alliuris

ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS.

Digital due diligence for company acquisitions

Ulrich Herfurth, lawyer in Hanover and Brussels

March 2025

Digital due diligence has developed into an independent, purchase price-relevant audit area in the context of company acquisitions. It supplements traditional financial and legal due diligence with a structured analysis of the digital substance of a target company. In an economy in which business models, value chains and innovation processes are increasingly driven by data and technology, the quality of digital structures is a decisive factor in determining the sustainable value of a company.

The focus of digital due diligence is therefore not only on individual IT systems or software solutions, but also on their legal protection, organisational embedding and strategic future viability.

This article examines these issues along key audit dimensions: technical and organisational IT security, the legal system for software and data, data protection and digital dependencies including cloud, outsourcing and AI structures. These areas are closely interlinked and only have an economic impact when they interact. In addition, there are the influencing factors of data rights, artificial intelligence and product liability for software and AI, especially under the provisions of the Data Act, the AI Act and the new Product Liability Directive.

Data security

Analyses of IT security show that risks often result less from a lack of individual measures than from structural deficits. Historically evolved architectures, inadequate documentation, a lack of responsibilities and a weak organisational anchoring of IT security mean that technical protective measures cannot take effect. In addition to pure defence against external attacks, resilience, restart capability and scalability of the security architecture are becoming increasingly important. Humans remain a central risk factor, both in terms of operating errors and a lack of awareness.

IP and licences

The rights system forms the legal basis of digital value creation. Unclear or incomplete licences, unsecured rights of use for individual software and the uncontrolled use of open source components can give rise to considerable economic risks. In addition, there are limited or non-transferable rights to embedded software in proprietary products. Transaction practice regularly shows that a lack of transparency regarding software and data rights leads to subsequent licensing requirements, restrictions on use or barriers to integration.

Data protection

Data protection is a liability and reputational factor in its own right. A lack of transparency regarding processing procedures, insufficient technical and organisational measures and inadequate preparation for data protection incidents significantly increase the risk of severe fines and operational restrictions. Data protection should not be seen solely as a compliance obligation, but increasingly as an expression of organisational maturity and as a prerequisite for trust-based business models.

Digital sovereignty

Digital dependencies on cloud providers, platforms and IT service providers characterise a company's long-term ability to act. Vendor lock-in effects, a lack of exit scenarios and third-country references can make post-merger integration considerably more difficult and require additional investment. The same applies to the use of AI systems, whose functionality, database and governance structures are often only transparent to the acquirer to a limited extent.

Product liability for software and AI

In addition to the regulatory requirements, product liability for software and AI systems is becoming increasingly important. The traditional distinction between product and service law is becoming increasingly blurred by software-based and learning systems. Defective software, faulty updates or inadequately trained AI models can cause considerable damage and trigger liability claims.
As part of digital due diligence, it is therefore necessary to check whether the target company is exposed to liability as a manufacturer, provider or operator and whether appropriate risk precautions have been taken. This applies in particular to quality assurance processes, documentation, monitoring and existing insurance cover. Product liability risks can have a lasting impact on the economic viability of digital business models.
The overall evaluation of digital due diligence makes it possible to identify red flags at an early stage, assess risks economically and make well-founded decisions on purchase price, contract design and integration strategy. In an increasingly digitalised economy, digital due diligence is therefore not an optional additional tool, but a key success factor for professional M&A transactions.

Liability and insurance

Another key aspect of digital due diligence concerns liability risks and their insurance coverage. Digital business models are regularly exposed to both operational and product liability risks, which are significantly increased by the use of software, data-based services and AI systems. The audit must therefore analyse whether and to what extent existing business and product liability insurance policies actually cover digital risks or whether there are exclusions for software errors, data loss or financial losses.
Specialised IT and cyber insurance policies are particularly important. IT insurance policies can cover risks from software errors, system failures, data loss or project delays, while cyber policies cover damage from cyber attacks, data protection breaches, business interruptions and crisis management costs in particular. It is important to check not only the existence of corresponding policies, but also their scope of cover, deductibles, obligations and exclusions.
Insufficient or inadequate insurance cover can lead to digital risks remaining entirely with the company and threatening its existence in the event of damage. Analysing liability and insurance structures is therefore an integral part of digital due diligence and has a direct impact on risk assessment, purchase price determination and the contractual structure of the transaction.
The overall evaluation of digital due diligence enables red flags to be identified at an early stage, risks to be assessed economically and well-founded decisions to be made regarding the purchase price, contract design and integration strategy. In an increasingly digitalised economy, digital due diligence is therefore not an optional additional tool, but a key success factor for professional M&A transactions.

Overall evaluation of digital due diligence:

The overall evaluation of digital due diligence enables red flags to be identified at an early stage, risks to be assessed economically and well-founded decisions to be made regarding purchase price, contract design and integration strategy. In an increasingly digitalised economy, digital due diligence is therefore not an optional additional tool, but a key success factor for professional M&A transactions.

Consolidation of the audit results

Digital due diligence only reveals its full added value when the individual audit fields are summarised. IT security, legal systems, data protection as well as digital dependencies, cloud and AI structures are not isolated issues, but are closely linked in functional and economic terms. Weaknesses in one area regularly have an impact on other audit dimensions and can reinforce each other.

The aim of the overall evaluation is therefore to combine the individual findings into a consistent risk assessment. This is less about determining an abstract compliance level and more about the question of whether the digital structure of the target company is sustainable, manageable and future-proof. Digital due diligence therefore provides a qualitative supplement to quantitative valuation models.

Typical red flags in digital due diligence

Digital due diligence regularly identifies certain risk patterns that can be categorised as red flags in the transaction context. The most common of these include a historically evolved, undocumented IT architecture, missing or inadequately implemented security and data protection concepts and unclear responsibilities in IT and data protection issues.

Further red flags result from a non-transparent rights system. A lack of software registers, unclear licence scopes, unsecured rights to individual software or the uncontrolled use of open source components can give rise to considerable legal and economic risks. The same applies to extensive dependence on individual cloud providers or IT service providers without realistic exit options.

Recurring risk constellations can also be observed in the area of data protection, such as incomplete records of processing activities, a lack of emergency plans for data breaches or only formal involvement of the data protection officer. Such deficits regularly indicate a low level of organisational maturity and increase the risk of fines and liability claims.

Economic evaluation and purchase price relevance

The next step is to evaluate the identified risks from an economic perspective. A distinction must be made here as to whether these are shortterm remediable deficiencies, structural deficits or fundamental limitations of the business model. While the former can often be addressed through targeted investments or organisational measures, the latter can have a lasting impact on the value of the company.

In transaction practice, the results of digital due diligence are regularly reflected in purchase price adjustments, earn-out structures or investment reservations. In particular, foreseeable subsequent licences, necessary security investments or regulatory adjustments must be taken into account in the valuation. Digital due diligence therefore provides an essential basis for determining a realistic purchase price.
Effects on contract design and risk allocation.

Effects on the transaction

In addition to the purchase price issue, the results of the digital due diligence significantly influence the structuring of the company purchase agreement. Identified risks can be addressed through specific guarantees, indemnities or covenants. Closing conditions, such as proof of certain security or data protection measures, can also be derived from the audit results.

The results can also influence the choice of transaction structure. Particularly in the case of significant legacy issues in the IT or data protection area, the delimitation of liability risks can be a decisive argument in favour of or against certain deal structures.

Post-merger integration and strategic development

Digital due diligence does not end with the closing. Rather, it forms the basis for a structured post-merger integration. The weaknesses and dependencies identified indicate the areas in which action is required immediately after the acquisition and where medium-term investments are necessary.

At the same time, the results provide indications of strategic development potential. A consolidated IT architecture, a clearly regulated legal system and a robust data and AI strategy can be further developed in a targeted manner after the acquisition and contribute to a sustainable increase in value. Digital due diligence therefore not only acts as a risk instrument, but also as a strategic compass.

Conclusion

Digital due diligence has developed into an independent and indispensable component of professional M&A processes. It combines technical, organisational, legal and strategic issues into an integrated overall assessment of a company's digital substance.
A structured approach makes it possible to recognise risks at an early stage, clearly identify red flags and make well-founded decisions on purchase price, contract design and integration strategy. In an economy in which digital structures increasingly form the core of value creation, digital due diligence is no longer a supplementary audit tool, but a key success factor in every corporate transaction.

+ + +

From the Compact Series on Digital Due Diligence:

- Digital due diligence for company acquisitions
- Digital due diligence on data security
- Digital due diligence on data rights and IP
- Digital due diligence on data protection
- Digital due diligence on data sovereignty

+ + +

The Alliuris Group

The Alliuris Group consists of 20 law firms and 400 business lawyers within Europe, Asia and America.

Contact	Ulrich Herfurth
	Alliuris Communication
Web	www.alliuris.law
Mail	info@alliuris.org
Fon	+49-511-307 56-20
Fax	+49-511-307 56-21

IMPRINT

EDITORS: ALLIURIS A.S.B.L. ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS | BRUSSELS

MANAGEMENT: Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-20, Fax +49-511-307 56-21

BRUSSELS · PARIS · LONDON · AMERSFOORT · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · MOSCOW MINSK · SOFIA · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt