



White Paper Electronic Discovery.

The compliance of information management
results in major corporate benefits.

..... **T** Systems

Contents.

3	1. Introduction.
4	2. Electronic discovery.
4	2.1 The US view of eDiscovery.
5	2.2 Legal situation in Germany.
7	2.3 Status quo / The level of awareness amongst IT managers.
9	3. eDiscovery-compliant information management.
9	3.1 Current limits in in-house information management.
11	3.2 The right IT strategy helps.
13	3.3 eDiscovery for measuring the level of performance of information management.
14	3.4 Business benefits of eDiscovery compliance.
16	4. Summary and outlook.
17	5. Glossary.
20	6. List of figures.
21	7. Bibliography.

1. Introduction.

IT risk and compliance governance, business alignment, IT portfolio management and service-oriented architecture are specialist terms that every IT manager understands. However, if you ask about the importance of electronic discovery (or eDiscovery) for in-house information management, the most frequent reaction is a shrug. This ignores the fact that every internationally-oriented company with business activities in the USA must, at the latest in the face of impending legal disputes, be ready to disclose its electronic data as evidence based on “Electronic Discovery” regulations. Companies can therefore be obliged to hand over electronically stored information from the prosecuting party if this is considered to be evidence in a lawsuit.



The eDiscovery law forces the defendant company to generally hand over all requested documents to the opposing party.

Like many other provisions in the IT compliance area, the process-related requirements of eDiscovery also originate from the U.S. eDiscovery is the collection of evidence of electronically stored information set forth in the Federal Rules of Civil Procedure. This is part of an early stage of a legal dispute - the pre-trial discovery phase - in which a prosecutor can demand electronically stored information from the defendant in accordance with US civil law (Federal Rules of Civil Procedure, FRCP). The clarification of this issue relates to all relevant information (an elastic term) which can be used as evidence in court [FRCP 2009, Rule 26-b-1]. This claim can be enforced before it reaches legal proceedings [Spies 2008]. This is a tricky issue for German companies as the disclosure requirements of defendant US companies are also extended to their international organizations, e.g., to their German parent companies.

If eDiscovery is considered from the IT perspective of the defendant company, rather than from a legal point of view, this seems to be just another legal requirement to be met using the support and resources of IT, if applicable. Upon closer consideration, primarily of the many existing legal procedures, it quickly becomes clear, however, that a range of intra-company hurdles must be crossed when collecting information. For instance, browsing large quantities of access-protected data across various systems, alongside the legal usability to be checked in each individual case, is just one of the tasks to be dealt with. eDiscovery must therefore be used for checking in-house information management's efficiency and effectiveness in raising corporate success, and for implementing targeted measures.

This white paper deals with the topic of eDiscovery in detail in the following sections. First we will take a look at the generally applicable characteristics and practical consequences from a US and German point of view. Then we will present the results of a short market analysis on the level of awareness of eDiscovery amongst IT managers in the German manufacturing industry. Section 3 shows where the current internal difficulties lie when implementing eDiscovery. This is followed by an example, based on a company in the automotive industry, of how using the information-oriented IT strategy not only meets the requirements of an eDiscovery procedure but how significant contributions can be made to increasing shareholder value through suitable IT measures.

2. Electronic Discovery.

2.1 The US view of eDiscovery.

The widespread lack of awareness of the legal facts and the duty to collaborate in the pre-trial phase [K&L Gates 2008] during an eDiscovery procedure is not surprising since it was not until December 1, 2006, with the extension of the FRCP to include Rule 34-a as part of pre-trial information provision, that electronically generated and stored data (Electronically Stored Information, ESI) was affected [Thomas 2007]. The first convictions attracting media attention show that this is not just a storm in a tea cup [Applied Discovery 2009].

An eDiscovery procedure can be triggered by US lawyers, liquidators, auditors, tax inspectors or authorities. The investigations of the US Securities and Exchange Commission, for example, are based on compliance with regulatory requirements such as the Foreign Corrupt Practices Act [FCPA 1998] and the Sarbanes-Oxley Act (2002). Here the defending party is notified by a preservation letter or a discovery order. Within the context of gathering evidence or determining the facts in this "pre-trial phase" they thus receive access to diverse information, with legal protection through the FRCP.

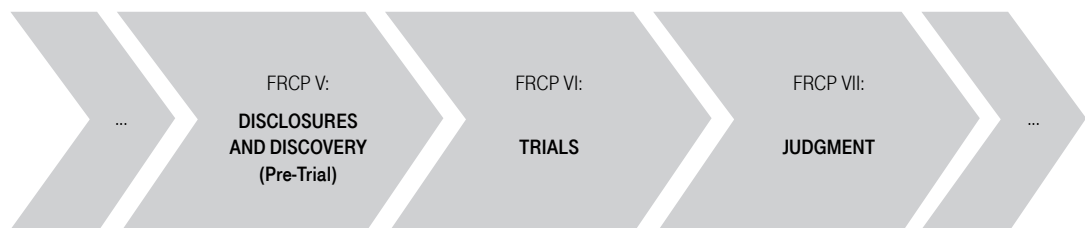


Figure 1: Workflow in the Federal Rules of Civil Procedure

Since the FRCP Rule 34-a-1-A talks of "any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations", in practice no data or information media are omitted. This means that blogs, e-mails, databases and PDAs are of no less interest than deleted data [Hilgard 2008].

What makes the process even more difficult is

- that it must be possible to access not only the final data or documents but also their history (e.g., versions at time x).
- that deliberately not storing evidence-related information or making false assertions that the information requested is not available is understood to be spoliation of evidence and is subject to sanctions (e.g., reversal of the burden of proof) [Hilgard 2008].
- that once it has become clear that a legal dispute is imminent, no data may be deleted ("Litigation Hold"), and the intentional destruction of evidence-related information will also be punished [Wilke 2007].

In brief, for the defendant in the US legal space, it must first of all be possible to call up all digital information during the relevant period under review.



Deleting, withholding, failure to find or changing requested information is severely punished in court.

The costs arising for prosecutors, defendants and judges for collecting, viewing and assessing the requested information alone quickly exceed the actual amount involved in the case. There is now talk of a “deluge” which will paralyze US civil courts and cost large companies several million dollars [Economist 2008].

2.2 Legal situation in Germany.

For German companies with transatlantic business activities, it is important to consider that the above-mentioned aspect of an eDiscovery procedure covers companies based in the USA but essentially also involves information which is located in associated parts of the company (e.g., subsidiary or parent company) abroad (e.g., Germany). These are companies registered on the New York Stock Exchange which are directly active in the US market with sales, development or production units or which maintain indirect business relations with these units, e.g., as suppliers.

Rath and Klug answered no to the question of whether German authorities can be committed to administrative assistance by US bodies. International cooperation agreements such as the Hague Convention on gathering evidence abroad cannot be applied to an eDiscovery procedure due to German reservations, either. There is also no direct “duty for German companies to cooperate” [K&R 2008]. Finally, Germany has a different legal system which is based on an entirely different understanding of how to deal with data.



Companies support eDiscovery because they are afraid of sanctions, even though US legislation is not effective in Germany.

However, in order to do justice to American and German interests, compromises are being sought at a European level via the “Article 29-Work Group” [EC 2009]. An initial working paper has been announced for February 2009 which should contain recommendations for handling American/European eDiscovery procedures. On an international scale, working group 6 of “The Sedona Conference” has also dealt with this issue as an interdisciplinary association of top-notch legal experts, university graduates and IT experts [Sedona 2008].

Practice, however, shows that German companies comply with US requests [Spies 2008]. Due to lack of know-how in dealing with American compliance topics, German decision-makers often react inadequately in critical situations [Tsolkas 2008]. A common reason is the fear of sanctions. If data or documents which could be used as evidence in an action of deceit are modified, deleted or hidden, this will be punished in the USA with up to 20 years imprisonment in accordance with the Sarbanes-Oxley Act § 1519. However, to reduce in-house costs, some companies are offering an overall package, thus giving the opposing party more information than requested. The associated disclosure of company secrets which are not case-relevant is often an undesirable side effect.

The problem with this data transfer is, however, not so much the process itself but the fact that in Germany the various laws stipulating the storage of special information also strictly regulate their use (see Figure 2). This concerns personal data in particular, e.g., in e-mails, phone calls, SMS text messages, and blogs. The response to current cases of data misuse at Landesbank Berlin, Deutsche Telekom or Deutsche Bahn show how sensitively data protection must be handled in Germany in order to avoid a devastating loss of image. Without the timely involvement of data protection officers and legal experts, German companies should therefore refrain from supplying electronic information from Germany for eDiscovery procedures in the USA.

Law	Example
German Commercial Code (Handelsgesetzbuch, HGB)	§257: Retention of documents. Retention periods
German Tax Code (Abgabenordnung, AO)	§147: Regulations on the retention of documents
German law on the new regulation of telecommunications monitoring and other determination measures covered and on the implementation of Directive 2006/24/EC	Data retention
German Telecommunications Act (Telekommunikationsgesetz, TKG)	§113a: Duties to store data
German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)	§29: Commercial data collection and storage for transfer purposes
German Works Constitution Act (Betriebsverfassungsgesetz, BVerfVG)	§87 No.6: Co-determination when dealing with e-mail and Internet usage
German Penal Code (Strafgesetzbuch, StGB)	§274 Para.1 (2): Penalty for non-permissible handling of evidentiary data
German Code of Civil Procedure (Zivilprozessordnung, ZPO)	§142: Arrangement of file transfer

Figure 2: Excerpt from German laws on dealing with data and documents

Since we all know that ignorance does not protect us from punishment and that we should be familiar with the regulations of the market in which we act, preventive action is the name of the game. However, the prerequisite is that the need for action is recognized to begin with, followed by implementation in accordance with current legislation. Above all, a level-headed and qualified response is expected from IT managers who play an important role in gathering and providing the requested information in an eDiscovery scenario.

Alongside specialist lawyers, they are supported primarily by solution providers from the service and software sector who now affix the “eDiscovery-compliant” label to their products, following the hype surrounding Basel II and the Sarbanes-Oxley Act. Consequently, solutions are being offered on the market again before the potential customers have even understood the problem [Gartner 2007], as is also shown by the results of the following survey on the level of awareness of eDiscovery.

2.3 Status quo / The level of awareness amongst IT managers.

The extent to which the company and its IT bosses are informed about the topic and are familiar with the possible consequences, as well as which preventive measures they have started, remained unclear in the run-up to this article due to a lack of reliable and current field data. For this reason, in December 2008 T-Systems started a first selective survey of 51 German medium and large-sized enterprises with business relations in the USA and a revenue of over EUR 200 million. A second survey of another 100 companies planned for January 2009 was shelved due to the clear trend of the first survey's results.

The high return rate of 34 % within two working days indicated a high level of interest. 23 companies answered in total that corresponds to an overall return rate of 45 %. 70% of the completed questionnaires came from automotive suppliers, 13% from machine and plant construction companies and the remaining 17% from companies in the industry and retail sector.



IT managers of international groups must deal with eDiscovery since ignorance does not protect from damage.

On the assumption that IT owners are aware of IT-relevant discussions within the company, they were asked about the role of eDiscovery in their respective enterprises. In the final evaluation, 61 % currently do not see that eDiscovery is important for their company, and 39% of companies have plans to develop expertise in this area (see Figure 3). However, none of the companies has employees outside the IT departments who work intensively on the topic.

