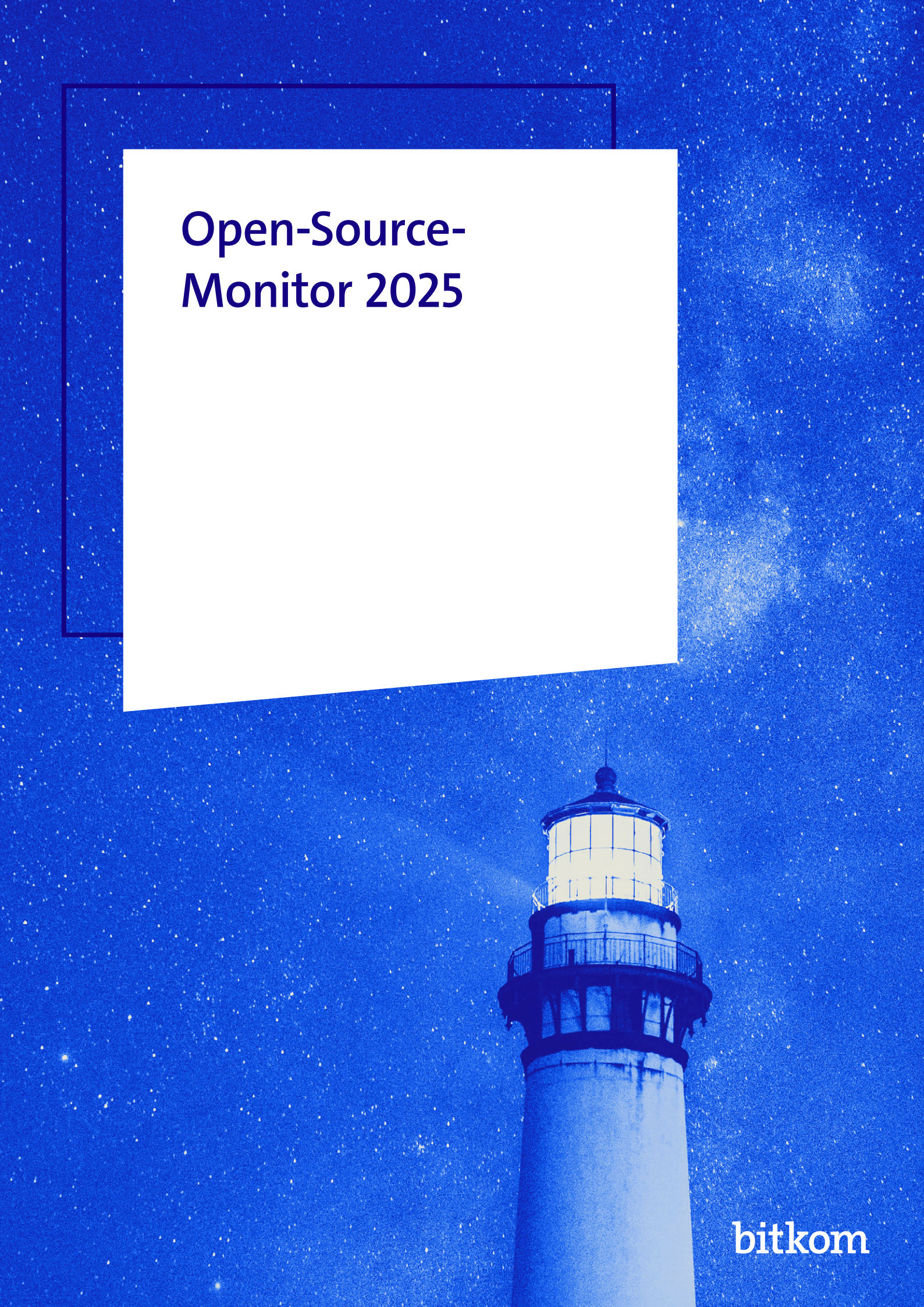
Open-Source-Monitor 2025



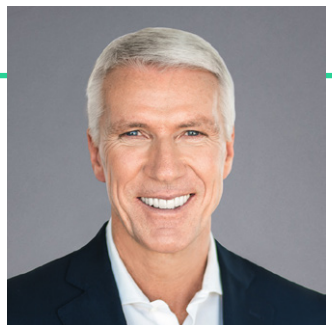
bitkom

Open-Source-Monitor 2025

DOI (German edition)
10.64022/2025-open-source-monitor

With friendly support from

Preface



Dr. Ralf Wintergerst
President of Bitkom

Open Source has continued to gain attention in 2025. Without Open Source solutions, internet traffic would grind to a halt, much of today's digital services and platforms would cease to function, and even our smartphones would be unable to operate without Open Source components. The Open Source community is also a key driver of innovation, particularly in areas such as cloud technologies and artificial intelligence.

What remains lacking, however, is a deeper understanding of Open Source — and this is precisely where the fourth edition of our »Open-Source-Monitor« comes in. For this report, we conducted a representative survey of more than 1,100 companies and additionally gathered insights from around 100 public-sector organisations. The results show that Open Source has become an integral part of the German economy and public administration. Around three-quarters of companies consciously use Open Source in one way or another, while in the public sector, two-thirds of authorities and organisations rely on it.

This widespread use is driven by the very specific and direct advantages of Open Source, such as lower costs, customised solutions and the ability to indefendently verify security. In addition, companies and administrations benefit from a vibrant developer community that continuously delivers new features and improvements. However, the importance of Open Source for our economy and society extends far beyond these aspects. By providing access to source code and the ability to make modifications ourselves, Open Source can help us move closer to the goal of digital sovereignty by enabling us to retain or regain control over the software we use.
Six in ten companies would like to see the government invest more heavily in Open Source software in light of the current geopolitical situation. At the same time, challenges remain: companies continue to face obstacles in deploying Open Source, ranging from a shortage of IT professionals to unclear warranty issues and legal uncertainties surrounding licensing.

Open Source must therefore be approached strategically. This includes defining goals, establishing responsibilities and firmly anchoring Open Source in the overall digital strategy. Here, too, there is still room for improvement: a majority of six out of ten companies have not developed any Open Source strategy at all. So despite all the progress that has been made, there still remains a lot to be done – for the Open Source community, companies and public administration. With this »Open-Source-Monitor 2025«, we want to make a contribution to that effort.

Key Findings

Use and Attitudes in Companies

- The majority of companies have a positive attitude towards Open Source Software (OSS): 24 percent are »very open« to it, and 37 percent are »somewhat open«. 42 percent expect its importance to increase in the future.
- 73 percent of companies use OSS—primarily internally without modifying the source code (67 percent), while 35 percent make their own adaptations. 25 percent integrate OSS into their products, and 7 percent develop independent OSS solutions.
- However, 60 percent of companies still lack an OSS strategy; 37 percent have a documented strategy for use (30 percent) or contribution (21 percent).

Policy & Compliance

- In 78 percent of cases, the CIO is responsible for OSS. Only 14 percent of companies have an Open Source Programme Office (OSPO), while 12 percent are planning to establish one.
- An OSS policy is missing in 62 percent of companies; 36 percent have a documented policy in place. Moreover, 52 percent have no compliance process for employees.
- Key drivers for compliance adjustments are the Cybersecurity Emergency Response (CER) (61 percent), the Cyber Resilience Act (CRA) (57 percent), and the Product Liability Directive (PLD) (44 percent).

Future prospects & AI

- 51 percent consider Open-Source-AI models to be recommendable, while 45 percent see them as a way to reduce dependencies.
- 73 percent view OSS as a tool to strengthen digital sovereignty; 60 percent call for increased government investment, and 57 percent support the Sovereign Tech Agency. However, only 17 percent have fully analysed and reduced their digital dependencies.

Public Sector

- Public administrations also take a predominantly positive view of OSS (52 percent are open to it). 63 percent use OSS, with an average of 4 full-time equivalents dedicated to management (compared with 1.9 in the private sector).
- 37 percent have an OSS strategy, and 60 percent have a policy in place. 57 percent have established a compliance process for employees.
- The main advantages cited by public authorities are cost savings (19 percent) and access to source code (12 percent), while the primary disadvantage is the shortage of skilled professionals (33 percent).
- Open Source Program Offices (OSPOs) are more common in the public sector, with 25 percent already established—higher than in the industry.

Content

Preface 3

Key Findings 4

1 Use of Open Source Software in companies 10

1.1 Attitude towards Open Source Software 10

1.2 Open Source Software strategy 11

1.3 Use of Open Source Software 12

1.4 Selection Criteria for Open Source Software 13

1.5 Engagement in the Ongoing Development of Open Source Software 15

1.6 Advantages of Open Source Software 16

1.7 Disadvantages of Open Source Software 17

1.8 Key Barriers to Open Source Software Adoption 18

1.9 Personnel Resources for Open Source Software 19

2 Policy & Compliance 21

2.1 Responsibility for Open Source Software 21

2.2 Open Source Software-Policy 22

2.3 European Compliance Frameworks 23

2.4 Compliance Policies and Instruments 24

2.5 Open Source Software Standards in the Supply Chain 25

2.6 Budget for Compliance Measures 26

3 Future Prospects, Politics & AI 28

3.1 AI in Software Development 28

3.2 Open-Source AI Models 29

3.3 Adoption and Concerns surrounding AI Code Generators 30

3.4 Open-Source as a Tool for Digital Sovereignty 31

4 Open Source in the Public Sector 33

4.1 General Attitude towards Open Source Software 33

4.2 Use of Open Source Software 34

4.3 Selection Criteria for Open Source Software 35

4.4 Open Source Software Strategy 37

4.5 Engagement in the Ongoing Development of Open Source Software 38
4.6 Advantages of Open Source Software 39
4.7 Disadvantages of Open Source Software 40
4.8 Open Source Programme Offices (OSPOs) 41
4.9 Open Source Software-Policy 42
4.10 Compliance Process for Employees 43
4.11 Open Source Software as a Tool for Digital Sovereignty 44
4.12 AI in Software Development 45
4.13 Open-Source as a Tool for Digital Sovereignty 46

5 Case Studies 48

5.1 OCCTET: Open Source Compliance for the CRA – practical and free of charge 48
5.2 Open Source Compliance in the Supply Chain 49
5.3 Bridges and Operating Systems – The Hidden Frameworks that hold Everything together 50
5.4 Open Source Is Everywhere – and Officially Regulated from 2027 51
5.5 Open Source Enables Added Value and Digital Sovereignty 52
5.6 Achieving Transparent AI Use Through Open Source 53
5.7 NeoNephos Foundation: Open Source for Europe's Digital Sovereignty 54
5.8 Expert Statement 55
5.9 Automated Software Testing with the Badge System 56

6 Methodology 57

Figures

1 Figure 1: Attitude towards OSS 10

2 Figure 2: Expected importance of OSS within companies 10

3 Figure 3: Strategies for Using and Contributing to OSS 11

4 Figure 4: Forms of OSS Use in Companies 12

5 Figure 5: Selection Criteriafor OSS: Security, Functionality, and Regulatory Requirements 13

6 Figure 6: Selection Criteria for OSS: Licensing, Support, and Community Aspects 14

7 Figure 7: Participation in OSS Development 15

8 Figure 8: Perceived Benefits of OSS for Companies 16

9 Figure 9: Perceived Disadvantages of OSS for Companies 17

10 Figure 11: Barriers to the Use of OSS: Resources and Skilled Personnel 18

11 Figure 10: Barriers to the Use of OSS: Legal and Security Aspects 18

12 Figure 12: Barriers to the Use of OSS: Economic Viability and Acceptance 18

13 Figure 14: Employees Primarily Responsible for OSS Management 19

14 Figure 13: Personnel Responsibilities and Resources for OSS Management in Companies 19

15 Figure 15: Responsibility for OSS within the Company 21

16 Figure 16: Proportion of Companies with Open Source Program Offices 21

17 Figure 18: OSS-Policy within the Company 22

18 Figure 17: Compliance Processes for Employees in Handling OSS 22

19 Figure 19: Start of Engagement with Compliance Issues 23

20 Figure 20: Impact of European Regulations (CER, CRA, PLD, DORA, NIS2) on Compliance Processes 23

21 Figure 21: Compliance Measures and Instruments used in OSS Management 24

22 Figure 23: Adoption of Standards in the Supply Chain (ISO 5230, ISO 18974, BSI 03183) 25

23 Figure 22: Use of SBOMs in Companies 25

24 Figure 24: Developments of Budgets for OSS Compliance 26

25 Figure 25: Use of AI in Software Development in Companies 28

26 Figure 26: Perceptions of Open-Source AI Models 29

27 Figure 27: Perceived Risks of AI-Generated Code 30

28 Figure 28: Use of AI Code Generators in Companies 30

29 Figure 29: Views on OSS as an Instrument for Digital Sovereignty 31

30 Figure 30: General Attitude towards OSS: Industry vs. Public Sector 33

31 Figure 31: Comparison of OSS Use and Staffing: Industry vs Public Administration 34

32 Figure 32: Selection Criteria for OSS in the Public Sector: Security, Functionality, and Rights 35

33 Figure 33: Selection Criteria for OSS in the Public Sector: Community and Support Structure 36

34 Figure 34: OSS Strategies: Industry vs Public Administration 37

35 Figure 35: Participation in the Development and Further Development of OSS: Industry vs Public Administration 38

36 Figure 36: Perceived Advantages of OSS in Public Administration 39

37 Figure 37: Perceived Disadvantages of OSS in Public Administration 40

38 Figure 38: Proportion of Organisations with OSPOs in the Public Sector 41

39 Figure 39: Existence of an OSS Policy: Public Sector vs Industry 42

40 Figure 40: Compliance Processes for Employees: Public Sector vs Industry 43

41 Figure 41: Agreement with Statements on OSS as a Tool for Digital Sovereignty in Public Administration 44

42 Figure 42: Use of AI in Software Development: Public Sector vs Industry 45

43 Figure 43: Perceptions of Open Source AI Models in Public Administration 46

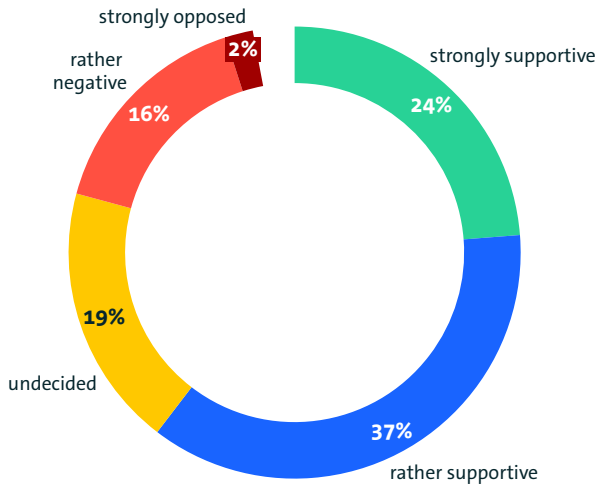
1 Use of Open Source Software in companies

1 Use of Open Source Software in companies

Open Source Software (OSS) refers to program modules, source code and libraries, programming tools, as well as complete operating systems or software solutions whose source code is made publicly available and whose licence permits users to freely run, analyse, modify and distribute the software, whether in its original or altered form. In addition to open access to the source code, this also means that no licence fees are incurred.

1.1 Attitude towards Open Source Software

What is your company's general position on the topic of Open Source Software?



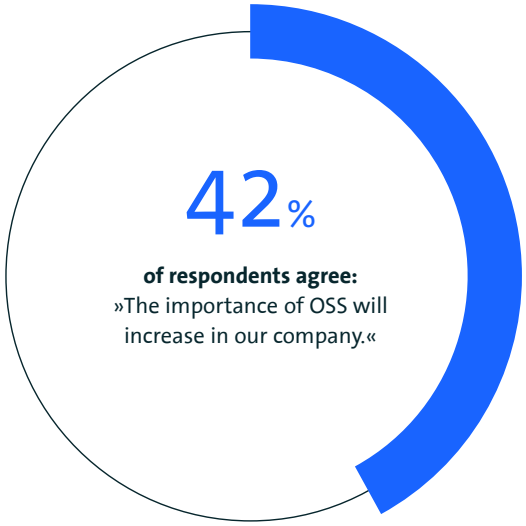
Base: All respondents (n=1,152) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 1: Attitude towards OSS

The majority of companies take a generally positive view of OSS. 24 percent describe their attitude as »very open«, and another 37 percent as »somewhat open«. In total, more than six out of ten companies are open to OSS.

19 percent are undecided, while a smaller group is more sceptical: 16 percent are »somewhat negative«, and only 2 percent are »very negative«.

42 percent of the companies surveyed expect the importance of OSS within their organisation to increase in the future. This means that nearly one in two companies views OSS as a growing factor for its work and strategic development.



Base: All respondents (n=1,152) | Source: Bitkom Research 2025

Figure 2: Expected importance of OSS within companies

1.2 Open Source Software strategy

The majority of surveyed companies currently lack a strategy for using or contributing to Open Source Software. Sixty percent report that no OSS strategy exists within their organisation. Nevertheless, 37 percent have developed corresponding plans.

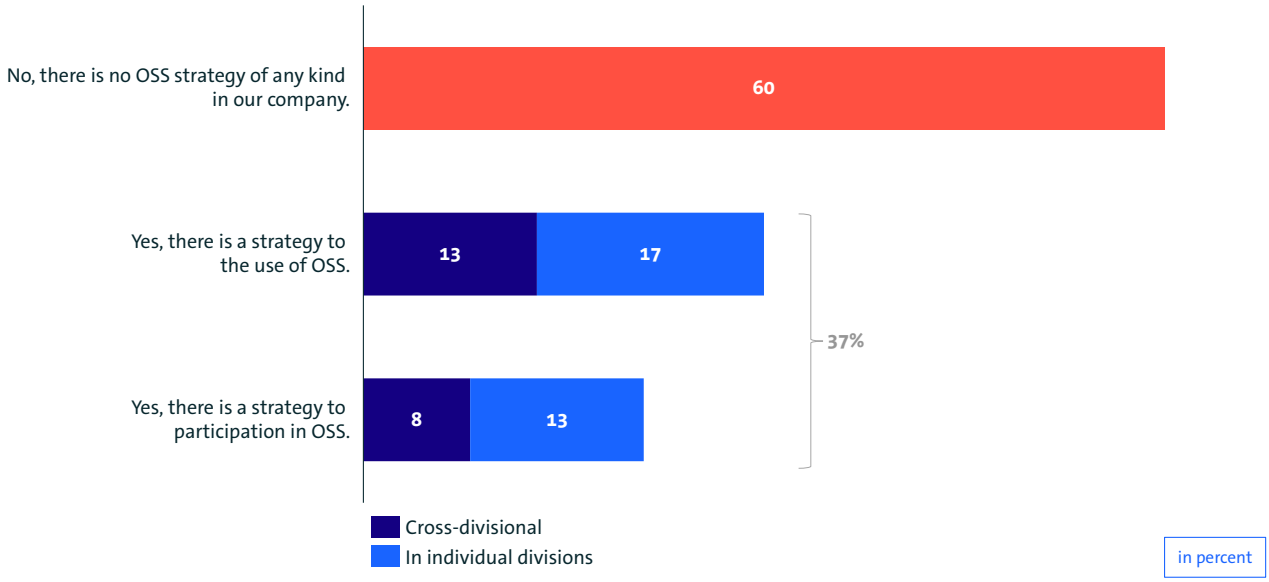
Strategies for the use of OSS are somewhat more common than those for active participation: 30 percent pursue a usage strategy, while 21 percent have a contribution strategy in place.

Differences also emerge between company-wide strategies and those limited to individual departments.
Regarding OSS usage, 17 percent rely on concepts confined to specific departments, whereas 13 percent have company-wide approaches. In terms of participation, 13 percent have departmental strategies and 8 percent cross-departmental ones.

Overall, this shows that while about one-third of companies pursue OSS strategies, the majority still lack a structured approach.

> The number of companies with an OSS strategy has been rising over the years:
>
> In 2021, 25 percent had a strategy for using or contributing to OSS; by 2023, the figure had increased to 32 percent, and in 2025 it reached 37 percent.

Is there a strategy* in your company for using or participating in OSS?



*By strategy, we mean goals and plans written down in a document for the use or participation of OSS in your company.
Base: All respondents (n=1,152) | Multiple answers were possible | Not shown: »Don't know/no information« | Source: Bitkom Research 2025

Figure 3: Strategies for Using and Contributing to OSS

1.3 Use of Open Source Software

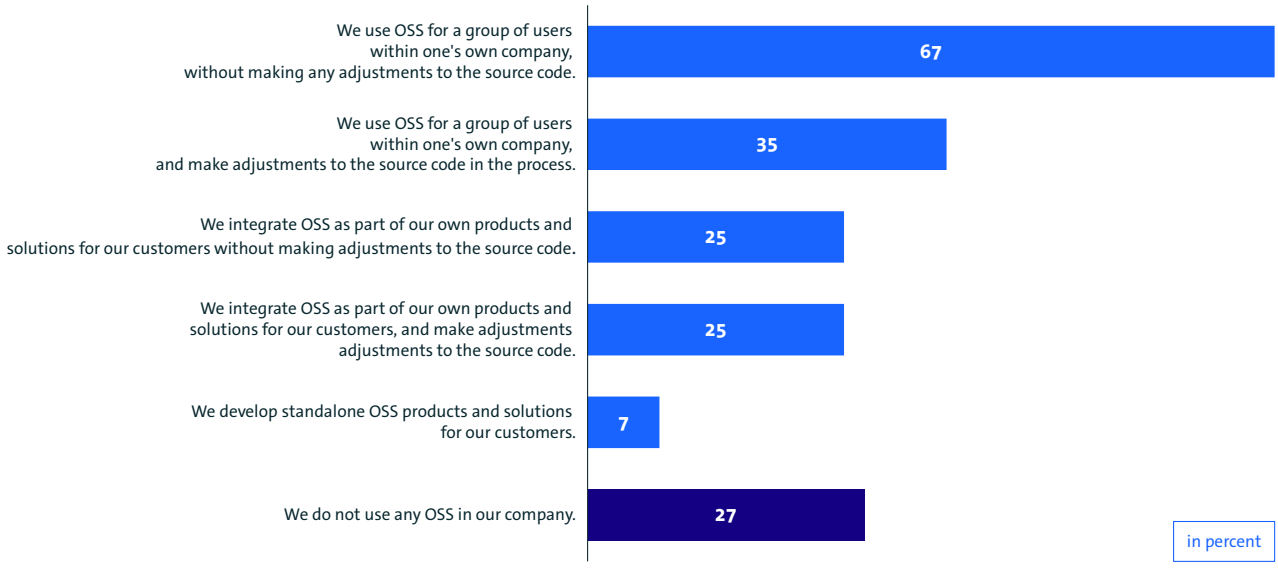
In most companies, the use of Open Source Software (OSS) is primarily internal. Sixty-seven percent deploy OSS within their own organisation without making any modifications to the source code. Another 35 percent also use OSS internally but adapt the source code to their specific needs.

A quarter of companies (25 percent) integrate OSS into their own products or customer solutions—some without altering the source code, others with adjustments. By contrast, only a small minority of 7 percent develop independent OSS products or solutions for external clients.

Overall, the findings show that OSS is mainly used as an internal solution, while integration into customer products or the independent development of OSS offerings remains limited to a smaller group of companies.

> The proportion of companies using Open Source Software has remained stable at around 70 percent: In 2021, 71 percent reported using OSS; in 2023, the figure was 69 percent; and in 2025, the proportion rose slightly to 73 percent.

Does your company use OSS?



Base: All respondents (n=1,152) | Not shown »Don't know/no information« | Multiple answers were possible | Source: Bitkom Research 2025

Figure 4: Forms of OSS Use in Companies

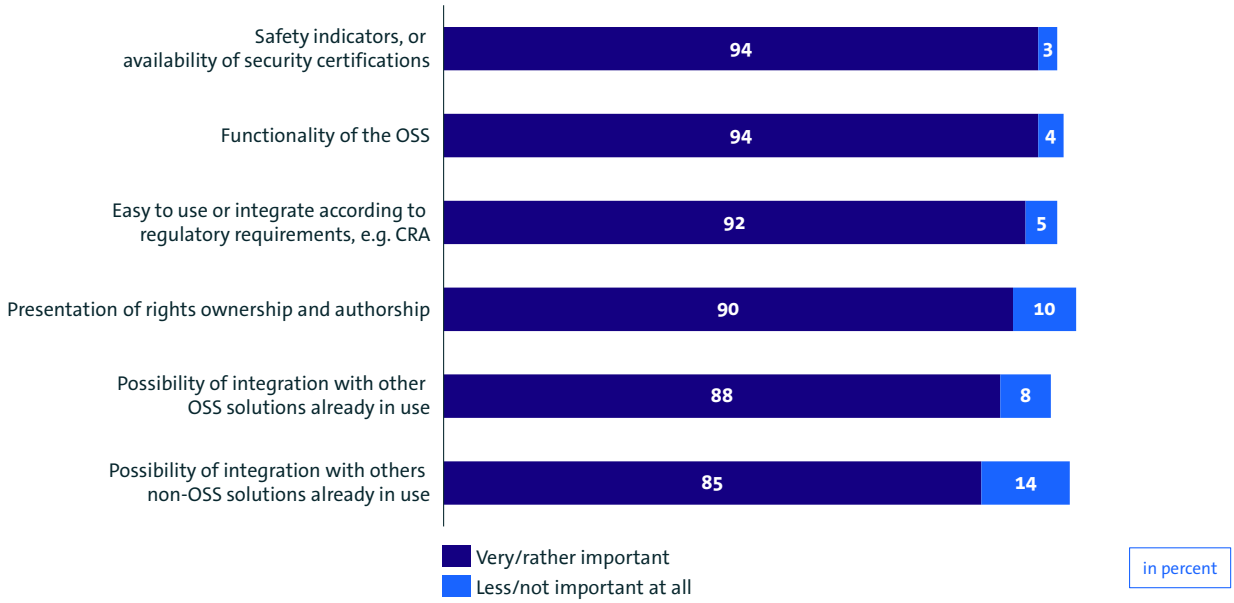
1.4 Selection Criteria for Open Source Software

When selecting Open Source Software projects, companies place particular emphasis on security and functional aspects. 94 percent consider security indicators or security certifications, as well as the functionality of the OSS, to be very or rather important.

Ease of use and integration under regulatory requirements—such as those imposed by the Cyber Resilience Act (CRA)—is significant for 92 percent of respondents. Ninety percent also pay attention to clear statements about ownership and authorship rights.

Integration capability is also seen as a crucial criterion: 88 percent rate the ability to integrate with other OSS solutions already in use as important, while 85 percent focus on compatibility with non-OSS solutions. Overall, virtually all surveyed companies regard these criteria as highly relevant.

How important are the following criteria to you when selecting OSS projects?



Base: Companies that use, integrate or (further) develop OSS (n=839) | Multiple answers were possible | Other: »Don't know/no information« | Source: Bitkom Research 2025

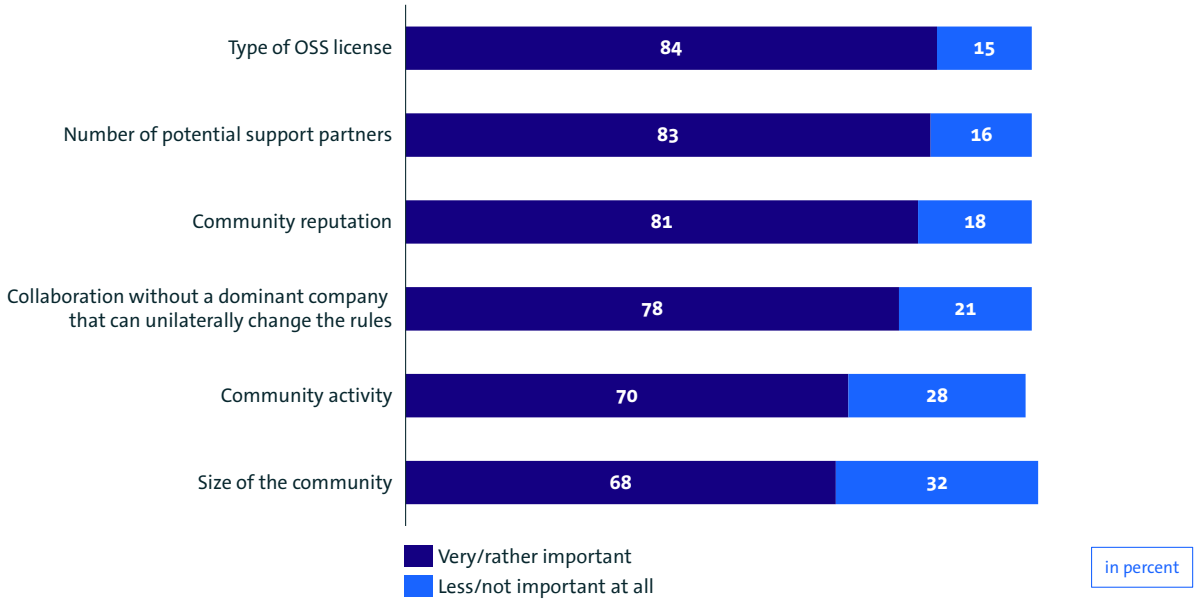
Figure 5: Selection Criteriafor OSS: Security, Functionality, and Regulatory Requirements

84 percent of companies consider the type of OSS licence to be very or rather important. Almost equally significant is the number of potential support partners (83 percent). The reputation of the respective community is also taken into account by 81 percent of respondents.

78 percent pay attention to whether there is any dominant company that could unilaterally change the rules. Slightly less importance is placed on the level of community activity (70 percent) and the size of the community (68 percent).

Overall, the findings indicate that while the structure and vitality of the community are relevant, most companies place greater emphasis on legal clarity and reliable support options.

How important are the following criteria to you when selecting OSS projects?



Base: Companies that use, integrate or (further) develop OSS (n=839) | Multiple answers were possible | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 6: Selection Criteria for OSS: Licensing, Support, and Community Aspects

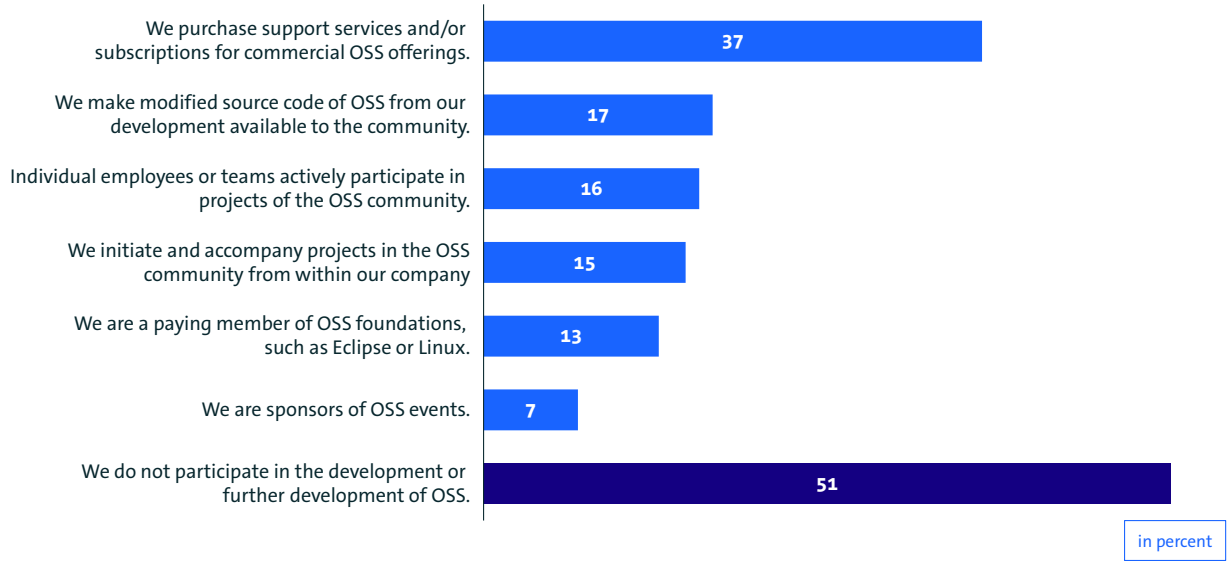
1.5 Engagement in the Ongoing Development of Open Source Software

47 percent of companies participate in the development or further development of Open Source Software.

37 percent do so by purchasing support services or subscriptions for commercial Open Source Software.

Other forms of participation are far less common: 17 percent make their own modifications to OSS source code available to the community, and 16 percent report that individual employees or teams actively contribute to OSS projects. 15 percent initiate their own OSS projects, and 13 percent pay membership fees to OSS foundations such as Linux or Eclipse. A small share of 7 percent sponsor OSS events themselves. A full 51 percent of companies do not participate in OSS development or further development at all.

To what extent does your company participate in the development or further development of OSS?



Base: All respondents (n=1,152) | Not shown: »Don't know/no information« | Multiple answers were possible | Source: Bitkom Research 2025

Figure 7: Participation in OSS Development

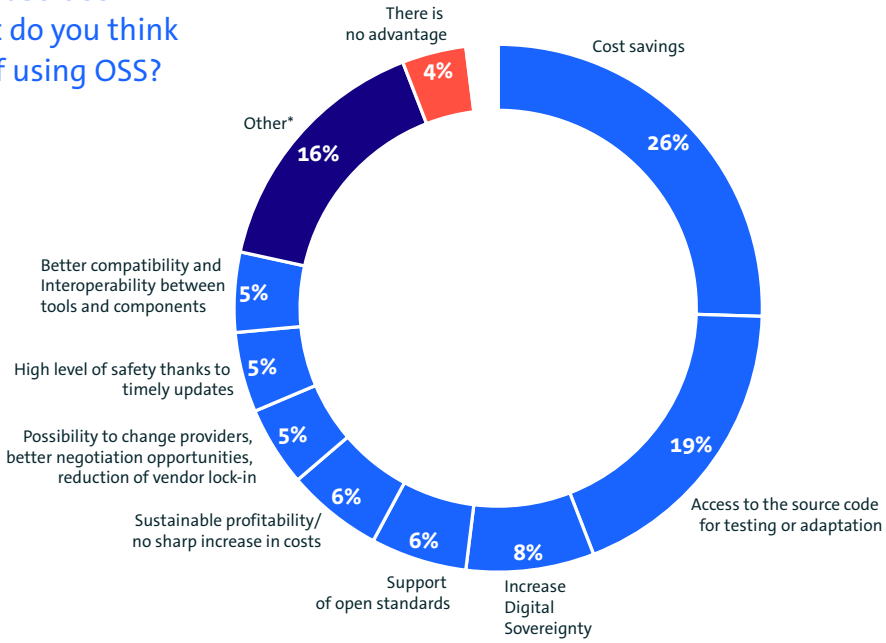
1.6 Advantages of Open Source Software

Cost savings are seen by most companies as the main advantage of using Open Source Software: 26 percent consider this aspect decisive. Access to the source code—whether for review or individual customization—ranks second, cited by 19 percent.

Other benefits include enhanced digital sovereignty (8 percent) and support for open standards (6 percent). A further 6 percent highlight sustainable cost efficiency and the absence of steep cost increases. Less frequently mentioned advantages include the ability to switch providers and reduce dependencies (5 percent), high security through timely updates (5 percent), and improved compatibility and interoperability between tools and components (5 percent).

16 percent of respondents point to other benefits, while only 4 percent state that they see no advantages in OSS at all. Overall, positive assessments clearly prevail, particularly regarding cost efficiency and flexibility.

Regardless of whether you use OSS in your company or not, what do you think is the biggest advantage of using OSS?



Base: All respondents (n=1,152) | Other: »Don't know/no information« | Source: Bitkom Research 2025
*Wide range of OSS components (4%); Broad and active knowledge sharing community (4%); Attractive IT workplace, motivation for employees (2%); Possibility to adapt to one's own needs/adaptation (2%); Variety of OSS vendors offering commercial support (1%); Better competitive opportunities for our company (1%); High stability, low susceptibility to errors (1%); Short innovation cycles (1%)

Figure 8: Perceived Benefits of OSS for Companies

1.7 Disadvantages of Open Source Software

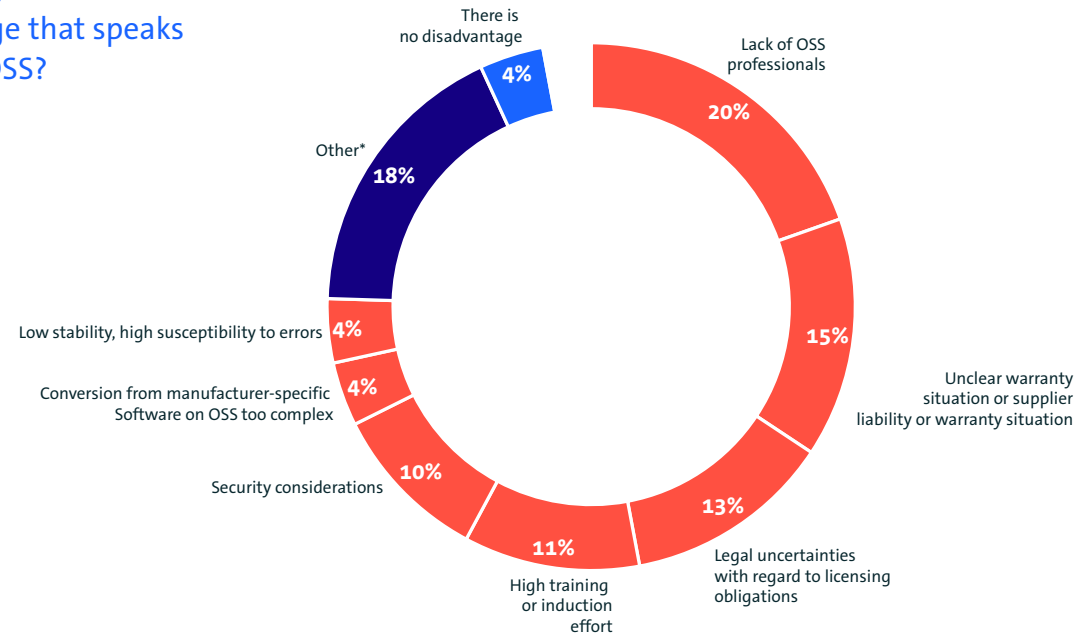
The biggest disadvantage of using Open Source Software (OSS), according to companies, is the lack of skilled personnel: 20 percent see this as the main obstacle. Unclear warranty conditions as well as questions of supplier liability or guarantees are also frequently mentioned (15 percent). 13 percent consider legal uncertainties regarding licence obligations problematic.

A high need for training and onboarding is highlighted by 11 percent as a disadvantage, while 10 percent view security aspects critically. Low stability and high error susceptibility (4 percent), as well as the effort required to switch from vendor-dependent software to OSS (4 percent), play a less important role.

Notably, 18 percent mention other disadvantages, while 4 percent of respondents see no disadvantages at all.

Overall, it becomes clear that personnel, legal, and organisational challenges are the main factors hindering the broader adoption of OSS.

And in your opinion, what is the biggest disadvantage that speaks against the use of OSS?



Base: All respondents (n=1,152) | Other: »Don't know/no information« | Source: Bitkom Research 2025
*Lack of interfaces to other systems (3%); Lack of training opportunities (3%); Lack of commercial support, missing enterprise versions (3%); Lack of certifications for OSS (3%); Supply Chain Security Challenges (2%); Lack of OSS solutions for our use cases (2%); Lack of acceptance in the company (1%); Poor reputation of OSS (1%)

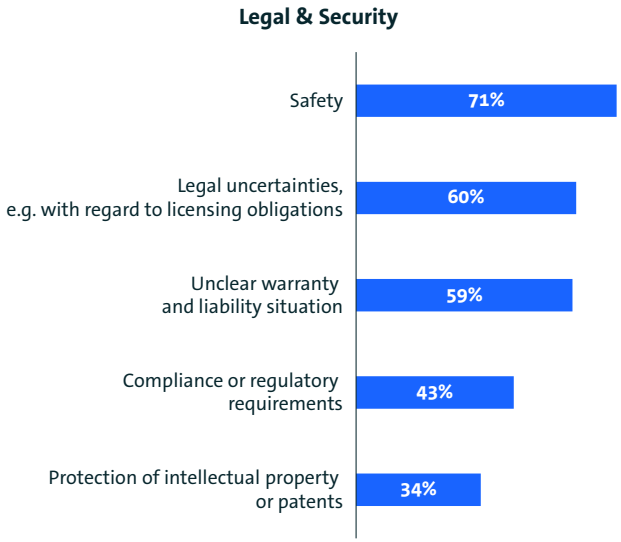
Figure 9: Perceived Disadvantages of OSS for Companies

1.8 Key Barriers to Open Source Software Adoption

Security concerns are the most frequently cited reason for not using Open Source Software – 71 percent of companies view this as a key obstacle. Legal uncertainties regarding licence obligations (60 percent) and unclear warranty and liability issues (59 percent) are also widespread. In addition, 43 percent cite compliance or regulatory requirements as barriers, while 34 percent see the protection of intellectual property or patents as problematic.

Another major obstacle is the lack of human resources. 71 percent report a shortage of qualified staff within their own company, while 46 percent point to insufficient support compared with commercial offerings. The lack of OSS experts in the labour market (42 percent) and the high effort required for migration (36 percent) also have a dampening effect. 46 percent state that no suitable OSS solutions are available for their specific use cases. 32 percent complain about a lack of internal acceptance, and 25 percent express uncertainty about long-term support.

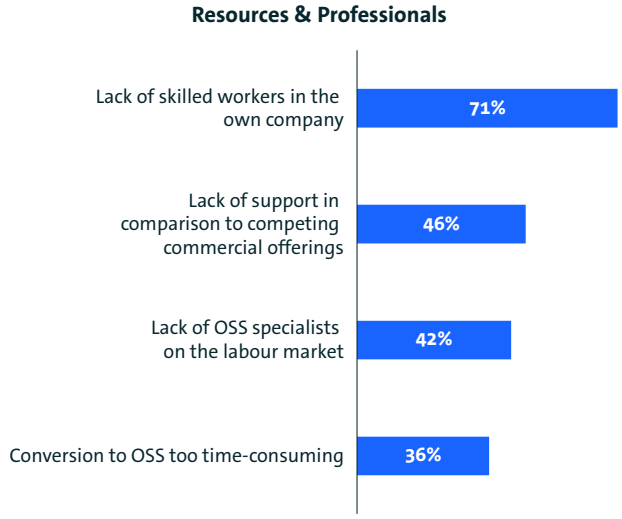
What are the reasons you do not integrate OSS into your company or specific departments?



Base: All respondents (n=1,152) | Multiple choices were possible | Source: Bitkom Research 2025

Figure 10: Barriers to the Use of OSS: Legal and Security Aspects

What are the reasons you do not integrate OSS into your company or specific departments?



Base: All respondents (n=1,152) | Multiple choices were possible | Source: Bitkom Research 2025

Figure 11: Barriers to the Use of OSS: Resources and Skilled Personnel

What are the reasons you do not integrate OSS into your company or specific departments?

Base: All respondents (n=1,152) | Multiple choices were possible | Source: Bitkom Research 2025

Figure 12: Barriers to the Use of OSS: Economic Viability and Acceptance

1.9 Personnel Resources for Open Source Software

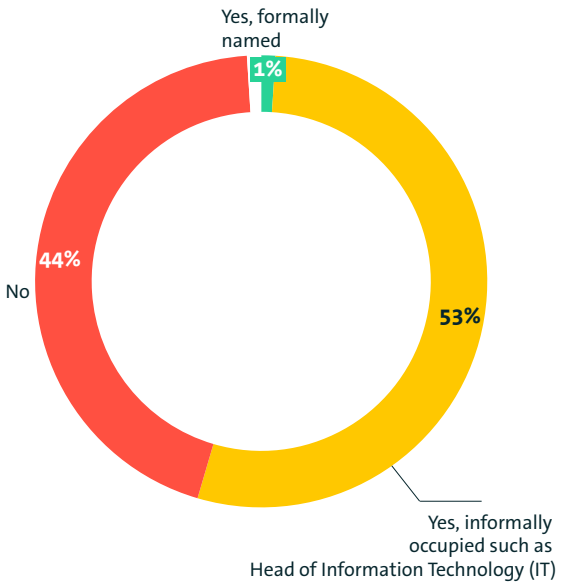
In most companies (44 percent), there is no formally designated person responsible for Open Source Software. Only 1 percent of respondents have an officially appointed OSS representative.

In many companies, only a small number of employees focus primarily on managing OSS. On average, this corresponds to 1,9 full-time equivalents (FTE).

Almost half of the companies (49 percent) assign between one and five full-time employees to OSS management. 10 percent employ fewer than one FTE, while 4 percent allocate five or more FTEs.

At the same time, many companies have no fixed assignment of responsibilities: 18 percent handle OSS-related tasks internally as needed, 3 percent outsource them, and in 8 percent OSS management plays no role at all.

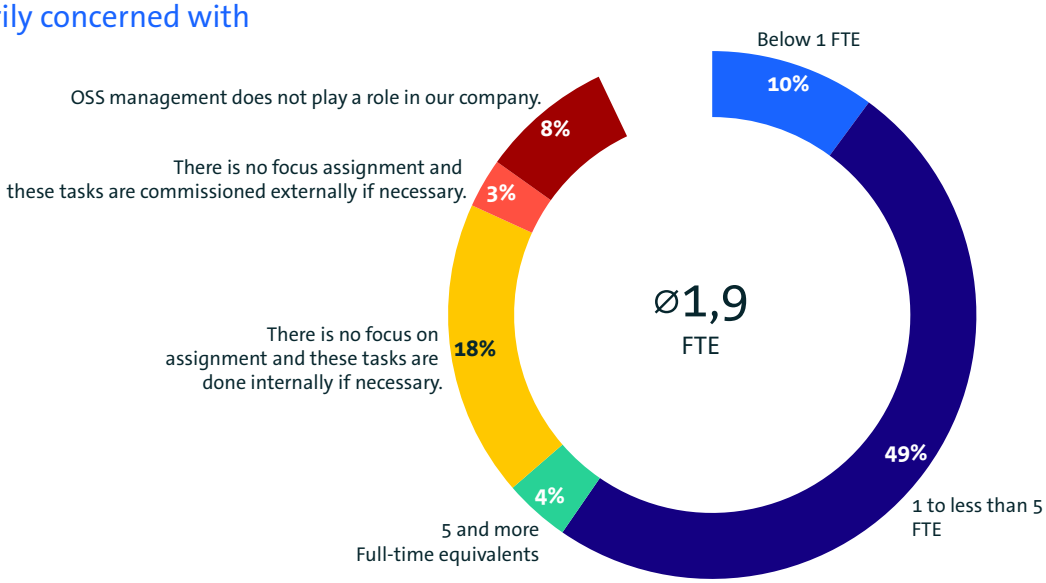
Is there a person in your company who is responsible for the topic of Open Source Software?



Base: All respondents (n=1,152) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 13: Personnel Responsibilities and Resources for OSS Management in Companies

How many employees in your company are primarily concerned with OSS management*?



*By OSS management, we mean the practices and processes used to control and coordinate the development and deployment of OSS within your organisation.
Base: Companies that use, integrate or (further) develop OSS (n=839) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 14: Employees Primarily Responsible for OSS Management

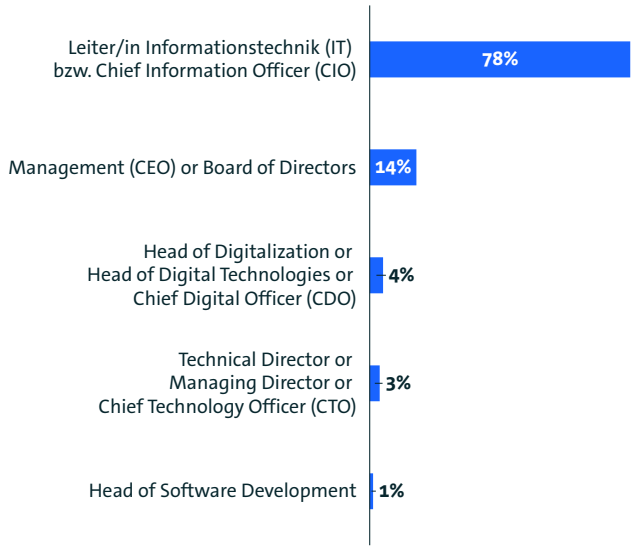
2 Policy & Compliance

2 Policy & Compliance

Responsibility for Open Source Software (OSS) extends beyond its use, integration and further development to include compliance with legal and regulatory requirements. Only 1 percent of companies have a formally designated person responsible for OSS (see ↗ Chapter 1.7). Far more frequently (in 53 percent of companies), this responsibility is handled informally by specific individuals, such as IT management. Nearly every second company (44 percent), however, has no designated person responsible for OSS at all.

2.1 Responsibility for Open Source Software

Who in your company is responsible for the topic of Open Source Software?



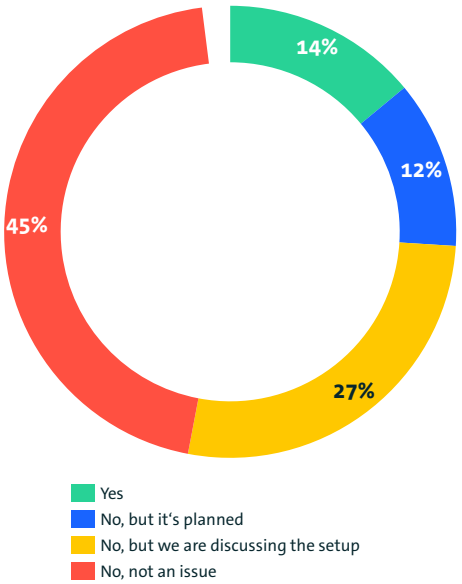
Base: Companies where one person is informally responsible for Open Source Software (n=616) | Source: Bitkom Research 2025

Figure 15: Responsibility for OSS within the Company

78 percent state that the head of information technology or the Chief Information Officer (CIO) is responsible for OSS. In 14 percent of companies, this responsibility lies with the executive management or board of directors. Other roles are far less frequently in charge: 4 percent name the Chief Digital Officer (CDO) or the Head of Digitalization, and 3 percent refer to the Chief Technology Officer (CTO) or technical directors.

Only a few companies have so far established an Open Source Programme Office (OSPO). Merely 14 percent already have such a central organisational unit dedicated to open source matters. Another 12 percent are actively planning to set one up, and 27 percent are currently discussing the idea. Almost half of the companies (45 percent), however, state that establishing an OSPO is not under consideration for them.

Have you set up an Open Source Program Office* (OSPO)?



*a central organizational unit that takes care of Open Source Software issues across the board
Base: Companies that use, integrate or (further) develop OSS (n=839) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 16: Proportion of Companies with Open Source Program Offices

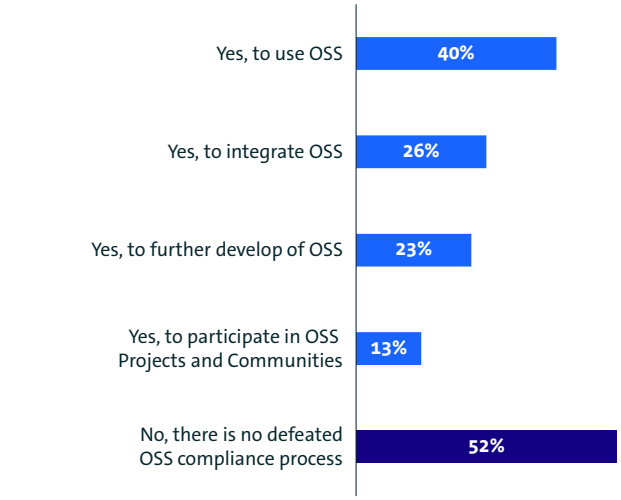
2.2 Open Source Software-Policy

The majority of companies dealing with Open Source Software (OSS) do not have a general OSS policy—that is, written guidelines and rules for handling OSS: 62 percent report that no such regulations exist within their organisation. The proportion has been rising steadily: 22 percent in 2021, 26 percent in 2023, and 36 percent in 2025.

Nearly one-third (29 percent) have established policies governing the use of OSS. Other areas are covered far less frequently: 16 percent have a policy for the integration of OSS into their systems, and 15 percent have rules for its development or further development.

More than half of the companies (52 percent) have no written compliance guidelines that require employees to adhere to regulatory requirements. Among those that do, rules for OSS use are the most common: 40 percent have implemented binding processes for this purpose.

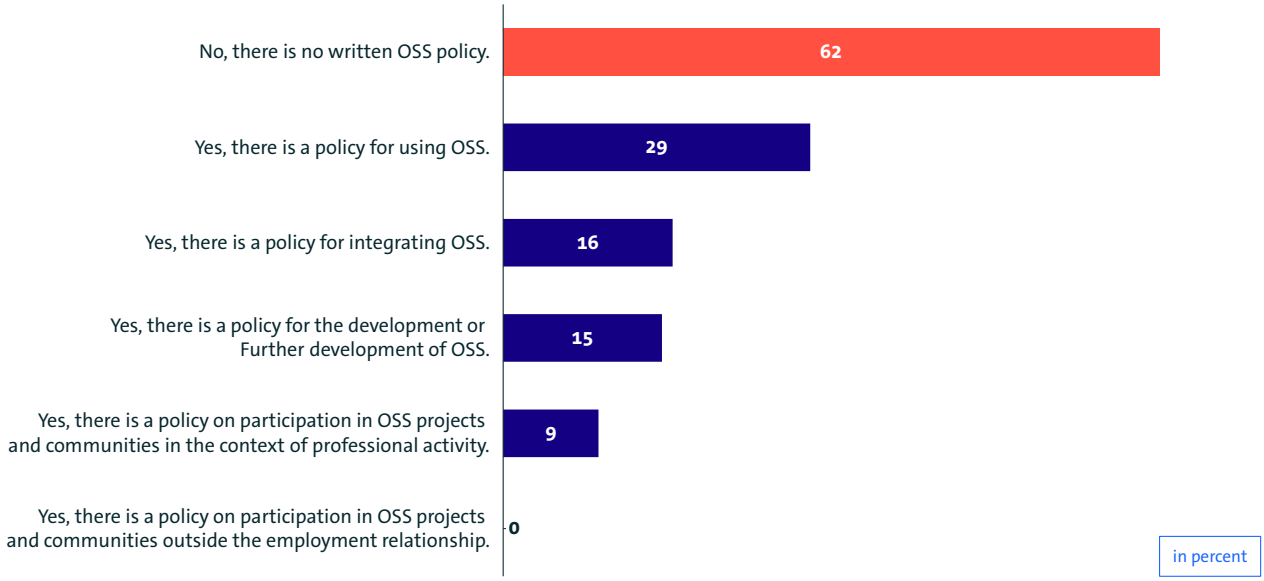
Are there any compliance processes written down in your company that make it mandatory for employees to comply with regulatory requirements when dealing with OSS?



Base: Companies that use, integrate, (further) develop, or otherwise participate in OSS (n=841) | Multiple choices were possible | Source: Bitkom Research 2025

Figure 17: Compliance Processes for Employees in Handling OSS

Is there an OSS policy* in your company?



*i.e. a document in which guidelines and rules for dealing with OSS in your company are written down
Base: Companies that use, integrate, (further) develop, or otherwise participate in OSS (n=841) | Multiple answers were possible | Not shown: »Don't know/no information« | Source: Bitkom Research 2025

Figure 18: OSS-Policy within the Company

2.3 European Compliance Frameworks

The way companies have approached compliance over the years has developed differently. 7 percent of the surveyed companies have been actively addressing compliance issues since before the year 2000.

One quarter (25 percent) began doing so between 2000 and 2010, another 23 percent between 2010 and before 2020, and a further 23 percent indicate that they only started focusing more intensively on compliance from 2020 onward.

For many companies, regulatory changes served as the trigger to redefine or replace their compliance processes. The Critical Entities Resilience (CER) Directive was a decisive factor for 61 percent of companies, followed closely by the Cyber Resilience Act (CRA) with 57 percent.

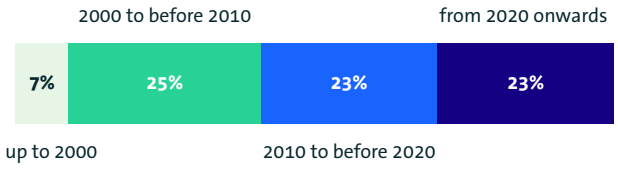
The Product Liability Directive (PLD) played a role for 44 percent, while 38 percent adapted their compliance processes because of the Digital Operational Resilience Act (DORA).

The Network and Information Security Directive (NIS2) had comparatively little impact, influencing only 2 percent of respondents.

In addition, 25 percent of companies report that non-regulatory events or other factors were decisive for changes in the compliance domain. Overall, this shows that European requirements—particularly CER and CRA—are the main drivers for adjustments in corporate compliance.

> 58 percent of companies that develop or integrate OSS into their products state that, as a result of the CRA, they will »integrate more OSS.« For 31 percent, usage is expected to »remain unchanged«, while 6 percent plan to integrate less OSS ↗ Bitkom-Dataverse.

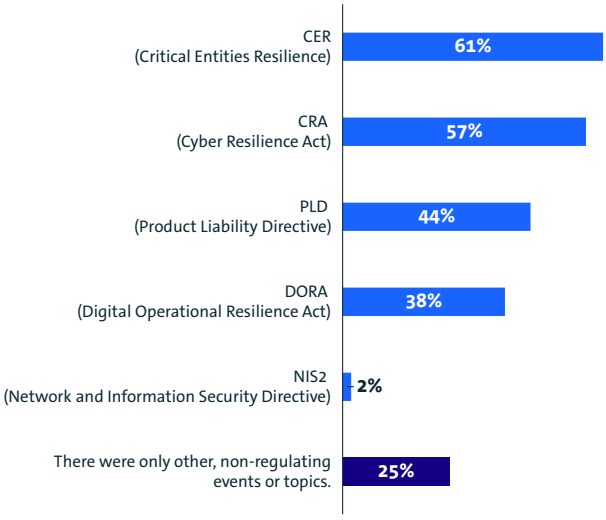
In which year did your company start to focus more on the topic of compliance?



Base: Organisations with a compliance process (n=367) | Not shown: »Don't know/no answer« | Source: Bitkom Research 2025

Figure 19: Start of Engagement with Compliance Issues

What regulatory innovations were decisive for defining a compliance process or replacing the existing compliance process?



Base: Organisations with a compliance process (n=367) | Not shown: »Don't know/no answer« | Source: Bitkom Research 2025

Figure 20: Impact of European Regulations (CER, CRA, PLD, DORA, NIS2) on Compliance Processes

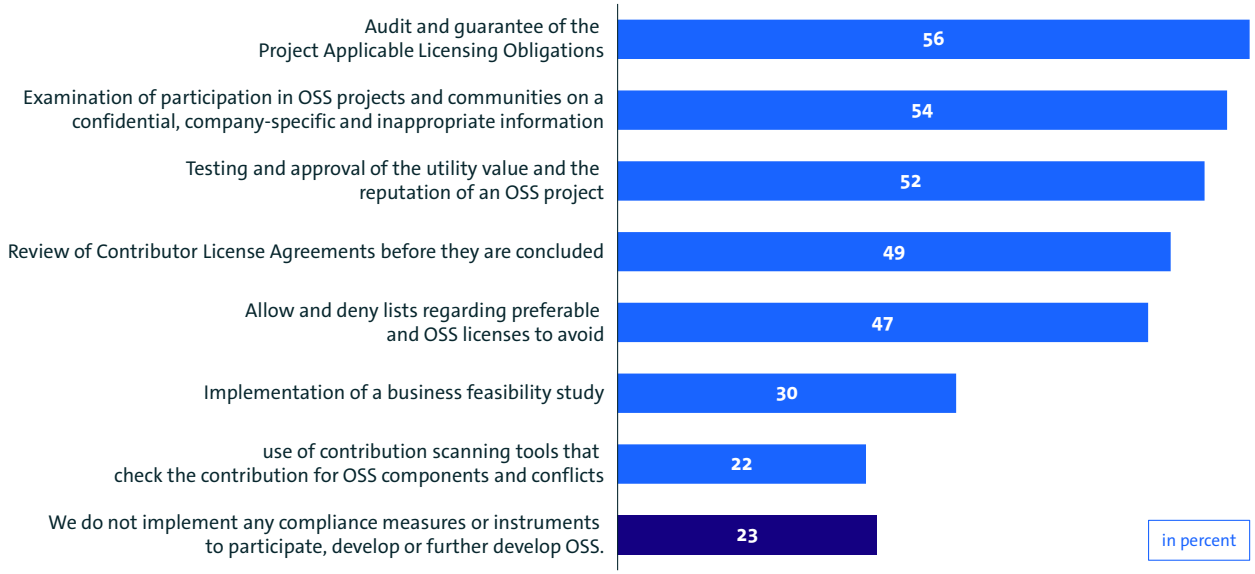
2.4 Compliance Policies and Instruments

In internal compliance management related to participation in Open Source Software (OSS) projects or the further development of OSS, companies primarily rely on formal review and control mechanisms. The most frequently mentioned measure is the review and assurance of applicable licence obligations (56 percent).

Similarly, 54 percent examine participation in projects and communities for confidential or company-specific information. 52 percent assess and approve the usefulness and reputation of a project. Nearly half of the companies review Contributor Licence Agreements (49 percent) or use allow- and deny-lists to specify preferred or excluded licenses (47 percent).

Less common are business feasibility assessments (30 percent) or the use of contribution scanning tools (22 percent). Notably, 23 percent report that they do not apply any compliance measures or instruments in this area.

What measures and instruments are used for your internal compliance management for participation in OSS projects or for the (further) development of OSS?



Base: Companies that use, integrate or (further) develop OSS (n=839) | Multiple answers were possible | Not shown: »Don't know/no information« | Source: Bitkom Research 2025

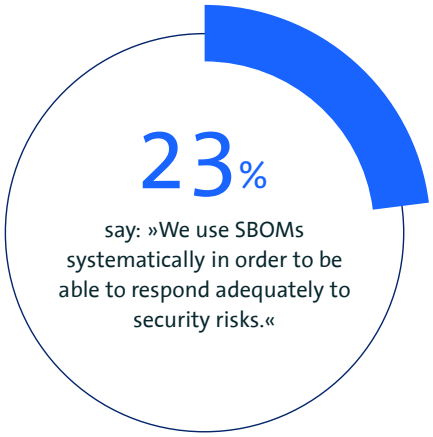
Figure 21: Compliance Measures and Instruments used in OSS Management

2.5 Open Source Software Standards in the Supply Chain

In handling their supply chain in the context of Open Source Software management, companies apply various standards. The most frequently used is ISO 5230 for licence compliance, employed by 37 percent of respondents.

32 percent utilize the BSI guideline 03183 on SBOM (Software Bill of Materials)—which corresponds to 23 percent of all companies—as well as 32 percent using ISO 18974 for OSS security.

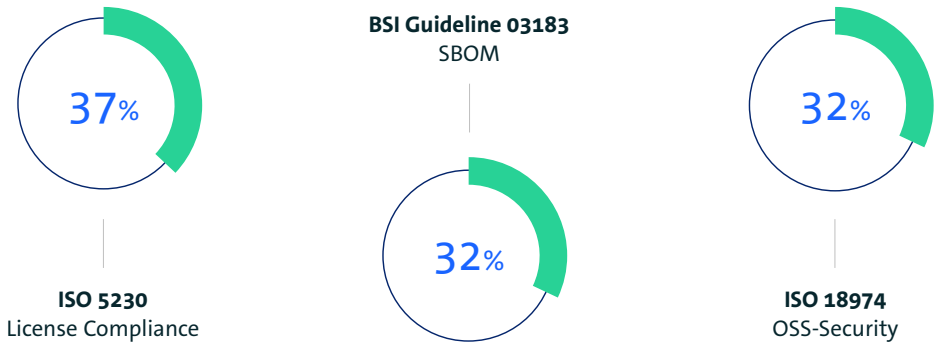
This shows that while standards are applied in some companies, none of the mentioned frameworks is used by a majority. Licence compliance via ISO 5230 is the most widespread, whereas security and transparency standards currently attract attention in only about one third of companies.



Base: All respondents (n=1,152) | Source: Bitkom Research 2025

Figure 22: Use of SBOMs in Companies

Which of the following standards do you use in your company for OSS management in dealing with the supply chain?



Base: Companies that use, integrate or (further) develop OSS (n=839) | Multiple answers were possible | Source: Bitkom Research 2025

Figure 23: Adoption of Standards in the Supply Chain (ISO 5230, ISO 18974, BSI 03183)

2.6 Budget for Compliance Measures

Compared with 2024, the situation regarding OSS compliance budgets appears largely stable. 39 percent of companies report that their budget has remained unchanged. 21 percent have more resources available—14 percent »slightly more« and 7 percent »significantly more«.

In contrast, only 10 percent report a decrease in financial resources, divided into 6 percent »slightly less« and 4 percent »significantly less.«

It is also noteworthy that one quarter of companies (25 percent) have no dedicated budget for OSS compliance.

Overall, the trend points toward stable or slightly increasing budgets, while substantial cuts remain relatively rare.

Compared to 2024: Do you have more or less budget available for OSS compliance this year?

in percent

Base: Companies that use, integrate, (further) develop, or otherwise participate in OSS (n=841) | Not shown: »Don't know/no information« | Source: Bitkom Research 2025

Figure 24: Developments of Budgets for OSS Compliance

3 Future Prospects, Politics & Artificial Intelligence

3 Future Prospects, Politics & AI

A look into the future shows that Artificial Intelligence (AI) and Open Source are closely interconnected. So far, companies have been rather cautious in using AI for their own software development: 38 percent do not plan to use it, one third (33 percent) are preparing for implementation, while 29 percent already use AI occasionally or regularly.

At the same time, more than half of respondents (51 percent) consider Open Source AI models to be recommendable, and 45 percent see them as a means of avoiding future dependencies.

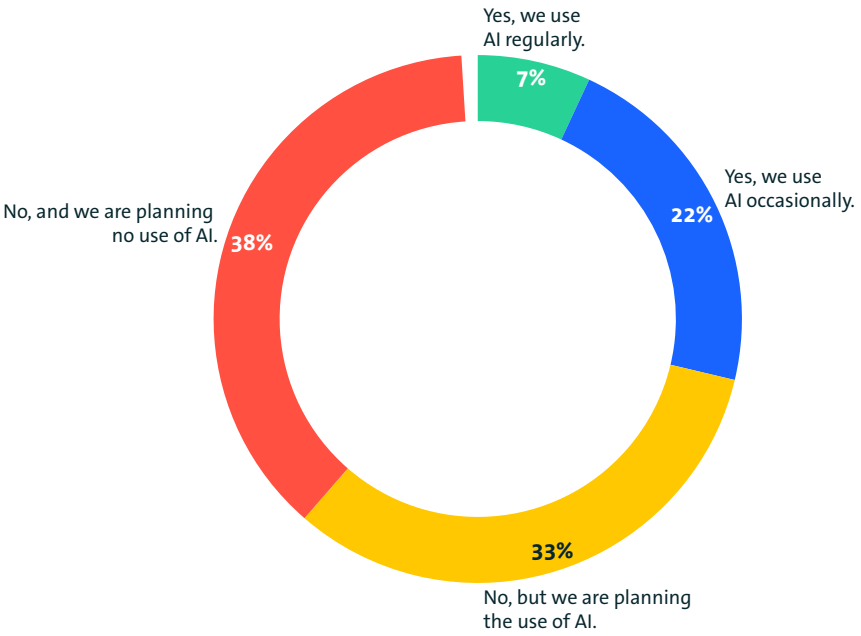
3.1 AI in Software Development

The use of Artificial Intelligence (AI) in software development still has room for growth in many companies. 38 percent state that they currently do not use AI and have no plans to do so. Another third (33 percent) also do not yet use AI but are planning its introduction.

AI is actively used in just under three out of ten companies: 22 percent use it occasionally, while only 7 percent report using AI regularly in software development.

This reveals a mixed picture: while some companies are already gaining initial experience with AI, for the majority it remains either a topic for the future or one that currently plays no role.

Is your company already using AI in software development?



Base: All respondents (n=1,152) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 25: Use of AI in Software Development in Companies

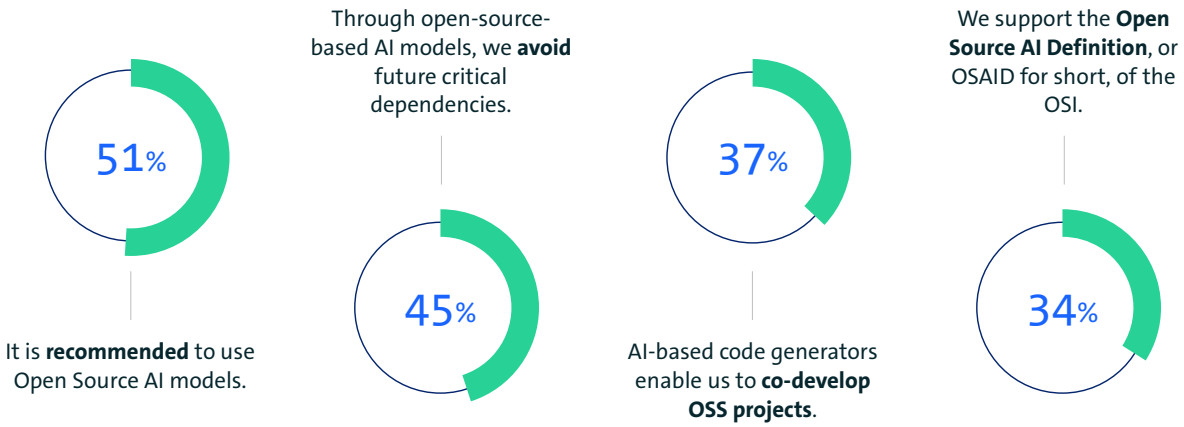
3.2 Open-Source AI Models

More than half of the surveyed companies (51 percent) consider the use of open-source AI models to be advisable. 45 percent also see them as an opportunity to avoid critical dependencies in the future.

37 percent state that AI-based code generators enable them to actively contribute to open-source projects. In addition, one third of companies (34 percent) support the Open Source AI Definition (OSAID) of the Open Source Initiative (OSI).

Taken together, these findings show that many companies regard open-source AI as a valuable and forward-looking approach; whether to strengthen independence, encourage active participation in projects, or promote shared standards.

To what extent do the following statements apply to your company or in your opinion?



Base: All respondents (n=1,152) | Responses to »Totally Agree« and »Tend to Agree« | Source: Bitkom Research 2025

Figure 26: Perceptions of Open-Source AI Models

3.3 Adoption and Concerns surrounding AI Code Generators

Base: All respondents (n=1,152) | Values for »Completely true« oder »Likely« | Source: Bitkom Research 2025

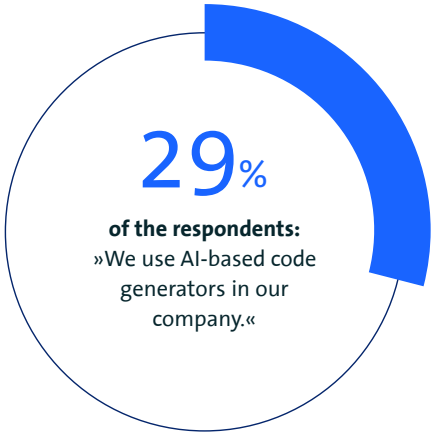
Figure 27: Perceived Risks of AI-Generated Code

More than half of the companies view the use of AI-generated code critically. 56 percent of respondents agree that using such code poses a potential threat.

This indicates that, despite the growing importance of AI in software development, significant security and trust concerns remain. Many companies see potential risks—particularly regarding quality, security, or legal issues—as outweighing possible benefits.

Nearly three out of ten companies already use AI-based code generators in their software development. 29 percent of respondents confirm that such tools are in use within their organisations.

Although AI is finding practical applications, its adoption is still limited. While some companies are already taking advantage of its potential, many others appear to hesitate—possibly due to concerns about quality, security, or legal implications.



Base: All respondents (n=1,152) | Values for »Completely true« oder »Likely« | Source: Bitkom Research 2025

Figure 28: Use of AI Code Generators in Companies

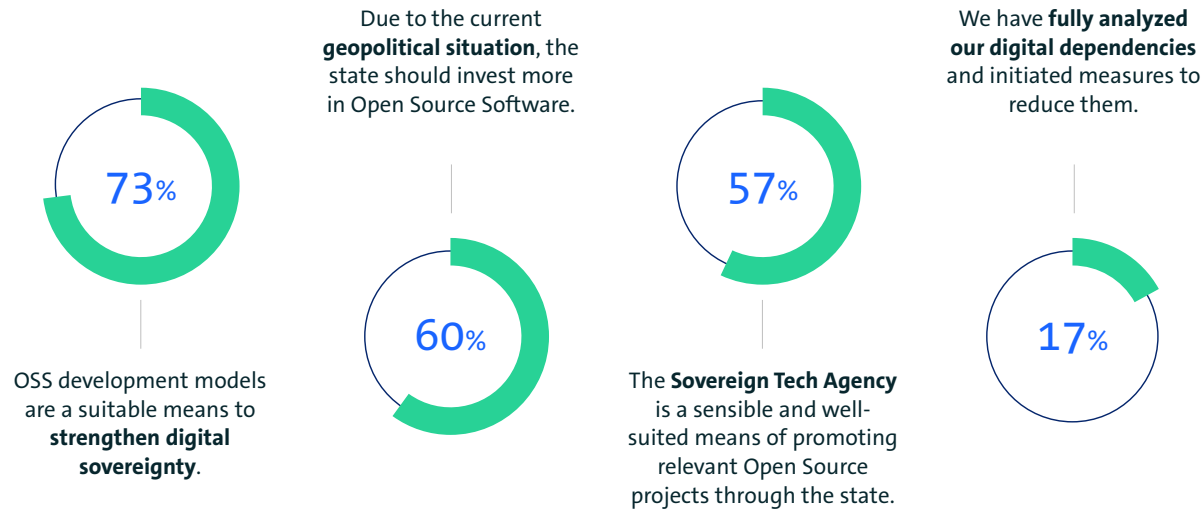
3.4 Open-Source as a Tool for Digital Sovereignty

The majority of companies view Open Source Software as an important instrument for strengthening digital sovereignty. 73 percent agree that OSS development models are particularly well suited for this purpose.

60 percent also believe that, given the current geopolitical situation, the state should invest more heavily in OSS. Government funding instruments such as the Sovereign Tech Agency are also met with approval: 57 percent of respondents consider them a meaningful way to support key open-source projects.

However, support is considerably lower when it comes to practical implementation within companies. Only 17 percent state that they have already fully analyzed their digital dependencies and taken concrete measures to reduce them.

To what extent do the following statements apply to your company or in your opinion?



Base: All respondents (n=1,152) | Source: Bitkom Research 2025

Figure 29: Views on OSS as an Instrument for Digital Sovereignty

4 Open Source in the Public Sector

4 Open Source in the Public Sector

Open Source is widely used in the public sector, although the areas of focus partly differ from those in the industry. 63 percent of the surveyed public authorities and organisations use OSS, allocating an average of 4 full-time equivalents (FTEs) for its management—about twice as many as in the private sector.

The general attitude toward OSS is predominantly positive: 52 percent are very or somewhat open to it, while 32 percent remain undecided.

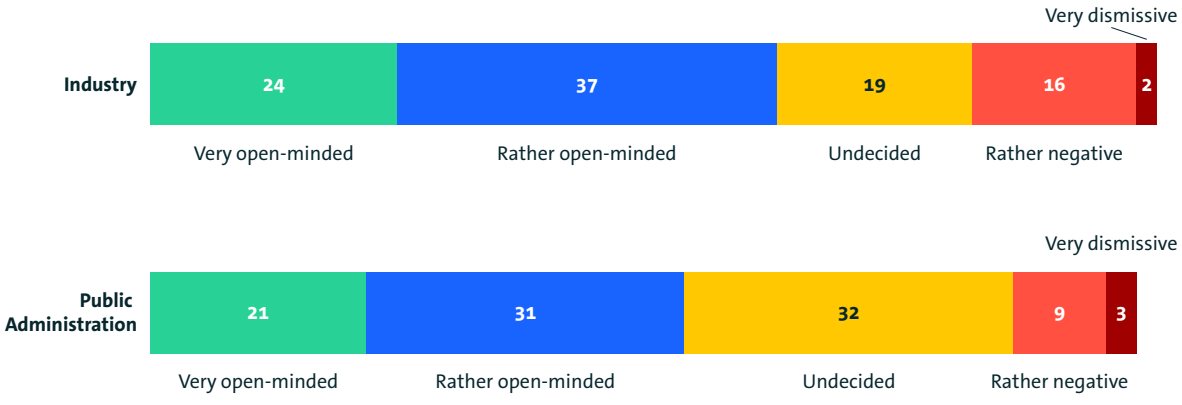
4.1 General Attitude towards Open Source Software

In the private sector, the attitude toward Open Source Software (OSS) is predominantly positive: 24 percent are very open and 37 percent somewhat open. Thus, more than half of the companies demonstrate a clear openness toward OSS. 19 percent are undecided, while 16 percent are somewhat negative and only 2 percent very negative (see ↗ Chapter 1.1).

A similarly positive picture emerges in public administration, though with slightly lower approval levels. Here, 21 percent are very open and 31 percent somewhat open. However, the share of undecided respondents is noticeably higher: 32 percent have not taken a clear positive or negative stance. 9 percent are somewhat negative and 3 percent very negative.

Overall, OSS is viewed positively in both the private and public sectors. While businesses tend to show stronger approval, public administrations are more reserved, with a significantly higher proportion of undecided respondents.

What is your organisation's general position on OSS?



in percent

Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 30: General Attitude towards OSS: Industry vs. Public Sector

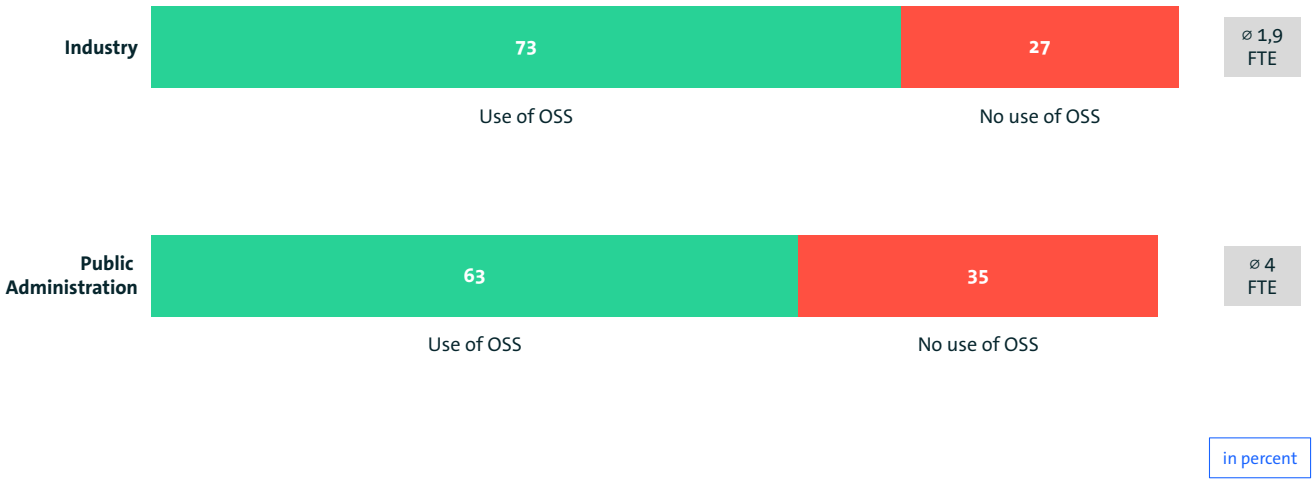
4.2 Use of Open Source Software

In the private sector, 73 percent use OSS, while 27 percent do not (see ↗ Chapter 1.3). In public administration, the share is slightly lower: 63 percent use OSS, whereas 35 percent do not.

Another aspect is the number of employees primarily engaged in OSS management. In the private sector, the average is 1,9 full-time equivalents (FTEs), whereas public administration deploys significantly more capacity, averaging 4 FTEs.

Overall, OSS is used by the majority of both businesses and public sector organisations. While its prevalence is somewhat higher in the private sector, public administration invests, on average, more personnel resources in OSS management.

Does your organisation use OSS?
And if so: How many employees are primarily involved in OSS management?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 31: Comparison of OSS Use and Staffing: Private Sector vs Public Administration

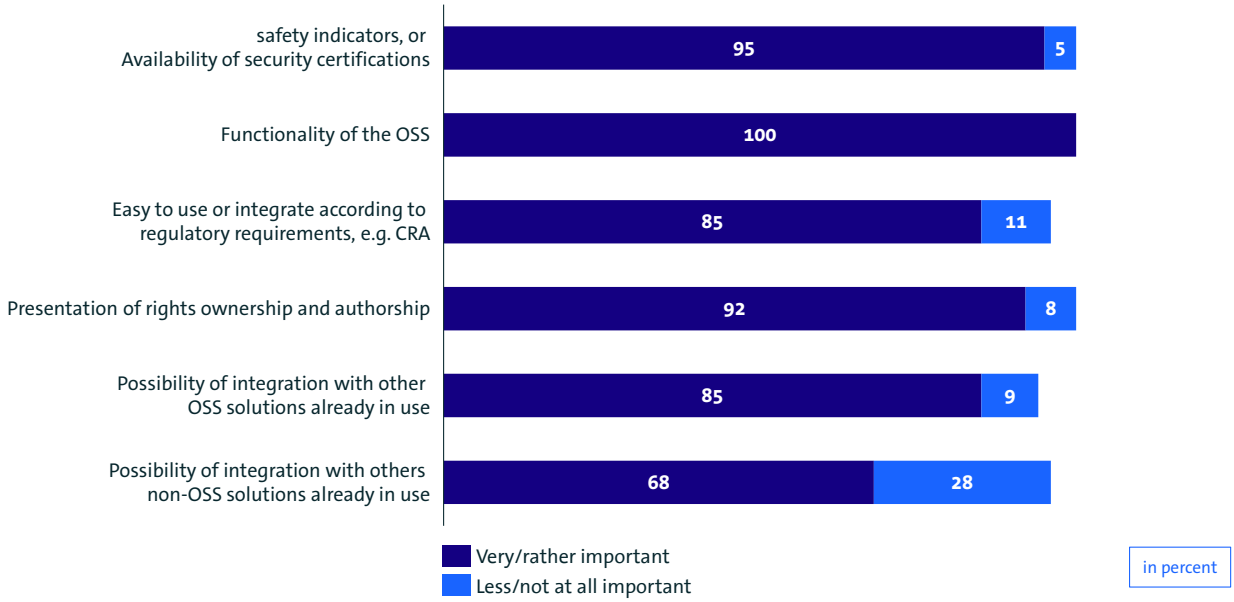
4.3 Selection Criteria for Open Source Software

In the public sector, functionality ranks first: all respondents (100 percent) rate this criterion as very or rather important when selecting OSS projects (the figure is similarly high in the private sector at 94 percent; see ↗ Chapter 1.4). Security aspects also play a major role, with 95 percent paying attention to security indicators or certifications.

The clarification of ownership and authorship rights is a relevant selection criterion for 92 percent of public sector organisations. Ease of use and integration in line with regulatory requirements—such as the Cyber Resilience Act (CRA)—is considered important by 85 percent. The same proportion (85 percent) value the ability to integrate OSS with other open-source solutions already in use.

The importance of integration with existing non-OSS solutions is somewhat lower: 68 percent regard this as an important criterion.

How important are the following criteria to you when selecting OSS projects?



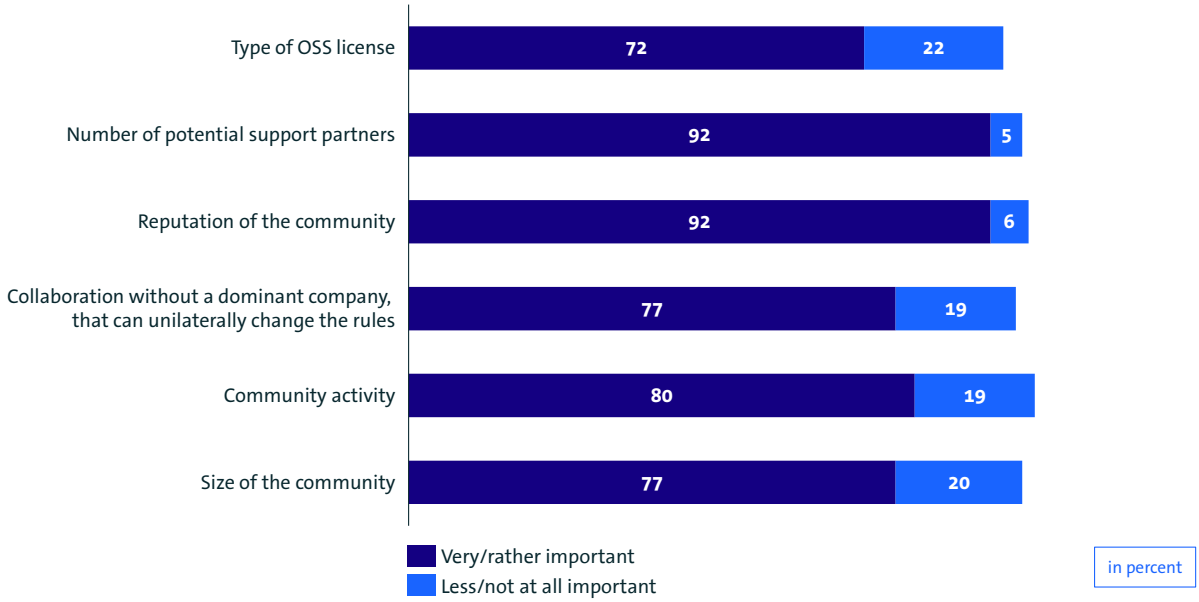
Base: Organisations that use, integrate or (further) develop OSS (n=65) | Multiple answers possible | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 32: Selection Criteria for OSS in the Public Sector: Security, Functionality, and Rights

The number of potential support partners (92 percent) and the reputation of the community (also 92 percent) are particularly highly valued. Community activity is likewise important for 80 percent of respondents.

Both the size of the community and the ability to collaborate without a dominant company capable of unilaterally changing rules are considered important by 77 percent each. The type of OSS licence, by contrast, plays a somewhat lesser role: 72 percent regard this as important, while 22 percent consider it less or not important at all.
Overall, it becomes clear that, in the public sector, alongside technical aspects, the structure of the community and the availability of support options play central roles in the evaluation of OSS projects.

How important are the following criteria to you when selecting OSS projects?



Base: Companies that use, integrate or (further) develop OSS (n=65) | Multiple answers were possible | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 33: Selection Criteria for OSS in the Public Sector: Community and Support Structure

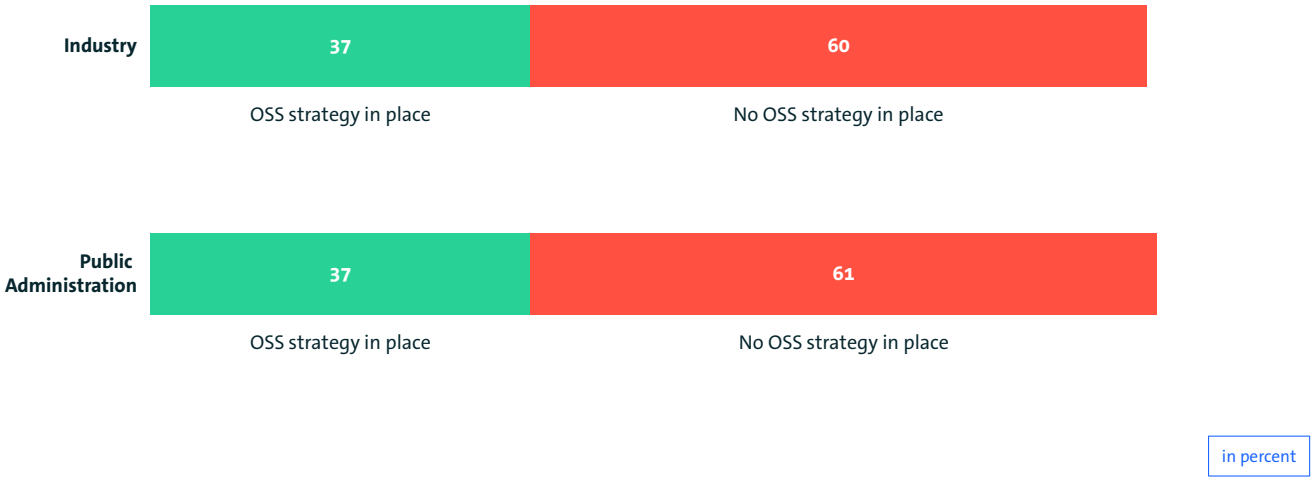
4.4 Open Source Software Strategy

In the private sector, 37 percent of respondents report having an OSS strategy, while 60 percent do not (see ↗ Chapter 1.2).

A nearly identical picture emerges in public administration: here too, 37 percent state that they have an OSS strategy, while 61 percent do not.

This shows that in both business and public administration, only a minority have a clear strategic direction for OSS, while the majority continue to operate without a defined strategy.

Is there a strategy in your organisation for using or participating in OSS?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 34: OSS Strategies: Industry vs Public Administration

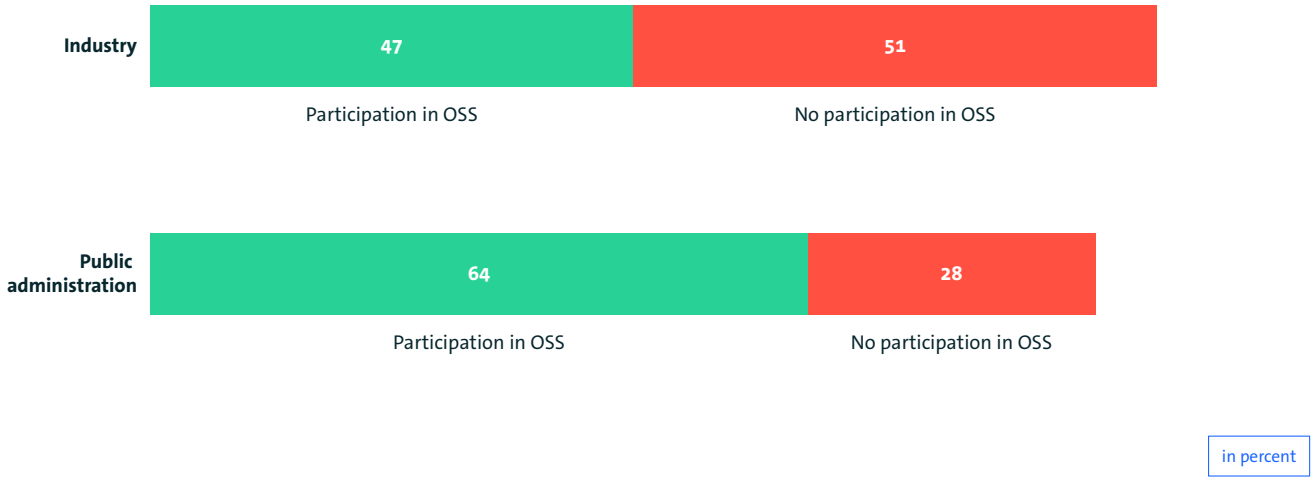
4.5 Engagement in the Ongoing Development of Open Source Software

In the industry, 47 percent actively participate in OSS projects, while 51 percent report no involvement (see ↗ Chapter 1.5).

In public administration, the picture is considerably more positive: 64 percent take part in the development or further development of OSS, while only 28 percent are not involved.

Whereas participation in the private sector is roughly balanced, the majority of public sector organisations are actively engaged in the OSS environment.

Are you involved in the development or further development of OSS?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 35: Participation in the Development and Further Development of OSS: Industry vs Public Administration

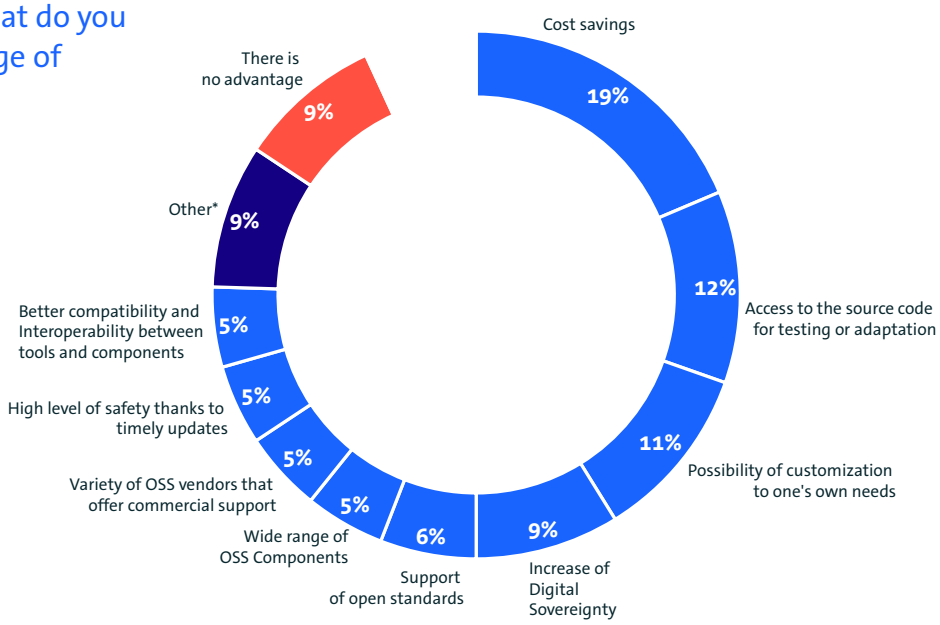
4.6 Advantages of Open Source Software

In public administration, cost leadership remains the strongest argument for open-source solutions: the most frequently cited advantage is cost savings, mentioned by 19 percent of respondents. Other key benefits include access to the source code for review or modification (12 percent) and the ability to adapt software to specific organisational needs (11 percent).

A further 9 percent cite enhanced digital sovereignty and »other« benefits, while another 9 percent state that they see no advantage in OSS. This share is lower in the private sector, at 4 percent (see ↗ Chapter 1.6).

Additional aspects mentioned by 5 percent each include the wide range of OSS components, the large number of vendors offering commercial support, high security through timely updates, and improved compatibility and interoperability between tools and components.

Regardless of whether you use OSS in your organisation or not, what do you think is the biggest advantage of using OSS?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025
*High stability, low susceptibility to error (3%); Attractive IT workplace, motivation for employees (2%); Sustainable profitability/no sharp increase in costs (2%); Short innovation cycles (1%); Possibility to change providers, better negotiation options, reduction of vendor lock-in (1%)

Figure 36: Perceived Advantages of OSS in Public Administration

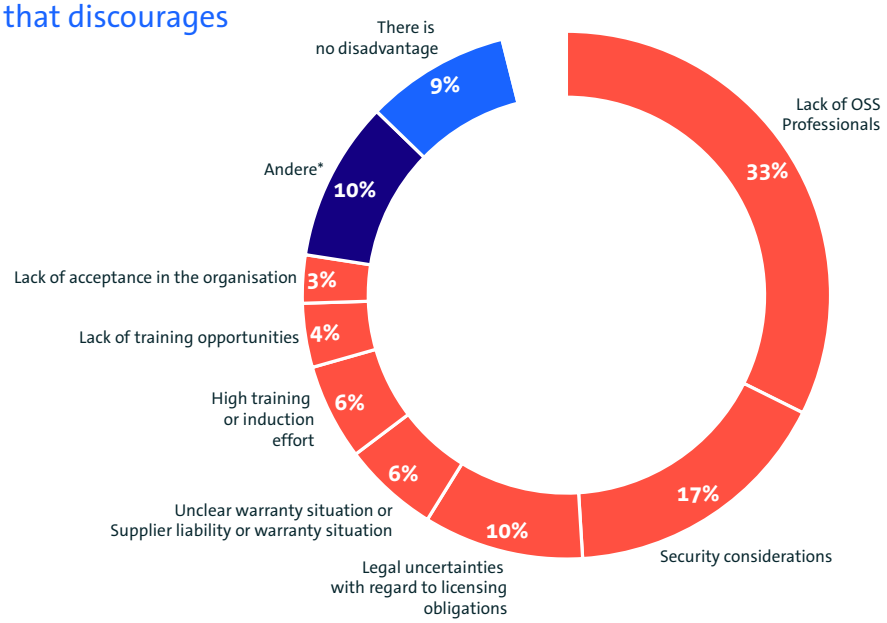
4.7 Disadvantages of Open Source Software

The most frequently cited issue is the shortage of OSS specialists: 33 percent of respondents consider this the greatest problem. Security aspects rank second, highlighted by 17 percent.

Legal uncertainties regarding licensing obligations are mentioned by 10 percent, as are »other« disadvantages. Unclear warranty conditions or supplier liability, as well as high training or onboarding requirements, are relevant for 6 percent each. A lack of training opportunities is cited by 4 percent, and low organisational acceptance by 3 percent.

Notably, 9 percent of respondents state that they see no disadvantages in using OSS. In the private sector, this share is lower, at 4 percent (see ↗ Chapter 1.7).

And in your opinion, what is the biggest disadvantage that discourages the use of OSS?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025
*Conversion from vendor-specific software to OSS too time-consuming (2%); Uncertain future of OSS (2%); Lack of interfaces to other systems (1%); Low stability, high susceptibility to errors (1%); Supply Chain Security Challenges (1%); Other (3%)

Figure 37: Perceived Disadvantages of OSS in Public Administration

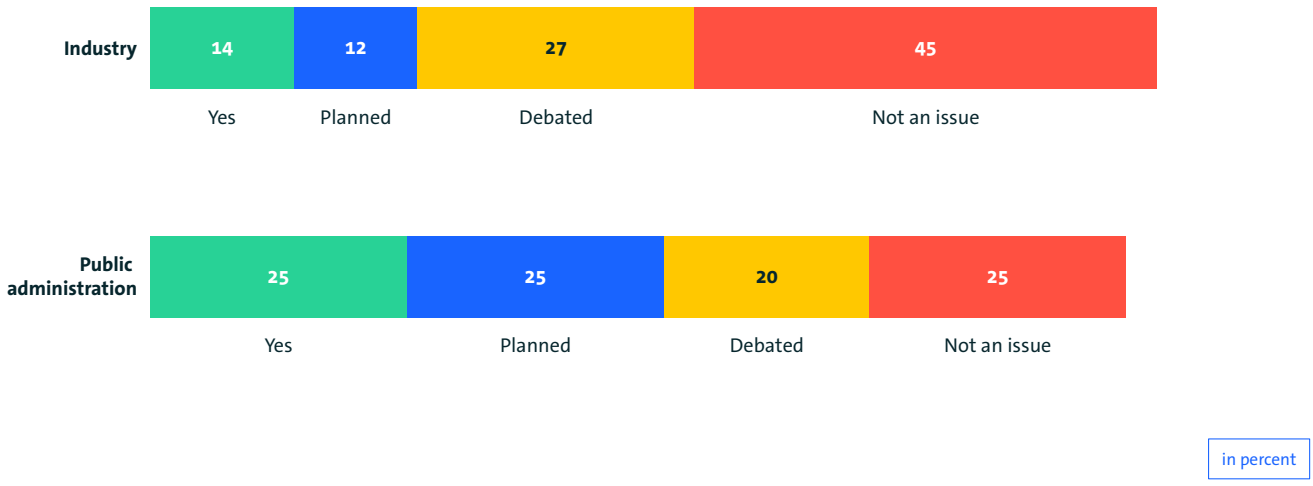
4.8 Open Source Programme Offices (OSPOs)

In the industry, 14 percent have established an Open Source Programme Office (OSPO), while another 12 percent are planning to introduce one. 27 percent are discussing the topic, whereas for 45 percent an OSPO is currently not under consideration (see ↗ Chapter 2.1).

In public administration, the proportion of those that have already set up an OSPO is significantly higher, at 25 percent. A further 25 percent are planning to establish one, and 20 percent are discussing the topic. Only one quarter of respondents (25 percent) state that an OSPO is not a topic within their organisation.

Overall, OSPOs are more widespread and more concretely planned in public administration, while in the industry almost half of respondents report no engagement with the topic.

Have you set up an Open Source Program Office (OSPO)?



Base: Companies that use, integrate or (further) develop OSS (Industry: n=839 | Public administration: n=65) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 38: Proportion of Organisations with OSPOs in the Public Sector

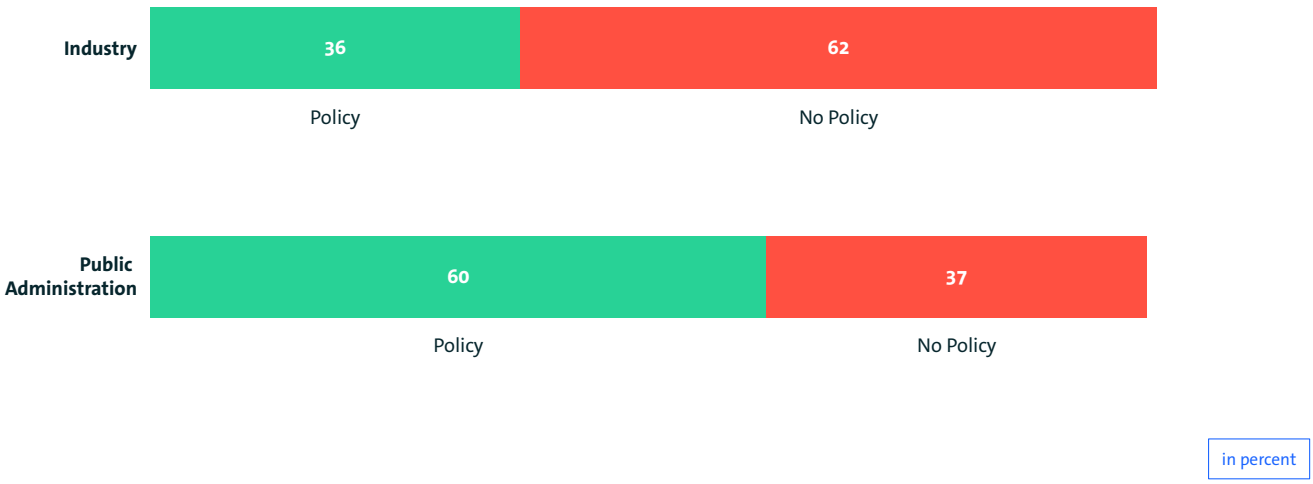
4.9 Open Source Software-Policy

In the industry, 36 percent have a document outlining guidelines and rules for handling Open Source Software (OSS), while 62 percent have no established regulations (see ↗ Chapter 2.2).

In public administration, the picture is almost reversed: 60 percent report having an OSS policy, while 37 percent do not.

This shows that public administration approaches the formal handling of OSS in a more structured manner than the industry. While the majority of businesses operate without defined guidelines, most public sector organisations have established clear rules.

Does your organisation have an OSS policy, i.e. a document that writes down guidelines and rules for dealing with OSS in your company?



Base: Companies that use, integrate, (further) develop, or otherwise participate in OSS (Industry: n=841 | Public administration: n=68) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 39: Existence of an OSS Policy: Public Sector vs Industry

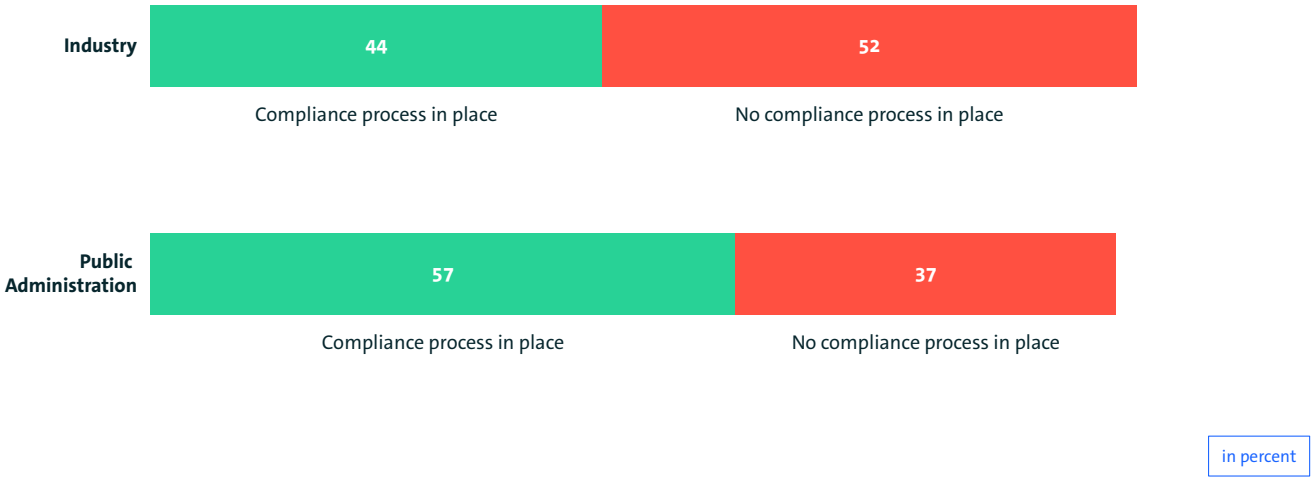
4.10 Compliance Process for Employees

In the industry, 44 percent have an established compliance process that requires employees to adhere to regulatory obligations, while 52 percent state that no such process exists (see ↗ Chapter 2.2).

In public administration, the proportion is higher: more than half (57 percent) have implemented a compliance process, and only 37 percent do not.

Overall, this shows that public administration applies a more structured approach with binding processes for the use of OSS, while in the industry slightly more than half still operate without formalised procedures.

Is there a written compliance process in your organisation for how employees deal with OSS?



Base: Companies that use, integrate, (further) develop, or otherwise participate in OSS (Industry: n=841 | Public administration: n=68) | Other: »Don't know/no information« | Source: Bitkom Research 2025

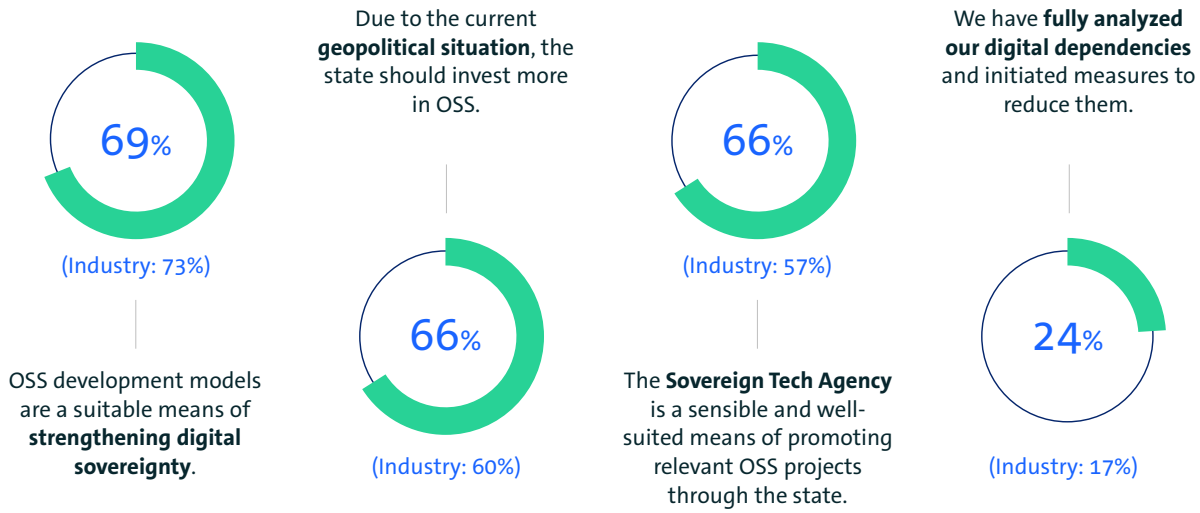
Figure 40: Compliance Processes for Employees: Public Sector vs Industry

4.11 Open Source Software as a Tool for Digital Sovereignty

69 percent view OSS development models as an effective means of strengthening digital sovereignty. In the industry, this share is slightly higher at 73 percent.

66 percent of respondents agree that, given the current geopolitical situation, governments should invest more heavily in open source. Likewise, 66 percent consider the Sovereign Tech Agency a useful instrument for supporting relevant OSS-projects through public funding. Approval is significantly lower when it comes to analysing and reducing digital dependencies: only 24 percent state that they have already fully assessed their dependencies and taken appropriate action. In the industry, the share is even lower, at just 17 percent (see ↗ Chapter 3.4).

To what extent do the following statements apply to your organisation or in your opinion?



Base: All respondents (industry: n=1,152 | Public administration: n=103) | Source: Bitkom Research 2025

Figure 41: Agreement with Statements on OSS as a Tool for Digital Sovereignty in Public Administration

4.12 AI in Software Development

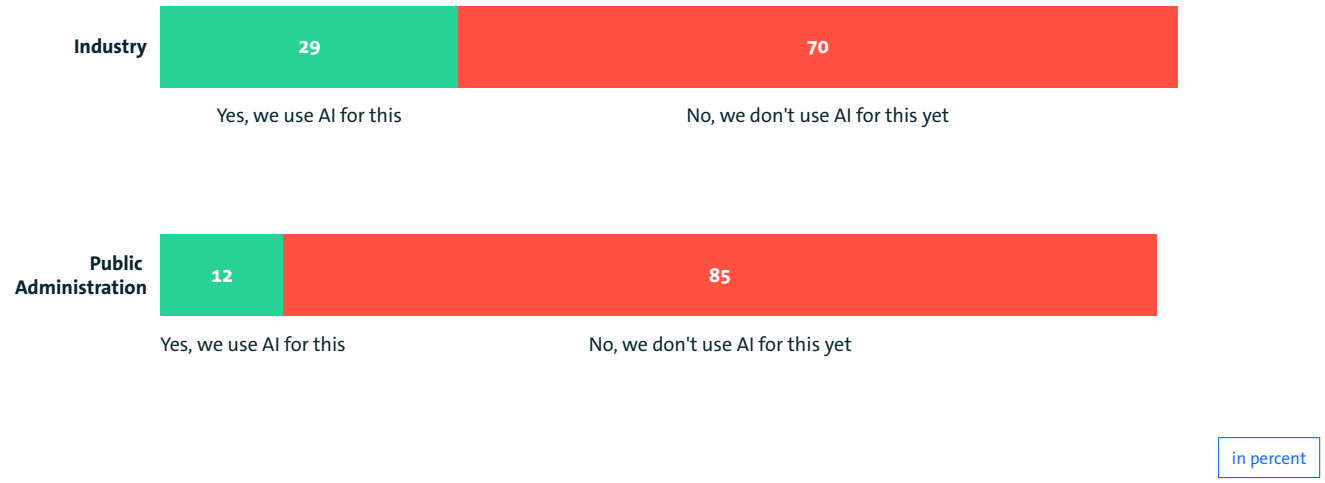
In the private sector, 29 percent of companies already use AI in the area of software development, while 70 percent do not (see ↗ Chapter 3.1).

In public administration, the share is significantly lower: only 12 percent use AI in software development, whereas 85 percent do not.

Both the industry and public administration view AI-generated code largely critically: 56 percent of respondents in each group state that they consider it »a risk.«

↗ Bitkom-Dataverse

Is your organisation already using AI in software development?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 42: Use of AI in Software Development: Public Sector vs Private Sector

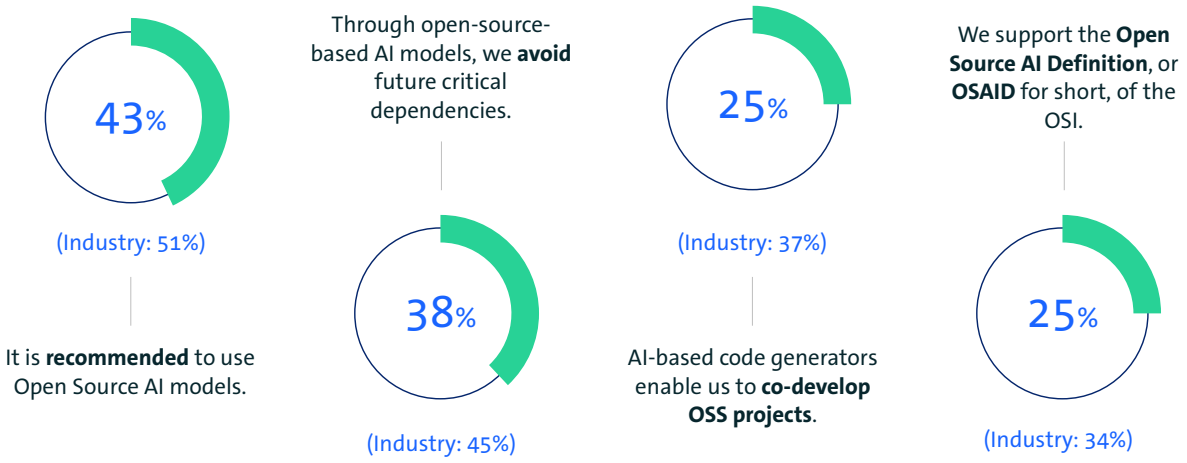
4.13 Open-Source as a Tool for Digital Sovereignty

In public administration, 43 percent consider it advisable to use Open Source AI models. In the industry, this figure is slightly higher at 51 percent (see ↗ Chapter 3.2).

38 percent agree that open-source-based AI models can help avoid future critical dependencies, with the industry again above the overall average at 45 percent.

Agreement is considerably lower for two other statements: only 25 percent see AI-based code generators as a way to contribute to OSS projects, and the same proportion—25 percent—support the »Open Source AI Definition« (OSAID) of the OSI.

To what extent do the following statements apply to your organisation or in your opinion?



Base: All respondents (Industry: n=1,152 | Public administration: n=103) | Responses to »Totally Agree« and »Tend to Agree« | Other: »Don't know/no information« | Source: Bitkom Research 2025

Figure 43: Perceptions of Open Source AI Models in Public Administration

5 Case Studies

Note

The following contributions are case studies provided by Bitkom member companies. They offer insights from a corporate perspective and showcase projects as well as practical solutions.
The case studies are presented in this publication as part of a sponsorship. Each company is solely responsible for the content of its respective page.

5.1 OCCTET: Open Source Compliance for the CRA – practical and free of charge

Open Source is ubiquitous and increasingly subject to regulatory scrutiny. Modern software products are composed of more than 90 percent Open Source components. This acceleration in development, however, also brings security risks.Under the new Cyber Resilience Act (CRA), the EU requires all manufacturers of digital products to implement comprehensive measures: vulnerabilities must be continuously identified, documented, and remedied — including those affecting open-source components.
The challenge is that these requirements also apply to small and medium-sized enterprises (SMEs), which often lack the expertise and resources to meet such complex compliance obligations.

SBOMs & Cybersecurity

For demonstrating CRA compliance, a complete Software Bill of Materials (SBOM) is required, along with regular checks on security status and update strategies. However, many components are deeply embedded or difficult to identify. Fully automated scans are often inaccurate, while manual follow-up work is costly. The time and financial burden can be a particular obstacle for SMEs and often results, in practice, in a lack of transparency regarding the actual Open Source components included in the product.

Solution: Bitsea: AI for Legally Compliant Licence Analyses — OCCTET

The OCCTET Project (Open Source Compliance Comprehensive Tools and Resources) is an EU-funded initiative aimed at enhancing cybersecurity and ensuring compliance with the Cyber Resilience Act (CRA). The project focuses on developing an Open Source toolkit to automate the compliance process for free and Open Source Software used in digital products—specifically tailored to the needs of European SMEs.

The toolkit includes, among other components:

- a CRA-Compliance checklist
- an intelligent scanner for generating SBOMs, including the identification of related known security gaps
- a federated database platform for publishing the results of OSS component assessments, enabling contributions from various stakeholders
- a reporting tool for documenting security and licensing status

OCCTET is supported by a consortium of cybersecurity experts, Open Source organisations, and European SMEs. It builds on established tools such as the OSS Review Toolkit and ScanCode, which are being specifically expanded and refined.

A key project member is Bitsea, contributing AI-based functionalities. The main focus lies on the automation of open-source detection. Here, an AI system analyses code fragments and metadata using extensive datasets to correctly identify components—saving substantial time while reducing errors. The AI also filters out false positives to further improve accuracy.

Conclusion: CRA-Compliance as Open Source

OCCTET demonstrates that CRA compliance does not have to be expensive or complex. Through open development and active community involvement, the project creates a tool that supports not only individual companies but also strengthens European cybersecurity as a whole. Further information can be found at occtet.eu. The release is planned for mid-2026. Please feel free to contact us regarding this topic.

Bitsea identifies hidden risks in software systems and supports organisations in maintaining IT compliance. We advise clients on the sustainable use and management of open-source software. Our customers include leading enterprises across all industries. Bitsea is a member of Bitkom and a partner of the OpenChain Project.

Dr. Andreas Kotulla
Managing Director
Bitsea GmbH

5.2 Open Source Compliance in the Supply Chain

Modern software development without the inclusion of open-source components is virtually unthinkable today. According to the Harvard Business School study «The Value of Open Source", many commercial applications consist of more than 90 percent open-source components, thereby generating substantial commercial value for their users. Even in niche applications, development tools based on Open Source Software (OSS) are frequently used. It is therefore all the more surprising that the use of OSS often appears to take place in a more or less uncoordinated manner.

At least, this is suggested by the responses to the question in the current edition of the Bitkom Open Source Monitor regarding whether companies have an OSS policy in place. This impression is further reinforced by the low prevalence of Open Source Program Offices (OSPOs). The willingness to establish an OSPO can be seen as an indicator that a company recognizes the importance of OSS both from a compliance perspective and as a strategic asset. Within collaborative development between suppliers and customers, OSPOs represent a valuable trust-building entity, serving as a reliable point of contact for both internal and external inquiries.

Regulations such as the Cyber Resilience Act (CRA) and other requirements concerning security, vulnerabilities, or SBOMs will transform software development—particularly within collaborative development networks—toward greater transparency. These changes require an OSS strategy that should be managed consistently through an OSPO.

Drawing on twelve years of OSPO experience at Bosch and involvement in various communities, the following steps have proven essential when working with Open Source Software:

Step 1: Organisation and Processes

With the OpenChain Specification (ISO 5230), we have a foundation that defines process descriptions as well as organisational measures for ensuring OSS compliance. This standard is available free of charge, together with a wide range of supplementary documents, checklists, and a self-assessment method.

Step 2: Tools

A comprehensive OSS compliance toolchain encompasses the analysis of dependencies, source code scanning, identification of vulnerabilities, application of governance frameworks, and documentation of results.

The acquisition of such tools is often a cost issue, leading to a wide variety of solutions across the supply chain. In recent times, several open-source projects have been launched in this area.

From our perspective, the Open Source Review Toolkit (ORT) and the Eclipse Apoapsis Project, which builds upon it, are solutions that can drive standardisation within an organisation—one of the reasons why Bosch is actively involved in their development. ORT is also part of the toolchains used in the EU-funded OCCTET Project, which aims to support SMEs and open-source developers in achieving compliance with the Cyber Resilience Act (CRA). This underscores the wide range of possible applications for different types of organisations.

Step 3: Exchange Formats

Currently, we have several standards for exchange formats of compliance information, along with numerous norms and legal regulations that require different types of information.

From our perspective, the SEPIA Project, organised within the SBOM Study Group of the OpenChain Project, represents a viable solution. However, as with all open-source initiatives, its success depends on the contribution of diverse perspectives and active participation.

5.3 Bridges and Operating Systems – The Hidden Frameworks that hold Everything together

Open Source Software is the foundation of our digital world — it powers mobility systems, safety-critical control units, cloud platforms, and increasingly also public administration. Yet, much like roads and bridges, we often only recognise its importance when it no longer carries the load.

What makes open source possible is often invisible — but essential to the system as a whole.

At Kernkonzept GmbH, we take responsibility for one of these foundational layers as the maintainer of the Open Source operating system framework L4Re. L4Re is a microkernel technology used worldwide in certified infrastructures — from automotive systems and smartphones to DSL routers and avionics.

Versions of L4Re are deployed in applications certified up to VS-GEHEIM (Top Secret, Germany) or ISO 26262 ASIL B, and are themselves approved for handling data classified up to VS-GEHEIM and NATO SECRET. They are also Common Criteria EAL 4+ certified — all of it based on the Open Source version.

What L4Re enables — verified security based on Open Source — is the result of nearly 30 years of continuous development: it began at TU Dresden, was carried forward by successive generations of researchers, and was ultimately transferred into a legally accountable company. Today, we take responsibility for security, certification, and patch policies — not just for code. We stand behind this infrastructure with our name, our liability, and our long-term commitment.

»Such infrastructures cannot be secured through idealism and cross-subsidisation alone. Anyone who takes digital resilience seriously must also consider the need for a clear governmental commitment to research and maintenance.«

The Bitkom Open-Source-Monitor 2025 shows that 73 percent of companies use open-source software, but only 47 percent actively contribute – and most of those primarily through subscriptions and services. What appears to be freely available is, in fact, often silent infrastructure work – increasingly strained by liability concerns, security pressures, and new EU regulations.

»Some see open source as public code. We see it as infrastructure. L4Re is like a digital bridge – deep within the system, barely visible, yet providing security. To ensure it holds, reliable cooperation among all stakeholders is essential.«

Practice and studies show that when use is not accompanied by shared responsibility, overuse and erosion become real risks. A functioning Open Source ecosystem requires clear roles, fair participation, and structural feedback — not merely new obligations.

If Open Source is to be part of digital sovereignty, both political and economic reliability are essential. The continued development of open source, as well as the work of maintainers, is not a peripheral concern but a core element of digital public infrastructure.

What does this require? A sustainable procurement policy that understands open source and treats it as equal — or even gives it preference. The courage to take responsibility, and the necessary knowledge — on the side of businesses. And educational pathways in schools, universities, and companies that enable young people not only to be users but to become creators of our digital infrastructure.

Dr.-Ing. Adam Lackorzynski
CTO & Founder

Katrin Kahle
Head of Product

5.4 Open Source Is Everywhere – and Officially Regulated from 2027

With the Cyber Resilience Act (CRA), the EU has, for the first time, introduced comprehensive cybersecurity legislation for digital products containing software. Although many Open Source projects are exempt from the CRA itself, it nevertheless affects every company that integrates Open Source components into its products and markets them commercially — in other words, virtually the entire industry.

Particularly in focus are **the obligations to create and maintain Software Bills of Materials (SBOMs), to provide security updates over several years, and to establish a structured vulnerability disclosure process.** Anyone using Open Source components will, in the future, also be liable for the associated risks — regardless of whether those components were developed in-house or sourced from third parties.

This Changes Everything

What is new here is not the need for legal governance, but the fact that it is now being made a statutory requirement for the first time. Whereas open-source compliance was previously driven mainly by licence terms, the Cyber Resilience Act (CRA) now adds explicit security-related obligations to these requirements. This affects contract design, internal processes, and collaboration with suppliers.

Companies now need not only technical, but also **legal governance** around open source: Who is responsible for licence and security reviews? How can the use of open source be transparently documented throughout the product lifecycle? And how can it be ensured that affected components are patched or replaced in good time?

The good news: the Cyber Resilience Act (CRA) can become a catalyst for better **Open Source Management** — provided that companies act early. Those who invest now in an **Open Source Programme Office (OSPO)**, establish clear **Open Source Policies**, and implement tools for **automated SBOM tracking** will achieve not only compliance, but also **greater market trust.**

The Cyber Resilience Act (CRA) is coming — and with it, the responsibility to use open source **strategically, in full legal compliance, and with resilience.**
For companies, this means not only new obligations, but also an opportunity to make their digital products more robust, transparent, and trustworthy.

Osborne Clarke regularly advises companies on establishing legally compliant OSS processes, for example through:

- contract design with suppliers (Open Source clauses)
- creation and review of SBOMs
- compliance audits and risk assessments
- establishment of incident response structures in the OSS context

Dr. Hendrik Schöttle
Lawyer, Partner,
Certified Specialist in IT Law

5.5 Open Source Enables Added Value and Digital Sovereignty

OSS Maturity as a strategic advance

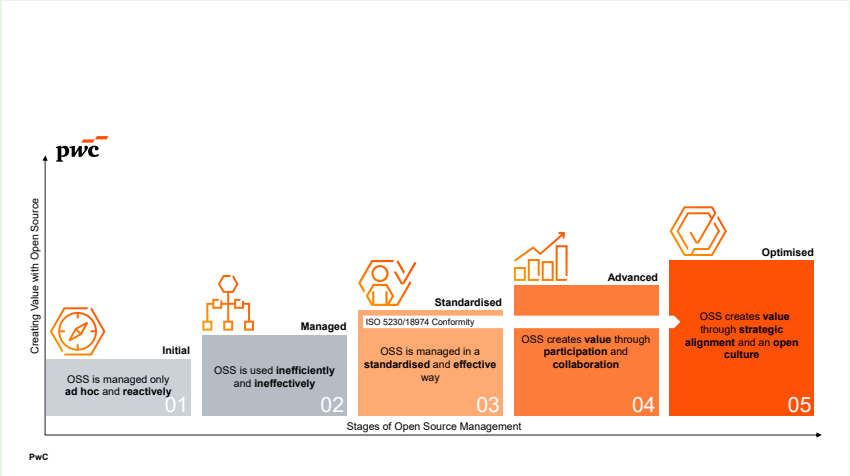
Given the current geopolitical tensions, Open Source Software (OSS)[1] is becoming a crucial tool for digital sovereignty. A recent Bitkom survey revealed that more than 70 percent of respondents view OSS development models as an appropriate means of strengthening digital sovereignty. An equal share reported that they already use OSS, yet only a few organisations have an established OSS strategy, and fewer than 40 percent have implemented effective compliance measures. To truly reinforce digital sovereignty, however, OSS must be deployed in a standardized and structured manner. In terms of our maturity model, this corresponds to at least Maturity Level 3. At this stage, an organization has effectively implemented a comprehensive OSS strategy, along with policies, processes, compliance and security tools featuring automated workflows that ensure complete and accurate Software Bills of Materials (SBOMs), as well as appropriate training measures. Once these foundations are in place, organisations can begin to create additional value. Higher levels of OSS maturity provide strategic advantages and, through collaboration and openness, enable maximum value creation both through and with OSS. In the long run, this fosters a culture of openness, making OSS the central driver for strengthening, expanding, and developing sustainable business models.

Regulation drives and supports OSS maturity

Regulations such as CRA, DORA, PLD, CER, and NIS2 mandate a structured approach to open source. International standards like ISO/IEC 5230 and ISO/IEC 18974 provide a clear basis: they require standardized processes for licence and security management and thereby support compliance with regulatory requirements. A robust practice of producing SBOMs and role-based training promotes correct application. Particularly in the financial sector, one observes: organisations that manage OSS professionally not only increase digital resilience, but also attain higher maturity levels faster—and position themselves as trustworthy market participants and ICT service providers.

Fostering Open Source Maturity

Our services — from OSS strategy to operational implementation, from policy design to code scanning and SBOM generation — are designed to optimize your organisation's open-source maturity. Through targeted benchmarking, we identify the current maturity level of your OSS practices and support your strategic alignment. We assist in establishing or optimizing your Open Source Programme Office (OSPO) to strengthen OSS security, compliance, and value creation. Higher maturity levels are achieved through a clear service model, strategic collaboration, and frameworks that enable contribution, co-creation, and inner source practices.



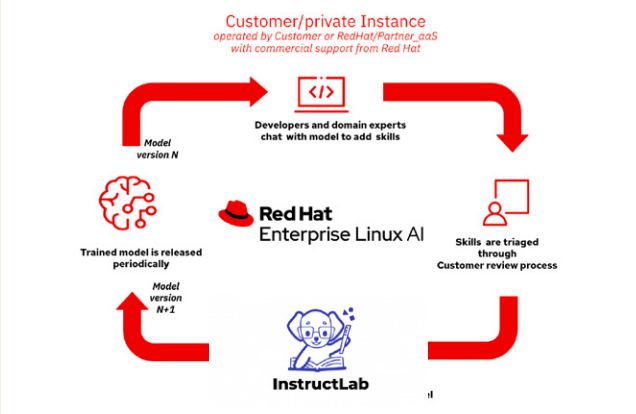
1 https://www.pwc.de/opensource

Marcel Scholze
Director | Open Source Services,
Digital Sovereignty

5.6 Achieving Transparent AI Use Through Open Source

To remain competitive and future-proof, companies cannot afford to ignore artificial intelligence. However, in critical business areas, unrestricted use of this technology is rarely justifiable. Security, transparency, stability, and independence must be maintained. It is precisely here that Open Source principles, technologies, and solutions are coming increasingly into focus.

Open Source is characterised by transparency, interoperability, and the avoidance of vendor lock-in. In addition, Open Source stands for agility, flexibility, scalability, and strong innovative capacity driven by dynamic, community-based development. These advantages of Open Source are particularly relevant in the field of AI. When using AI, a high degree of traceability should always be ensured. Few companies are willing to accept a black box when it comes to algorithms, training data, or models. Moreover, Open Source–based platforms, tools, and technologies provide an optimal foundation for the successful and flexible operation of AI models – regardless of whether these ultimately meet the formal definition of Open Source AI. In the AI context, the Open Source approach also means access to certified AI partners within an ecosystem framework. This enables companies to make use of complete solutions for the development, deployment, and management of models for AI-driven applications relatively easily and quickly.



The community project InstructLab, initiated by IBM and Red Hat, supports simplified experimentation with generative AI models and optimised model adaptation. | Source: Red Hat

The success story of Open Source and open standards in the software sector has been ongoing for more than three decades. In the field of AI, Open Source concepts are set to play the same catalytic role. Only an open approach will ultimately make it possible to keep pace with the rapid development of AI. The growing importance of Open Source in AI is underscored by the many projects currently being driven forward with great intensity. Examples include the InstructLab project and the Granite family of Open Source–licensed models. InstructLab is a solution for optimising LLMs that requires fewer data and computing resources to train a model. It is also accessible to users who are not data scientists. The Granite 3.0 model family enables companies to address AI use cases such as code generation, natural language processing, or deriving insights from large datasets. Another widely discussed initiative is the Open Source project vLLM, whose technology allows computations with an LLM to be performed more efficiently – for example, through improved GPU memory utilisation. This enhances the speed, performance, and flexibility of generative applications.

The fact that companies are increasingly turning to Open Source for AI is also confirmed by the latest »Open Source Monitor« from Bitkom Research. More than 1,100 companies participated in this study on Open Source adoption in Germany. Over 50 percent consider it advisable to use Open Source AI models, and more than half state that Open Source–based AI models can help avoid future critical dependencies. There is no doubt that the broad Open Source community will continue to drive Open Source AI innovation forward. This will further open and democratise the world of AI – a development of particular significance in times of geopolitical disruption, when digital sovereignty is becoming ever more important. Open Source AI can be a key building block in achieving this independence.

Gregor von Jagow
Senior Director & Country Manager Germany

5.7 NeoNephos Foundation: Open Source for Europe's Digital Sovereignty

On 31. March 2025, the NeoNephos Foundation was established as a non-profit foundation affiliated with the Linux Foundation Europe. Its aim is to promote open-source technologies that align with the strategic objectives of the European funding programme IPCEI-CIS (Important Project of Common European Interest in Cloud Infrastructure and Services).

A recent market report by the Synergy Research Group (July 2025) highlights the urgency of the situation: **European cloud providers hold only 15 percent of the market**, while U.S. hyperscalers dominate. NeoNephos addresses this challenge with the goal of reducing technological dependencies and strengthening digital sovereignty through open reference architectures and openly accessible software components.

The IPCEI-CIS budget of 3.5 billion euros is being invested in more than 110 projects involving over 100 companies from 12 EU Member States. In line with the EU Digital Strategy, the investment aims to strengthen Europe's digital sovereignty, reduce technological dependencies, promote interoperability, ensure sustainability, and enhance cybersecurity within a decentralised multi-provider cloud-edge continuum.

SAP plays a key role in developing standards and reference architectures within the IPCEI-CIS funding programme through its Apeiro Reference Architecture (ApeiroRA) project. SAP has contributed all Apeiro components to the NeoNephos Foundation as open source under the Apache 2.0 licence. This enables vendor-neutral governance and collaborative further development with other companies, in line with the principles of public funding.

Many of the projects contributed by SAP are already in productive use at SAP and among other partners, or are initiatives that SAP is currently developing and supporting within the NeoNephos Foundation for future deployment. This productive use ensures continued development well beyond the duration of the IPCEI-CIS programme.

The founding members of NeoNephos – including STACKIT, Deutsche Telekom, TNO, Cyberus Technology, Clyso, and 23 Technologies – aim to strengthen this ecosystem with their own complementary open-source projects. These contributions purposefully expand the reference architecture with additional functionalities and promote its adoption across the European market.

For example, Deutsche Telekom, together with other European telecommunications providers, is contributing the **Katalis** project to the foundation. This project aims to standardise access to telecommunications services and resources.

The idea of fostering openness and interoperability to build a sustainable and innovative cloud infrastructure in Europe is attracting growing interest. Following the foundation's establishment, x-cellent and Elastx have joined as members, and additional potential partners have expressed their interest.

Linux Foundation Europe provides NeoNephos with a neutral governance structure and access to an established open-source ecosystem. Through its close connection with the Cloud Native Computing Foundation (CNCF), the projects benefit from best practices and community standards without being directly managed by the CNCF.

The NeoNephos Foundation thus marks the emergence of a strategic, open technology ecosystem that serves as an operational pillar of the European cloud initiative – vendor-neutral, collaboratively developed, and geared toward long-term sovereignty.

Peter Giese
Director of SAP Open Source Programme Office

5.8 Expert Statement

Since 2021, the Open Source Monitor has tracked how the public sector perceives Open Source software. From an initial 32 percent positive response rate in 2021, this figure has risen to 52 percent in 2025. Meanwhile, the share of respondents with a negative view remained steady at 23 percent until 2023 but has almost halved over the past two years to 12 percent.

This development clearly reflects the ongoing debate about open technologies and the need to reduce technological dependencies on individual vendors in times of geopolitical change. Organisations such as ZenDiS have played a particularly positive role in shaping the perception of Open Source software within the public sector.

The World Is Changing

A look at the perceived advantages and disadvantages also clearly reflects these shifts in the IT landscape. The share of respondents who see Open Source software as a means of increasing digital sovereignty has more than doubled, from 4 percent (2023) to 9 percent (2025). At the same time, the share of those who see no advantage of Open Source over proprietary software has halved, from 16 percent to 9 percent. Nevertheless, the overall use of Open Source has remained relatively stable over the years — 64 percent, 59 percent, and 63 percent, respectively.

Open Source as an Economic Factor

This development in the public sector appears to be driven primarily by one factor: a shortage of qualified personnel (2023: 28 percent, 2025: 33 percent). It is often overlooked that the use of Open Source software offers potential specialists a modern, flexible, and future-oriented IT environment, making employers significantly more attractive. Is this therefore a classic circular dilemma?
To overcome entry barriers, Germany's strong Open Source ecosystem provides commercial solution providers and service companies. Open Source, in particular, enables liberal and entrepreneurial action through its development models and innovative strength, creating opportunities to involve and strengthen the domestic digital economy.

Thus, the use of Open Source is also a form of industrial policy, which in turn helps promote the development of skilled professionals in the region.

Economically Sustainable

Even though 17 percent of respondents view lower costs as a key advantage of using Open Source software, only 2 percent consider this from a long-term perspective in the context of economic sustainability. Yet from a strategic standpoint, the latter is crucial. Transitioning from existing solutions to Open Source usually involves migration costs, which may offset or even exceed the initial financial benefits from eliminating licence fees. Thus, the real cost advantage often emerges only over time.

The strategic value of Open Source, however — namely the ability to pursue a multi-vendor strategy — becomes apparent much earlier. Its openness, transparency, and interoperability prevent individual providers from imposing price controls, since other vendors can always offer a competitive alternative.

That said, we recommend following the »Procurement Criteria for the Sustainable Acquisition of Open Source Software« to actively support the OSS ecosystem and enable the long-term, environmentally responsible use of Open Source solutions.

All in all, the time has come in Germany to move beyond debate and into implementation — to make greater use of Open Source. As Goethe put it: »Knowing is not enough; we must apply. Willing is not enough; we must do.«

Torsten Hallmann
Consultant for Innovation and Open Source in the Public Sector

5.9 Automated Software Testing with the Badge System

Digital sovereignty has emerged as a central topic in public discourse. As a result, the range of Open Source solutions—a key enabler of sovereignty—is steadily increasing. However, openness of source code alone is not a mark of quality. The software must be secure, correctly licensed, and actively maintained. Until now, this has largely been ensured through individual assessments — a demanding and time-consuming process. To prevent public administrations from facing scalability issues, simple and efficient procedures are needed. The Badge Programme on openCode paves the way by making activity and integrity measurable, thereby facilitating the reuse of software.

openCode

Since January 2024, the Centre for Digital Sovereignty of Public Administration (ZenDiS) has managed the openCode platform, launched in 2022. Within just three years, openCode has become the main hub for Open Source projects in the public sector, with over 8,000 users working on 3,000 projects and around 200 new projects added each month. To promote reuse, the Badge Programme was introduced in early 2025.

Key Aspects: Maintenance, Use, Security

The Badge Programme automatically evaluates software projects against defined criteria and, based on the results, issues a detailed report and corresponding badges. In addition to assessing project activity, software licences, and reusability, the programme focuses on security and software quality.

Paradigm Shift: Moving Beyond Case-by-Case Reviews

openCode aims to bring about a paradigm shift in software evaluation. Traditionally, the suitability of software for use has been determined through case-by-case reviews based on local criteria — a time- and resource-intensive process that openCode leaves behind with its Badge Programme. Instead, the focus is on the reliability of the assessment process itself, meaning that the evaluation goes beyond code quality alone. Rather, the Badge System assesses verified use, project activity, and clear security characteristics. Compared with case-by-case reviews, this process is low-effort and largely applicable to all software products, as the evaluation is based on uniform criteria. This makes the assessment efficient, consistent, and automatable, while also enabling comparable results. Snapshots are a thing of the past.

Overall, the openCode Badge Programme enables a scalable assessment process that meets the demands of an increasing volume of software. It keeps pace with the innovation speed of Open Source technologies and, through a uniform and standardised procedure, fosters transparency and trust in software evaluation. By identifying risk factors early, it shifts security testing from reaction to prevention and can thus become a key building block for a digitally secure public sector landscape.

Learn more about the programme:
↗ https://badges.opencode.de/

Leonhard Kugler
Head of the Open-Source-Platform

6 Methodology

Survey Industry

On behalf of	Bitkom
Methodology	Computer Assisted Telephone Interview (CATI)
Statistical population	Companies in Germany with at least 20 employees
Target persons	Persons responsible for Open Source software within the company
Nominal sample size	n=1.152
Period of interviewing	From week 15 to week 21 of 2025
Weighting	Representative weighting of the dataset based on the current Business Register of the Federal Statistical Office of Germany
Statistical fault tolerance	+/- 3 percent

Survey Public Sector

On behalf of	Bitkom
Methodology	Computer Assisted Telephone Interview (CATI)
Statistical population	Organisations in Germany with at least 20 employees
Target persons	Persons responsible for Open Source software within the organisation; alternatively: persons responsible for software deployment or software development
Nominal sample size	n=103
Period of interviewing	From week 16 to week 22 of 2025
Weighting	No weighting
Statistical fault tolerance	-

Publisher
Bitkom e. V.
Albrechtstr. 10 | 10117 Berlin

Policy and Content Lead
Felix Ansmann

Head of Research
Bettina Lange

Editorial Team
Alissa Geffert
Lennart Glamann

DOI
10.64022/2025-open-source-monitor

The study examines the state of Open Source Software (OSS) in German companies and public administrations in 2025. It shows that 73 percent of companies and 63 percent of public authorities already use Open Source Software, mostly internally and to reduce costs. Security and functionality are the main selection criteria, yet many organisations still lack strategies, policies, and specialised staff. European regulations such as the Cyber Resilience Act (CRA) are driving the development of compliance structures, although only 14 percent of companies have established an Open Source Programme Office (OSPO) so far. Artificial intelligence is used cautiously: 29 percent employ AI-based code generators, while 56 percent perceive risks in doing so. A majority regard Open Source as a key to digital sovereignty — 73 percent of companies and 69 percent of public administrations see it as an effective means to reduce dependencies. The study is based on a representative survey of 1,152 companies with 20 or more employees and 103 public-sector organisations in Germany.

DOI
10.64022/2025-open-source-monitor

bitkom