LIONS Monitor

Resilience and Digital Sovereignty in Organizations

LIONS

funded by

dtec.bw

Funded by the European Union
NextGenerationEU

1st Edition, 2023

Publisher: Prof. Dr. Ulrike Lechner

The LIONS Monitor report is produced by the research project „LIONS – Ledger Innovation and Operation Network for Sovereignty“. The project is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr.
dtec.bw is funded by the European Union – NextGenerationEU.

LIONS Monitor research design:

Manfred Hofmeier, Maximilian Greiner, Isabelle Fries, Michael Grabatin, Isabelle Haunschild, Michael Hofmeier, Prof. Dr. Wolfgang Hommel, Prof. Dr. Ulrike Lechner, Prof. Dr. Friedrich Lohmann

Survey conducted by:
Maximilian Greiner, Manfred Hofmeier

Data analysis:
Manfred Hofmeier, Maximilian Greiner

Design: Artes Advertising GmbH, Munich

Printing and bookbinding:
Rechenzentrum der Universität der Bundeswehr München

ISBN: 978-3-943207-68-2
URN: urn:nbn:de:bvb:706-9077


LIONS

LIONS RESEARCH PROJECT

LEDGER INNOVATION AND OPERATION NETWORK FOR SOVEREIGNTY

The interdisciplinary research project LIONS establishes a research platform for the exploration of distributed ledger technology as a digitalization technology to increase resilience and digital sovereignty.

LIONS develops technical and analytical competencies, provides a laboratory environment with infrastructure for DLT of realistic size, and is building a community from the Bundeswehr, government agencies, and the private sector. Indicators and tools for analysis, design, and implementation of DLT-based information systems and their contribution to resilience and digital sovereignty are developed, taking into account three perspectives of analysis: (1) individual, (2) supply chain, and (3) society.

The project is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

To learn more about the project, visit the LIONS homepage at

https://www.unibw.de/lions

Universität der Bundeswehr München

Helmut Schmidt Universität
Universität der Bundeswehr Hamburg

Universität des Saarlandes

PREFACE

Dear Reader,

Digital sovereignty is an important goal on the political agenda. Being able to protect valuable assets as well as democratic values and the safety of the civil society is paramount in times of geopolitical changes and supply chain volatility. We live in times of multiple, interdependent, and mutually reinforcing crises. The digital infrastructure unfortunately plays a crucial role in fueling the crises, but also in overcoming them by providing trustworthy and timely information to respond adequately to crises, and with information systems to support all aspects from distribution of information to production, logistics of supplies, and strategic decision making.

Digital sovereignty is the capability to ensure the security and resilience of the digital realm. Society has been undertaking efforts to leverage IT security and resilience. It seems that it is now time to move forward, learn from the experiences in increasing security and resilience, change perspective from reacting to threats and changes to a more proactive and strategic stance: to ensure security and resilience in the future, and have the willpower to do so.

Digital sovereignty includes technical, organizational, and strategic dimensions, and it affects individuals, organizations, and public institutions of the state. It is a matter of awareness and willpower.

What does it take to build a digital infrastructure for more digital sovereignty? A digital infrastructure that is itself secure and trustworthy and that provides the services and products society relies upon. These questions motivate the Monitor study.

The Monitor study addresses resilience and digital sovereignty in companies and as the potential for new technologies such as blockchain, for increasing digital sovereignty.

Companies from various industries in German-speaking Europe (DACH) were surveyed for this study. The questionnaire was designed in spring 2022, involving all project partners of the LIONS research project. The online survey took place from June to September 2022. 152 respondents took part in the survey, 112 of which completed the questionnaire.

This study continues the Monitor series, which originated in the VeSiKi and NutriSafe projects, with the Monitor studies on information security of critical infrastructures and the NutriSafe Monitor on Resilience and Blockchain Technology in Food Production and Logistics.

This study is conducted by the LIONS research project. We would like to thank the participants in this survey, the multipliers who distributed the survey, and, above all, dtec.bw and the EU for funding the LIONS project.

Prof. Dr. Ulrike Lechner

LIONS project lead and und Professor at the University of the Bundeswehr in Munich

CONTENTS

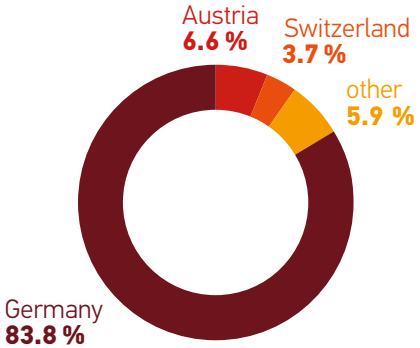
PREFACE
SURVEY PARTICIPANTS 08
DEMOGRAPHY 09
INDUSTRIES 10
SMES 11
RESILIENCE 12
THREATS 13
VULNERABILITY AND COPING CAPABILITIES 14
INSIDER THREATS 15
DIGITAL SOVEREIGNTY 16
ASPECTS OF DIGITAL SOVEREIGNTY 17
CURRENT SITUATION 18
CORPORATE GOALS 21
DIGITAL IDENTITIES 22
IDENTITY MANAGEMENT SYSTEMS 23
ELECTRONIC SIGNATURES 25
BLOCKCHAIN TECHNOLOGY 28
TECHNOLOGY ASSESSMENT 31
BLOCKCHAIN GOVERNANCE 33
CONCLUSION 36

SURVEY PARTICIPANTS

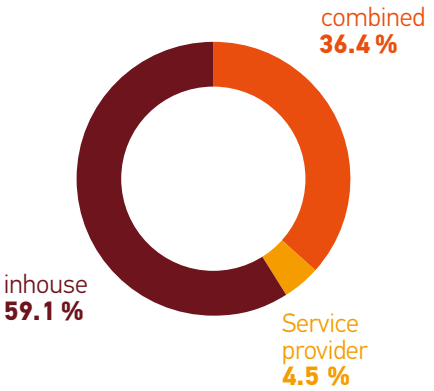
The participants in this study are decision-makers in companies. Individuals at management or similar decision-making levels contributed their views on security threats, digital sovereignty, and aspects of blockchain technology.

The online survey was conducted from June to September 2022 with 152 participants, 112 of whom completed the questionnaire. The participating organizations are primarily located in Germany, Austria and Switzerland.

In which country is your company located?



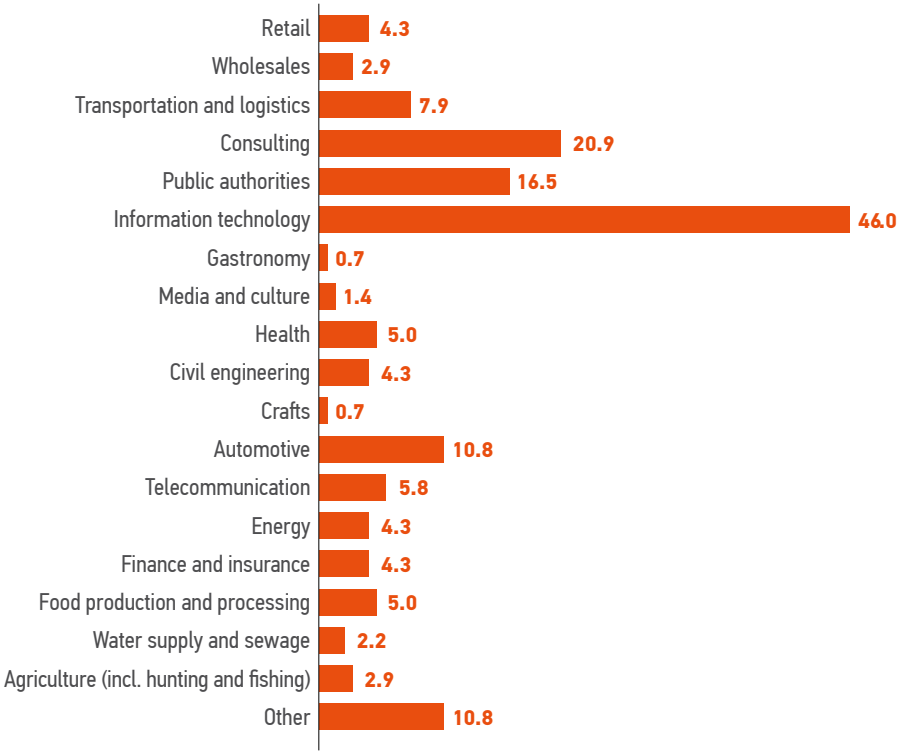
Who manages the IT in your company?



INDUSTRIES

The organizations participating in the study come from a wide range of industries, with information technology being the most represented sector, followed by consulting and public authorities.

Industries [%]



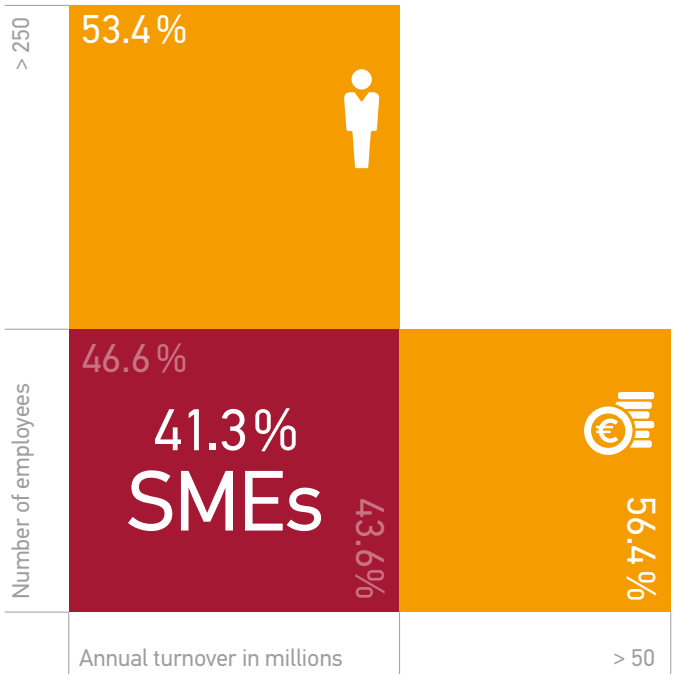
SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)

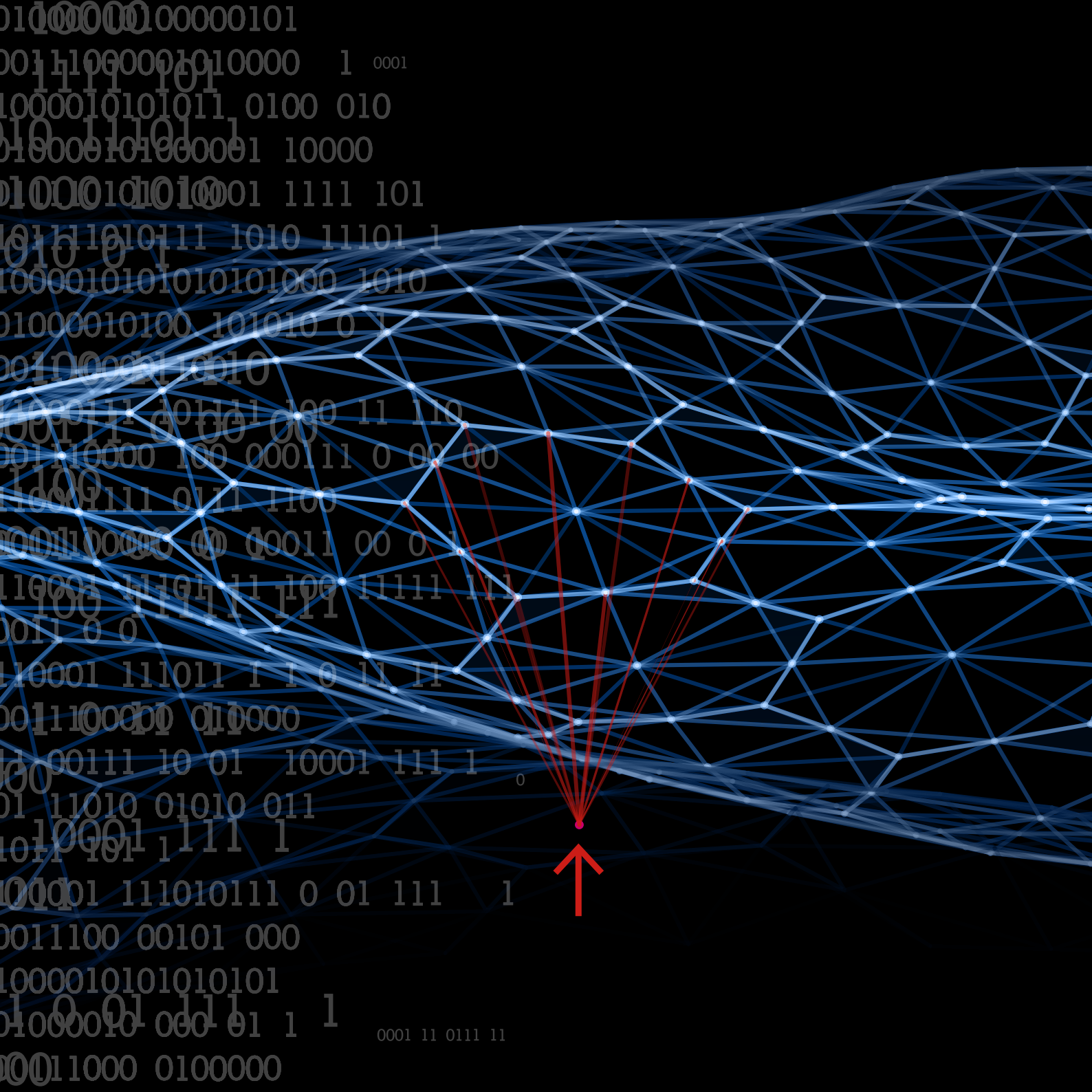
DEFINITION:

"The category of micro, small and medium-sized enterprises (SMEs) is made up of enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million[...]."

