Digital due diligence and data security

Ulrich Herfurth, attorney at law in Hanover and Brussels

April 2025

The acquisition of a company is no longer determined solely by financial, tax and legal parameters. With the ongoing digitalisation of virtually all business processes, information technology has become a key value driver and, at the same time, a risk factor in its own right. Production control, customer interaction, supply chain management, accounting and compliance are now heavily dependent on functioning, secure and available IT systems. Against this backdrop, Digital Due Diligence (DDD) forms an indispensable part of modern transactions.

Digital Due Diligence serves to systematically analyse the digital capabilities, security and organisational maturity of a target company. It complements traditional due diligence with a technical and organisational perspective that is increasingly relevant to the purchase price. Whilst financial metrics are history-oriented, the analysis of the IT security structure allows conclusions to be drawn about future risks, investment requirements and integration capability.

At the heart of Digital Due Diligence lies the question of whether the target company's IT is capable of supporting ongoing business operations in a secure, stable and compliant manner. In this context, it is not only the status quo that is decisive, but also the ability to respond appropriately to disruptions, attacks and regulatory changes. IT security in particular plays a key role, as vulnerabilities not only cause operational disruptions but can also result in significant liability, reputational and financial losses.

Security architecture and technical foundation

The starting point for any in-depth IT security review is the security architecture of the IT system. It forms the structural foundation upon which all technical and organisational protective measures are built. As part of digital due diligence, it must be examined whether a consistent, documented and traceable architecture exists, or whether the IT infrastructure has evolved historically, is heterogeneous and is only secured in isolated areas.

A key assessment criterion is the degree of system separation and segmentation. Modern security architectures typically follow the principle of layered defence and operate with clearly defined security zones. The separation of office IT, production systems, development environments and externally accessible systems reduces the risk of security incidents spreading unchecked. Concepts such as multi-zone models or zero-trust architectures are indicators of an increased security maturity level, even if their mere existence does not guarantee effective implementation.

In addition to the logical architecture, infrastructural aspects are of considerable importance. Securing technical connections, cables and the power supply represents an often underestimated area of risk. In particular, it is necessary to check whether internet connections are designed with redundancy, how site networks are secured, and what technical measures protect remote access by employees and service providers. A lack of redundancy or inadequately protected VPN access can lead to complete operational downtime in the event of a breach.

Equally relevant is the power supply to the IT infrastructure. The presence of uninterruptible power supplies, emergency power plans and clear restart procedures is a key factor in ensuring reliability. Shortcomings in this area have a direct impact on the availability of business-critical systems and can cause significant financial damage.

Resilience, maintainability and scalability

Beyond merely defending against external attacks, digital due diligence must assess how resilient the IT security architecture is overall. Resilience describes a system's ability to remain operational even in the event of disruptions, partial failures or security incidents. It is therefore necessary to check whether security mechanisms themselves are designed to be redundant, whether there are clear recovery strategies in place, and whether critical security components are tested regularly.

Another aspect concerns the maintainability and scalability of the security architecture. Complex, historically evolved security landscapes with a multitude of non-integrated individual solutions not only increase the administrative burden but also the susceptibility to errors. In the context of a transaction, it is therefore relevant whether security solutions can be centrally managed and whether they are compatible with the expected business growth or with integration measures.

Finally, the quality of documentation must also be assessed. Missing or outdated architecture and security documentation pose a significant operational risk, as they hinder a rapid and coordinated response in the event of a crisis. Robust documentation is therefore not only an indication of a higher level of maturity, but a security factor in its own right.

Technical and organisational security measures

The security architecture only becomes effective through the consistent implementation of technical and organisational measures (TOMs). These form the operational backbone of IT security and are a key focus of digital due diligence. It must be analysed whether such measures are systematically defined, documented and regularly reviewed, or whether they exist merely in an informal and reactive manner.

At a technical level, this includes, in particular, the use of network security components such as firewalls and intrusion prevention systems, the protection of end devices and servers by up-to-date security software, and effective patch and vulnerability management. Outdated systems, missing security updates or unsupported software versions pose a significant risk, as known vulnerabilities can be exploited in a targeted manner.

Another key focus is on backup and recovery strategies. It is necessary to check not only whether regular data backups are carried out, but also whether their recoverability is tested and whether protective mechanisms against tampering or encryption by malware are in place. Missing or inadequate backup strategies are among the most common causes of damage that threatens a company's existence following cyber attacks.

