address the question of what their contribution to digital transformation success looks like in the context of their societal responsibility. The opportunities of OSS are clearly in the foreground. Whether states, corporations, or individuals: Together, we need to recognise and exploit the opportunities of OSS. It is up to all of us to support, use, and actively participate in the advancement of the OSS community. We can shape a strong and sustainable digital future for Germany, Europe and the world by promoting Open Source as an essential driver of innovation and progress.

Publisher
Bitkom e.V.
Albrechtstraße 10 | 10117 Berlin

Contact person
Greta Schnaack
Senior Research Consultant Bitkom Research
T 030 27576-194 | g.schnaack@bitkom-research.de

Dr. Frank Termer
Head of Software Division Bitkom
T 030 27576-232 | f.termer@bitkom.org

Authorship
Greta Schnaack | Bitkom Research
Dr. Frank Termer | Bitkom

Editors
Greta Schnaack | Bitkom Research
Dr. Frank Termer | Bitkom

Design
Sabrina Flemming | Bitkom

Picture credits
Titelbild © Umberto – unsplash.com

This publication constitutes general, non-binding information. The content reflects the view of Bitkom at the time of publication. Although the information contained herein has been compiled with the utmost care, no liability is assumed concerning its accuracy, completeness or topicality. In particular, this publication cannot consider the particularities of individual cases. The reader is therefore personally responsible for its use. Any liability shall be excluded. All rights, including the duplication of any part, are reserved by Bitkom.

Imprint

Bitkom represents more than 2,200 member companies in the digital sector. In Germany, they generate around 200 billion euros in turnover with digital technologies and solutions and employ more than two million people. Our members include over 1,000 mid-size companies, 500 start-ups, and nearly all global players. They offer software, IT services, telecommunication or internet services, manufacture devices and components, are active in digital media, create content, offer platforms, or are otherwise part of the digital economy. Eighty-two percent of the companies involved in Bitkom have their headquarters in Germany, another 8 percent come from the rest of Europe, and 7 percent are from the USA. Three percent come from other regions of the world. Bitkom promotes and pushes the digital transformation of the German economy and supports broad societal participation in digital development. The goal is to make Germany a powerful and sovereign digital location.

Bitkom e.V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org