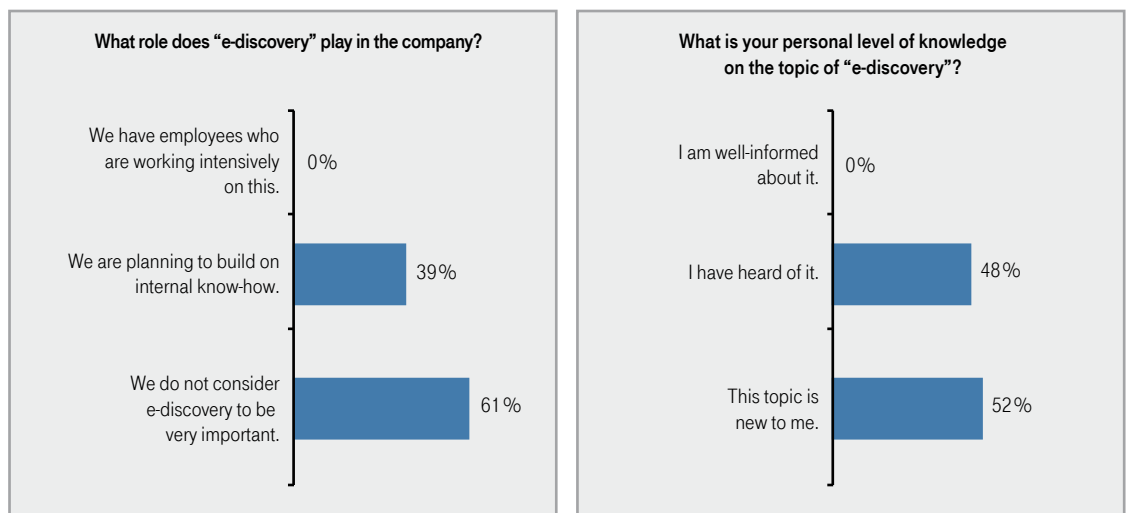


Figure 3: The role of eDiscovery in the company (source: T-Systems)

When asked about their personal level of knowledge, 52% of the CIOs or IT managers questioned said that the topic was new to them. 48% had at least heard something about it. One CIO of a global automotive supplier was very well informed about eDiscovery but did not want to be included in the statistics – he is currently involved in an investigation at one of his US sites. He also anticipated that, depending on the situation, one of two legal opinions will be pursued: finding either all or nothing.

The general lack of awareness is not surprising, considering how - especially in the IT sector - old concepts are constantly being sold as something new using fancy alternative terms. As a consequence, 83% of the CIOs surveyed in the IT areas did not have any experience of what they should do in the case of eDiscovery either. 13% of IT departments understood the risks and have started to develop appropriate IT expertise. A few CIOs (4%) who had heard of the topic already have staff who are working intensively with eDiscovery.

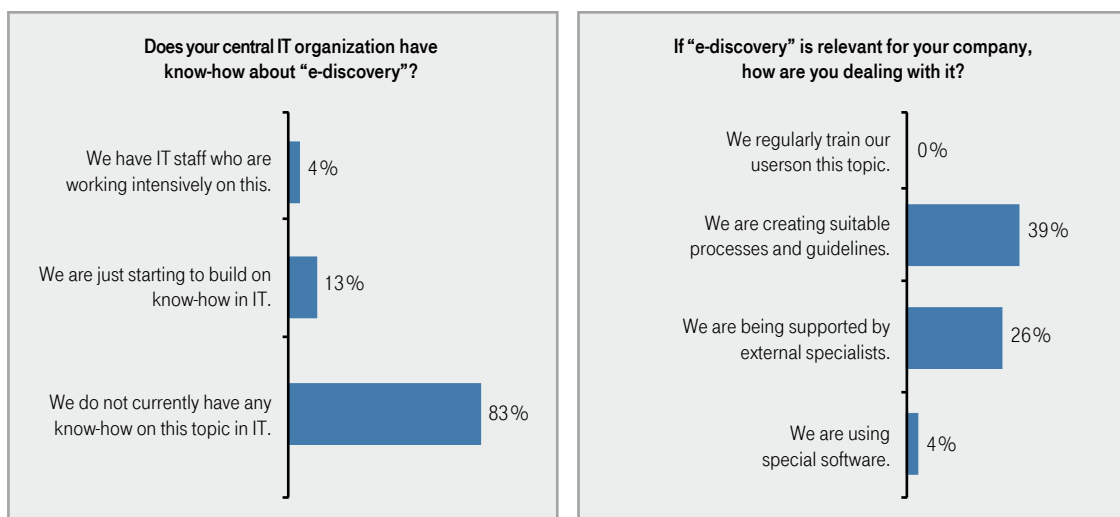


Figure 4: Preventive measures (source: T-Systems)

When asked how they tackle the subject of eDiscovery if it is relevant to their company, the majority of those questioned (39%) mentioned adjusting their internal workflow organization (processes and guidelines) and 26% said they also get support from external specialists. The fact that only 4% use eDiscovery software points to different conclusions: either the IT managers do not see any need for action or special software with eDiscovery-related functions is not seen as an adequate solution. It is also possible that the sales arguments of the software manufacturers have not made it all the way to the IT departments yet. It is also astonishing that none of the IT managers trains his users on how to use eDiscovery. However, as it is precisely their data and information which is subject to close examination in an eDiscovery scenario, the awareness of compliance-related topics must be raised accordingly.

In summary, it can be stated that among the group of companies questioned, the topic of eDiscovery was largely unknown up until the end of 2008. Preventive measures for emergencies are missing, as is relevant know-how on how to deal with eDiscovery scenarios on a case-by-case basis.

3. eDiscovery-compliant information management.

3.1 Current limits of in-house information management.

In addition to legally correct conduct, the basic task is collecting the information requested in the required scope, assessing it as regards its relevance, and making it available to the opposing party.

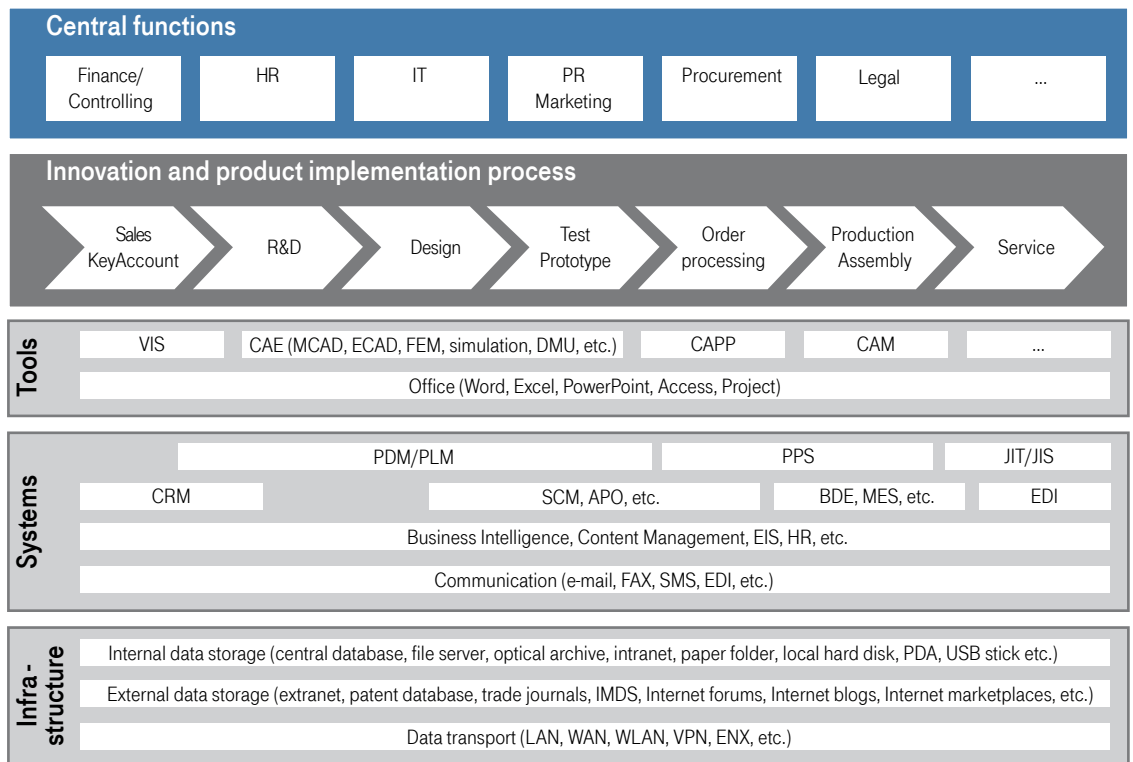


Figure 5: Example of the system environment of an automotive supplier

The first step of collecting information is one of the main problems here. If, for example, we consider the IT environment of an automotive supplier (see Figure 5), there are various hurdles along the value chain which must be overcome:

- The central and specialist departments partly work locally and partly across countries. Even if the trend is going towards data management systems integrated across the company, a large amount of information is stored locally (e.g., on PCs/laptops) and offline (digitally on CD/DVD) or, in the least ideal case, even recorded analog on paper.
- Information on one and the same patent, project, product or customer process (e.g., order, complaint) is saved and processed in different systems (e.g., sales information system, CAD, PLM, ERP) with various access controls. A product often has different names or identifiers depending on the owner (e.g., constructor, buyer, production engineer) or national language.

- Search routines generally record metadata or information in the file name. Information for which a search is being carried out is, however, kept within the digital documents (e.g., CAD drawings, graphics, video recordings, test reports, e-mails). These files are normally saved in a format which can only be read by the program in which they were generated. If they are managed by a document management system or on a file server, they can only be opened with appropriate authorization.
- Enterprises in the automotive sector (manufacturers and suppliers) in particular work closely together across companies as part of collaborative engineering (CE). In all phases of the product development process, rapidly increasing volumes of data and files are exchanged between partners on all possible communication paths and platforms, saved redundantly, logged and passed on, having been modified, at various points in time. The question as to what level of information was known to which user at a specific time can only be answered following extensive investigations.
- Information changes over time, both in terms of its content (e.g., through increasing level of maturity in pre-development, testing and production), and in terms of its importance (e.g., resulting from new test reports, market analyses or risk assessments). Rules (policies) on what statuses at what point in time information must be definitively saved or deleted are not in place, not known to the user or not designed to fit individual or situation-specific requirements.
- IT systems save their information in specified or adapted database structures. The standard search functions hence only support the syntactical call-up of predefined paths within the system and fail as soon as syntactical and semantic relationship knowledge is of interest beyond the system boundaries. In German, the syntactically clear word “Bank” can, for example, be semantically understood to mean a “financial institution” or a “bench”. The high number of hits on Google which have low relevance to the results illustrates this problem.
- The volume of information saved by a global company is rapidly increasing. The BMW Group, for example, is planning to increase its global backup volume from 2.8 to 7.6 pentabytes between 2008 and 2013. This corresponds to a growth of 270% within 5 years. If the infrastructure performance does not develop at the same pace, the time spent on searching for information increases in accordance with the higher volumes of information stored.
- Automated information storage by IT systems is not only technically restricted by its maximum storage capacity, but also expensive when it comes to subsequent backup and archiving. The cost of online availability of saved and redundantly backed up data (as backup or managed storage) must currently be calculated as around EUR 800 per terabyte per month. The basis for this total-cost-of-ownership calculation is a managed storage environment with a capacity of 50 terabytes. For this reason, it is understandable that there are high restrictions on storing data securely.

The company-wide search for information on a special issue, key word or time-related event can, for the above-mentioned reasons, only be triggered manually by appropriately qualified staff. The result of collecting information is a conglomeration of digital and analog data, documents, minutes, e-mails, database extracts, etc.



The information management systems of German automotive suppliers cannot efficiently and effectively meet the requirements of eDiscovery.

In a second step, this flood of information is to be structured, analyzed for its actual relevance and matched against applicable data protection provisions and corporate interests. The resulting costs are huge and cannot normally be borne by the relevant companies alone. A number of providers and organizations have now established themselves on the market to provide support. The offer ranges from methodical procedures and data exchange formats [EDRM 2009] to software solutions and electronic evidence backup from the computer forensics area [Kern 2005] through to professional legal or IT-related eDiscovery consulting. The problem persists, however, that by the time these services have been commissioned, the damage is already done.

In the Web 2.0 age, the huge manual effort required for a context-based evaluation of company-wide, digital knowledge is quite astonishing, considering that the need for structured information provision should not be anything unusual. This becomes clear if you exchange the hostile initiator of an eDiscovery phase with an internal company employee, for example a representative from management, auditing or product development. These and other people are required to make corporate decisions on a daily basis based on full and current information. Corporate practice shows that the opposite applies: Overflowing e-mail systems after a vacation, a flood of useless information from the Internet, corporate changes, staff turnover as well as cost pressure and fierce competition on the market. All these issues must first be overcome, which means that there is ever less time left to strategically develop information in the company as a business management resource [Schmid 2008].

3.2 The right IT strategy helps.

As shown above, it does not make any difference in practical terms whether a company or its IT is prepared for a legal eDiscovery dispute or not - the content-related requirements still remain. The task of searching for and assessing all the relevant information for a special case from various sources should be a routine exercise in everyday internal work. The new topic of eDiscovery should hence be used to re-shift the focus to the original task of an IT function, i.e., to provide employees with information in the best possible way. Due the complexity of the matter, the solution can only be found in a strategic, preventive approach. The structural starting points and arguments for this stem from the discussion on IT strategies.

This discussion describes the long-term target status of information provision, the way to achieve it, the dependencies and the consequences, hence ensuring that the corporate strategy and corporate targets are supported [Schmid 2008]. Normally, the external and corporate requirements are geared to defined IT targets, IT organization, IT processes, IT systems and the applications, as well as to the required IT infrastructure (see Figure 6).

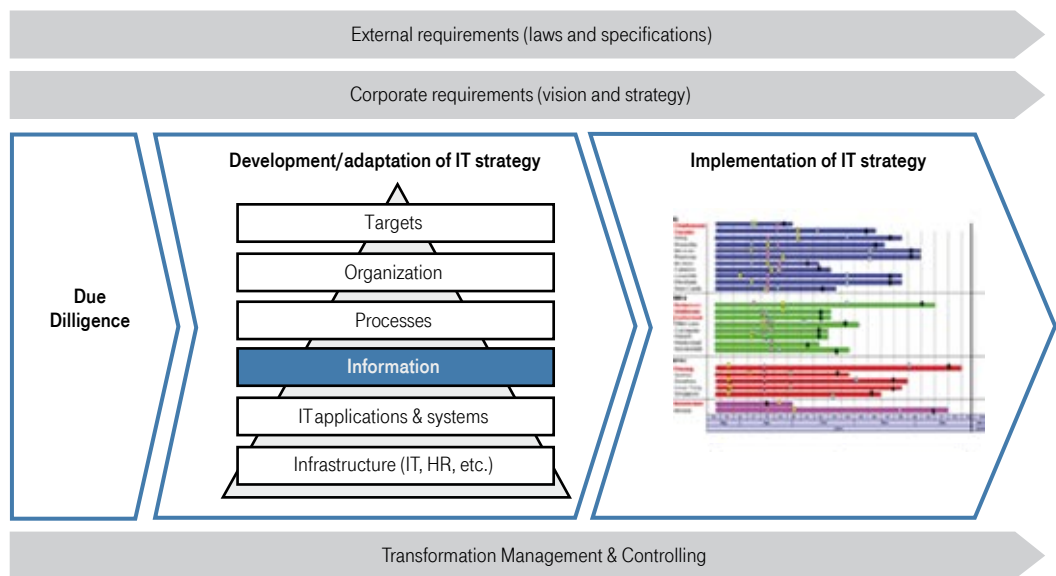


Figure 6: Components of an IT strategy development

The often neglected level of information, also known as the corporate data model [Scheer 1995], however, includes the central data objects, their static and dynamic variants and their mutual relationships. It is the valuable knowledge which exists outside the heads of employees and survives many technical and human changes. Even in the current economic situation, the strategic IT discussion should not just involve the reduction of IT costs. It must cover much more, including what information is required to optimally control business processes (data hygiene), and how the IT systems need to be structured so that information can be generated, modified, saved, found again and reused without any losses (data technology).

The most promising approaches in this context are the following:

- Standardized specifications on using IT resources (e.g., using e-mail, Internet, software for business use only) and continual training of users in data management and the requirements of governance and risk-management compliance [ITGI 2006].
- Company-wide standardization and harmonization of IT processes (e.g., based on ITIL or ISO 17799/27002), systems (primarily PLM, ERP), applications (e.g., Office, e-mail) and infrastructure components (e.g., data centers, servers, archives).
- Data integration via open, service-oriented system architectures (SOA) and standardized interfaces (e.g., XML, STEP).

- Definition and implementation of company-wide rules for standardized master data management (e.g., product, customer and supplier information) and related authorizations. This also includes indexing and classification of unstructured knowledge, e.g., via virtual repositories.



The objectives of information management - standardization, harmonization and integration - must be pursued even more intensively.

- Setup of a company-wide, standardized Identity Management System (IMS) for managing the identities and access rights of IT users, taking into account sociological, legal and technical general conditions [ULD-i 2003].
- Automation of data storage via suitable archive systems and effective destruction of data based on legal data retention duties [Hilgard 2007] and the remaining information value at a given time (x).
- Automation of report tasks (e.g., via business intelligence systems) and integration of modern search technologies (e.g., Autonomy).

Even if these approaches are state-of-the-art, years will pass before they are introduced across all companies and used confidently by employees.

3.3 eDiscovery for measuring the level of performance of information management.

The ability to meet the requirements of an eDiscovery procedure, also referred to as eDiscovery compliance, can however also be determined without any external initiation. A CEO or chairman would only have to instruct his IT owners, as part of an internal IT audit, to gather all cases and documents a former employee has worked on in the last six months (e.g., passing on insider knowledge when changing jobs as in the case of Daimler versus Younessy [Younessy 2008]). Or he can request all e-mails, agreements, development and test reports, documentation as well as publications and presentation documents on a patent dispute over an innovative new product (as in the case of Baxter Healthcare versus Fresenius 2008 [Baxter 2008]).

In order to meet the requirements for measuring the performance of in-house information management, a methodical procedure should be used. This requires, as a minimum:

- a clear specification of the search request (e.g., what information is being searched for, and what is not; criteria for relevance, time period),
- the search area to be specified (e.g., all locations, all file servers, ERP and e-mail systems),
- a quality assurance function for assessing completeness (e.g., through specifically “hiding” a relevant document, an e-mail or a set of data), and
- determining the structure of the results documentation and visualization (e.g., in full or summarized and referenced; original formats or generated standard format).

Duration of information acquisition and relevance of the result would be reliable parameters for measuring the performance and efficiency of in-house information management (IM). Carrying out such exercises regularly means that problem areas or deficits can be identified very quickly and that sensible measures can be worked out. This provides an opportunity to reasonably allocate IT budgets in the long-term. According to [Galdy 2007], even higher IT investments would then pay off.

3.4 Business benefits of eDiscovery compliance.

As with every investment decision, the question naturally arises as regards eDiscovery as to how the company will benefit operationally and economically from orienting its IT-related investments towards the specific eDiscovery requirements of a company-wide information management system. The answer with respect to the operational benefits can be found in a causal argumentation chain between the general requirements of information management, the resulting eDiscovery-compliant measures and their impact and results. These argumentation chains are illustrated in Figure 7. The requirements for information management can be sub-divided into general and eDiscovery-related requirements. A second structure level results from the viewpoint of those enforcing the requirements: corporate management, IT users or the IT specialist department. Every requirement can be realized using a range of measures or activities which impact on one or several areas within the company. Last but not least, the benefits define the scope of the impact in terms of money, time and/or quality.



Investing in meeting the requirements of eDiscovery offers significant business management benefits.

The argumentation chains in Figure 7 show an example of how a company can achieve conformity with laws and provisions through various measures. The following measures have a direct influence on the implementation and results of eDiscovery procedures:

- Call for IT governance and IT strategy.
- Creation of internal guidelines and work instructions for implementing legal requirements (e.g. “Litigation Hold”, see Section 2.1).
- Use of modern search technologies and report systems.
- Structured information archiving in central systems (ERP, PLM, etc.).
- Process for automated data destruction taking into account legal specifications on data retention (see Section 2.2.).
- Company-wide identity management system.
- Storage, backup and archive management.
- Regular training of users in dealing with legal provisions (primarily data protection, data retention).

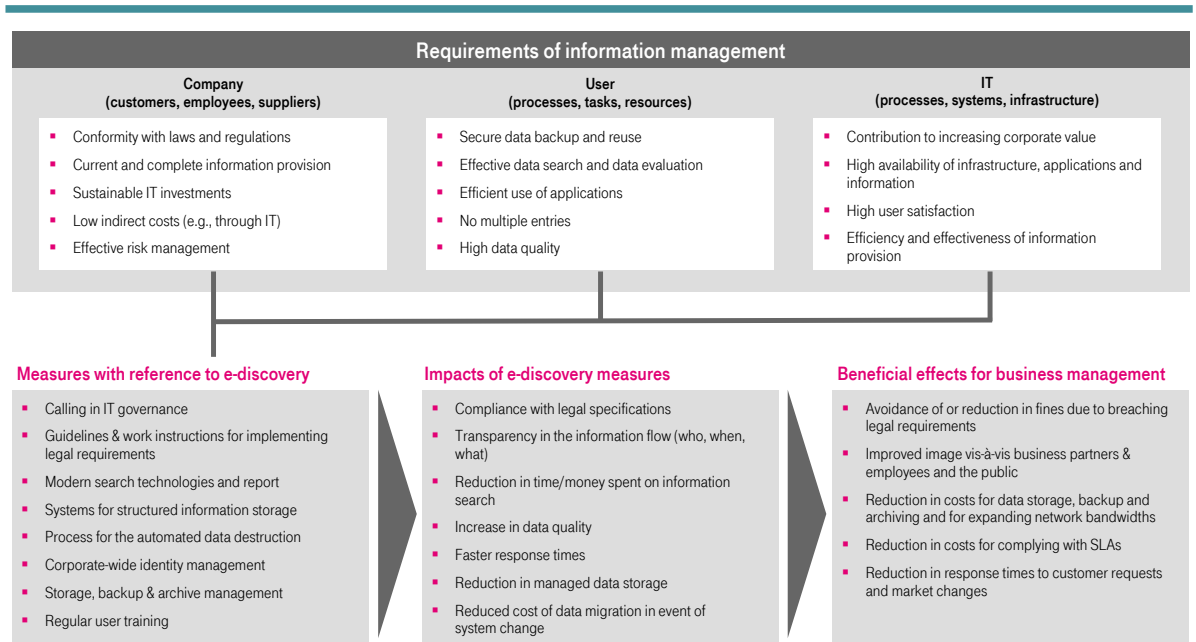


Figure 7: Business management benefits of eDiscovery-compliant information management

In the example of the measure “Process for automated data destruction”, various impacts can be forecast:

- Compliance with legal specifications on data storage will be systematically ensured.
- It reduces the volume of the required primary storage, the secondary backup and the digital long-term archive.
- As a reduced data volume must be combed through for its compliance with the criteria of search requests, the time spent on the information search is reduced (shorter duration with same infrastructure performance) in an eDiscovery scenario.

Different benefits in terms of quality can be derived from these impacts. Systematic compliance with eDiscovery rules helps avoid fines due to breaching legal procedural requirements, and prevents a negative image vis-à-vis the public, business partners and in-house staff. Furthermore, the accompanying reduction of “managed storage” does not just lead to reduced costs for data storage, backup and long-term archiving, but also to the longer usage of existing bandwidths in the data lines between the company locations. It is easy to calculate from the numerical examples in Section 3.1 that the cost drivers of storage and bandwidth can involve a great deal of money.

While the effects mentioned can be attributed to eDiscovery compliance, the corporate benefits can also be noticed in other areas. It takes less time to perform business processes (e.g., request/order process). The increased up-to-dateness, reliability and availability of data at the time of the offer is reflected in the offer/order hit rate and in the positive result of subsequent order cost accounting. Likewise, the increased satisfaction of users with their IT environment can be measured.

4. Summary and outlook.

As has been shown, in a pending procedure in the USA, the defendant company can be intensively involved in gathering evidence during the eDiscovery phase. The consequences of incorrect information being provided or unprofessional conduct are extensive. Even though German companies with business relations in the USA may be affected, as shown in the short study mentioned, eDiscovery is not very well known amongst the IT managers surveyed. Even if there is no eDiscovery trial pending, a large number of rulings give sufficient reason to look into the topic, primarily if a company is active on the US market. . What is much more interesting from an IT manager's point of view is the attempt to act out an eDiscovery procedure in practice on his own initiative. The experience gained, combined with adequate IT portfolio management [Zimmermann 2008], can be used directly for a strategy designed to improve information management.

The IT-related side of eDiscovery will also become much more important in the future, even without any legal pressure. The increase in information in companies is vast. In spite of this, the necessity for sustainable IM, partly due to time pressures and often also due to a lack of money, is still being ignored. Here the requirements of eDiscovery on IM can be used to derive sufficient measures, the impact of which is directly noticeable in cost savings, improvements in the quality of information management and faster processes.

Some initial response is also coming from IT system providers. Dassault Systems, one of the world's leading providers of software and services for product development, can be named as a positive example in the jungle of providers. This company has now equipped its new V6 PLM platform with a new search engine [Dassault 2007]. Specialists in the long-term archiving area are also looking for new solutions designed to counteract the digital, archiving nightmare [Warnke 2008].

If we take a look at the future, new cloud computing architectures will be used whereby software programs, storage space and computer performance are made available to the user online as required. However, the question of how information will be found in the long-term as part of electronic discovery should be made the subject of new research projects already today.

5. Glossary.

BASEL II	Basel II refers to all regulations on equity proposed by the Basel Committee on Banking Supervision over the past few years. The use of these regulations has been mandatory in the Member States of the EU for all banks and financial service institutions since January 1, 2007.
Business Alignment	Reciprocal agreement on objectives, strategies, architectures, services and processes between IT areas and specialist areas in the company.
CAD	Computer Aided Design (CAD) describes the creation of construction documents for mechanical, electrical or electronic designs with the help of special software.
CIO	The Chief Information Officer (CIO) is generally responsible for the tasks relating to the strategic and operational management of information technology (IT) in the company.
Collaborative Engineering	Processes, workflows and organization of cross-company collaboration in product development processes (e.g., in the automotive industry).
Compliance	All reasonable measures which form the basis for the legally-compliant conduct of a company, its organizational members and its employees with respect to legal requirements and bans.
Computer forensics	Computer forensics (also referred to as IT forensics) covers investigating suspicious incidents concerning IT systems as well as establishing the facts and the offender by recording, analyzing and evaluating digital traces in computer systems.
Corporate Governance	Definition of and compliance with rules of conduct - via legislators, owners, employees, supervisory or administrative boards, management, business partners or other interested parties - which apply for the employees of a company or the company itself.
CRM	Customer Relationship Management (CRM) describes the procedure and technologies with which the relationship between the customer and supplier can be mapped.
EDMR	Electronic Discovery Reference Model
ESI	Electronically Stored Information
ERP	The term "Enterprise Resource Planning" describes the corporate task of using the resources available in a company (capital, equipment or staff) efficiently for the operational process.

FCPA	The Foreign Corrupt Practices Act (FCPA) of 1977 is a Federal law in the USA which obligates all companies listed on the stock exchange to create documents which document transactions accurately and truthfully. In addition, every company listed on the stock exchange is obligated to have an adequate internal finance system
FRCP	The Federal Rules of Civil Procedure (FRCP) describe the procedure according to which a civil suit takes place in the USA.
IM	In the context of this article, Information Management (IM) is understood to be the sum of all activities used to create, manage, save, search and reuse information (data and documents).
IMS	Identity Management Systems (IMS) are used to administrate and describe identity features. Identity management describes the targeted and deliberate dealing with identity, anonymity and pseudo anonymity. A personal identity card is an example of a form of identification specified by the state.
ISO17799/27002	International standard which includes control mechanisms for information security.
IT Governance	Comprises management, organizational structures and processes which ensure that IT supports the corporate strategy and objectives.
ITIL	The IT Infrastructure Library (ITIL) is a collection of good practices which describe a possible implementation of IT Service Management (ITSM) and apply internationally as a de-facto standard. These rules and definitions describe the processes, tools and structural organization needed to operate an IT infrastructure.
IT Portfolio Management	IT Portfolio Management is the operational planning and management of IT systems, IT solutions, interfaces and entire IT architectures based on economic criteria.
Litigation Hold	In court, a litigation hold refers to the tracing evidence procedure referred to as Discovery in the USA, which is essentially just an obligation to carry out data backups for trial purposes. With electronic media, we talk about eDiscovery with specific legal and factual security precautions.
Pentabyte	Unit for specifying the quantity of data which corresponds to 1,000 terabytes.

PDA	A Personal Digital Assistant (PDA) is a compact, portable computer which, alongside many other programs, is mainly used for personal calendar, address and task management. PDAs can also be used to edit Office files.
PLM	Product Lifecycle Management (PLM) covers all strategic, organizational and technical IT measures for company-wide, innovation-driven management of all product-related information throughout the product lifecycle, from the initial idea through to recycling.
Preservation Letter	Written paper sent to the defendant at the beginning of the trial in which he/she is requested to ensure specific evidence
Pre-trial phase	Legal preliminary proceedings or pre-trial discovery before a possible trial.
SOA	Service-Oriented Architecture (SOA) is a management concept which only requires a system architecture concept in a second step. This concept aims for an infrastructure geared towards relevant business processes which can quickly respond to modified requirements in a business environment.
SOX	The Sarbanes-Oxley Act (SOX) is a US capital-market law that came into being in 2002, according to which all companies listed on U.S. stock exchanges must have their internal control system (ICS) checked, documented and certified by auditors.
STEP	STEP (STandard for the Exchange of Product model data) is a standard for describing product data. This description covers physical and functional aspects of a product. STEP is suited for data exchange between different systems and is formally defined in ISO standard 10303.
Terabyte	Unit for specifying the quantity of data which corresponds to 1,000 gigabytes.
TCO	Total Cost of Ownership (TCO) is a cost/calculation procedure and is used to help consumers and companies to estimate all costs incurred from capital goods such as software and hardware.
US-Securities and Exchange Commission	Institution responsible for monitoring securities trading in the USA.
XML	The extensible markup language (XML) displays hierarchically structured data in the form of text data which is used, e.g., for exchanging data between computer systems, especially via the Internet.