Of particular importance is the ability to detect, analyse and handle security incidents in a structured manner. Monitoring, logging and alerting systems are central elements of an effective security organisation. If appropriate structures are lacking or log data is not analysed, the majority of attacks remain undetected for extended periods. This not only increases the extent of the damage but can also lead to legal consequences, for example in the event of delayed reporting of data breaches.

Organisation, responsibilities and access policies

IT security is not a purely technical discipline, but to a large extent a matter of organisation and governance. A key focus of digital due diligence is therefore the organisational embedding of IT and information security within the company. It must be examined whether clear responsibilities are defined and whether these are accompanied by sufficient decision-making and enforcement powers.
The existence of clearly defined roles, such as a CIO, CISO or information security officer, is an important indicator, but is not sufficient in itself. What is crucial is whether security tasks are actually carried out, whether policies exist and whether compliance with them is monitored. In the absence of such a governance structure, security decisions are often made on an ad hoc basis and remain dependent on individual personnel.

Closely linked to organisational embedding is the management of identities and access rights. Authorisation structures that have evolved over time, featuring far-reaching or no longer required access rights, represent one of the greatest IT security risks. As part of digital due diligence, it is therefore necessary to check whether a structured identity and access management system exists, whether permissions are regularly reviewed and adjusted, and whether a clear separation between user and administrator rights is in place.

Critical systems and human risk factors

Another focus of the audit is the identification of particularly critical systems and data sets. These typically include ERP and financial systems, production and control systems, customer-related databases, and central cloud and platform services. These systems form the core of operational value creation and are therefore particularly worthy of protection.

Vulnerabilities in these areas have a direct impact on the company's business operations. Accordingly, it must be checked whether special protective measures are in place, such as enhanced access restrictions, separate monitoring or additional hardening measures. A lack of differentiation in security levels often indicates a low level of maturity in the IT security organisation.

In addition to technical aspects, people play a central role in the security framework. Inadequately trained staff, a lack of awareness of phishing and social engineering attacks, and unclear guidelines on how to use IT systems significantly increase the risk. Reliance on individual key personnel with exclusive system knowledge also poses a significant organisational risk. The maturity level of security awareness is therefore a key qualitative factor in digital due diligence.

Certifications, service providers and cyber security

Certifications and standards such as ISO/IEC 27001, the BSI IT-Grundschutz or industry-specific security requirements provide important indications of the formal maturity level of IT security . However, as part of due diligence, it is always necessary to check the actual scope of a certification and whether it covers the systems relevant to the business model. Certificates do not replace a substantive review of actual security practices.

External IT service providers deserve particular attention, as they often have access to critical systems or provide key operational services. Their contractual rights and obligations, liability provisions, access rights and exit scenarios must be carefully assessed. Unclear responsibilities or a lack of security provisions in service agreements can give rise to significant risks.

In addition, it must be checked whether IT or cyber insurance is in place and to what extent risks are covered. Insurance cover can reduce the potential for financial loss, but does not replace an appropriate technical and organisational security structure.

Economic significance and transaction relevance

Deficiencies in IT security can lead to production downtime, contractual penalties, fines, reputational damage and a lasting loss of trust. These risks must be adequately taken into account within the context of the transaction, for example when determining the

purchase price, through contractual guarantees or through targeted measures in the post-merger phase. Digital due diligence thus provides a robust basis for well-founded economic decisions.

Conclusion

Digital due diligence, with a focus on technical and organisational IT security, is a distinct and highly relevant area of assessment in corporate acquisitions. It enables a realistic assessment of the stability, resilience and future viability of the IT infrastructure, and allows hidden risks to be confirmed or refuted. In an increasingly digitalised economy, it is not an optional extra, but an integral part of professional M&A processes.

+ + +

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 · UTRECHT · KNOKKE · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HELSINKI · HANOVER · VIENNA · SOFIA · WARSAW · POZNAŃ · ATHENS · ISTANBUL · DUBAI ·MOSCOW · GUANGZHOU · BEIJING · SHANGHAI · NEW DELHI · MUMBAI · NEW YORK · SAO PAULO ·BUENOS AIRES · LIMA · SANTIAGO DE CHILE MEXICO CITY

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt