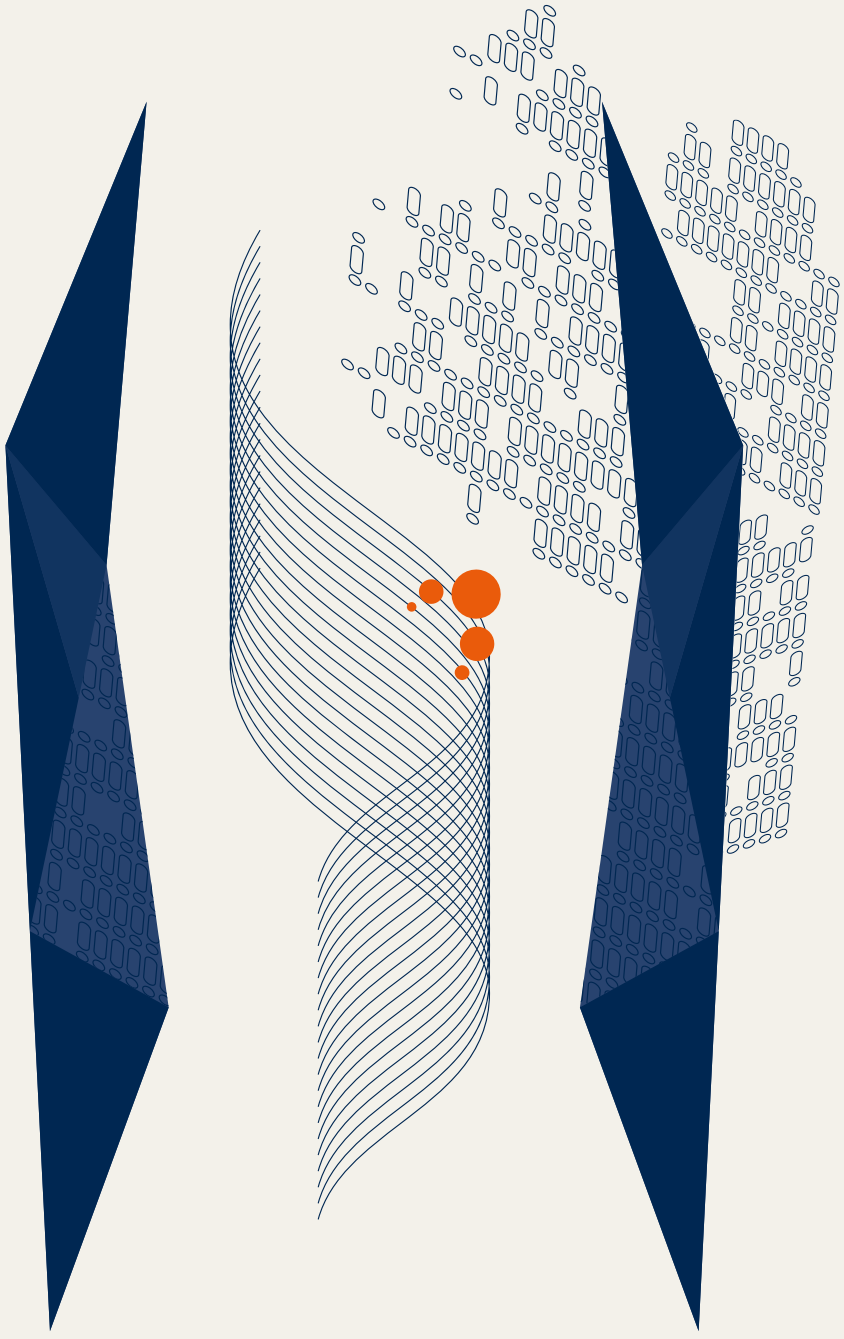
Digitalisation and Compliance

Compliance Study 2021



In cooperation with:

Technische Universität München

Noerr

Preface

Although the *Bundestag*, the national parliament of the Federal Republic of Germany has now quashed the federal cabinet's draft bill (of the German Federal Ministry of Justice and Consumer Protection) for a law on "combating corporate crime", which had previously been waved through in 2020. The requirements to be met by business owners and compliance officers have nevertheless increased in recent months. Countless new laws and regulations have come into force at federal and European level and mean additional work for business executives. In the light of these developments, we are pleased to present our latest compliance study.

To put together this study, we once again conducted 300 interviews with managers from private-sector companies at the first and second decision-making levels and have summarised the findings for you in a manageable format. We trust that you will come across many interesting details when reading our study.

If you have any comments or would like to provide ideas and impulses for future studies, please do not hesitate to contact us. We look forward to receiving your feedback.

Professor Peter Bräutigam

Dr Julia Sophia Habbe

Professor Dirk Heckmann

Inhalt

Executive summary

Advancing digitalisation is presenting companies with a range of organisational challenges. This also applies to compliance, as new technologies are creating new compliance risks. It is up to the management to identify these risks and allocate responsibility for tackling them correctly within the organisation.

Yet the companies surveyed by us often see themselves as inadequately positioned as far as their digital set-up is concerned, even though the need for action seems to be especially urgent in the area of compliance. This is even truer for smaller companies, which regard their level of digitalisation as being lower than that of large organisations. On top of this, many organisations lack dedicated positions for monitoring digital compliance risks and the technical expertise this calls for.

While the vast majority of companies taking part in our study have taken action and looked into the legal risks associated with digitalisation, many of them have nevertheless experienced such risks first-hand. The legal risks that can arise when using new technologies are especially underestimated. When it comes to using compliance tools there often appears to be a lack of risk awareness.

On the one hand, the Covid-19 pandemic has given the use of digital work equipment an extra boost. The study shows that many companies consider their use to be a concern from a compliance point of view. On the other hand, the coronavirus outbreak does not appear to have led to any compliance policies being relaxed.

Organising digital compliance is a management task

It is the management's job to identify digital compliance risks and to allocate responsibility for dealing with them correctly within the company. The responses to our survey suggest, however, that only a few companies see their management as being responsible for digital risks.

There is an urgent need for action. Management must take appropriate measures to create and maintain the company's cybersecurity. Yet, according to the feedback received from the companies we surveyed, responsibility for digital infrastructure is often misjudged.

Many companies see themselves as having an inadequate digital set-up

Companies must have appropriate structures and processes in place to cope with the growing challenges of digitalisation. The majority of the managers interviewed see a need to catch up in this area and assess the digital readiness of their own company as being low to medium. Of the various corporate divisions, the compliance department performs poorest. Only one-third sees a high to very high level of digital readiness.

As dedicated positions for digital compliance risks are often lacking, and if they are in existence, technical expertise is underrepresented

This self-assessment of limited digital readiness is also reflected in organisational terms. Many companies have not established dedicated positions for dealing with digital compliance risks, with around **70%** saying that they do not have such positions in place.

The professional background of compliance officers also shows a mixed picture. This may admittedly be due to the fact that there is no reliable data available on the expertise required in this area. It is still the case that the majority of those entrusted with compliance tasks have a business management or law degree, while dedicated technical expertise appears underrepresented. Only slightly more than a quarter of compliance officers have a technical or IT background.

Around half of the companies surveyed have already experienced digital legal risks first-hand

Digital legal risks have increased in recent years. This finding is in line with the feedback received from the decision-makers questioned.

While the vast majority of companies taking part in the study have looked into the legal risks associated with digitalisation (e.g. by identifying their risk exposure in SWOT analyses), around half of the study participants have already had first-hand experience of these legal risks, such as in the form of hacking attacks or data privacy breaches.

The legal risks posed by newer technologies are especially underestimated

It is notable that companies frequently underestimate the legal risks posed by newer technologies. In the area of cloud computing, artificial intelligence and big data analysis, about half of the companies surveyed rate the legal risks as being low. This perception, however, is at odds with the constantly growing regulatory requirements, such as those placed on data protection or IT security.

In its Schrems II ruling of 16 July 2020, the European Court of Justice declared the "EU-US Privacy Shield" invalid and thus made legally compliant data transfers to the USA considerably more difficult. Yet, many cloud services are provided or hosted by US providers. Since supervisory authorities focus on ensuring that the transfer of personal data to third countries is data-compliant, there is a risk of high fines and claims for damages by third parties affected by breaches.

Requirements under IT security law are also getting tougher. With the "German IT Security Act 2.0" passed on 23 April 2021, the Bundestag, as the national parliament of the Federal Republic of Germany, abandoned its sector-specific approach and extended the obligations under IT security law to include "companies of special public interest". In addition, from 1 May 2023 onwards "critical infrastructure operators" must use "attack detection systems". Infringements can result in fines of up to €20 million.

Regulatory requirements are also increasing with respect to artificial intelligence and big data analysis. On 21 April 2021, the European Commission presented a draft "AI Regulation". The proposal follows a risk-based approach and in some cases places strict requirements on the technical structures and use of AI. If a company infringes the prohibitions, the draft regulation provides for fines of up to €30 million or 6% of its worldwide annual turnover.

While information and process tools are widespread, risk awareness remains low

According to the feedback received, information and process tools make up the majority of existing compliance tools. These include analysis and monitoring tools as well as e-learning platforms, for example. About a third of the companies use tools developed by them in-house.

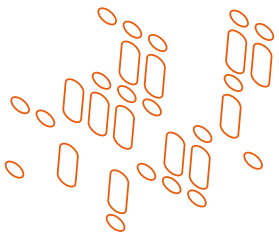
However, the majority of respondents do not seem to be aware of the fact that the use of such tools can itself involve compliance risks. Only **32%** of the companies based abroad and **16%** of those based in Germany see risks in the use of compliance tools.

Use of digital tools is widespread despite compliance concerns

Even if companies tend to generally underestimate the legal risks brought by newer technologies, there is at least a certain awareness of compliance risks with regard to the digital work tools they use. For example, about a fifth of the decision-makers questioned state that video conferencing, SharePoint systems or collaboration tools involve high to very high compliance and data protection risks. Nevertheless, digital tools have become an integral part of today's working life. The Covid-19 pandemic has served to drive up their widespread use even further.

Hardly any relaxation of compliance policies during the pandemic

Few companies appear to have eased their compliance policies during the Covid-19 pandemic. Around two-thirds of the respondents said that compliance policies in their industry had neither been suspended nor relaxed. This may come as a surprise, as many companies have had to find flexible solutions to counter the effects of Covid, for example through working from home. It is therefore likely that internal rules have been relaxed more often than the answers suggest.



1. Organising compliance in a company's digital environment

Corporate compliance is changing. It is facing new challenges, especially due to digital technologies and the increasing digitalisation of business processes.

New technologies change employees' everyday work and force companies to recognise, assess and manage the digital risks involved. At the same time, many businesses have greater exposure to digital risks; this is apparent, for example, in the increasing threat of cyberattacks. To properly meet digital challenges, companies must take adequate preventive and reactive compliance measures, with management being responsible for organising and monitoring these measures.

Many of the decision-makers interviewed do not consider their companies adequately positioned as far as their digital set-up is concerned. In addition, there often seems to be a lack of dedicated positions for people working on digital compliance risks, and the necessary technical expertise appears to be underrepresented.

1.1 Digital compliance as a management task

Organising digital compliance is a management task.

Management is responsible for organising and maintaining its company's digital compliance using suitable measures. For example, management board members of a German stock corporation must exercise the care of a diligent and prudent manager (section 93(1) sentence 1 German Stock Corporation Act (*Aktiengesetz* – AktG). Managing directors of German limited liability companies (*Gesellschaft mit beschränkter Haftung* – GmbH) have the same responsibility (section 43(1) German Limited Liability Companies Act – GmbH-Gesetz). It is up to the management to establish the company's organisational compliance structures, while also adapting them to factors including the nature, size, business and financial situation of the company as well as its management structure. Although delegating responsibilities is generally possible and often sensible, the buck ultimately stops with the management, who should at least be in a position to use reports on relevant topics to keep up to date on the situation in their company.

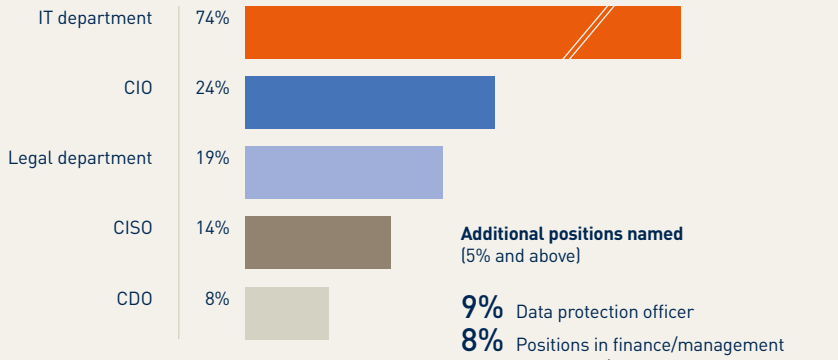
In the event of a real threat such as a cyberattack, the management's duty to monitor grows. If a company suspects that its systems may have been infiltrated, it must immediately take all steps to limit the risk of damage to the company. Any weaknesses in the compliance system that have come to light as a result have to be remedied.

There were wide variations among those interviewed as to who is responsible for digital risks.[1] Where no dedicated position for digital compliance risks exists, in the overwhelming majority of cases (74%) the **IT department** is assigned the responsibility for digital risks. In companies headquartered in Germany, this applies even more often than in companies whose parent companies are headquartered in other countries (75% as opposed to 67%). The same is true for smaller companies with fewer than 1,000 employees. In almost four out of five such companies, the IT department is involved.

[1] Note on methodology: As the percentage values shown are rounded to whole numbers, they may not add up to 100%. For the same reason, categories combined by addition (for example, "top two values" such as "very satisfied" and "somewhat satisfied") may differ from the sum of the individual categories shown. For questions where it is possible to give several answers, the sum of the answers may exceed 100%. The percentages in the text refer to the results of the survey. Particularly important results of the survey are also shown graphically.

Company positions with responsibility for digital risks

Even if the responsibilities are sometimes assigned very differently, the IT department is usually involved



Additional positions named
(5% and above)

- **9%** Data protection officer
- **8%** Positions in finance/management accounting/financial planning
- **6%** Management, management board
- **5%** Positions in the compliance department

Question: To which positions in your organisation is the responsibility for digital risks assigned?

Basis: Companies without dedicated positions for digital compliance risks; more than one answer possible; figures in per cent

Source: Kantar – Quantitative Survey 2021 on behalf of Noerr

The legal department plays an important role in the area of digital risks, notably in larger companies and in companies whose parent company is headquartered outside Germany. While the legal department is responsible for digital risks in more than one in four of the companies surveyed with at least 1,000 employees (27%) or with headquarters abroad (28%), only **12%** of the smaller companies and only **17%** of those headquartered in Germany involve the legal department in this issue.

The picture also varies greatly when it comes to dedicated positions for digital compliance risks. In addition to the positions mentioned above, the decision-makers interviewed most frequently name the **Chief Information Officer** (CIO).

In fourth place comes the **Chief Information Security Officer** (CISO), who has overall responsibility for information security in the company. In **14%** of the companies surveyed that did not have a dedicated digital compliance position, the responsibility for digital risks is placed here. Large companies have this position twice as often as smaller ones with fewer than 1,000 employees (18% as opposed to 9%).

A **Chief Digital Officer** (CDO) was cited by less than **10%** of the respondents. Other positions, such as **data protection officer**, positions in finance, management accounting and financial planning or in the **compliance department**, are also mentioned relatively rarely.

1.2 How companies rate their own digital readiness

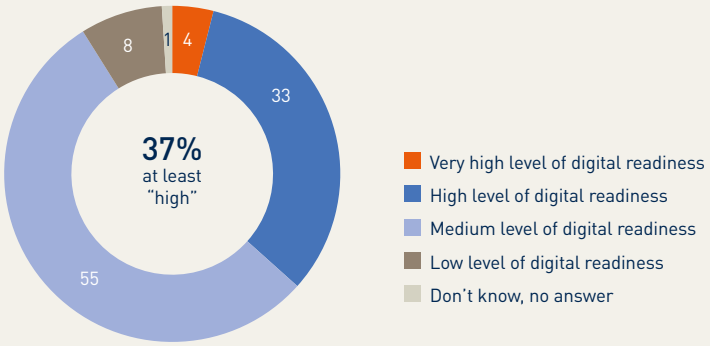
Many companies do not see themselves as having adequate digital structures in place.

Digital readiness is an important indicator of the extent to which companies are adjusting to digital progress and how exposed to digital risks they consider themselves.

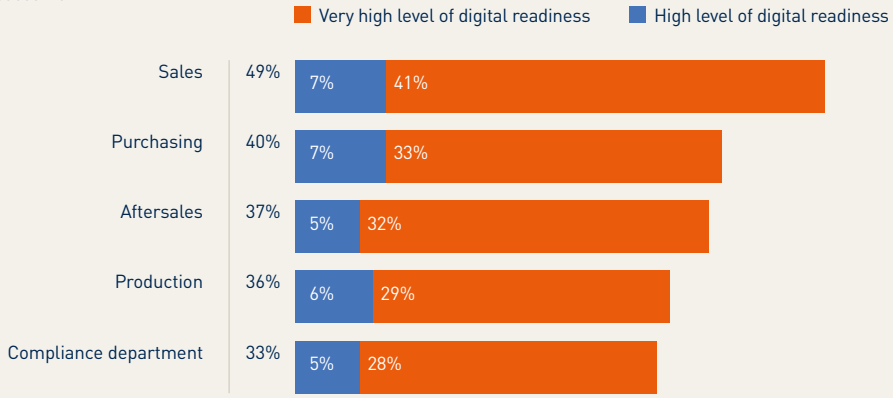
Digital readiness

Only slightly more than one-third of experts assess their own company as having a high level of digital readiness – compliance departments need to catch up

Overall evaluation



Digital readiness of various departments
Basis: Respondents who provided an assessment



Question: How do you assess your company's digital readiness? And how do you assess the digital readiness of the following departments in your company?

Basis: All companies; respondents who provided an assessment of the digital readiness of individual departments; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Many respondents consider their companies as having inadequate digital structures in place. Those in management positions were more reticent in their assessment of the company's level of digital readiness compared to respondents from specialist departments. It is not surprising that listed companies rate their level of digitalisation as being significantly higher than the overall average. When it comes to individual company departments, it is the compliance department that sees the greatest need to catch up.

Senior management, executive level and specialist departments

It is striking that the assessment of digital readiness seems to vary at different company levels. There is a marked difference in the assessments by senior management and specialist departments.

Senior managers assess the digital readiness of their own company rather cautiously. Only slightly more than a quarter of them assume that their own company has a high or very high level of digital readiness (27%). The vast majority assess their firm's digital readiness to be at a medium level at best.

The view at **executive level** is definitely more optimistic. Here, **37%** of the managers questioned view their company as highly or very highly digitalised. A clear majority of executives, however, rate the digital readiness level as medium (55%) or see a need to catch up (low digital readiness level, 8%). In a sector comparison, the **banking and insurance sectors** is particularly noteworthy, with the majority of the managers questioned considering the digital readiness level of their company to be high (63%).

The proportion of employees in the **specialist departments**, such as IT, compliance and legal, who assume a high to very high level of digital readiness is significantly higher. Here, the figure is between **39%** and **46%**.

Listed companies

It may come as no surprise that a comparatively large number of **listed companies** rate their level of digitalisation as high or very high (42%). This is significantly higher than **the overall average** (37% with a high or very high level of digital readiness). Even in the banking and insurance sectors, the companies surveyed attest less often to a high to very high level of digital readiness (40%).

Corporate divisions

The assessments of digital readiness also vary widely between corporate divisions.[2]

The respondents see the **greatest need to catch up** in the area of **compliance**. Only one in three companies that gave an assessment rated the compliance department as having at least a high level of digital readiness (33%). In companies with at least a high level of digital readiness, the compliance officers themselves rate their own department better (41%), but in companies with a lower level of digital readiness, even the assessments by the compliance officers are average at best.

The situation is different in the areas of **purchasing, after sales and production**, for example. Here, between **36%** and **40%** rate the level of digitalisation as at least high. **Sales** has the **best score**. Here, almost half of the respondents see at least a high level of digital readiness (49%). However, the majority of respondents in the other corporate divisions also consider the level of digital readiness to be at most medium.

Overall, there seems to be considerable potential for catching up in corporate divisions, and especially in the compliance departments.

[2] To prevent skewing of the results, only experts whose expertise made an assessment possible were included. Depending on the business sector surveyed, between 8% and 31% of respondents were unable or unwilling to make an assessment.

1.3 Positions for digital compliance in companies

Many companies do not have dedicated positions for dealing with digital compliance risks; the necessary technical expertise is in any case often underrepresented.

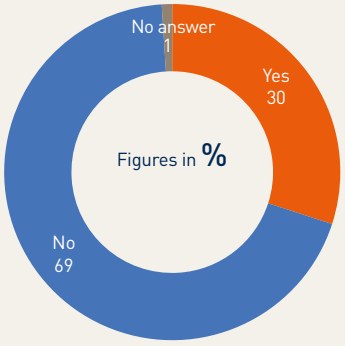
Senior management can delegate the task of digital compliance within the organisation. It often makes sense for the senior management to entrust this task to employees who have the necessary special expertise. This does not relieve the senior management of its overall responsibility, but its duty to act is transformed into a duty to select and monitor.

The study shows that companies often have no dedicated positions for dealing with digital compliance risks. In addition, the feedback we received indicates that technical expertise is rather underrepresented in such positions.

Positions with responsibility for digital compliance risks

A dedicated position exists in 3 of 10 cases.

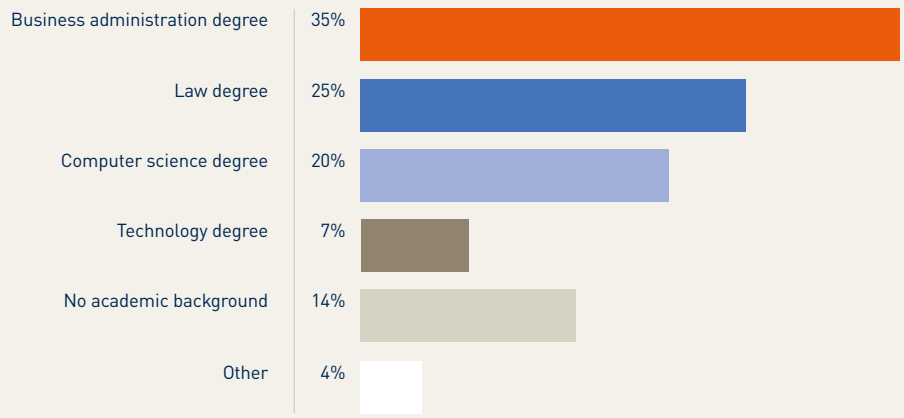
Is there a dedicated position for digital compliance risks?



If so:
Most common job title (top 3)

26% (Digital) Compliance Officer
20% IT Security Officer, IT Governance Officer or similar
12% Data Protection Officer

If position exists: educational background of the responsible compliance officer



Question: Is there a position in your company that is expressly responsible for digital compliance risks? What is the job title for this position? And can you tell us what the compliance officer's educational background is?

Basis: All companies; companies with a dedicated position for digital compliance risks; more than one answer possible in some cases; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Explicit responsibility for digital compliance risks

A mere three out of ten surveyed companies have created a position that is dedicated to digital compliance risks. It is noteworthy that companies that consider themselves to have a lower level of digital readiness are also less likely to have established dedicated positions to deal with digital compliance risks (26%).

There are also major differences in the individual sectors. While more than one in two of the companies in the **financial sector** that took part in our survey has created a digital compliance position (53%), the proportion in the manufacturing sector is significantly lower (27% at the most).

The **listed and unlisted companies** surveyed also differ, although the difference is smaller in comparison. More than a third of the listed companies have established a dedicated position for digital compliance risks (35% as opposed to 30%).

Company size alone does **not seem to play a decisive role**, even though the vast majority of listed companies taking part are fairly large ones with over 1,000 employees. They are slightly less likely to have a digital compliance position than smaller companies with fewer than 1,000 employees (29% as opposed to 32%). In the larger companies with more than 1,000 employees, the compliance officer or an IT security officer holds this position with above-average frequency (33% and 23%, respectively). The exact position designations show that those responsible for digital compliance risks very often come **directly from compliance or IT departments**. The most common titles for this position are "Digital Compliance Officer" (26%) or "IT Security/Governance Officer" (20%). In 12% of the companies surveyed, the position is held by the data protection officer. In addition, the respondents have a variety of different job titles for this role, ranging from unspecified IT positions to risk managers to digital transformation managers.

Interestingly, the feedback indicates that companies with a higher level of digital readiness also entrust the compliance department with the task of handling digital compliance risks more often (38% at least high as opposed to 16% at most medium digital readiness). In contrast, in the surveyed companies with a low or medium digital readiness level, the IT department, data protection officers or risk managers are more often responsible (IT security/governance officer: 22% with a low or medium as opposed to 17% with a high readiness level; data protection officer: 17% as opposed to 7%; risk manager: 8% as opposed to 2%).

A compliance department is not compulsory. However, the vast majority of respondents with a digital compliance position say they have one (85%).

Technical expertise

In the dedicated compliance positions that deal with digital risks, technical expertise is often underrepresented.

Only one-fifth of the companies taking part state that employees in this position have a **degree in computer science**. A **technology degree** is extremely rare (7%). In the companies surveyed, digital compliance risks are most often managed by **economists** (35%), followed by **lawyers** (25%).

Larger companies with 1,000 or more employees say they employ lawyers about twice as often as smaller companies (35% as opposed to 18%). In the surveyed companies with a high level of digital readiness, lawyers are also more frequently found in the position of digital compliance officer than in companies with a lower level of digital readiness (31% as opposed to 20%).

Thus, the vast majority of employees tasked with managing digital compliance risks have an academic background. Only 14% of the employees expressly responsible for the compliance risk function do not hold a degree. It is striking that the proportion in smaller companies is almost twice as high as in larger companies with more than 1,000 employees (18% as opposed to 10%).

2. Digital legal risks

The digital legal risks companies can face are on the rise and at the same time becoming more complex.

Given this, it is no surprise that around half of respondents have already experienced digital risks first-hand. Companies that have not yet been affected may well advised to catch up with compliance management for ransomware attacks and copyright infringements. However, the vast majority of survey participants have already taken compliance measures to mitigate digital legal risks. But when it comes to newer technologies, the legal risks are frequently still underestimated.

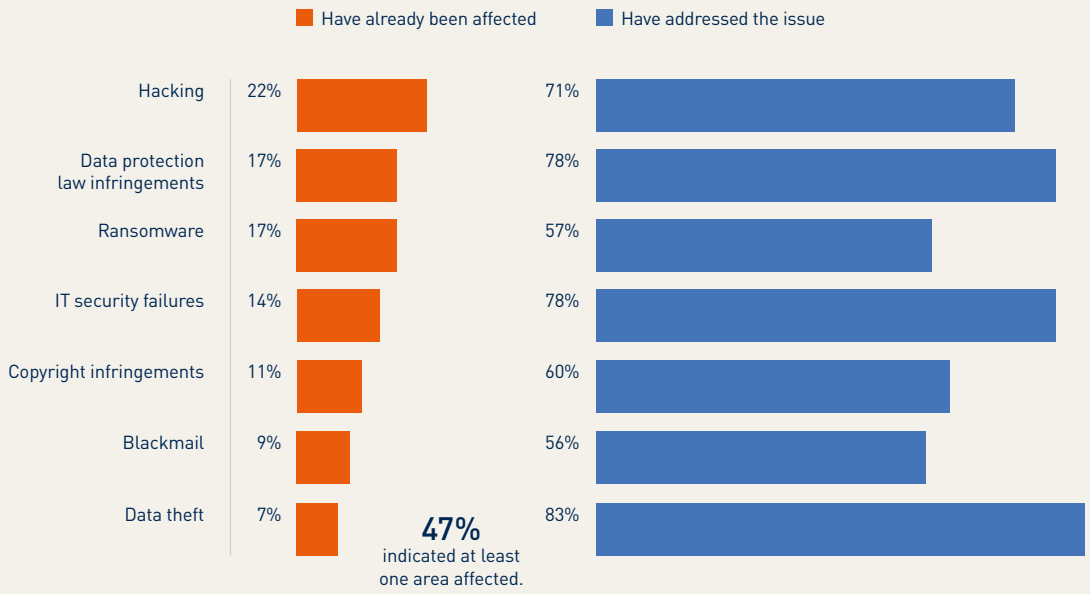
2.1 Companies affected

Around half of the companies have already experienced digital legal risks first-hand.

More than one in five of the companies surveyed have been victims of an attack by hackers (22%). Of the larger or listed companies or those with parent companies outside Germany, almost three out of ten were affected (27% to 28%).

Legal risks from digitalisation

Almost half of companies already affected – need for improvement on blackmail, ransomware and copyright law



To what extent has your company addressed the following legal risks related to digitalisation?

Basis: All companies; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

These figures correspond to the **stricter legal requirements** for digital technologies and the **growing threat** posed by cyberattacks for many years. In its current report on IT security in Germany, the Federal Office for Information Security notes that around 117 million new malware program variants were circulated in 2020 alone. In its current federal snapshot of cybercrime, the Federal Criminal Police Office (Bundeskriminalamt) states that the number of cybercrimes is steadily rising (by almost 8% from 2019 to 2020). In recent years, ransomware attacks have posed enormous challenges for companies around the world. In simple terms, the attacker often encrypts crucial company data in these attacks and extorts a digital ransom for their release.

About one in six companies reported they had already been victims of a **ransomware attack** (17%). The proportion of **listed companies** is remarkably high (37%). A little smaller, but still comparatively high, is the proportion of **larger companies** surveyed with at least 1,000 employees or companies with **foreign parent companies**, a quarter of which have already been targeted by ransomware attacks (25% in each case).

According to the responses, **IT security failures** and **copyright infringements** appear to make up a smaller proportion (14% and 11%, respectively). **Data theft** in particular seems to be even less common, although this comparatively small number (7%) is rather surprising given the high number of hacking and ransomware attacks. In these areas too, the **listed companies** surveyed are attacked more frequently than non-listed companies. For instance, about three times as many listed companies reported they had been the target of unauthorised spying on confidential or personal data (21% as opposed to 7%).

2.2 Risk assessment of unaffected companies

We asked the companies that had not yet experienced any risks first-hand whether they had addressed those risks.

In the case of **ransomware attacks** as well as in the case of **copyright infringements**, which are both on the rise, there seems to be **more need for protection**. On the one hand, only about three out of five respondents report they have addressed these risks (between 56% and 60%). If you add the companies in which those violations have already happened, between a third and a quarter of the respondents either lack experience in these issues or have not yet dealt with them (26% to 35%). On the other hand, over two-thirds of decision-makers have already dealt with the topics of hacking, data breaches, IT security failures and theft (over 70% in each case).

2.3 Risk reduction measures

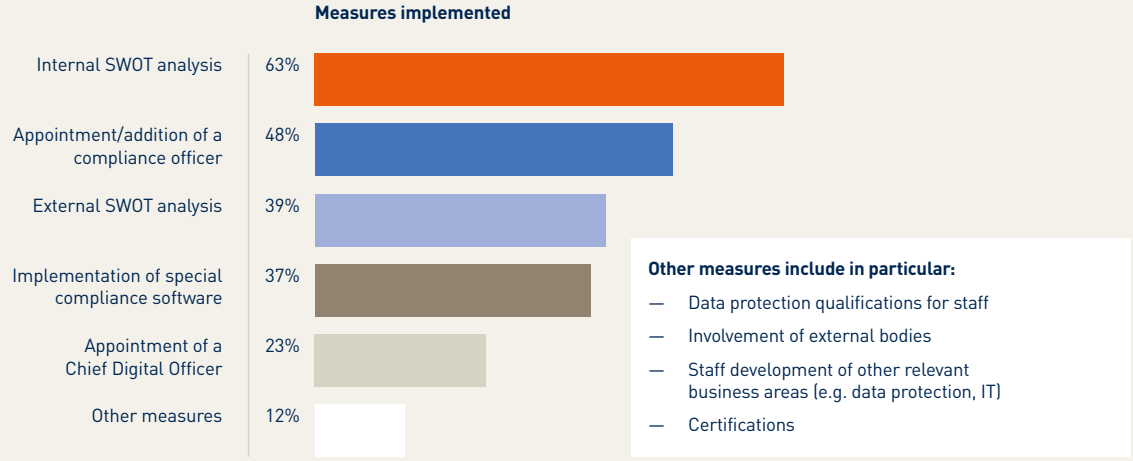
The vast majority of companies surveyed have already taken compliance measures to reduce digital legal risks.

It is welcome news that the vast majority of the companies approached have already introduced some type of compliance measures to mitigate digital legal risks.

89% of the decision-makers interviewed mention at least one of the five following individual measures or refer to other measures.

Measures against compliance risks

9 out of 10 companies have implemented measures, mostly an internal SWOT analysis



Question: Which of the following measures have you taken to address compliance risks from digitalisation?

Basis: All companies; multiple answers possible; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

The most common measures are **internal SWOT analyses**, used in **63%** of the companies questioned as part of their strategic risk prevention. These reviews of the strengths, weaknesses, opportunities and threats to their own company are most common in the **financial and insurance sectors** (84%).

It is also welcome news that almost half of all companies have appointed a **compliance officer** or have expanded their **compliance team** (48%). The responses suggest companies are increasingly implementing measures when there is a compliance officer or a dedicated compliance department. For example, respondents with an established compliance department perform internal SWOT analyses (68%) or implement special compliance software (41%) much more frequently than the companies questioned who do not have a compliance department (51% and 27%). However, these figures cannot hide the fact that only three out of ten of the companies surveyed have an employee specifically responsible for digital compliance risks (see page 12).

It is striking that **larger companies with at least 1,000 employees, listed companies and those with foreign parent companies** appear to be much more likely to implement measures against digital risks than smaller, non-listed companies headquartered in Germany. For example, **77%** of listed companies surveyed have carried out an internal SWOT analysis, while only **61%** of unlisted companies have done so.

By comparison, a similar result is found among the companies surveyed that have **high or very high levels of digital readiness**, which are less reluctant to implement compliance assurance measures (taking an average of 2.5 measures) than companies with lower digital readiness (which take an average of 2.0 measures).

Compliance measures are carried out comparatively often as a **tool for responding** to compliance breaches. For example, companies already affected carry out internal SWOT analyses or create special compliance software more often than companies that have not yet experienced compliance incidents (a difference of eight to 14 percentage points in each case). It would be good to see companies take more of a preventive approach so as to avert compliance incidents as far as possible, rather than having to react to them later.

2.4 Technologies

The legal risks posed by newer technologies are especially underestimated.

The digital compliance risks at a company depend greatly on the technologies used. The responses show that overall risk awareness at companies still needs to be raised. Respondents consider the legal risks in almost all the technology areas surveyed to be mostly low or medium. The legal risks of newer technologies are often underestimated, this although compliance requirements will continue to become more complex in this field.

General risk assessment

In **almost all technology areas**, most of the companies questioned assess the associated legal risks as being **low or medium** (71% to 88%).

Companies with a high level of digital readiness also rate the compliance risks of technologies as being higher than companies with a lower level of digital readiness. For example, companies with a **high level of digital readiness** perceive compliance risks from web services and big data analytics to be significantly higher (17% and 13% as opposed to 8% and 5%).

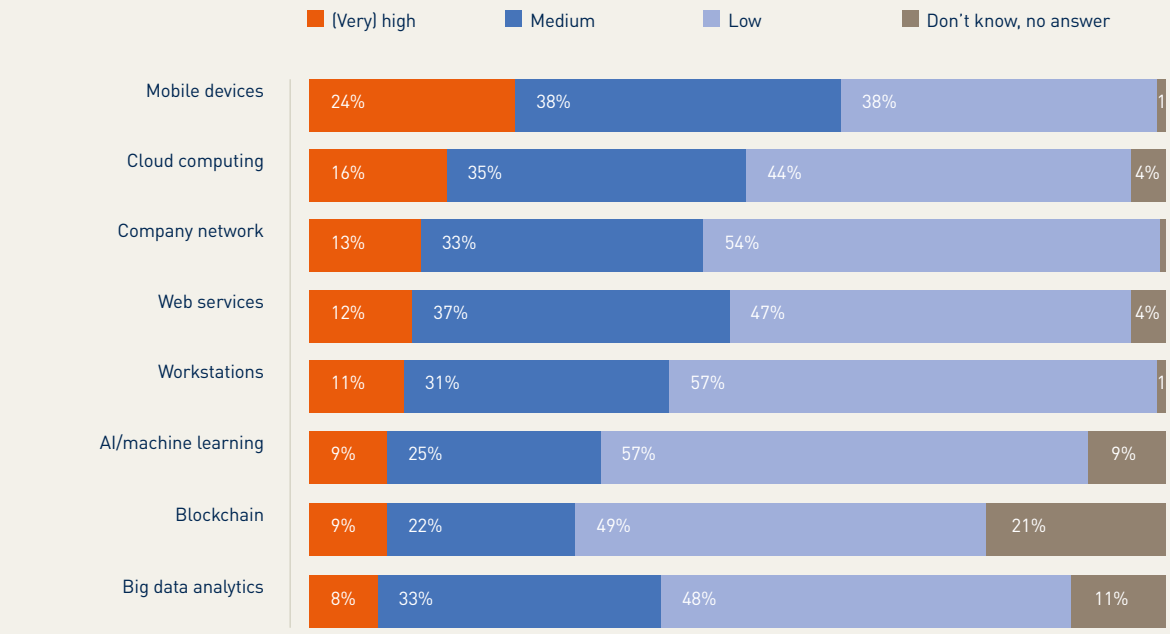
This suggests that companies that consider the issue of digital compliance more closely are able to identify and address digital legal risks of technologies more frequently.

Technology-specific risk assessment

Especially with **newer technologies** such as blockchain, the use of artificial intelligence (**AI**) or big data analytics, it is evident that the companies we interviewed often underestimate the associated risks.

Laptops, smartphones and tablets most likely to be at risk

Risk of legal breaches in digital technologies



Question: Thinking about the digital technologies used in your company, how do you rate the risk of legal breaches?

Basis: Companies using the technology in question; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Senior management considers these technologies to pose higher legal risks comparatively more often than managers from the specialist departments, with the former's percentage being at least twice as large as on average. Nevertheless, the absolute number is comparatively low, as about one-fifth of the managers and managing board members interviewed and about one-tenth of the total respondents see high legal risks in these technologies.

Mobile devices, such as laptops or smartphones, are still considered the riskiest by the decision-makers surveyed. **24%** of respondents whose employees use such devices on the job assume that these devices involve a high to very high compliance risk. Among respondents in the IT sector, the proportion is even higher (29%).

For **cloud computing**, risk awareness across the board is fairly low (24% among IT managers surveyed as opposed to 16% from other departments). **Company networks, web services** and the **traditional workstation** are seen as medium risk. Only one in every eight to nine companies sees a high or very high risk of legal breaches here.

AI or blockchain applications and big data analyses are even less likely to be seen as risky. Fewer than one in ten of the companies surveyed sees high compliance risks in each of these technologies. This is probably mainly because these technologies are still relatively new, and many companies are not yet using them much. Additionally, up to one-fifth of respondents cannot or do not want to provide information on the legal risks of these technologies (21% to 9%).

New technologies involve increasingly complex compliance

In recent years, European and German legislators have become much more active in the field of digital regulation. The case law of the European Court of Justice also compounds the complexity of the situation.

One driver of this increased activity is, firstly, the real threat posed by the vulnerability of the technologies used. Due to the ongoing digitalisation and automation of processes, companies face a constant risk of attacks from outside, especially hacking, which in the worst case can ruin a company's business by encrypting critical data.

Secondly, rapid technological progress entails a risk of loss of control. For instance, the evolution of AI means that its outcomes and reactions can no longer be fully controlled by humans.

The statements above are confirmed by a brief look at IT security law, data protection law and the new approaches to regulating AI applications.

IT security law

The German Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* – **BSIG** = "**Information Security Act**") lays down specific requirements for certain types of companies on how to organise and monitor their IT systems. Similarly, these companies have an obligation to report malfunctions of their IT to the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, "**BSI**"). Fines of up to €20 million may be imposed if breaches are committed (first sentence of section 14(5) of the Information Security Act; third sentence of section 30(2) Administrative Offences Act (*Ordnungswidrigkeitsgesetz* – OWiG). With the recently adopted IT Security Act 2.0, the group of addressees as well as the contents and range of obligations have been considerably expanded. The addressees are not only companies in certain sectors, but also "companies of special public interest" which are of "considerable economic importance for the Federal Republic of Germany or which are essential as suppliers to such companies" (see point 2 of the first sentence of section 2(14) of the Information Security Act). The reference to suppliers in this definition appears to have significantly widened the personal scope of the law.

In any event, these companies must declare to the Federal Office in detail what certifications and security audits they have carried out in the last two years and report any malfunctions of their IT systems without delay (section 8f(1), (7) and (8) Information Security Act). Operators of critical infrastructure, i.e. companies in certain sectors that are of great importance to the functioning of the community, must meet even stricter requirements. These include, among other things, the obligations to proactively protect IT systems with organisational and technical precautions (section 8a(1) Information Security Act), to report the use of certain IT products (section 9b(1) Information Security Act) and to use "intelligent" attack detection systems (section 8a(1a) Information Security Act) in future.

Data protection law

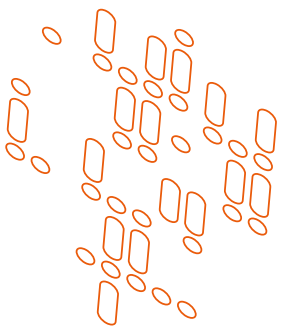
Hacking often leads to personal data being compromised. The most recent example is the attack by the hacker collective Hafnium, which managed to access various email accounts and introduce malware into the systems through a critical vulnerability in on-premise versions of the Microsoft Exchange program. Companies are also required under data protection law to eliminate vulnerabilities in their IT systems without delay. In the event of a loss or disclosure of personal data, the competent supervisory authorities (Article 33(1) General Data Protection Regulation, "GDPR") and, where appropriate, the data subjects (Article 34(1) GDPR) must be notified.

However, data protection challenges arise not only when protecting the IT infrastructure from infiltration by hackers, but also when using digital tools, especially cloud-based software-as-a-service solutions that process personal data. In its Schrems II ruling of 16 July 2020 (Case C 311/18), the European Court of Justice declared the EU-US Privacy Shield, a legal instrument designed to ensure secure data transfers to the US, invalid. As many cloud solutions for companies come chiefly from US providers, the question of whether these services are useable in compliance with data protection law is of the utmost importance. In line with the recommendations given by the European Data Protection Board (Recommendations 01/2020), companies should closely assess the legal situation and practices of the public authorities in the country of destination of the data transfer and, where appropriate, take additional steps such as data encryption to ensure an adequate level of data protection.

Regulation of AI

The threat of loss of control described above, especially when using AI, has now also put the legislator on the spot. The European Commission recently presented a proposed AI Regulation (COM(2021) 206 final) in which it intends to regulate the use of AI systems.

The proposal follows a risk-based approach that makes the admissibility of the use of AI dependent on the associated risks. In the event of breaches, the proposal provides for significant fines of up to €30 million or 6% of the company's annual turnover worldwide. The threshold for applying these rules is extremely low. The European Commission's proposal uses a very broad definition of AI, which it says already exists when software is developed according to certain approaches and techniques and can influence the environments they interact with by means of "recommendations, or decisions" (Article 3(1) of the proposed AI Regulation). The AI Regulation thus appears to cover applications that have been classified as "normal" software to date. The Commission's proposal is likely to undergo significant changes in the further procedure before it actually comes into force. However, it is already apparent that the regulatory approach taken by the European Commission will pose major (compliance) challenges for companies.



3. Digitalisation of compliance processes

Companies not only have to ensure their compliance despite the advance of digitalisation. Digitalisation also opens up new opportunities to counter potential compliance risks. Advancing digitalisation is therefore becoming increasingly important for compliance processes in many companies. Its enormous relevance is also reflected in the fact that many decision-makers questioned would like to invest more in digital compliance tools in the coming years.

While the majority of study participants already use compliance tools, especially information and process tools, there still seems to be a lack of flexible solutions, as a significant proportion of respondents develop compliance tools themselves. Many of the companies taking part do not seem to be aware that the tools used can in turn be associated with compliance risks.

3.1 Relevance of advancing digitalisation in the area of compliance

Advancing digitalisation is becoming increasingly important for compliance processes in many companies.

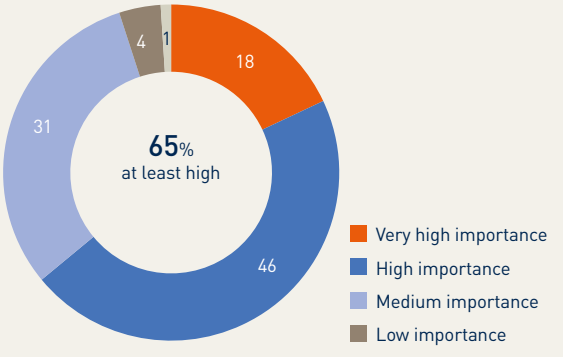
When it comes to improving compliance, **two out of three of the study participants** attach **high to very high importance** to digitalisation.

Close to a third of the **managers** questioned assume that it is of medium importance (31%). Hardly anyone states that advancing digitalisation is only of minor relevance for compliance (4%).

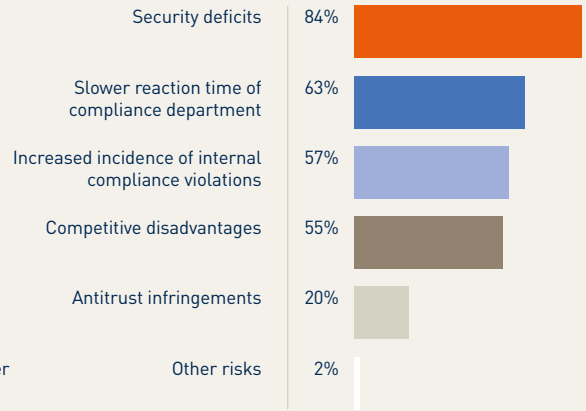
Relevance of advancing digitalisation in the area of compliance

For two-thirds, the issue has high importance – especially to prevent security deficits

Importance of improved compliance through digitalisation



Risks due to delayed digitalisation of compliance processes



Question: What importance do you attach to the possibilities of digitalisation to ensure compliance? Which of the following risks do you see in the company if compliance processes fail to keep pace with digitalisation?

Basis: All companies, figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Above all, the respondents in **compliance departments** assume that digitalisation is extremely relevant for compliance. Almost three-quarters of the **managers** from compliance departments who were questioned attach high to very high importance to digital tools and processes (73%). However, the number of colleagues from **IT departments** who share this assessment is lower (56%).

Companies that have already been **affected** by compliance breaches consider digitalisation to be more important for improving compliance than companies who have not had such incidents (72% as opposed to 58%). This view is also shared by the larger organisations and listed companies surveyed. They also attach greater importance to digitalisation than smaller companies (69% as opposed to 61%) and unlisted companies (77% as opposed to 63%).

The respondents see a danger of security deficits in their compliance processes as a result of **delayed digitalisation**. More than four out of five study participants assume there will be **increased security risks** in the company if compliance processes do not keep pace with digitalisation (84%). A large proportion also worry about the compliance department being slower to react to potential incidents (74%). Above all, this aspect worries the compliance departments themselves. Three out of four managers from the compliance departments of the companies taking part in our study see a significant risk here (76%).

Furthermore, a majority of respondents fear an increased incidence of **internal compliance breaches** and **competitive disadvantages** if compliance processes are not sufficiently digitalised (57% and 55%, respectively). Companies with a foreign parent company assess these risks even higher than companies headquartered in Germany (67% as opposed to 54% and 67% as opposed to 52%, respectively). One in three managers at **listed companies** (35%) believes that not going digital also makes **antitrust compliance breaches** more likely.

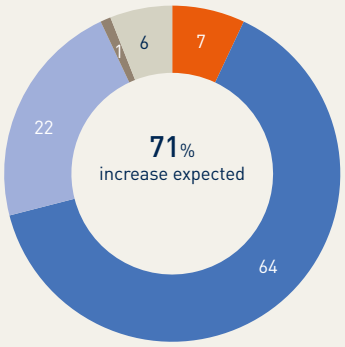
3.2 Budgets for digital compliance processes

Many companies would like to invest more in digital compliance tools in the coming years. Little information is available on current budgets for digital compliance tools.

Budget development

The feedback suggests that increasing investments in digital compliance tools can be expected in the next three years. Digital tools are thus seen as an **important future issue** by a large majority of the experts surveyed.

Future development of compliance budgets for digital tools



Overall result

- Strong increase
- Increase
- Remain roughly the same
- Decrease
- Don't know, no answer

Digital tools are definitely seen as a future topic worth investing in – even more so among companies with pent-up demand

Result by digital readiness of companies
Shown: increase expected

65%
(Very) high level of digital readiness

75%
Medium/low level of digital readiness

Question: Would you say your compliance budget will decrease, stay about the same, increase or greatly increase over the next three years?

Basis: All companies; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Seven out of ten of the decision-makers we asked anticipate an **increase in the compliance budget for digital tools** at their companies over the next three years (71%). In particular, those who assess their digital readiness level in the study as low or medium intend to invest more in digital tools in the future (75%), while participants with an already high digital readiness level expect this less frequently (65%). Hardly any of the companies surveyed plan to cut their budget for digital tools in the future (1%).

It is worth noting that **listed companies** in particular want to **top up** their digital tool budgets significantly more often than non-listed companies (84% as opposed to 69%).

Current budgets

While almost every second company we surveyed has already been affected by the legal risks of digitalisation, only very few can or want to comment on the budgeting of digital tools within compliance. Overall, the share of the total compliance budget still seems to be comparatively low.

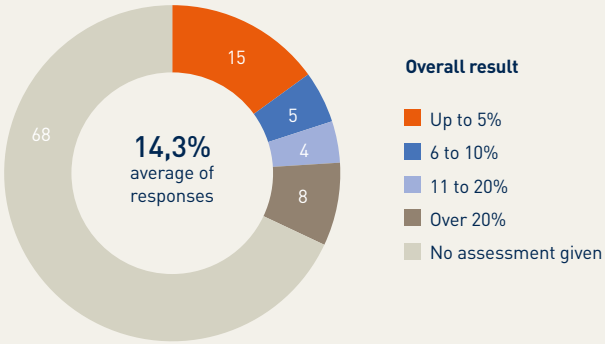
Only just under a third of the executives commented on the current proportion of the compliance budget that is used for **digital compliance tools** (32%) in their responses. This is similarly true for respondents in compliance positions (38%) or in management (40%). This comparatively large blind spot should be taken into account in the following comments.

Based on the information provided by those who made an assessment, on average **every seventh euro** of the compliance budgets of the companies surveyed (14.3%) is used for digital tools. In larger companies, this budget share is higher (17.2%). The same applies to the study participants who consider themselves to have a high level of digital readiness (16.9%).

Especially companies that already have a **special position** for digital compliance risks invest comparatively more money in digital compliance tools. Here, **every fifth euro** (20%) of the budget is spent on digitalising compliance processes.

A good two-thirds are unable or unwilling to make an assessment

Compliance budget for digital tools



Question: What percentage of your company's compliance budget is used for digital tools?

Basis: All companies; figures in per cent Source: Kantar – Quantitative survey 2021 on behalf of Noerr

3.3 Use of digital compliance tools

Digital compliance tools: overview and systematic approaches

Advancing digital transformation is creating new opportunities for companies to ensure or increase compliance by using digital tools. Possible uses of such digital compliance tools are manifold and the range of tools available on the market is broad and constantly growing. Therefore, a **structured overview** of digital compliance tools is provided below.

If digital compliance is approached on a systematic level, two methodical approaches can be identified that allow a rough subdivision. A distinction can be made between **compliance by design** and **compliance by detection**. The main distinction between the two approaches is that compliance by design is intended to **proactively** ensure compliance, while compliance by detection is intended to **reactively** ensure compliance.

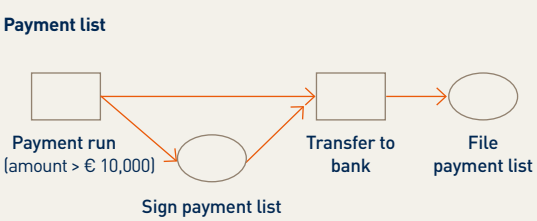
This subdivision is originally found in particular in the context of automated compliance. This describes digital applications that not only digitalise manual measures, but in the best case implement them in such a way that human activity is only needed for monitoring. However, not all digital compliance tools offered on the market are covered by this. For the purpose of systematisation, an expanded understanding of compliance by design and compliance by detection is therefore used here. In this way, digital tools that cannot be automated or can only be automated to a certain degree, such as policy management, can also be covered by these terms.

Compliance by design

Compliance by design is a proactive approach aimed at preventing compliance breaches from occurring in the first place. In a (hypothetical) perfect compliance-by-design-system, any **compliance breach is ruled out from the outset**. The system would be created in such a way that it monitors and limits non-compliant behaviour of employees. For this purpose, especially in the basic case of the automated compliance-by-design system, it must be **clearly defined in advance** what the desired rule-compliant behaviour must look like in each situation. The implementation in the automated compliance system can then occur in two ways. On the one hand, a company can define what behaviour should be permitted: in this case, the system would not allow deviating behaviour. On the other hand, it can define what behaviour is not allowed, and this kind of behaviour would then be blocked. In both cases, however, this means that all conceivable scenarios must be recorded and entered into the program beforehand. This has the **disadvantage** that the system does not allow for flexibility and must be constantly adapted to reflect changing requirements. However, the broader approach of compliance by design used here, as described above, also includes non-automated compliance tools that can also be designed more flexibly.

The following diagram shows an example of a bank's approval process for transfers of more than €10,000. A program checks transfers to see if they involve an amount of more than €10,000. If this is the case, the transaction is first stopped and presented to an employee. Only after the employee has accepted the transaction it can be completed. Afterwards, the program archives the approval for later checks.

Compliance Rule Graph Example



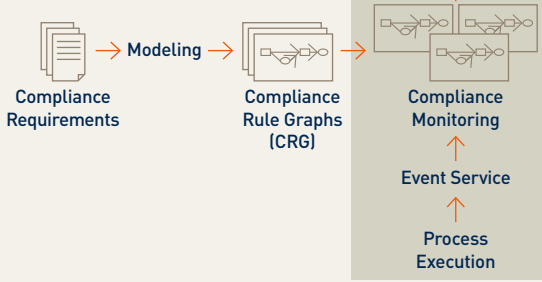
Before a payment list with amount beyond €10,000 is transferred to the bank, the payment list has to be signed by an officer. After being transferred to the bank, the payment list has to be filed for later audits.

Source: *Ly/Rinderle-Ma/Knuplesch/Dadam*, Monitoring Business Process Compliance Using Compliance Rule Graph

Compliance by detection

Compliance by detection is a reactive approach that aims to reliably **detect** compliance breaches and, in the best case, to **interrupt** the process. In addition, the processes should subsequently be redesigned in such a way that the same breach does not occur again. This is also a major advantage of the compliance-by-detection approach. It allows wide room for manoeuvre and flexibility, since unlike compliance by design, the permitted boundaries for compliant behaviour do not have to be clearly defined in advance. In order to cover all available and conceivable possibilities of reactive, retrospective compliance, compliance by detection also includes non-automated tools in our discussion below (as with compliance by design). One example of such a not completely automated tool is a digital whistleblowing system.

The following diagram shows on the left how a compliance assurance tool is created and, on the right, how it is used, beginning with "process execution". In the context of this, events ("event services") occur, which are automatically checked at the "compliance monitoring" point. After the check, the program creates a report and makes it available to the people responsible. On the one hand, this report can state that the event is classified as legally compliant or, on the other hand, that the breach of a rule has been identified. The responsible persons can then react to the event and, for example, adjust the initial process.



Source: https://www.uni-ulm.de/in/iui-dbis/forschung/abgeschlossene-projekte/seaflows/ (last download 2 August 2021).

When designing and implementing a digital compliance system, it will hardly be possible **in practice** to rely exclusively on one of the two strategies. The goal must always be to achieve the most comprehensive protection against compliance breaches possible through a **combination of both approaches**. For example, in some business processes it may well make sense to pursue a compliance-by-design approach, as no flexibility is required due to clear requirements. At the same time, in other areas it may be advantageous to initially give the processes free rein in order to "refine" them afterwards so that compliance can be established.

Compliance by mapping

In addition to the strategies of compliance by design and compliance by detection presented above, the possibilities digitalisation offers have led to the emergence of the **method compliance by mapping**. This can be used to **design** and to **monitor** compliance with internal and statutory rules and regulations. Compliance can thus be realised in a more **resource-conserving, time-saving and generally more efficient** way by means of mapping. This is already widespread in the field of anti-corruption compliance and in data protection law. Mapping can also be advantageous with regard to IT security.

Compliance by mapping describes the identification of threats, which are then assigned to specific determinations in order to subsequently be able to assign specific compliance measures to them. This has been done by academics, especially for cloud computing. There, the authors assigned a proposal for a specific threat and the affected area to the various lists of compliance measures. A **practical** example is exeon, a Swiss software company, which helps its customers to ensure compliance in the context of cybersecurity. For this purpose, the software can initially visualise even complex networks and make data flows more visible. This makes it easier to ensure compliance, as undesired data flows can be easily recognised.

If a company is subject to many different regulations and standards that must first be identified, it is a good idea to use mapping to generate a uniform, ordered list of requirements that are necessary to achieve compliance as a whole. Mapping makes it easier to compare the different standards, frameworks, etc. and to identify overlaps. Companies do not have to carry out the mapping itself as specia-

lised providers already exist, in the field of IT security CIS Controls and CIS Benchmarks are worth mentioning.

RegTechs

Over the last decade, an **independent industry** has emerged that is geared towards making compliance processes more digital. Especially in the financial sector, the density of regulation has increased significantly in recent years, not least in the wake of the global banking and financial crisis.

As a result, the need for suitable digital compliance tools has also grown. Under the buzzword "RegTech", a large number of start-ups have specialised in developing software solutions to facilitate compliance with the extensive laws and regulations in the financial sector. Due to this pioneering role, in the practical examples selected we mainly focus on compliance tools for the **financial sector**. However, it is apparent that many of the products offered by RegTech companies can also be extended to other sectors.

Practical examples

The following practical examples illustrate the range of digital compliance tools available on the market. Subdivided according to the various tasks that the tools can perform, this section is designed to provide an overview of the options for ensuring digital compliance.

Risk analysis: Risk analyses are indispensable for ensuring compliance. They must clarify at the outset which compliance measures are necessary. Besides this, it is vital to continuously review whether the previous risk assessment is still valid or needs to be adjusted. Based on the risk analysis, organisations can also assess for which areas of the company a compliance-by-design or compliance-by-detection approach makes sense.

For example, the company *risklytics* offers comprehensive data analyses to assess risks. For this purpose, various data can be analysed live and thus a comprehensive picture of the risk-bearing capacity can be made available.

Codes of conduct: Digital tools can also be used to create and, above all, update a code of conduct. In particular, software can be used to check the legal requirements for any changes. This ensures that rules are always up to date.

The company *APIAX*, for example, goes one step further and provides its clients with machine-readable databases. In this way, the rules implemented in programs can also be kept up to date automatically. This measure is a very good example of compliance by design in the broader sense. Although creating and updating a code of conduct cannot entirely rule out compliance breaches, it is a classic tool for prevention.

Informing staff about the code by providing training: In addition to continuously updating their internal rules, companies have to communicate them to staff as a further preventive measure. Digital tools are also offered for this purpose.

For example, the creators of the *otris compliance* software state that their GRC software not only allows internal rules and regulations to be distributed to the right places in the company, but also to check whether staff have actually read them.

In addition, the use of e-learning methods can be included in this area. During such briefings staff can be trained on all possible compliance issues.

Whistleblowing systems: One way to reactively ensure compliance is to set up a whistleblowing system. Such a system can be constructed in a purely analogue manner by appointing an ombudsperson to whom whistleblowers can turn. But such a system can also be set up digitally. This could have the advantage that the threshold for the whistleblower is significantly lower, especially if the information can be given anonymously.

A web-based whistleblowing system is offered, for example, by the solution *Trusty*. A further step in this area could also be the use of whistleblower chatbots.

Reporting systems: Digital tools are also increasingly available in the area of reporting, i.e. compiling reports for the company's management. The aim is to enable decision-makers to have the best possible overview of the company's situation at all times. Digital reporting systems are designed to make data visible automatically and at the same time to present it in a particularly clear way.

For this purpose, dashboards are often used that provide a quick and intuitive overview of a large number of key figures.

Another subcategory of reporting is regulatory reporting. This is not only about reporting the key figures to company management, but also about notifying the responsible supervisory authorities in accordance with the law. *Cleversoft*, for example, offers services of this type.

Monitoring systems: One area where compliance-by-design and compliance-by-detection approaches can be used simultaneously is the monitoring of transactions. This is to ensure that legal provisions designed to combat money laundering and terrorist financing are not undermined.

The RegTech company *Clarus*, for example, is active in this area. It allows financial institutions to have transactions by their customers checked. For this purpose, the institution transmits the data from the transactions. Clarus analyses the data automatically and identifies any suspicious transactions. These can then be examined more closely with the help of Clarus' "Investigation Platform".

Corruption prevention systems: A corruption prevention system can be designed to be both preventive and reactive. On the one hand, preventive work can be done by providing training, especially via e-learning. On the other hand, automated compliance design tools can be used very well here. In a digital process, for example, staff could be required to record every benefit they receive from business partners in a system. The system checks whether the gift can be accepted in accordance with the code of conduct and then provides feedback to the person concerned.

BMW, for example, stated the following in its 2020 Annual Report: "Various IT systems support BMW Group employees with the assessment, approval and documentation of compliance-relevant matters. For example, all exchange activities with competitors must be documented and approved in a special compliance IT system. The same applies to verifying legal admissibility and documenting benefits, especially in connection with corporate hospitality."

Know your customer systems ("KYC"): Such a KYC-system is intended to ensure that companies do not enter into business with persons or companies that pose a compliance risk, for example because they are on a sanctions list. At the same time, the goal of KYC is precisely to clearly identify the business partner. This is relevant above all in the financial sector, where the prevention of money laundering is key.

The RegTech company *GlobalPass*, for example, has specialised in the area of KYC. One of the tools offered, "Name Search", automatically creates a kind of dossier on a wanted person. For this purpose, not only Europol and Interpol wanted lists are checked, but also sanctions lists and even media and social networks. This is to make any possible negative reporting visible. These dossiers can be updated daily. Another *GlobalPass* tool, "Real Time Screening", is designed to ensure the verification of the identity of customers and business partners.

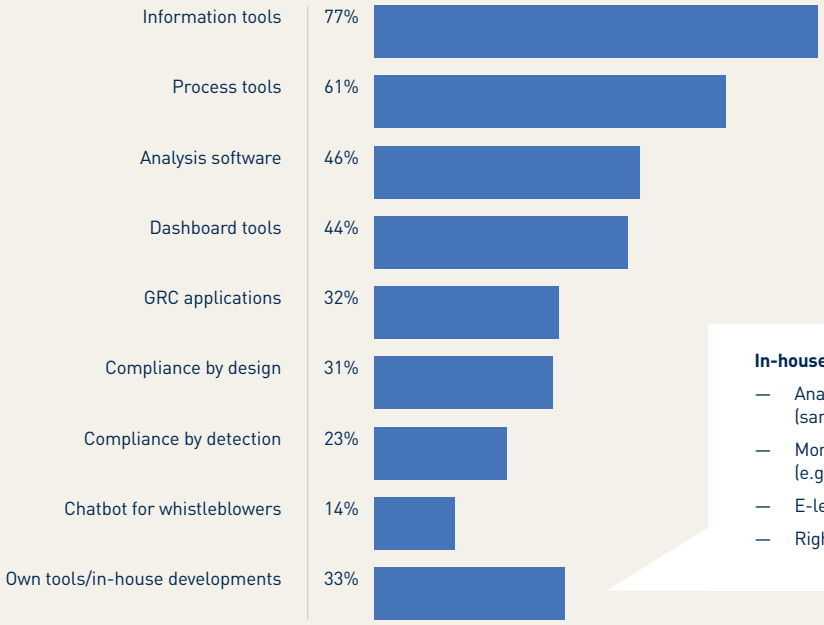
Widespread use of information and process tools

Information and process tools are widespread.

The companies surveyed use a wide range of compliance tools.

Information tools are most widespread – one-third refer to in-house developments

Use of compliance tools and processes in the company



In-house developments mentioned:

- Analysis, detection, documentation tools (sanctions list comparisons, risk analyses)
- Monitoring tools (e.g. dashboards, process analysis)
- E-learning platforms, prevention
- Rights and approval management

Questions: Which compliance tools and processes do you use?

Basis: All companies; multiple answers possible; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

By far the most common tools used by respondents are **information tools**, such as training software or e-learning for staff. More than three-quarters of the study participants (77%) use such tools to train their staff on key compliance requirements. Especially in **listed and larger companies as well as in companies with a foreign parent company**, compliance information tools are practically part of the **standard repertoire** with more than **80%** in each category (86% of listed companies, 82% of larger companies with more than 1,000 employees and 85% of companies with a foreign parent company).

The decision-makers surveyed also use **process tools**, such as checklists to check compliance with legal requirements, comparatively often (61%) in order to prevent possible legal breaches in the ongoing production or sales process.

In the category of **listed companies** and those with foreign parent companies, **at least two-thirds** of the decision-makers state that they use process tools in their company (67% and 71%, respectively).

In contrast, the majority of companies surveyed do not use **analysis software** to identify compliance breaches and **dashboard** tools that summarise process data from different sources and present it visually (only 46% and 44% use these tools, respectively). The exceptions are companies whose **parent company is based abroad**, which predominantly rely on such applications to reduce compliance risks. Thus, 54% use analysis software and 58% dashboard tools.

More complex GRC applications or dedicated IT systems are used less frequently. **GRC applications** that support governance and risk management in addition to compliance by identifying, analysing and including regulatory requirements, are used by almost every third company surveyed. This also applies to IT systems that are structured by design in such a way that compliance breaches are at least less likely (**compliance by design**). By contrast, the more retrospective IT systems that comprehensively record company processes and staff behaviour in order to be able to detect breaches after they have taken place (**compliance by detection**) are only used by just under one in four of the companies surveyed (23%).

Whistleblower chatbots are relatively rarely used as compliance tools. These applications are based on the "EU Whistleblowing Directive" ((EU) 2019/1937), which has been in force since the end of 2019 and is intended to enable whistleblowers to report wrongdoing in the company without fear of reprisals. According to the requirements of the directive, companies with at least 50 employees have to establish internal reporting channels through which persons with a connection to the company can point out violations of EU law (Article 8). These internal reporting channels must be designed in such a way that the whistleblower's identity remains protected (Article 16). In order to implement the EU Whistleblowing Directive in due time by 17 December 2021 (for companies with 50 to 249 employees by 17 December 2023), the German Federal Ministry of Justice has already submitted a draft for a national Whistleblower Protection Act (*Hinweisegeberschutzgesetz* – HinSchG). Even though the EU Whistleblowing Directive allows companies to freely choose the type of reporting channel (analogue or digital) (see recital 53), digital whistleblowing systems such as chatbots have not yet become established. They are currently only used in every seventh company surveyed (14%). However, **listed companies** use them twice as often (28%). Also, just under one in five larger companies with at least 1,000 employees (19%) say they already use such AI-supported whistleblowing systems, while only just under one in ten smaller companies use such systems (9%).

Every third company also states that it uses **compliance tools developed by them in-house**. These are mostly in-house analysis, detection and documentation tools as well as special tools, for example for monitoring or digital rights and approval management.

As expected, almost all digital tools are more widespread in the surveyed companies with a high level of digital readiness and especially in companies with a dedicated position for digital compliance risks than in companies with a lower level of digital readiness (+7 percentage points on average) or without a dedicated digital compliance position (+10 percentage points on average).

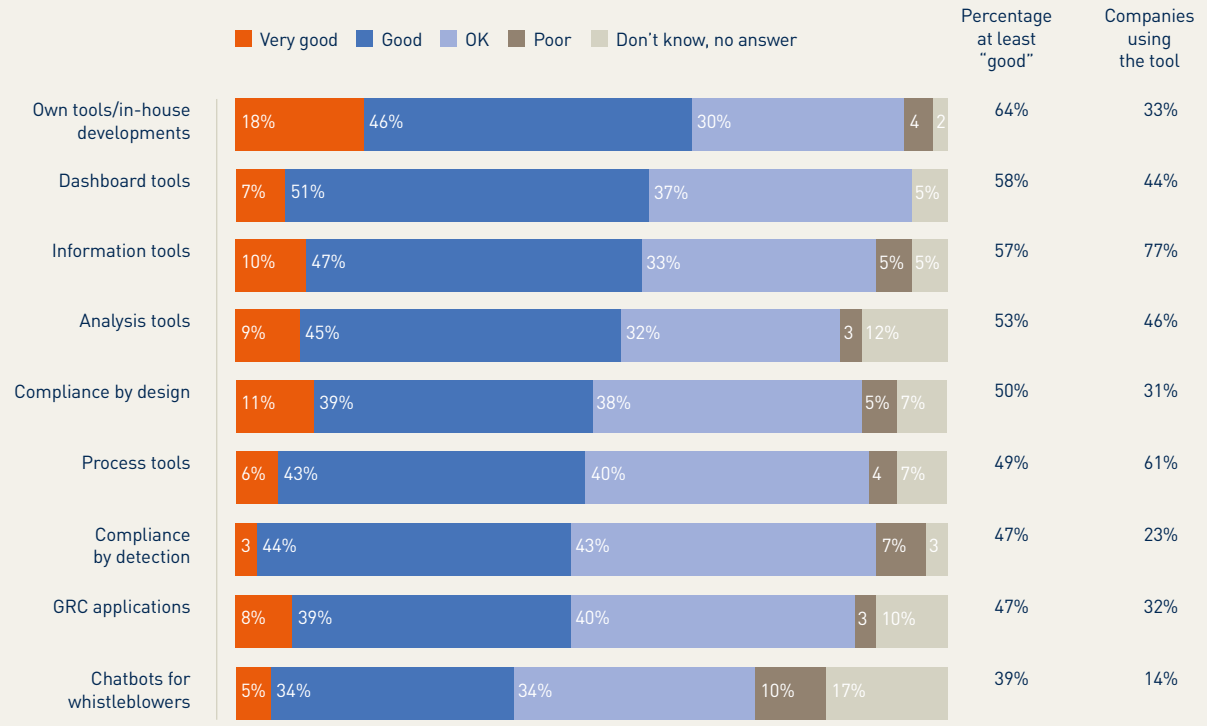
Satisfaction

Flexible tool solutions that sufficiently reflect the individual compliance needs of a company often seem to be lacking.

Satisfaction with the compliance tools used varies among the respondents. Flexible tool solutions that sufficiently reflect the individual compliance needs of a company still often seem to be lacking. This is supported by the fact that many of the companies questioned have developed their own compliance tools and are significantly more satisfied with them than with other solutions.

Assessment of compliance tools in use

Specialised tools developed in-house perform best – mixed ratings for chatbots



Question: What is your experience to date with the compliance tools and procedures you use?

Basis: Individual tool is used; for the proportion of companies that use the tool, the basis is: all companies; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Almost two-thirds of the companies surveyed that use **compliance tools developed in-house** rate them as **good or even very good** (46% and 18%, respectively).

The majority of managers surveyed are also satisfied with **dashboard tools**, **information tools** and **analysis software** (between 58% and 54% "good" or "very good"). IT systems based on the principle of **compliance by design** or **compliance by detection** as well as **process tools** and **GRC applications** still receive good ratings from about half of the respondents (between 47% and 50%).

Whistleblower chatbots are rated comparatively negatively by managers. As many as one in ten respondents gave such tools a bad report card. In any case, every sixth manager has difficulties making an assessment of such tools at all (17%).

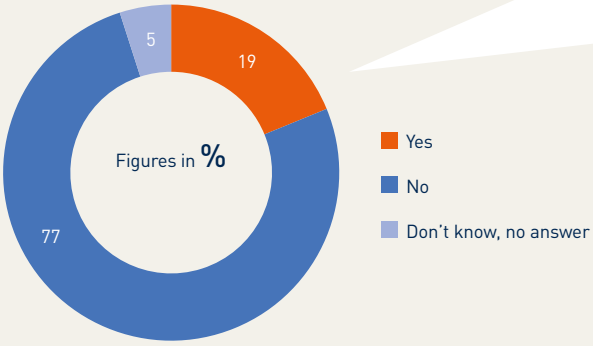
Risk awareness

The fact that the use of compliance tools can itself involve risks for companies is often not recognised.

Compliance risks from compliance tools

One in five companies reports critical opinions

Are there also opinions in your company that the use of compliance tools itself creates new compliance risks?



Detailed results,
percentage "Yes"

Companies with **fewer than 1,000 employees**	16%
Companies with **1,000 employees and more**	22%
Companies headquartered **in Germany**	16%
Companies headquartered **abroad**	32%

Question: Are there also opinions in your company that the use of compliance tools itself creates new compliance risks?
Basis: All companies; figures in per cent
Source: Kantar – Quantitative survey 2021 on behalf of Noerr

The **vast majority of respondents** state that there is no discussion in their company as to whether the use of compliance tools itself entails compliance risks (77%). Only one in five of the companies surveyed sees corresponding risks in the use of compliance tools (19%).

While the concerns are most frequently placed with the decision-makers in the compliance departments (23%), senior management seems to be addressed less frequently (11%).

In larger companies with 1,000 or more employees and in listed companies, these opinions are slightly more prevalent than in smaller and unlisted companies (22% and 24%, respectively as opposed to 16% and 18%, respectively).

At companies headquartered abroad, this issue is apparently raised much more frequently. Every third manager surveyed has already heard of such assessments (32%).

4. Digital compliance during the Covid-19 pandemic

The Covid-19 pandemic is placing a heavy burden on businesses in a variety of ways. It also has a particular impact on digital compliance at companies. For example, the pandemic has boosted the use of digital tools to an extent previously unheard of. At the same time, the crisis has led to a widespread increase in working-from-home workplaces. So it is worth looking at how the companies taking part in the survey assess the increased use of digital tools and whether the pandemic has inevitably led to internal compliance guidelines being relaxed.

The responses to the two topics differ markedly. Although digital aids are now an indispensable part of everyday work, many of the companies surveyed have compliance concerns when using them. Most companies do not state that the pandemic led to any relaxation of compliance guidelines, although they have noticed such relaxation within their specific sector.

4.1 Compliance risks of digital tools

Use of digital tools is widespread despite compliance concerns.

Partly due to the pandemic, digital tools have become an indispensable part of everyday work today. This applies in particular to collaboration and conferencing tools, which enable teamwork via audio or video conferencing, chats or shared file editing.

Virtually none of the companies taking part completely refrain from video conferencing in one form or another. SharePoint systems and collaboration tools are now also being used by around nine out of ten study respondents. In **listed companies**, the proportions of users are even higher (95% and 98%, respectively).

As convenient as it may be to use these tools, their use poses legal risks, especially for data protection. The use of cloud solutions may involve the transfer of personal data to countries where there is no adequate level of data protection. The user input (e.g. communication in a virtual meeting or sharing content) is processed on central servers of the provider, which can be scattered all over the world. However, according to the judgment given by the European Court of Justice on 16 July 2020 (Case C 311/18 – Schrems II), companies can no longer rely on the provider's contractual commitments and are required to check whether the contractual obligations can be effectively complied with by the data importer and that the data being transmitted is protected against access by foreign intelligence authorities.

Compliance risks of digital tools in the area of data protection

At least one-fifth in each case has considerable concerns – but the technologies are still widely used

Question: In your opinion, what are the compliance risks of the following digital tools – especially in the area of data protection?

Basis: Companies using the technology; the proportion of companies using the technology is the basis; all companies; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Many companies are well aware of the compliance risks posed by the various digital tools – especially in the field of data protection. In the **majority of companies surveyed** (51% to 56%) where the technologies in question are also deployed, the use of collaboration tools, SharePoint systems and video conferencing tools entails at least **medium, if not high, compliance or data protection risks**.

Respondents express **considerable concerns about data protection**, especially with regard to **collaboration tools** for teamwork such as Teams, Slack or Trello, which allow for joint document editing, project chats or central task management of joint projects, but also with regard to **SharePoint systems**, which are used for company-wide file storage and communication systems and often as an intranet. One in five managers questioned (20% in each case) sees high compliance and data protection risks in this area.

In particular, the experts in the **IT departments** consider them risky from a compliance point of view. **More than two-thirds** of the IT decision-makers surveyed have **concerns about data protection and compliance** (68% and 72%, respectively). **33%** of IT decision-makers even have major concerns about compliance and **27%** about data protection. Interviewed companies with a high or very high level of digital readiness also have an increased risk awareness with regard to collaboration tools and SharePoint systems (60% moderate or high-risk awareness, respectively).

Video conferences are considered to be slightly less risky. Although the conferencing tools used make the contents of conversations digitally available and divisible and the audience is relatively easy to expand, they represent a large risk for only **15%** of the respondents and a risk that is at least not negligible for **36%**. It is striking that this risk awareness is comparatively high in companies whose parent company is located abroad. More than three out of five study participants (63%) fear at least medium risks, and almost one in five (19%) high risks..

4.2 No relaxation of compliance guidelines in most cases

Virtually no relaxation of compliance guidelines during the Covid-19 pandemic.

The Covid-19 pandemic has put a lot of pressure on companies in many ways. The question is whether the risk of potential sales losses or regulatory requirements has led companies to relax their internal guidelines due to the Covid-19 pandemic. Yet, based on the answers of the vast majority of respondents, this does not seem to be the case.

However, **just over one in five (22%) managers have observed in their own specific sector** that compliance guidelines were relaxed or even cancelled during the pandemic.

Respondents in **smaller companies** with fewer than 1,000 employees were particularly often aware of such relaxations of regulatory or internal standards (26%). By contrast, respondents from larger companies with 1,000 or more employees (18%) less often report a crisis-related relaxation of compliance guidelines.

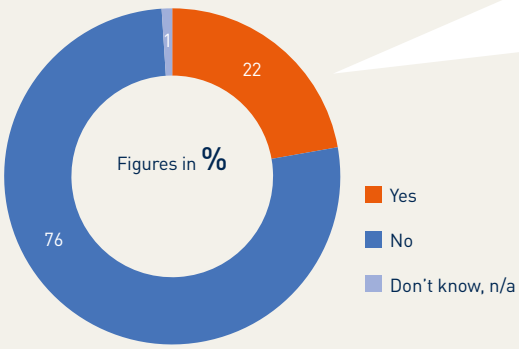
It is also striking that **listed companies** have obviously eased their compliance guidelines a lot less frequently than unlisted firms. While just over one in ten of the managers interviewed of listed companies reported that compliance guidelines have been eased as a result of the pandemic (12%), the percentage of non-listed companies was twice as high (24%).

Yet, whether these responses give a realistic picture is certainly open to question, considering the extreme challenges we have all seen during the pandemic so far. This thought is supported, for example, by the high proportion of people working from home, which in turn has implications for employment law and data protection law in particular. It can be assumed that compliance guidelines have been relaxed during the pandemic significantly more than has in fact been reported.

Relaxation of compliance guidelines during the pandemic

Relaxation reported primarily in smaller companies

Relaxation/cancellation of guidelines observed in industry environment



Detailed results
Percentage answering "Yes"

Companies with **fewer than 1,000 employees**	26%
Companies with **1,000 or more employees**	18%
Companies **headquartered in Germany**	12%
Companies **headquartered abroad**	24%

Question: For over a year, companies in Germany have had to deal with the consequences of the pandemic. Have you observed in your industry that compliance guidelines have been cancelled or relaxed during the pandemic?

Basis: All companies; figures in per cent

Source: Kantar – Quantitative survey 2021 on behalf of Noerr

Study design

On behalf of Noerr, Kantar Public conducted telephone interviews with decision-makers in companies in Germany between March and May 2021. The target group was first- and second-level management in private companies with 250 employees or more. The questionnaires for the interviews were prepared by Noerr in collaboration with the Technical University of Munich. This report incorporates the results of a total of 300 interviews conducted by Kantar Public

The results are subject to the following methodological considerations: since the percentages shown are rounded to whole numbers, they may not add up to 100%. For the same reason, combined categories (e.g. top-two scores such as "very satisfied" and "fairly satisfied") may differ from the sum of the individual categories presented. For questions with multiple response options, the sum of the responses may exceed 100%. The percentages in the text refer to the results of the survey. Particularly important results of the study are also presented graphically.

About the Chair of Law and Security in Digital Transformation – Professor Dirk Heckmann

With the appointment of Professor Dirk Heckmann, an expert in constitutional law and a pioneer in internet law, to the Technical University of Munich (**TUM**) in October 2019, the Chair of Law and Security in Digital Transformation was newly set up as a joint appointment of the TUM School of Governance and the Department of Informatics. With this chair, the TUM emphasises the particular importance of law, especially in the interdisciplinary field of digitalisation covering technology, society and regulation. Additional professorial positions related to law have meanwhile been filled at TUM, for example in Legal Tech and Digital Commerce. From October 2021, Professor Heckmann's chair will be a key element of the newly founded School of Social Science and Technology.

With his team of employees, which now has grown to some 15 members, Professor Heckmann focuses on the fundamentals of law in digital society, legal tech and legal issues in the development and use of artificial intelligence. AI in higher education is a focus of teaching offered by the chair as well as a junior research group – both headed by the departmental postdoc, Dr Lorenz Marx.

To place even greater emphasis on the areas of digital administration, digital education and digitalisation in the healthcare sector, Professor Heckmann and his general manager Sarah Rachut set up the TUM Center for Digital Public Services in June 2020, initially financed by the Bavarian State Ministry for Digital Affairs. As a research centre, it is integrated into the department.

The numerous publications Professor Heckmann oversaw in his time as a professor at the University of Passau will continue to be overseen by the department at TUM – especially *juris Praxis Kommentar Internetrecht. Das Recht der Digitalisierung*, a practical commentary on internet law and the law of digitalisation which Professor Heckmann and his colleague Anne Paschke (TU Braunschweig) have edited since the 7th edition in 2021 and in which Dr Lorenz Marx also contributed as an author.

The former Passau department and now the TUM already have close links with Noerr in research and teaching. These include Professor Heckmann and Anne Paschke's contributions to the legal manual *Rechtshandbuch Internet of Things* by Professor Peter Bräutigam and Torsten Kraul (2021) and Professor Heckmann's contribution to the core manual *IT-Outsourcing und Cloud Computing* (4th edition 2019).

About Noerr

Noerr stands for excellence and an entrepreneurial approach. With highly experienced teams of strong characters, Noerr devises and implements solutions for the most complex and sophisticated legal challenges. United by a set of shared values, the firm's 500+ professionals are driven by one goal: our client's success. Listed groups and multinational companies, large and medium-sized family businesses as well as financial institutions and international investors all call on the firm.

Entrepreneurial thinking

Noerr's advisors make their clients' challenges their own and are always thinking one step ahead. In doing so, they assume responsibility and are at liberty to make their own decisions. The firm is committed to always going the extra mile for its clients and to resolving complex matters with the perfect mix of experience, excellence and sound judgement.

Innovative solutions

In complex and dynamic markets new approaches are regularly required – and delivered by experts who bring both the know-how and the necessary passion. This is precisely what Noerr excels at: implementing integrated and innovative solutions in the most efficient way.

Global reach

As one of the top European law firms, Noerr is also internationally renowned. With offices in eleven countries and a global network of top-ranked "best friends" law firms, Noerr is able to offer its clients truly cross-border advice.

In addition, Noerr is the exclusive member firm in Germany for Lex Mundi, the world's leading network of independent law firms with in-depth experience in 100+ countries worldwide.

Capacity in Central and Eastern Europe

Noerr has long had its own offices in all major Central and Eastern European capitals. The firm regularly advises on greenfield investments, joint ventures, acquisitions and divestments in Central and Eastern Europe by investors from all over the world. With more than 100 professionals, Noerr is one of the leading law firms in the region.

Noerr Group

Noerr PartGmbB – Noerr Consulting AG – TEAM Treuhand GmbH – NOERR AG Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

Offices

Alicante, Berlin, Bratislava, Brussels, Bucharest, Budapest, Dresden, Düsseldorf, Frankfurt, Hamburg, London, Moscow, Munich, New York, Prague, Warsaw

Authors

Professor Peter Bräutigam

Rechtsanwalt (Lawyer), Certified Specialist in IT Law
Partner and Co-Head of the Practice Area Commercial

T +49 89 28628145
peter.braeutigam@noerr.com

Professor Peter Bräutigam Bräutigam is a proven specialist in the field of IT law and Digitalisation/Industrie 4.0. His working areas include IT outsourcing/BPO, framework and project contracts and service level agreements, data protection, data rights, cyber security, liability issues, (software) licensing issues and problems in the IP environment. He is an honorary professor of media and internet law at the University of Passau and regularly publishes in these areas of law (e.g. he is (co-)editor of the legal handbooks "IT Outsourcing and Cloud Computing", "E-Commerce" and "Internet of Things". Professor Bräutigam is vice-chairman of the board of the Gesellschaft für Recht und Informatik (Society for Law and Information Technology), vice-chairman of the board of directors of the Stiftung Datenschutz (Data Protection Foundation) and co-editor of the NJW, to mention but a few.

Dr Julia Sophia Habbe

Rechtsanwältin (Lawyer)
Partner
Co-Head of the Practice Area Compliance & Investigations

T +49 69 971477252
sophia.habbe@noerr.com

Dr Julia Sophia Habbe heads the Compliance & Investigations practice group together with Dr Torsten Fett.

She has extensive experience in complex compliance regulatory and internal investigations and advises on process and crisis management after such investigations. Julia Sophia Habbe represents listed and family-owned companies and their management bodies in compliance cases, in particular in the area of their accountability and liability. Another focus of here work is advising on corporate and capital markets law issues, including handling legal disputes before supervisory authorities and courts.

She regularly publishes articles on involving corporate, capital markets and civil procedure law issues.

Dr Philipp Gergen, LL.M. (Exeter)

Rechtsanwalt (Lawyer)
Associated Partner

T +49 69 971477219
philipp.gergen@noerr.com

Philipp Gergen is associated partner and advises national and international clients on complex investigations by the authorities and in internal investigations. The interface between compliance-relevant and technical or digital issues is a focus of his work. In addition, Dr Gergen has in-depth experience in banking and capital markets law and as a litigator before German courts. His special sector-related expertise also includes the banking and automotive sectors.

Andreas Daum, LL.M. (LSE)

Rechtsanwalt (Lawyer)
Associate

T +49 89 28628466
andreas.daum@noerr.com

Andreas Daum, LL.M. (LSE) specialises in providing legal advice on digitalisation processes and complex IT projects for national and international clients in various industries and the public sector (in particular agile software development, IT outsourcing, cloud computing, automation of corporate processes, data protection) as well as legal advice in connection with software as a service (SaaS), data use agreements, cyber security, IT transactions and software copyright.

Professor Dirk Heckmann

Prof Dr Dirk Heckmann held the Chair of Public Law, Security Law and Internet Law at the University of Passau since 1996 before accepting an appointment to the newly established Chair of Digitalisation Law and Security at the Technical University of Munich in October 2019. His teaching and research focuses on the intersection of IT and law, in particular data protection law, IT security law, e-government, e-health and digital education. In 2003, Professor Heckmann was elected part-time constitutional judge at the Bavarian Constitutional Court, in 2007 he was appointed to the expert group of the German government's National IT Summit and in 2018 to the German government's Data Ethics Commission. He has been Director at the Bavarian Research Institute for Digital Transformation bidt since 2018 and Director of the TUM Center for Digital Public Services since 2020. From 2007 to 2021, Heckmann was a member of the board of the German Society for Law and Informatics, and its chairman from 2014 to 2021.

Dr Lorenz Marx, LL.M.

Dr. Lorenz Marx, LL.M. (KCL) is a research associate at the Chair of Law and Security of Digitalisation at the Technical University of Munich. There, he conducts research on the legal challenges of the digital transformation, in particular on issues of platform regulation, AI regulation, competition law and data protection law. Previously, he worked for several years as a lawyer in international commercial law firms.

Jakob Auer

Jakob Auer is a research assistant and doctoral student at the Chair of Law and Security of Digitalisation at the Technical University of Munich. He conducts research in a broad field of topics in the area of the legal shaping of digitalisation.

This ranges from issues in the area of e-government to platform regulation and LegalTech. The predominant focus of his research work is on data protection law, in which he is also writing his dissertation.

Thimo Brand

Thimo Brand is a research assistant at the Chair of Law and Security of Digitalisation of Prof Dr Dirk Heckmann. He deals with the interface between legal issues of digitalisation and procedural law. In addition, Thimo Brand has in-depth knowledge of intellectual property law and international civil procedure law.

Editorial collaboration

Michael Bressler, TUM Center for Digital Public Services
Jonas Hacker, TUM Center for Digital Public Services
Valentin Vogel, TUM Center for Digital Public Services
Nadine Vogt, Noerr Partnerschaftsgesellschaft mbB

Editors

Noerr Partnerschaftsgesellschaft mbB
Brienner Straße 28
80333 Munich
T +49 89 28628-0
www.noerr.com

Chair of Law and Security in Digital Transformation
Technical University of Munich
Richard-Wagner-Straße 1
80333 Munich
T +49 89 907793-301
www.gov.tum.de/elaw
www.tum-cdps.de

Alicante
Berlin
Bratislava
Brussels
Bucharest
Budapest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moscow
Munich
New York
Prague
Warsaw

noerr.com