Extract of Article 2 of the Annex to Recommendation 2003/361/EC

Participants by number of employees and turnover





RESILIENCE

DEFINITION:

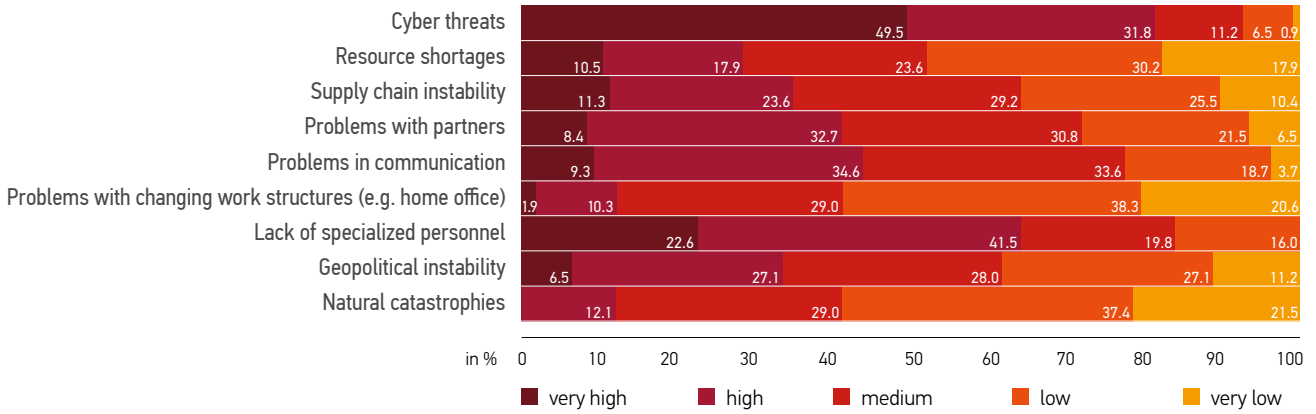
"Resilience is the ability of an individual, a household, a community, a country or a region to withstand, cope, adapt, and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without compromising long-term development."

European Commission (2016): Building Resilience – The EU's approach.

THREATS

Estimates of the threat situation particularly highlights cyber threats and lack of specialized personnel. The relevance of cyber threats is very high for almost half of the companies surveyed, and still high for 31.8% still view their importance as high.

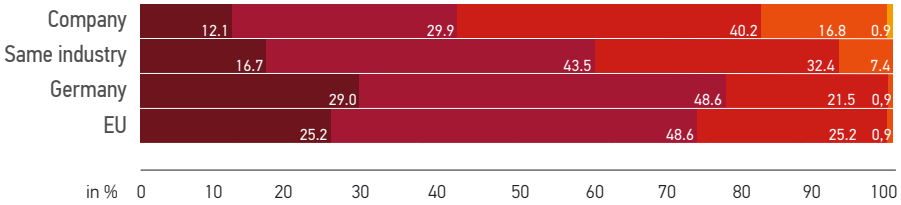
Threat relevance to companies



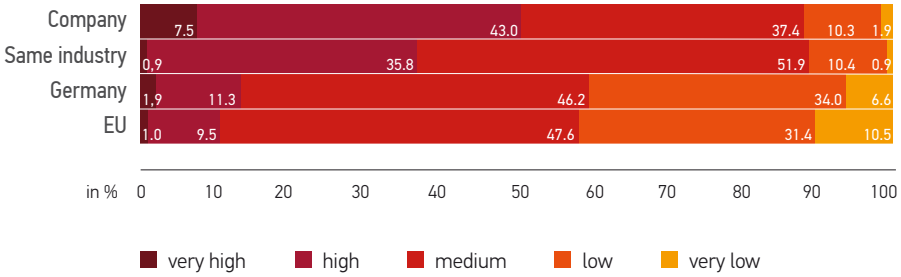
VULNERABILITY AND COPING CAPABILITIES

The estimates of vulnerability and coping capabilities show a clear optimism bias. Companies rate their vulnerability lower, and their coping capabilities higher, than those than that of industry in general. Overall, vulnerability is estimated as high.

Estimation of vulnerability



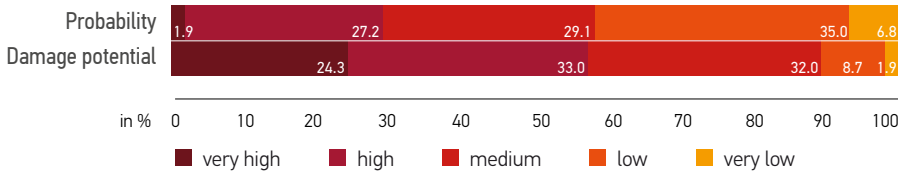
Estimation of coping capacities



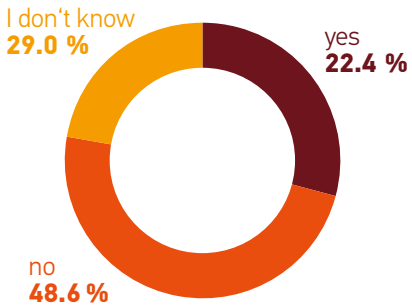
INSIDER THREATS

Security incidents by employees or individuals with privileged access (insider threats) are challenging to mitigate. Companies rate insider threats as rather unlikely, but at the same time they see high potential for damage. 22.4% responded that they had already been affected by insider threats, while 43.5% described these incidents as intentional.

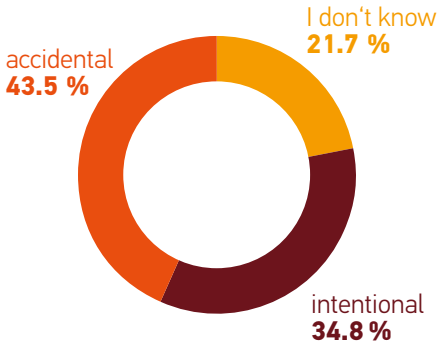
Estimation of insider threats



Occurrences of security incidents caused by employees or persons with privileged access



Nature of these incidents

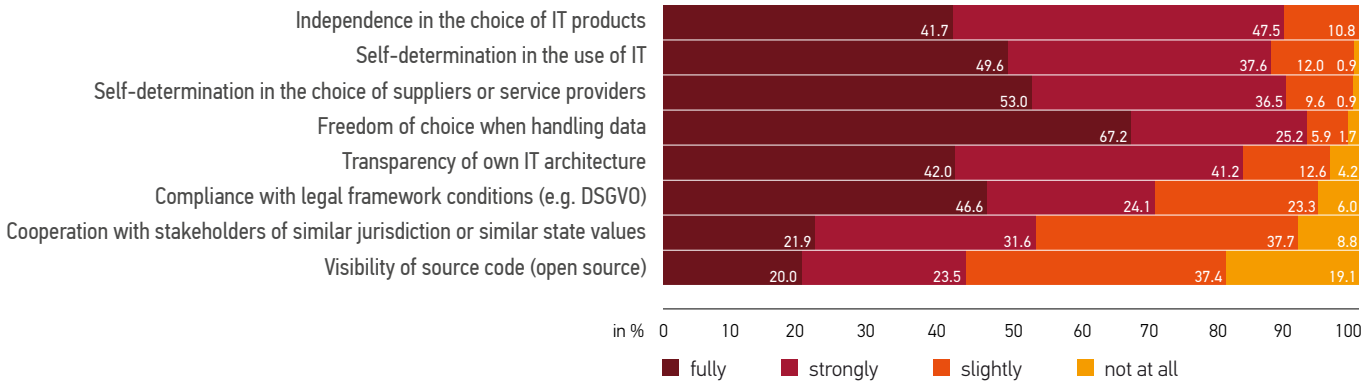


DIGITAL SOVEREIGNTY

ASPECTS OF DIGITAL SOVEREIGNTY

We queried the understanding of Digital Sovereignty. With the exception of source code visibility and cooperation with other stakeholders, the organizations strongly associated the aspects listed with the concept of digital sovereignty. The strongest associated aspect is freedom of choice when handling data.

To what extent do the following terms constitute digital sovereignty?

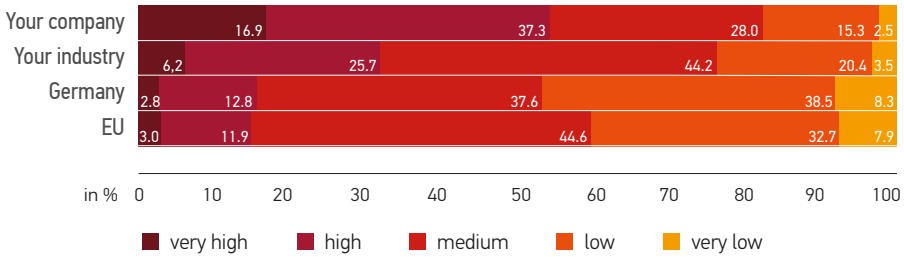


CURRENT SITUATION

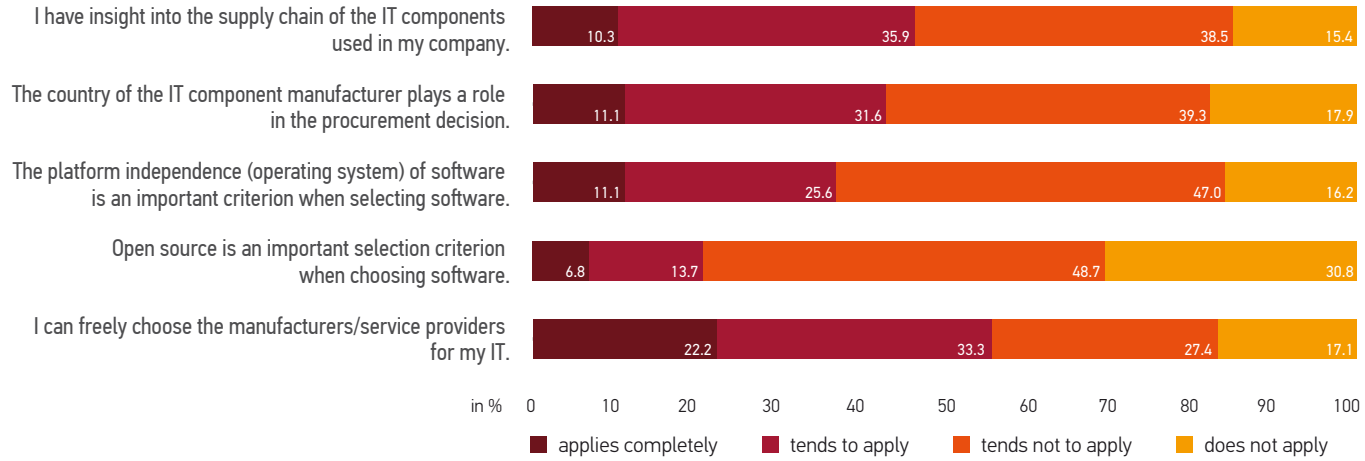
Freedom in the choice of providers is an essential component of an organization's digital sovereignty. According to the responses, it is easier to change providers when it comes to hardware and grid connection. In contrast, changing providers is difficult when it comes to operating systems and business applications.

Overall, companies generally rate their digital sovereignty higher than the digital sovereignty of their industry sector. Digital sovereignty is rated particularly low for the whole region (Germany and the EU).

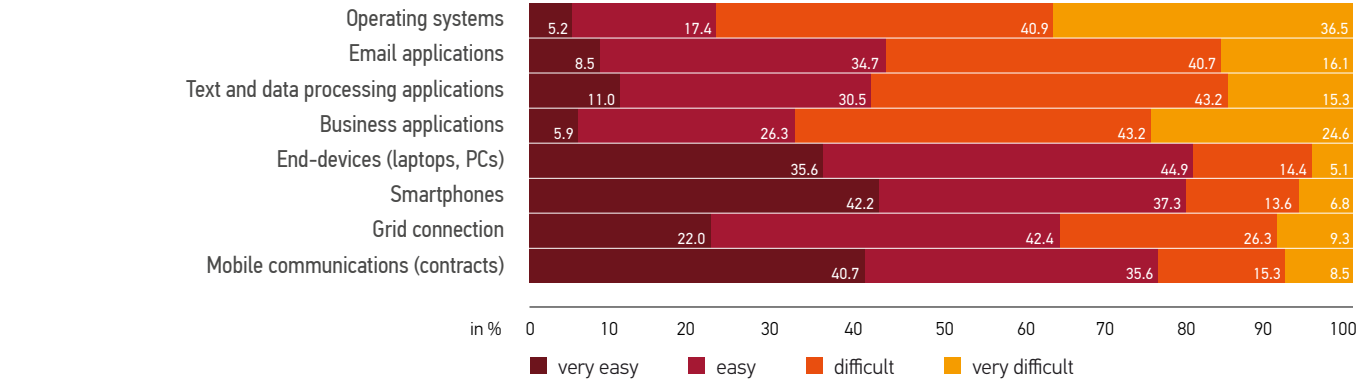
How do you generally rate digital sovereignty for...



To what extent do you agree with the following statements:

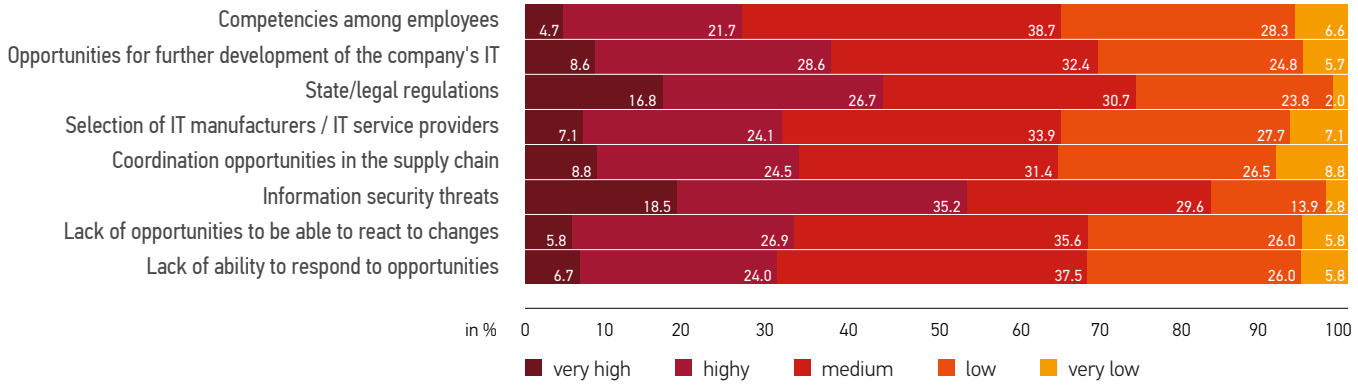


How easy would it be for your company to switch manufacturers/vendors of...?



According to the respondents, information security threats are the greatest limiting factor for an organization's digital sovereignty, followed by legal regulations. Overall, the majority of respondents assess each factor as at least a medium limiting factor. For instance, although competencies among employees are estimated as the least limiting factor, more than 65% still consider them to be at least medium limiting.

Where do you see limitations to your company's digital sovereignty?



CORPORATE GOALS

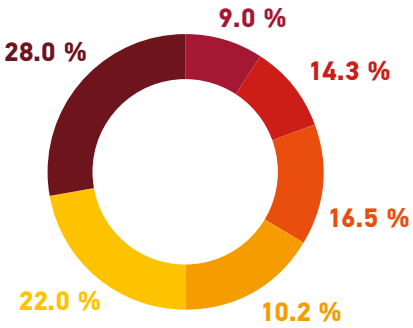
The respondents were asked to prioritize corporate goals. Most organizations assign the highest priority to the physical safety of their employees, followed by profitability. Only 9.1% assign the highest priority to information security within the organization.

The average rankings show that profitability and job security for employees take a back seat to the goals of physical safety and information security for employees and customers.

AVERAGE RANKING

1. Physical safety of employees
2. Information security within the company
3. Physical security of customers
4. Information security of customers
5. Job security of employees
6. Profitability

Goals ranked with highest priority

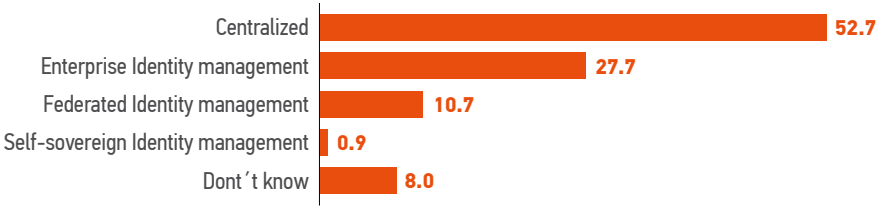


DIGITAL IDENTITIES

IDENTITY MANAGEMENT SYSTEMS

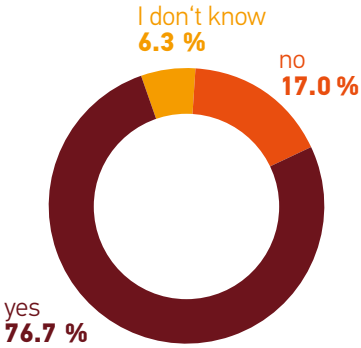
More than half of the organizations surveyed use centralized identity management systems (one set of credentials for one service), while about 27.7% use enterprise identity management systems such as Active Directory. Only 10.7% use federated systems such as SAML, Shibboleth, or OpenID. Self-sovereign identity management is rare in practice, accounting for less than 1%.

What types of digital identity management do you use? [%]

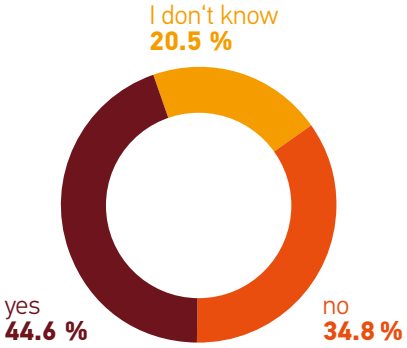


More than three-quarters of organizations use multi-factor or passwordless authentication methods. Most organizations would also be willing to use official eID systems such as electronic ID cards or citizen accounts for their identity management.

Do you use multi-factor or password-less authentication methods?



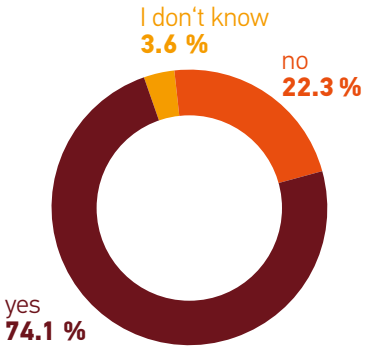
Can you imagine using official eID systems (e.g. electronic ID card, ELSTER certificate, citizen accounts) for identity management?



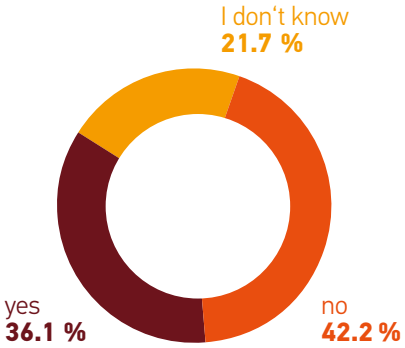
ELECTRONIC SIGNATURES

Electronic signatures are an enabling factor in the digital world. Most organizations use methods of signing emails or documents electronically, but in most cases the systems are not used consistently.

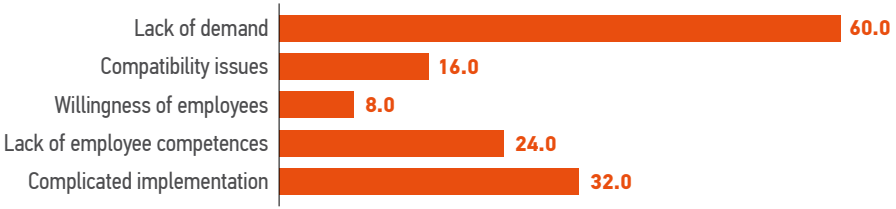
Does your company use methods of electronically signing emails and/or documents?



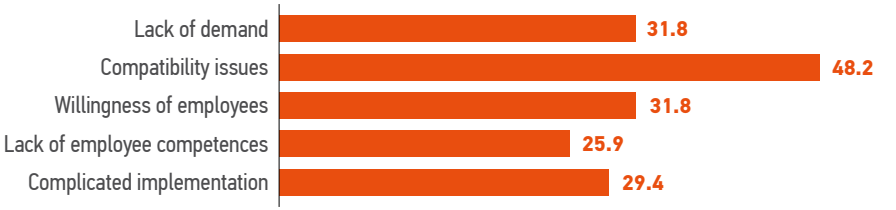
Is the system used consistently?



What were the reasons for not introducing electronic signatures? [%]

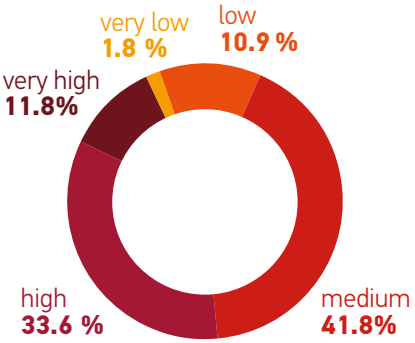


What are the biggest challenges in electronic signing? [%]

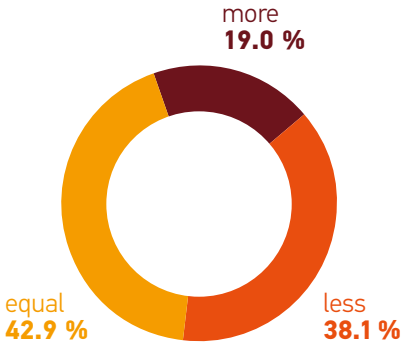


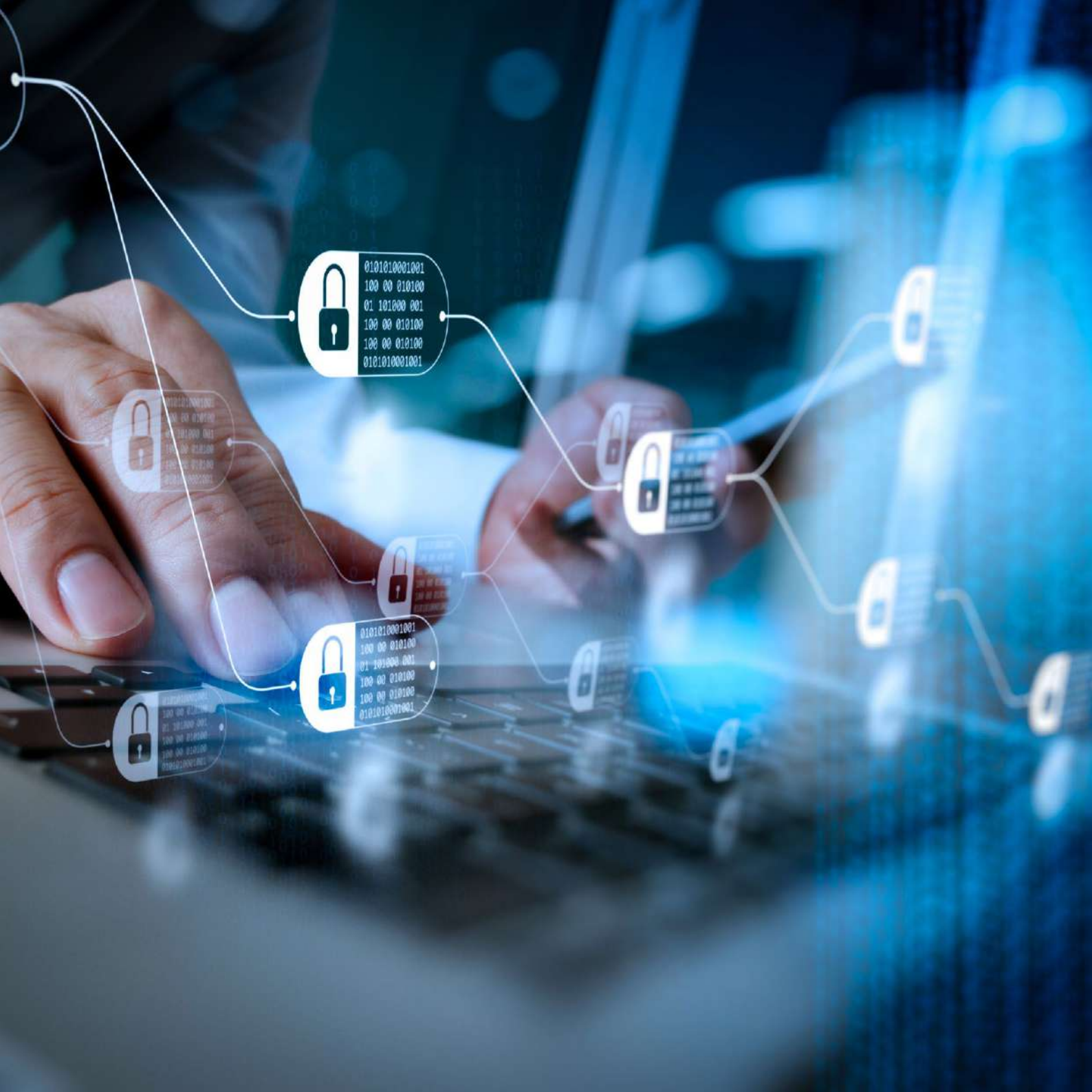
The most frequent reason given by organizations for not introducing electronic signatures was lack of demand, followed by complicated implementation. Compatibility issues are seen as a major obstacle to electronic signing. However, employee willingness and difficulties in implementation as well as employee competencies of employees are also relevant.

How high do you estimate the acceptance of systems for the electronic signature of e-mails and/or documents among employees?



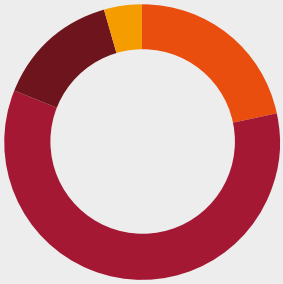
How do electronic signatures change the amount of effort required for use?




0101010001001
100 00 010100
01 101000 001
100 00 010100
100 00 010100
0101010001001

BLOCKCHAIN TECHNOLOGY

How familiar are you with the topic of blockchain?



4.5 %
I don't know anything about blockchain.

21.6 %
I have already heard about blockchain, but have not dealt with it yet

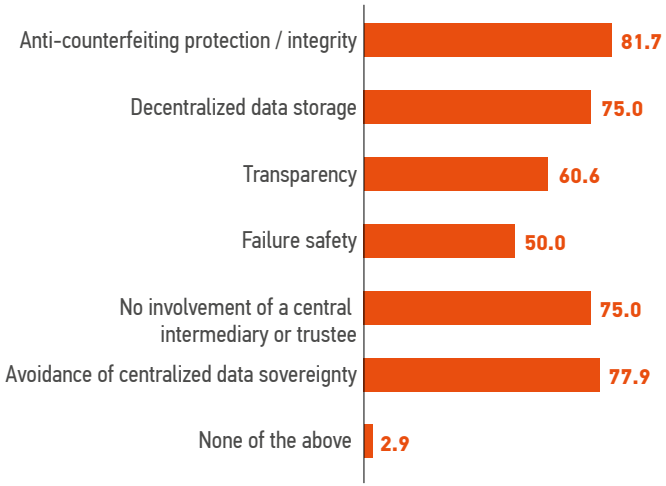
59.5 %
I have already heard about blockchain and have already dealt with it.

14.4 %
I have already used blockchain technology

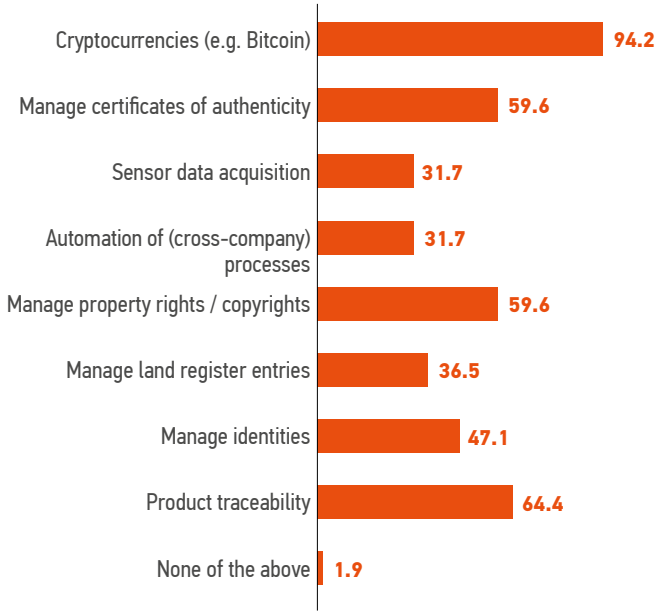
95% of the respondents are familiar with the term "blockchain." These survey participants were asked further questions about blockchain technology. The results of further blockchain-specific questions therefore relate to this subset of respondents.

The general characteristics and fields of blockchain application are largely known to the respondents. The most frequently selected characteristics are anti-counterfeiting protection/integrity (81.7%), avoidance of centralized data sovereignty (77.9%), as well as decentralized data storage and no involvement of a central intermediary or trustee (both 75.0%). Regarding application fields, most respondents are familiar with cryptocurrencies (94.2%).

Which of the following possible characteristics of blockchain are you already familiar with? [%]



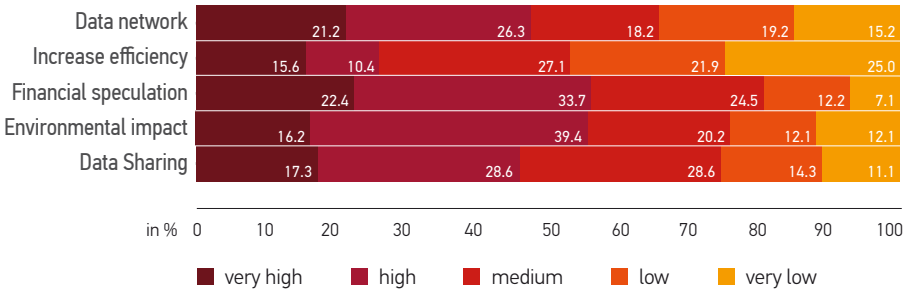
Which of the following application fields of blockchain are you already familiar with? [%]



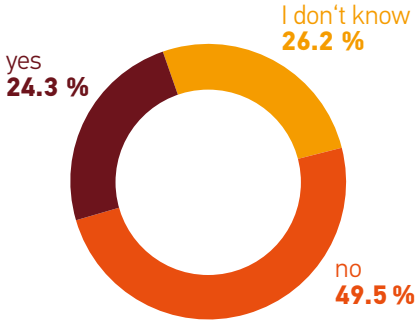
TECHNOLOGY ASSESSMENT

Most respondents associate blockchain with financial speculation and environmental impact. Legal concerns could play a significant role when blockchains are implemented within a company. However, around half of those surveyed have no legal concerns about adopting the technology.

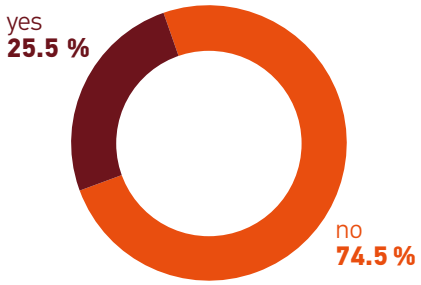
To what extent do you associate the following terms with blockchain technology?



Do you have legal concerns about using blockchain in your business?



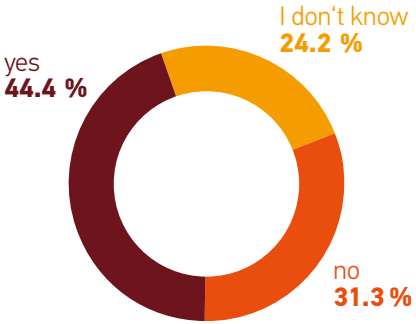
Have you already implemented DLT or blockchain-based projects in your company?



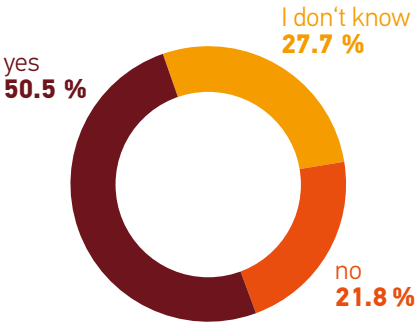
In response to the question of whether there are any specific areas of application for blockchain technology within their company, 44.4% of the respondents see possibilities for blockchain application.

When blockchain is implemented, collaboration with other companies within a consortium plays a significant role. 50.5 % of the respondents could imagine participating within a consortium even if competing companies are involved.

Are there any specific areas of application for blockchain applications in your company?



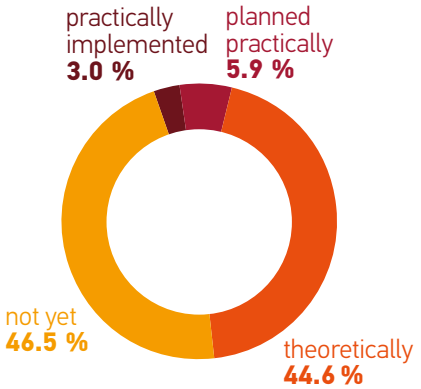
Could you imagine participating in a blockchain consortium that includes competing companies?



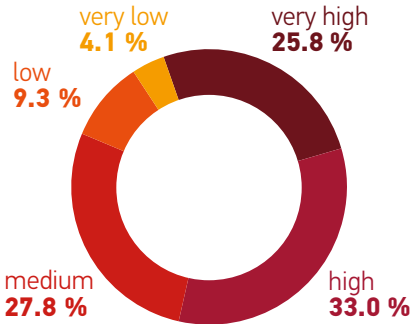
BLOCKCHAIN GOVERNANCE

In terms of control and regulations of blockchains, 44.6% of respondents have already addressed the topic theoretically, and about 9% have planned or implemented it practically. 58.8% judge the relevance of governance as high to very high when it comes to successfully integrating technology into the company.

To what extent have you already dealt with the control and regulation of a blockchain?

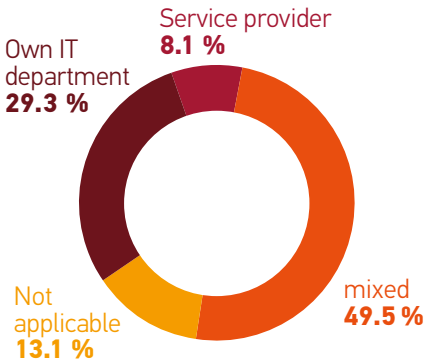


How high do you judge the relevance of organizational regulation and control (governance) in the introduction of blockchain technology?

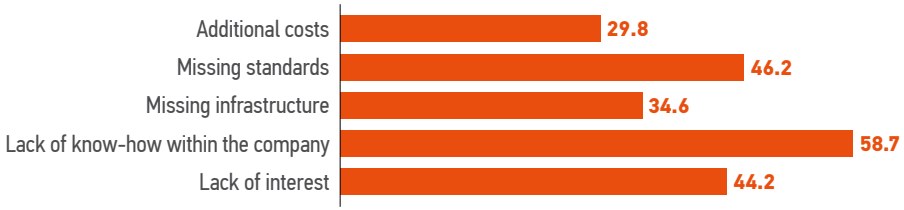


With respect to planning blockchain governance within their own company or using an external service provider, around half of the respondents opted for a mix of both. Lack of know-how within the company is seen as the most significant challenge (58.7%) to integrating blockchains into their business models.

Would you plan the blockchain governance within your own IT department or through external service providers?



What challenges do you see in integrating blockchain into your business?

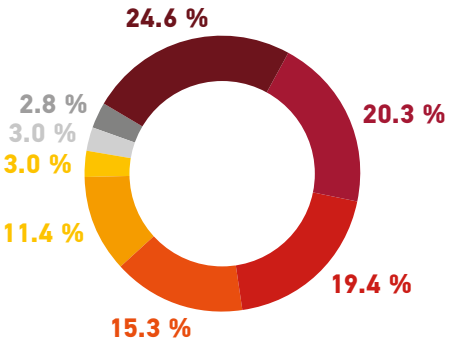


During implementation and operation of blockchain solutions, various decisions have to be addressed in advance. The most frequently prioritized factors consider who should participate in the consortium, how the technology should be integrated into the infrastructure, and what adjustments to the IT strategy are required.

AVERAGE RANKING

1. **Who may be part of the consortium?**
2. **How should the technology integrate into the current infrastructure?**
3. **Which adjustments to the IT strategy are required?**
4. **How is audit-proof storage of critical data handled? (e.g. storage for tax office)**
5. **Who decides on further development of the blockchain?**
6. **Who may resolve conflicts in the consortium?**
7. **How are conflicts in the consortium resolved?**
8. **Who resolves technical problems in the blockchain?**

Decisions ranked with highest priority



CONCLUSION

The digital transformation is leading to a change in information technology, which makes the consideration of digital sovereignty and resilience indispensable. In addition, the current geopolitical situation underlines the relevance of resilience and digital sovereignty, in particular for organizations.

Regarding this study's results, organizations' vulnerability is relatively high. Cyber threats and a lack of specialized personnel are the threats of most relevance to respondents, a combination which might require attention.

Digital sovereignty is a field of growing importance that involves a societal, political, and enterprise-related perspective. Most organizations consider themselves relatively sovereign. Dependence on vendors is of particular importance here, since hardware vendors are usually easy to replace and software vendors rather difficult.

Given the critical dependency on disruptive technologies such as the Internet of Things, big data, virtual reality, 5G, artificial intelligence (AI), and blockchain, geopolitical issues and aspects such as resilience, independence, self-determination, trust, and credibility are becoming more meaningful. But such technologies can also offer a chance to address these aspects.

Blockchain offers many areas of potential for business and government. However, the majority are familiar with the term "blockchain," although few are already working on blockchain-based projects. This is also associated with know-how from an organizational perspective; only very few of the respondents have dealt with the control and regulation of the technology.

Overall, this study shows that organizations' self-assessments of resilience and digital sovereignty are relatively good. However, there is still plenty of room for improvement here.

ACKNOWLEDGEMENTS

This work originates from the LIONS research project. LIONS is funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr, which we gratefully acknowledge. dtec.bw is funded by the European Union – NextGenerationEU. We also thank the study participants and the disseminators for spreading the survey.

QUESTION OVERVIEW

Question	Sample Size
How many employees does your company have?	n=133
What was your company's turnover last year?	n=133
Who manages and supports IT in your company?	n=132
In which country is your company located?	n=136
In which industries/sectors is your company active?	n=139
How easy would it be for your company to switch manufacturers/vendors at...? ▸ Operating systems ▸ Email applications ▸ Text and data processing applications ▸ Specialist applications ▸ End devices (laptops, PCs) ▸ Smartphones ▸ Grid connection ▸ Mobile communications (contracts)	n = 57
Have you already implemented DLT or blockchain-based projects in your company?	n=102
What types of digital identity management do you use?	n=112
Do you use multi-factor (MFA/2FA) or password-less (e.g. FIDO 2) authentication methods?	n=112
▸ Can you imagine using official eID systems (e.g. electronic ID card, ELSTER certificate, citizen accounts) for identity management?	n=112
▸ Does your company use methods to electronically sign/sign emails and/or documents?	n=84
How does this change the effort required for use?	n=84
Is the system used consistently?	n=83
How high do you estimate the acceptance of systems for the electronic signature of e-mails and/or documents among employees?	n=110
Please rank the following business goals according to priority in your organization. ▸ Physical security of employees ▸ Workplace security of the employees ▸ Physical security of customers ▸ Information security of customers ▸ Profitability of the company ▸ Information security in the company	n=110

Question	Sample Size
To what extent do you agree with the following statements: ▸ I have insight into the supply chain of the IT components used in my company. ▸ The country of the IT component manufacturer plays a role in the procurement decision. ▸ The platform independence (operating system) of software is an important criterion when selecting software. ▸ Open source is an important selection criterion when choosing software. ▸ I can freely choose the manufacturers/service providers for my IT.	n=117
What were the reasons for not introducing electronic signatures?	n=25
What are the biggest hurdles in electronic signing?	n=85
How high do you generally rate Digital Sovereignty for... ▸ Your company ▸ Your industry ▸ Germany ▸ EU	n=118
Where do you see limitations to your company's Digital Sovereignty?	n=106
Which of the following possible characteristics of a blockchain are you already familiar with? ▸ Anti-counterfeiting / integrity ▸ Decentralized storage of data ▸ Transparency ▸ Failure safety ▸ No involvement of a central intermediary or trustee ▸ Avoidance of central data sovereignty ▸ None of the above	n=104
Which of the following application fields of a blockchain are you already aware of? ▸ Cryptocurrencies (e.g. Bitcoin) ▸ Manage certificates of authenticity ▸ Sensor data acquisition ▸ Automation of (cross-company) processes ▸ Manage property rights / copyrights ▸ Manage land register entries ▸ Manage identities ▸ Product traceability ▸ None of the above	n=104

Question	Sample Size
Do you have legal concerns about using blockchains in your business?	n=103
▸ How much do you associate the following terms with blockchain technology? ▸ Data network ▸ Efficiency increase ▸ Financial speculation ▸ Environmental impact ▸ Data sharing	n=99
How strong is the focus on the blockchain topic within your medium- to long-term corporate strategy?	n=99
Are there any specific areas of application for blockchain applications in your company?	n=99
How can blockchain technology help you achieve your business goals?	n=99
To what extent have you already dealt with the control and regulation of a blockchain?	n=101
Are there any specific areas of application for blockchain applications in your company?	n=99
What hurdles do you see in incorporating a blockchain into your business?	n=104
Would you plan for blockchain governance within your own IT department or through external service providers?	n=99
Could you imagine participating in a blockchain consortium that includes competing companies?	n=101
How high would you rate the relevance of organizational regulation and control (governance) in the introduction of blockchain technology?	n=97
In the operation of a blockchain, various decisions have to be made and clarified in advance. How would you prioritize the following issues? ▸ Who may participate in the consortium? ▸ How are conflicts resolved in the consortium? ▸ Who is allowed to resolve the conflicts? ▸ Who decides on the further development of the blockchain (e.g. consensus protocol)? ▸ How should the technology be adapted into the current IT infrastructure? ▸ What adjustments need to be made to the IT strategy? ▸ Who solves technical problems in the blockchain? ▸ How is audit-proof storage of critical data handled? (e.g. storage for the tax office)	n=74
Have there already been security incidents in your company caused by employees or persons with privileged access or entry? (e.g. external service providers)	n=107
What was the nature of these incidents?	n=23

Question	Sample Size
How high do you estimate... ▸ the likelihood of security incidents by employees or individuals with privileged access or entry? ▸ the potential for damage in the event of security incidents by employees or persons with privileged access or entry?	n=103
How high do you assess the vulnerability (e.g., due to crisis events, cyber attacks) of... ▸ Your company ▸ Your industry ▸ Germany ▸ EU	n=108
How high do you rate the ability to manage disruptive events (e.g., crises, cyber incidents) of... ▸ Your company ▸ Your industry ▸ Germany ▸ EU	n=107
To what extent do the following threats matter to your business?: ▸ Cyber threats ▸ Lack of raw materials ▸ Supply chain instabilities ▸ Partner issues ▸ Communication issues ▸ Problems with changing work structures (home office, etc.) ▸ Lack of specialized personnel ▸ Geopolitical instability ▸ Natural disasters	n=107

LITERATURE

European Commission (2016): Building Resilience - The EU's approach.

NutriSafe (2020): NutriSafe Monitor – Resilienz und Blockchain-Technologie in Lebensmittelproduktion und -logistik. https://nutrisafe.de/monitor.

VeSiKi (2017): Monitor IT-Sicherheit Kritischer Infrastrukturen. https://monitor.itskritis.de.

VeSiKi (2018): Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen. https://monitor.itskritis.de.

More information on the LIONS project is available on the website

https://www.unibw.de/lions

or on Twitter

https://twitter.com/LIONS_Project

A digital version of this report is available at

https://www.unibw.de/lions/monitor

This report is created by LIONS

Institute for Protection and Dependability
Department of Computer Science
Universität der Bundeswehr München

Prof. Dr. Ulrike Lechner
Werner-Heisenberg-Weg 39
85577 Neubiberg
Germany

Tel: +49 89 6004-2504

LIONS Monitor contact:
Manfred Hofmeier
Tel: +49 89 6004-3392
Email: manfred.hofmeier@unibw.de

LIONS