6. Table of figures.

Figure 1:	Workflow in the Federal Rules of Civil Procedure
Figure 2:	Excerpt from German laws on dealing with data and documents
Figure 3:	The role of eDiscovery in the company (source: T-Systems)
Figure 4:	Preventive measures (source: T-Systems)
Figure 5:	Example of the system environment of an automotive supplier
Figure 6:	Components of an IT strategy development
Figure 7:	Business management benefits of eDiscovery-compliant information management

7. Bibliography.

- [Applied Discovery 2009] Keyword search “Electronic Discovery”, Applied Discovery Online Law Library, Jan.10, 2009
(<http://www.aplieddiscovery.com>)
- [Baxter 2008] Baxter Healthcare Holding, Inc. v. Fresenius Medical Care Holding, Inc. , WL 4547190 (N.D. Cal. Oct. 10, 2008), 2008
- [Dassault 2007] Dassault Systèmes chooses Autonomy Technology for its Future ENOVIA PLM Enterprise Search Capabilities, Dassault Systems, 2007
(<http://www.3ds.com/news-events/press-releases/release/1546/1/>)
- [Economist 2008] The big data dump - A deluge of electronic information may overwhelm American civil justice, The Economist, August 28, 2008
(http://www.economist.com/business/displaystory.cfm?story_id=12010377)
- [EDRM 2009] Electronic Discovery Reference Model XML Interchange Format (o.j.), Jan. 10, 2009
(<http://www.edrm.net>)
- [EC 2009] The European Commission – Justice and Home Affairs (o.J.), Jan. 10, 2009
(http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)
- [FRCP 2009] Federal Rules of Civil Procedure (o.J.), call-up on Jan. 10, 2009,
(<http://www.law.cornell.edu/rules/frcp/>)
- [FCPA 1998] Foreign Corrupt Practices Act, 1998
(<http://www.usdoj.gov/criminal/fraud/fcpa/>)
- [Galdy 2007] In IT investieren heisst Kosten senken, Alexander Galdy, 2007
(<http://www.cio.de/strategien/methoden/838162>)
- [Gartner 2007] Key Issues for Electronic Discovery, Debra Logan, Whit Andrews, John Bace, Gartner Press from Mar. 12, 2007 (ID number: G00146630), 2007
- [Hilgard 2007] Archivierung und Löschung von eMails im Unternehmen, Mark Hilgard, Zeitschrift für Recht (21/2007), 2007
- [Hilgard 2008] Electronic Discovery im Schiedsverfahren, Mark Hilgard, SchiedsVZ (3/2008), 2008
- [ITGI 2006] Board Briefing on IT Governance, 2nd Edition, IT Governance Institute , Jan. 18, 2006
(<http://www.itgi.org>)
- [Kern 2005] Computer Forensik – der Datenmanipulation auf der Spur, Reinhold Kern, MONITOR Kommunikation (4a/2005), 2005
(<http://www.monitor.co.at/index.cfm/storyid/7448>)

- [K&L Gates 2008] Electronic Discovery Case Database, K&L Gates, 2008
(<https://extranet1.klgates.com/ediscovery>)
- [K&R 2008] eDiscovery in Deutschland, Michael Rath und Saskia Klug, K&R Kommunikation & Recht (10/2008), 2008
- [Scheer 1995] Referenzmodelle für industrielle Geschäftsprozesse, August-Wilhelm Scheer, Springer-Verlag, 1995
- [Schmid 2008] Post Merger Integration: Ohne IT geht nichts!, Claus Schmid und Steffen Dahlberg, Mergers and Akquisitions Review (Book 11/2008, p. 520 et seq.), 2008
- [Sedona 2008] The Sedona Conference, 2008
(<http://www.thesedonaconference.org>)
- [Spies 2008] Auswirkungen der elektronischen Beweiserhebung (eDiscovery) in den USA auf deutsche Unternehmen, Axel Spies und Christian Schröder, Redaktion MultiMedia und Recht, 2008
- [Thomas 2007] Litigation in the Age of the Terabyte: The 2006 eDiscovery Amendments to the U.S. Rules of Civil Procedure, Peter Thomas und Gabriel Rottmann, DAJV-Newsletter (1/2007), 2007
- [Tsolkas 2008] Electronic Discovery – schon dagegen geschützt?, Alexander Tsolkas, Computerwoche from Jun. 8, 2008
- [ULD-i 2003]. Identity Management Systems (IMS): Identification and Comparison Study, Independent Centre for Privacy Protection, Unabhängiges Landeszentrum Für Datenschutz Schleswig-Holstein und Studio Notarile Genghini, 2003
(<http://www.uld-i.de/gutachten/idm/>)
- [Warnke 2006] Digitale Archive, Martin Warnke, IIE aktuell (Nr. 29), January 2006
- [Wilke 2007] Lösch! Mich! Nicht!, Katja Wilke, Financial Times Deutschland, Feb. 27, 2007
- [Younessi 2008] Daimler Truck N. Am. LLC v. Younessi, WL 2519845 (W.D. Wash. June 20, 2008), 2008
- [Zimmermann 2008] Governance im IT-Portfoliomanagement, Steffen Zimmermann, Wirtschaftsinformatik (5/2008, p. 357-365) 2008

