CORE®

DUE DILIGENCE FOR CORPORATE TRANSACTIONS IN THE AGE OF PLATFORM ECONOMY AND DIGITALIZATION

Christian Everts
Dr. Waldemar Grudzien

August 2017
COREtechmonitor | Blogpost

Key Facts

- Classic IT due diligence does not adequately cover all areas of digitization and therefore needs to be transformed into a digital due diligence
- The amount of data available as a result of digitization enables compliance risks to be identified more efficiently and in a more targeted manner for corporate transactions
- Cyber risks are becoming a risk field of their own, generating a higher necessity for cyber risk investigations

Report

Digitalization – A Transformation Process in All Economic Areas

Digitization is transforming the world as we know it. Our daily work will be challenged by increased automation (so-called Work 4.0), our production processes will be adapted to Industry 4.0, and our value chains will be broken up while platforms will enable new modular and customizable businesses.

These changes to our economic and social community, which are both evolutionary and disruptive, are becoming increasingly important it when it comes to M&A transactions. New audit and assessment fields have been designed to analyze the identified value drivers and identify risks as early as possible.

The market trends and analysis methods described below give an incomplete overview of current developments, which the CORE-institute was able to identify within the last year and which are going to be examined within the following months.

1. Transformation from IT Due Diligence to Digital Due Diligence

Already today, IT requires a substantial part of the resources related to Post Merger Integration (PMI).

As data processing and data interoperability is becoming more and more crucial, IT as part of corporate transactions will most likely become more important as well.

Considering these developments, the established components of IT due diligence need to be reviewed in terms of changes caused by digitalization and the transforming service landscape, in order to reflect the impact of digitization accordingly.

a) IT-Infrastructure

IT infrastructure analysis traditionally focus on financial information regarding the sustainability of the target's IT.

This financially-driven approach reaches its limits in an era of cloud and software-as-a-service solutions. As the age of installed

software/hardware is coming to an end, service-provider performance and contract design becoming more and more the real value drivers.

Consequently, the risks that need to be analyzed are no longer to be assessed solely in financial terms, but also legally (in the form of a service contract) and technologically.

b) Software

Software developed in-house is often the most valuable asset of young/startup companies, which makes it all the more important to review the value of this asset as part of the transaction.

i) Software as Intellectual Property

Software is usually created as a result of intellectual work of a programmer and is to be assessed as the programmer's intellectual property. Consequently, it is necessary to check whether the ownership rights to the software have been transferred to the target company.

The problem is enhanced by the increasing engagement of freelancers, who make their knowledge and expertise available through digital platforms around the world. While "normal" employees transfer their copyright (usually) to the employer, specific contractual agreements are required for freelancers, which ensure the transfer of the copyright to the contracting authority.

ii) Open Source Software as an IP Trap

Modern software programming today frequently involves the use of Free Open Source Software (FOSS) components for creating software. Using FOSS components can decrease development costs, but also involves the obligation to accept the licensing terms of the used Open Source components.

Currently, the most widespread GNU General Public License (GNU GPL) compels the user to distribute the software further in both its original and revised form. The source code of the software must therefore be disclosed and the new software has to be completely accessible to the public under the terms of GNU GPL.

At worst, the use of FOSS components can "infect" the entire software product, decreasing the chances for economic licensing.

c) Data

The era of digitization is based on market participants increasingly interacting with each other. Consequently, customers' requirements can be better determined and production processes thereby optimized. Most importantly however, all of these processes require data that can be evaluated.

Up to now, the legal framework for handling data has not been adequately clarified, as there are still some uncertainties regarding who actually owns the data and whether personal data can be owned by a company.

Furthermore, while certain regulatory frameworks, such as the General Data Protection Regulation (GDPR), create regulatory framework parameters for specific data types. Key issues like data ownership still remain legally disputed and therefore subject to legal uncertainties.

2. Digital Compliance

Similar to risk functions compliance mostly focus on the past. Following the plan-do-act-check principles, existing risk management systems focus on the identified weaknesses for closing loopholes. This backward-looking perspective is underlined by the fact that compliance functions are usually part of internal investigations once incidents have been identified, to ensure future consistency to the three-line-of-defense system.

The retrospective orientation of the compliance function often proves to be a mistake when it comes to corporate transactions; as the acquirer becomes reliable regarding the target's compliance risks as well.

This approach has proved increasingly hazardous due to the monetary risks that may result from organizational errors since contracting parties cannot protect themselves against criminal legal violations such as antitrust offenses, even by means of insurance products such as warranty & indemnity insurance policies.

In this case, modern analysis methods such as big data and predictive algorithms can help to reduce this risk dramatically.

As the business model becomes more and more digitalized, generating data and the number of available data points are steadily increasing. The combination of corporate-generated data and scientific research results from criminalistics, neurosciences, risk research, psychology and law enabling easy identification of inconsistencies and compliance risks.

The potential of modern data analytics has already been identified in certain sectors i.e. the banking industry. New market participants, such as RegTechs, are increasingly offering new, innovative solutions aimed at combating money laundering and terrorist financing, or supporting risk management in the financial sector.

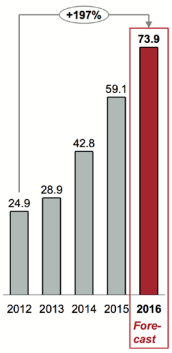
The expansion of obligated persons required due to the 4th AML Directive, which came into force on June 26, will further broaden the RegTech's potential customer group.

CORE®

Security incidents and damage to the economy continue to rise

Relevance of IT security

IT security incidents
(worldwide, all industries, m)[1]



Economic damage
(Germany, all industries, annually, EUR, bn)[2]

Direct costs …
… from plagerism, patent infringemet and loss of competition
14.7

Indirect costs …
…from loss, theft, injury, employee fluctuation, image damage, extortion
4.4

Consequential damage …
…from legal disputes, investigation and alternative measures, data protection
3.5

Nearly 55 billion Euro of negative financial impact per year
Negative financial impact in Germany (EUR, bn)[3]

	Negative financial impact (EUR, bn)
Cost of investigation and compensating measures	21,1
Revenue loss related to a loss of competitive advantage against competitors	17,1
Patent infringement (incl. before patent comes in to force)	15,4
Reputational damage against consumers and contractional partners	15,4
Litigation costs	11,0
Cancellation, theft or damage of information and production processes	10,5
Revenue loss due to plagiarism	6,9
Data protection measures (e.g. protection of client information)	6,4
Blackmailing related to stolen data or encrypted data	1,3
Other negative impacts	4,5
Total loss within the last two years	**109,6**

Sources: 1 PwC Global Security Survey 2015, 2016 | 2 Bitkom 2016 | 3 Statistisches Bundesamt 2017

3. Cyber Security

Cyber security has seen a dramatic increase of importance, not only since malware such as Wanna Cry hit the headlines by causing millions of dollars' damages.

In a recently published study, the German digital association 'bitkom' estimated that damages to the German economy sums up to 55 billion euros annually as a result of sabotage, espionage and data theft.

Even considering the fact that figures for damage related to cybercrime should always be taken with caution as they are difficult to record, there is no doubt amongst the broad community of specialists that the amount of damages (both known and estimated) that has been caused up to this point is enormous.

Examining whether a target company is up to date regarding the requirements of digitization and cyber security is, of course, difficult to evaluate, as no company voluntarily admits to being an easy target for cyber-attacks or to having weaknesses in terms of information security.

However, there are indications which make it possible to carry out an initial valid assessment:

a) Information Security and Data Protection Organization

The establishment of an effective and sustainable Information Security Management System (ISMS) is nowadays considered as a minimum requirement for companies in order to ensure information security. An ISMS (at least when in line with ISO 27001 et seq.) includes both technical and organizational components. The organizational structure is specifically important within a company, as the majority of incidents of misconduct and criminal acts are committed by employees, or at least as a result of employees being careless.

If, however, the ISMS installed throughout the company is enhanced by effective data protection compliance, and if IT security requirements are also geared towards both the BSI Standard IT basic protection catalog (modules, hazards and measures) and other best practice tools (based on the intended use), e.g. OWASP for web application, then the culmination of these factors is a good indicator of a sustainable IT security management. This involves a management system that is able to identify weaknesses and makes continuous efforts to reduce risks.

b) IT Architecture

Regardless of the organizational structure of the company, the technical design of the IT infrastructure can make a significant contribution to IT security.

But the general assumption "the more modern, the better" must not be taken as gospel; it is much more important to take the basic structure of the company into consideration.

Alignment with modern micro service architectures provides a much higher degree of security against monolithic applications. Security paradigms can already be established structurally through the IT architecture by using micro services. Examples of these include the reduction of the complexity of business logic, distributed and persistently

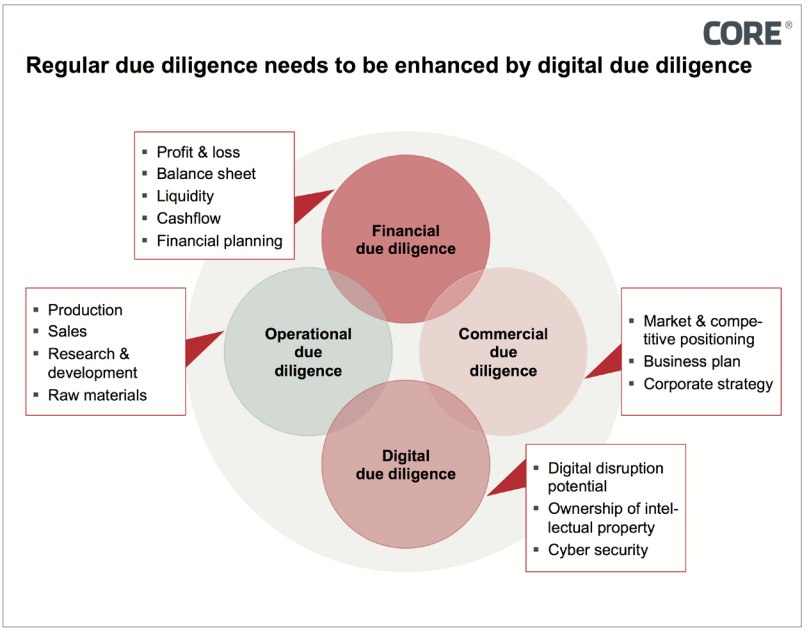
encrypted data storage/transport, and even high scalability and high availability. This means that a simple system component becoming infected is no longer enough for the system to become corrupted, but rather this is only possible as a result of independent successful attacks of several system components.

c) STEM expertise

The final decisive factor that needs to be mentioned is the company's STEM expertise. Those who possess scientific problem-solving expertise are more likely to have a "natural" ability to adequately respond to threats and even attacks, as well as develop adequate response measures and risk management systems in order to protect critical IT infrastructure.

Conclusion

The described changes reveal that digitization also creates new challenges for corporate valuation in M&A context. Corporate valuation based solely on financial, operational and commercial due diligence runs the risk to underestimate elementary valuation criteria. Nowadays corporate valuation needs to reflect the technological challenges by using enhanced analysis methods which incorporate necessary technological, operational and legal know-how.



Sources

Bitkom - Wirtschaftsschutz in der digitalen Welt 2017

Deploying Regtech Against Financial Crime - IIF 2017

Digitalisierung und das BGB – NJW 2016

Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen (IRZ 2017)

OWASP (The Open Web Application Security Project)

Regtech in Financial Services: Solutions for Compliance and Reporting - IIF 2016

Umgang mit Transaktionsrisiken – Legal Due Diligence in der Digital Economy (Expert Focus 2017)

Authors

Christian Everts is a Transformation Manager at CORE and is particularly experienced in the eld of regulation. Prior to joining CORE, Christian worked for several banks as a compliance manager, where he primarily implemented regulatory requirements in German and international investment and universal banks.

Mail: christian.everts@core.se

Christian Everts

Dr. Waldemar Grudzien is a Transformation Engineer at CORE and focused on the security regulations of the nancial industry and their technological effects on IT infrastructures. During his work at a national federation of the nancial industries he was a specialist for retail banking and banking technologies. He graduated in electrical engineering at the TU Berlin.

Mail: waldemar.grudzien@core.se

Dr. Waldemar Grudzien

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae