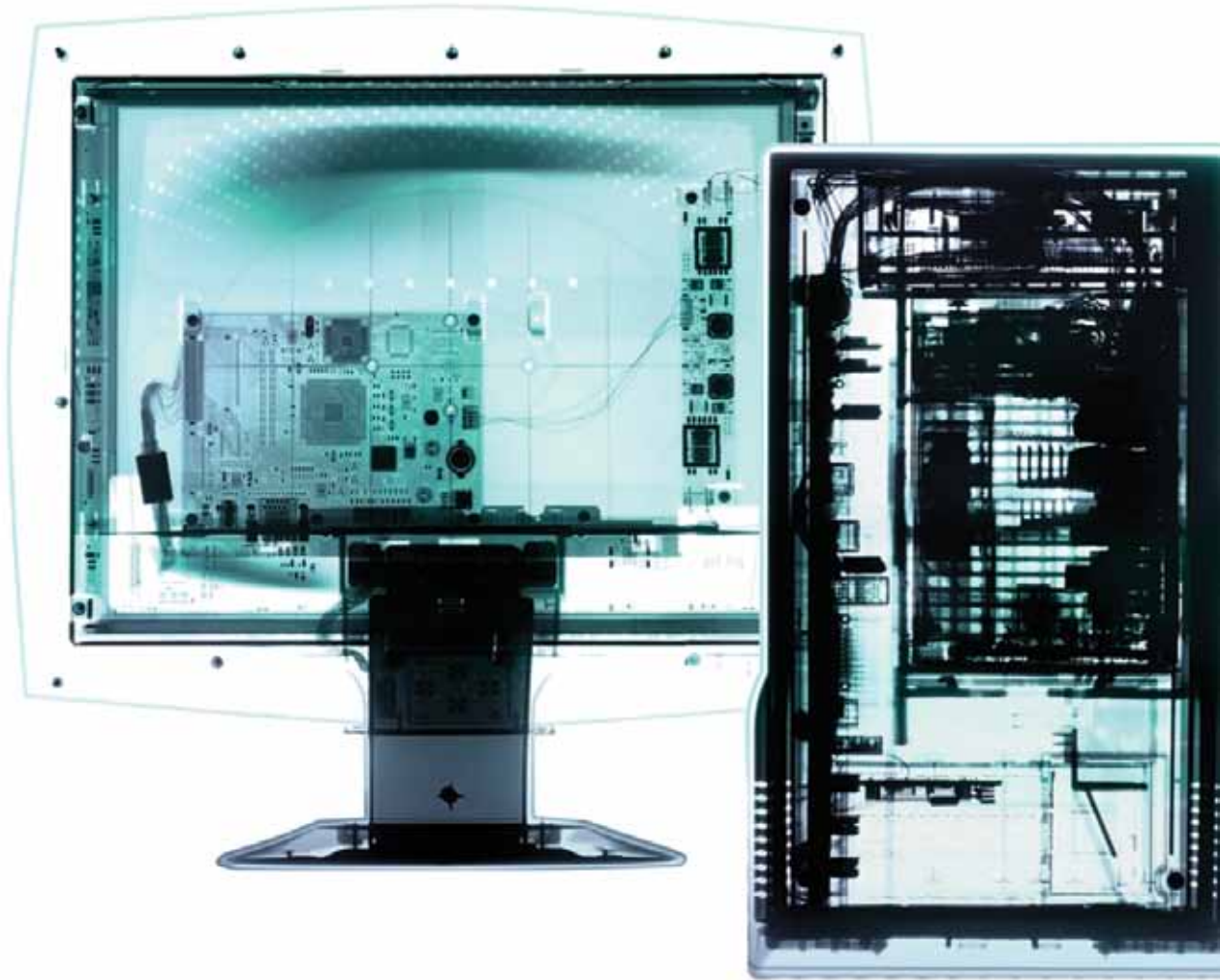


Inside

A triannual operational review, issue 1, June 2013



In the spotlight

Effective enterprise data management addresses the source of a data problem across its entire life cycle

Developments in data management shaped by tougher user requirements and greater complexity

Industry close-up

Electronic data management forms a key part of the European Union's Digital Agenda

Banking and asset management players are increasingly considering electronic data management to be a strategic activity requiring operational efficiency

Organising for analytics in healthcare

The impact of Solvency II on data management in insurance

Do you DLP? Maximising the business value of your Data Loss Prevention (DLP) solution

In this issue

6

10

14

18



4 **Foreword**

5 **Introduction**

In the spotlight

- 6 Effective enterprise data management addresses the source of a data problem across its entire life cycle
- 10 Developments in data management shaped by tougher user requirements and greater complexity

26

36

38



Industry close-up

- 14 European Institutions**
Electronic data management forms a key part of the European Union's Digital Agenda
- 18 Financial services**
Banking and asset management players are increasingly considering electronic data management to be a strategic activity requiring operational efficiency
- 26 Healthcare**
Organising for analytics in healthcare
- 36 Insurance**
The impact of Solvency II on data management in insurance
- 38 Data security**
Do you DLP? Maximising the business value of your Data Loss Prevention (DLP) solution
- 52 Contacts**



We are pleased to introduce you to *Inside*, a tri-annual Deloitte magazine focusing on operational excellence in banking, asset management, insurance, as well as the public and healthcare sectors. In each issue, we will put the spotlight on a new operational issue and provide you with an *Inside* perspective on the topic, presenting the main challenges and market best practices across the various industries.

Times of economic distress are commonly accompanied by efforts to improve regulation and reduce costs. The financial services industry finds itself at a turning point in history, having to face unprecedented operational, regulatory and economic pressures. Meanwhile, governments face structural issues related to the financing of public healthcare. At such times, maintaining a competitive advantage within the industry requires flexibility, a proactive approach, high quality standards and the ability to offer new products and services. Firms also need to be able to retain existing customers and attract new ones—customers who need to be assured of the financial stability and competence of their chosen business partners.

From a profitability standpoint, maintaining current margins, or expanding them, depends on the capacity of a business to efficiently manage its cost baseline, keeping it at an optimal level without compromising on the quality of its products or services. This means that a firm's cost structure choices are characterised by a number of trade-offs such as 'fixed vs. variable', 'in-house vs. outsourcing', 'customisation vs. standardisation', etc. A firm's responsiveness to changes in the regulatory and technological environment is a key consideration. Finally, changes in client requirements regarding both the volume of products or services purchased, together with changes in the characteristics of products or services should be taken into account.

Operational excellence via aligning a firm's cost structure to its needs should thus be considered as the basic ingredient of competitive advantage: it translates into increased operational flexibility and improved customer responsiveness, as well as cost minimisation and margin stabilisation. It aims at designing and implementing the most efficient business model, in terms of organisation, processes and systems, and focusing on delivering the best value to the end-customer with the limited amount of resources available.

Inside magazine will cover a wide range of topics across various corporate functions and provide you with tips and expert advice on each subject. Using global Deloitte expertise and proven methodologies, our aim is to help companies strengthen their competitive positioning through operational excellence.

We hope you engage in the topics covered in *Inside*, and we thank you for your interest and support.

A handwritten signature in black ink, appearing to read 'Basil Sommerfeld'. The signature is stylized and fluid, with a long horizontal stroke extending to the right.

Basil Sommerfeld
Partner
Advisory & Consulting
Deloitte

Welcome to our first edition of *Inside* magazine which will focus on enterprise data management in banking, wealth management, insurance, European institutions and healthcare industries.

Within the current market landscape, two different forces are at work when we talk about enterprise data management and the related pressure for operational excellence. First, firms in various sectors face continuously increasing regulatory requirements, demanding a stronger focus on transparency and reporting. Second, clients have become more 'sophisticated', displaying new and fast-evolving needs which requires companies to react quicker and adapt to client requirements while dealing with new and more complex products, as well as with the related, stringent reporting requirements. These factors lead to a sharp increase in data production. An example from the financial sector shows that a greater variety of financial instruments results in a more complex data environment for financial institutions to manage. Besides the volume of data, it is also the variety of sources and number of data users which has grown, leading to additional issues in terms of organisation and governance. Defining the right governance structure, rules and roles has become one of the major discussion topics in this area.

Master and reference data, along with all the processes and systems designed to manage data, form the parameters of business activities. For example, data on product or client characteristics are used for both high-level decision making and day-to-day business. Unreliable data can lead to unreliable decision making, operational failures or client incidents with a potentially detrimental impact on a firm's profitability and reputation. The quality of the underlying reference data should thus be considered a key strategic aspect in operational excellence, as it could impact numerous stakeholders and have significant consequences (i.e. commercial, reputational, compliance and regulatory etc.). Efficient, accurate and timely data management, among other factors, can help companies reduce risks and costs, as well as ensure compliance with new regulations.

Deloitte understands the unique challenges faced by various industries with regard to enterprise data management. In this first edition of *Inside* we will discuss the related trends and issues with respect to data management in general, and point out industry-specific hot topics. Furthermore, this edition will provide insight into data management models and market practices and present Deloitte's approach to optimum organisation, processes and controls, and corresponding system optimisation.

We hope you enjoy this first edition of *Inside*. Please do not hesitate to get in contact with us and share your thoughts.



Pascal Martino
Directeur
Advisory & Consulting
Deloitte

Julie Chaidron
Manager
Advisory & Consulting
Deloitte

Please contact:

Pascal Martino
Directeur - Advisory & Consulting
Tel: +352 451 452 119
Mobile: +352 621 246 523
pamartino@deloitte.lu,

Julie Chaidron
Manager - Advisory & Consulting
Tel: +352 451 454 807
Mobile: +352 661 451 300
jchaidron@deloitte.lu

Deloitte Luxembourg
560, rue de Neudorf, L-2220 Luxembourg
Grand Duchy of Luxembourg
www.deloitte.lu

Effective enterprise data management addresses the source of data problem across its entire lifecycle

Data problems can affect nearly every part of a company's business, from customer relationship management to finance, operations, marketing, risk management, vendor relations and beyond. In some cases, large companies with multiple product lines and sales channels may not even know how much business they're doing with their most important customers. Such problems can leave decision makers operating in the dark.

To help guide its analysis and optimisation efforts, Deloitte has developed a comprehensive framework which consists of a solid enterprise data management system with seven building blocks (cf. figure below). Effective enterprise data management addresses the source of data problems like these, but it doesn't stop there. Enterprise Data Management (EDM) also helps manage data across its entire life cycle. A comprehensive EDM solution includes capabilities in profiling, cleansing and monitoring to improve data quality.

This article focuses on the data itself and the way it has been impacted by recent developments. We will therefore elaborate mostly on the building blocks relating directly to the data, and to a lesser extent on the building blocks pertaining to the systems that are used to manage the data.



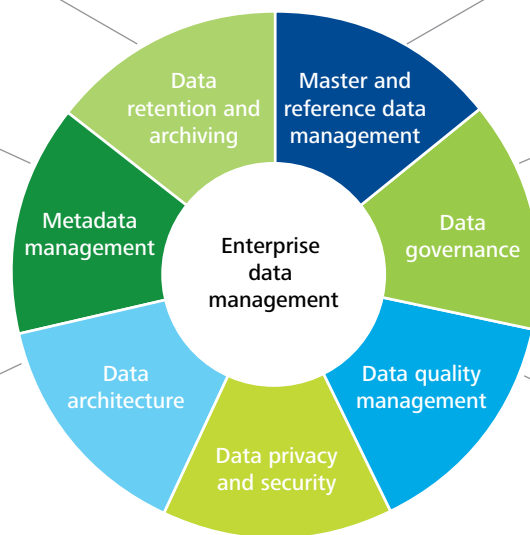
Enterprise data management system

Manages the collection, preservation and retirement of enterprise data assets to support application migrations, historical management reporting and regulatory compliance

Facilitates enterprise-wide data standardisation throughout its lifecycle (i.e. creation to consumption)

Identifies and lays out architectural components that provide a framework to facilitate storage, integration, usage, access and delivery of data assets across the enterprise

Focuses on securing enterprise data assets from any unauthorised infringement. It ensures that appropriate data security and access policies, checks, and controls are monitored



Addresses the harmonisation and integrity of enterprise data which is vital to ensuring a consistent and complete view of master data across the enterprise

Focuses on establishing organisational constituencies and a framework of policies, processes and enabling technologies to ensure that enterprise data is owned and stewarded accurately and consistently to meet business goals

Establishes a framework and supporting processes and procedures to appropriately diagnose business line data quality issues and resolve these

Master and reference data management

The concepts of 'master' and 'reference' data evolved from the need to differentiate data types according to their characteristics. Depending on the characteristics of the data, its management and systems should be adapted accordingly. There are two major types of data—master data and reference data. The main difference between the two is the frequency with which the data changes. Whereas master data or its values change frequently, referential data is essentially static, describing characteristics of a product that seldom change. The main goal of master and reference data management is to ensure that the data used to conduct business is complete and consistent.

Data governance

Data governance is a set of policies, processes and practices which set out the rules for managing data in the organisation. More specifically, it is the framework that ensures that enterprise data has a clearly defined owner who is in charge of the consistency and the exhaustiveness of the data necessary to conduct business. This implies assigning accountability for the defined policies, processes and practices to individuals.

Data quality management

As clean and correct data is the precondition for business decisions, a data quality management framework needs to be put in place to ensure the reliability of data. The owner of data quality management is responsible for identifying, analysing and resolving data quality issues. A key requirement for successful data quality management is the collaboration of business and technology groups within the organisation. Business groups or the internal users of data need to take responsibility for pointing out potential issues pertaining to data quality to IT staff.

To help guide its analysis and optimisation efforts, Deloitte has developed a comprehensive framework which consists of a solid enterprise data management system with seven building blocks



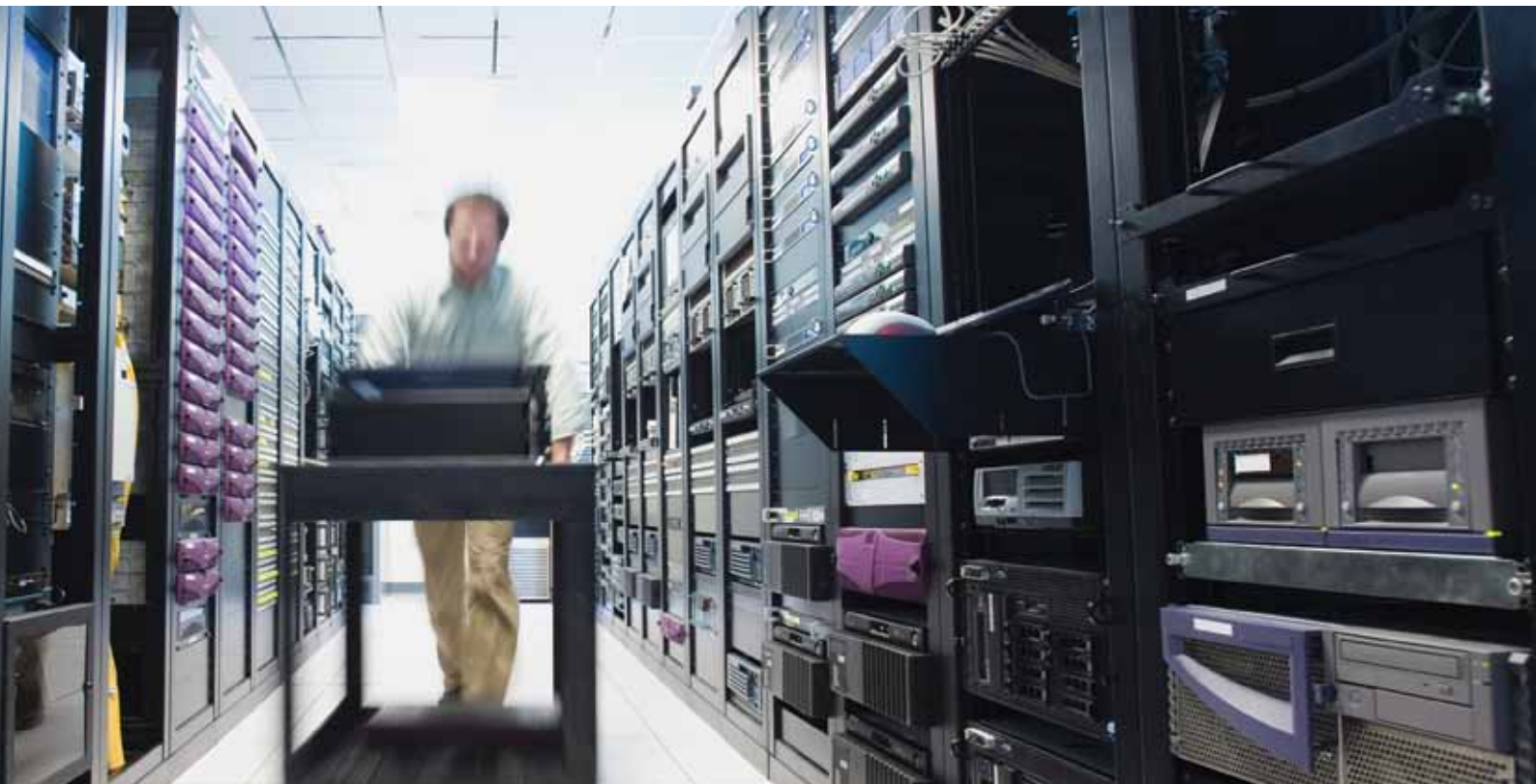
Data privacy and security

Leaks of confidential client data have caused major incidents in the recent past and led to substantial reputational damage for some institutions. Further action by national regulators aiming to prevent such events is very likely. Therefore, institutions need to have an inventory of the type of client information stored in their systems, and decide who has the right to access it to prevent leakage. In this context, a firm should consider trading off efficiency through widespread data availability against security through restricted access rights. The concept of protecting confidential client data should be systematically weaved into every company's IT policy, as it could avoid detrimental reputational effects and possibly act as a differentiator from competitor products.

Metadata management

Metadata is data about data. Metadata management facilitates enterprise-wide data standardisation throughout its life cycle (i.e. creation to consumption) by ensuring consistent definitions and usage.

A comprehensive EDM solution includes capabilities in profiling, cleansing and monitoring to improve data quality





Developments in data management shaped by tougher user requirements and greater complexity

Pascal Martino
Directeur
Advisory & Consulting
Deloitte

Julie Chaidron
Manager
Advisory & Consulting
Deloitte

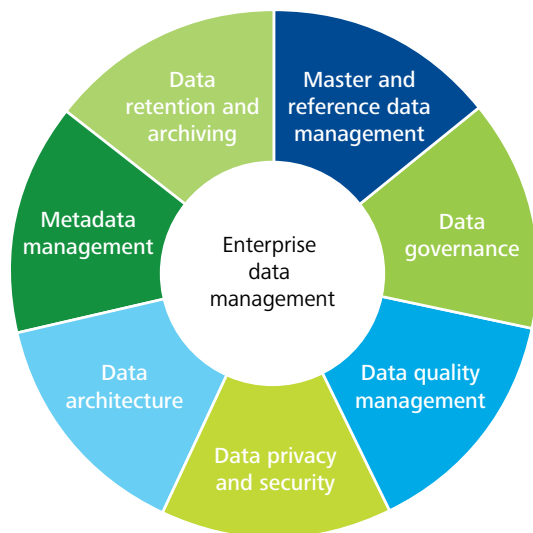
Elias Pankert
Analyst
Advisory & Consulting
Deloitte

There are two major trends that drive change in enterprise data—the growing requirements of data users and the rapid accumulation of ever more complex data.

Enterprise data management is impacted by growing data volumes, greater complexity and faster processes

In the current fast-paced environment, regulatory requirements for higher standards of transparency are becoming more stringent across all industries, while product differentiation and customisation create additional complexity. Process and system controls must be equal to the new regulatory requirements and the increasing complexity of products. Consequently, ever more data has to be collected to satisfy the requirements of external and internal clients (cf. figure below).

Enterprise data management system



Challenges

Increasing reporting and risk requirements

- Increasing requirements or reporting to regulators, local authorities, clients and business partners
- Increasing risk management requirements

Growing volume of data

- Sharp increase in data volume through systematic accumulation of data
- The constant effort to develop new products for new or existing markets is a key driver of rising data volumes

Controls

- Dealing with the growing complexity of controls arising from new regulation constraints (for example: regulatory capital requirements, etc.)

Higher complexity

- Newly developed products become increasingly complex and differentiated from existing products – to the extent of structuring projects specifically for a particular client
- This differentiation is a key driver of complexity as it becomes ever more difficult to distinguish these products



Data is becoming increasingly complex, it is recorded with an increasing frequency and needs to be free of errors in order to be useful for decision making. As a consequence, data volumes are accumulating at a very rapid pace.

Over the long term, the increasing complexity and volume of data will drive the complexity of data management systems and processes and the related work effort required to maintain and control systems and processes, and guarantee the desired quality, which will inflate costs. However, better availability and more detailed data could create substantial opportunities in the field of analytics, thus improving the understanding of internal business processes, products and stakeholders (clients, key business partners), as well as trends in the external environment that shape the company's competitive environment.

Internal and external clients have high and increasing expectations

Data users are aware of the pace of technological advancement and raise their expectations accordingly. This results, inter alia, in the need to obtain ever more detailed information on business activities, clients, suppliers, and to ensure that this data is readily available. As of today, the main expectations from internal and external customers with regard to reference data are:

- **Quality of data and transparency:** ensuring a high quality of data from external and internal providers, traceability of data, data consolidation, shared data definition, controls, common standards for effective communication both within and between firms, the capacity to make realistic impact analyses, etc.
- **Customisation of data and reporting:** offering different indicators of risk, performance, performance attribution, liquidity, graphics according to clients and business team requests, dashboards etc.
- **Independence:** being independent from IT functions to allow more flexibility and agility in terms of customisation and development
- **Quick data production through automated processes:** allowing for an almost completely automated 'data production' value chain of (1) external data imported from different market data providers whose input needs to be controlled at the point of insertion and (2) internal data from various sources that need sound Master Data Management (MDM) built on an architecture that ensures consistency of data. These database systems can be a centralised 'hub' which is linked to users. Alternatively, a service-oriented architecture (SOA) that avoids the replication of hub-user links can be set up. SOA is essentially a set of applications/ functions linked by an 'application service layer'. If correctly designed and implemented, automated data production results in a decrease in operational risk-related errors, reduces human resources-related costs and effort, while contributing to the quality and transparency of underlying data that is retrieved-

Companies have to be able to address such expectations in a cost-efficient manner, while keeping up with ever-evolving market, client and regulatory requirements.

Recent trends lead to series of potential issues and risks

In relation to the trends originating from product complexity and client requirements, the following potential consequences have been identified:

- **Lack of knowledge and data control:**
 - Data documentation not available or non-existent
 - Multiple sources, external and internal data flows giving rise to “data confusion” and difficulties in monitoring/tracking the underlying process flows
 - Ability to trace data and observe its progression throughout the entire life cycle
 - No data ownership or multiple owners of the same data
- **Lack of an overall concept:**
 - No data consolidation, silo approach: lack of a centralised data management system ensuring the completeness, integrity and quality of data
 - No unique data definition: the same type of data could be recorded under different nomenclatures/terminologies, e.g. due to different departments’ needs, giving rise to data confusion and duplication, and related management and maintenance costs. Internally, firms should set up data formats, codes and definitions that are harmonised across departments. Best practice examples for such standards are the proposed Legal Entity Identifier (LEI)¹ program, which is designed to create and apply a single, universal standard identifier to any organisation or firm involved in a financial transaction, or the SWIFT codes for communication of information between financial institutions
 - Multiplicity of systems and departments: different systems within different departments handle the same type of data with different parameters/needs giving rise, once again, to data duplication and related management and maintenance costs

- **Lack of data certification and follow-up:**
 - Data traceability is not always automated (crucial for regulations such as Solvency or Basel)
 - Lack of accuracy and exhaustiveness
 - No categorisation or standards

These potential issues could have an impact on quality risk, commercial risk, reputational risk or compliance risk:

- Risk in relation to clients in reporting the wrong data
- Risk in relation to regulatory authorities reporting the wrong data
- Risk in relation to management, control and risk management making decisions based on the wrong data
- Risk in relation to management of the company and its activities
- Risk in relation to partners and service providers

Data is becoming increasingly complex, it is recorded with an increasing frequency and needs to be free of errors in order to be useful for decision making

Electronic data management forms a key part of the European Union's Digital Agenda

European Institutions

Charles Delancray
Directeur
Advisory & Consulting
Deloitte

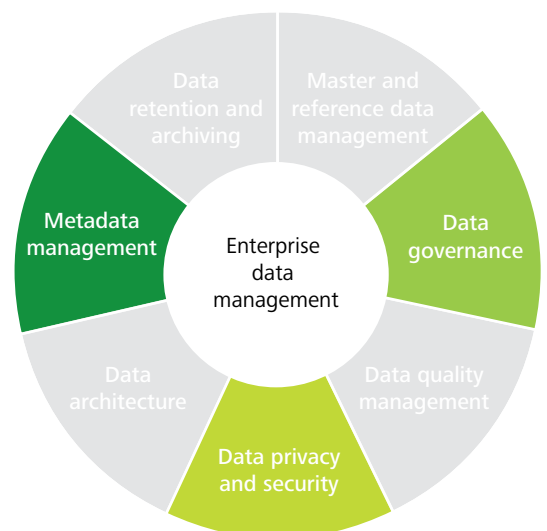
Lara Lorthiois
Manager
Advisory & Consulting
Deloitte

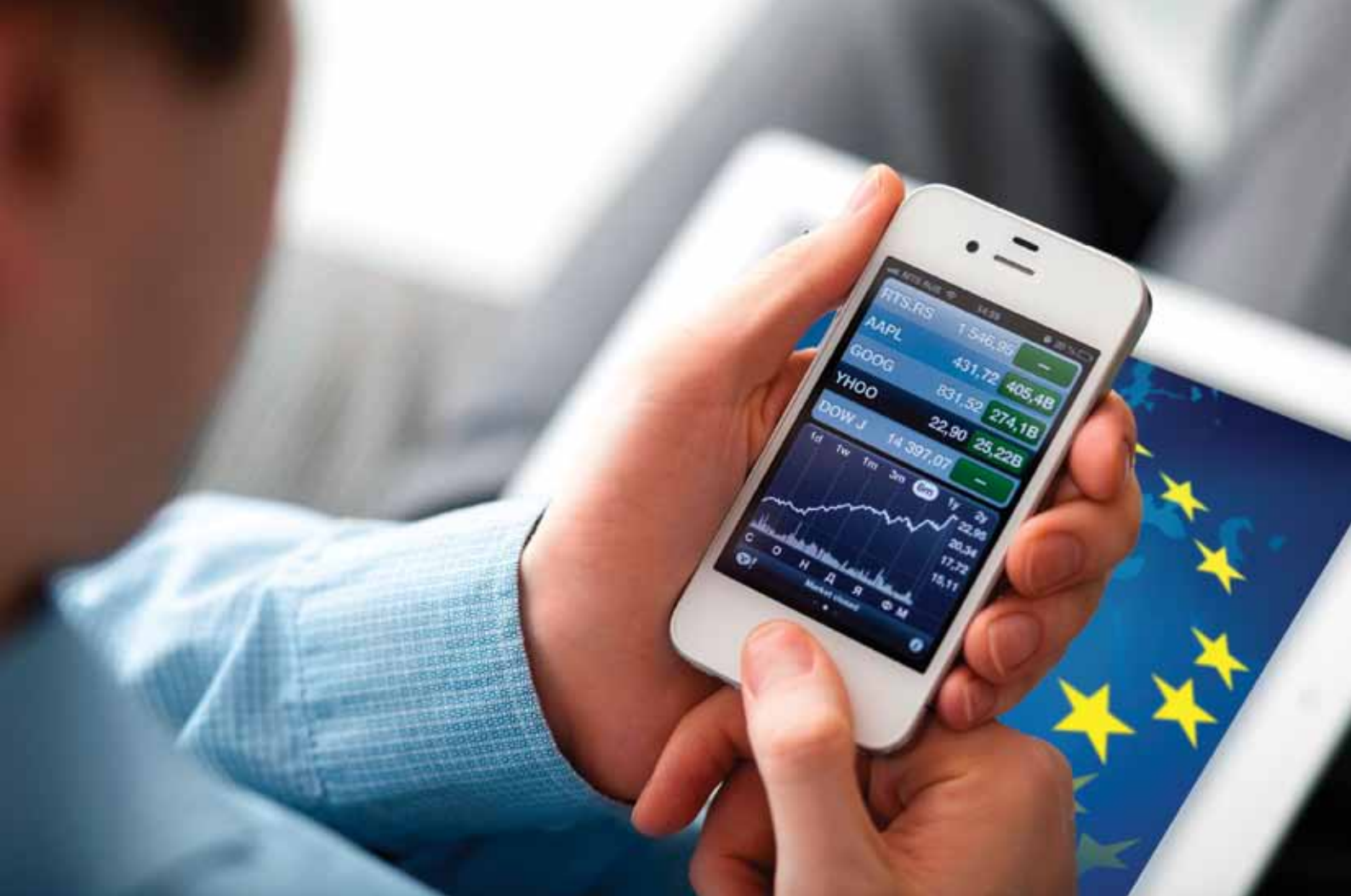
On 1 July 2013, Croatia is due to become the 28th member of the European Union. Through its enlargement policy, the EU has not only brought nations and cultures together; but also their associated data volumes and diversity.

European institutions have the particular feature of being driven by data and driving data: what other authority is better positioned to tackle the profound policy questions posed by this new-age of data-intensive flows? Europe has a special responsibility to take the lead rather than to react to events in this domain. The European Union has an important, coordinating role in achieving effective electronic data management (EDM), through its Digital Agenda (one of the priorities of 'EU 2020': the European Union's ten-year growth strategy), Framework Program and EDM-related policies and directives.

To meet the data management expectations of its internal and external 'clients' (i.e. data protection, data reliability, data transparency, data availability, reporting, etc.) and adapt to the Digital Age, European institutions and public administrations should give particular consideration to three main factors in their strategic decisions: data governance, data privacy and security, and metadata management.

Enterprise data management system





Data governance

Two years ago, the High Level Expert Group on Scientific Data reported that Europe was “currently encouraging its member states to include data management and governance considerations in the curricula of their secondary schools, as part of the IT familiarisation programs that are becoming common in European education”². Data governance, which ensures that data is owned and stewarded accurately and consistently, is a key development that will promote trust and interoperability at international level.

Data governance focuses on enabling technologies. Europe is currently investing in a ‘Collaborative Data Infrastructure’, in order to reach a broad, conceptual framework for how different governments, but also companies, institutions, universities and individuals would interact with the system. This is the solution to another challenge for the European public sector: implementing

infrastructures for shared data that would be local and global, secure but open, flexible yet reliable, affordable but high-performance.

Within European institutions, setting up a framework to provide efficient and effective data management processes, governance, organisation and controls is a major concern. For example, Deloitte supported the implementation of the following measures as the basis for data management within a Directorate General of the European Commission: the definition of data quality standards, the completion of data to meet quality standards, the standardisation of the encoding, validating and auditing processes; the establishment of central coordination and the identification/definition of the roles and responsibilities of key participants (e.g. data owners and encoders), and the implementation of controls (business rules and process automation).

² Riding the wave, How Europe can gain from the rising tide of scientific data, October 2010; <http://cordis.europa.eu/jp7/ict/e-infrastructure/docs/hlg-sdi-report.pdf>

Data privacy and security

European institutions and public administrations are under pressure to meet contradictory public expectations for both transparency and privacy.

To respond to these requirements, in January 2012 the European Commission proposed a comprehensive reform of data protection rules to revise the EU's 1995 Data Protection Directive (95/46/EC) with the objective of increasing the user's control of their data and cutting costs for businesses.

Europe supports data privacy and security by providing the relevant juridical framework to European institutions, national institutions and private organisations. The Irish presidency of the EU has made data protection one of its priorities, and is working hard to achieve a political agreement on the data protection reform by the end of the Irish presidency (June 2013)³.

Metadata management

The main aim of metadata ('data about data') is to improve resource recovery and to answer needs related to administrative control, security, personal information, content rating, rights management and preservation, etc. Metadata management is not only a key factor in the preservation of data, it is essential to semantic interoperability among member states.

On 1 January 2010, European Institutions launched a six-year program on interoperability solutions for European public administrations (the ISA program)⁴, with the aim of facilitating efficient and effective cross-border electronic collaboration between European public administrations. In the ISA⁵ report, 'Towards government open metadata', the European Commission encourages the management of metadata and addresses the requirements of public administrations: they should identify and document metadata, make it available for reuse, identify inconsistencies and opportunities for harmonisation and provide metadata both in human and machine readable formats.

It is only by harmonising the way member states approach metadata that quality, cross-referencing, integrity and reusability potential will be improved.

Enhancing metadata management is a policy priority of the European Commission: it is a core success factor for interoperability, and therefore, for the digital economy and the EU's Digital Agenda. Nevertheless, the policy evaluation of metadata management underway has demonstrated areas for improvement. European institutions and public administrations should further consider the integration of communications and awareness raising, the engagement of stakeholders and project management continuity, and the avoidance of overlaps and duplication, in order to successfully apply EU metadata management principles.

The Irish presidency of the EU has made data protection one of its priorities, and is working hard to achieve a political agreement on the data protection reform by the end of the Irish presidency (June 2013)

In the Digital Age, the collection and storage of personal information are essential, but the way data is collected, accessed and used has been profoundly changed by technological progress and globalisation. Data is used by all businesses—from insurance firms and banks to social media sites and search engines. The objective of this reform is to reinforce consumer confidence in online services: *"The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data"*, stated EU Justice Commissioner Viviane Reding, the Commission's Vice President. She added: *"A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation"*. This general Data Protection Directive has been supplemented by other legal instruments. Article 8 of the EU's Charter of Fundamental Rights and the Lisbon Treaty also recognise the right to the protection of personal data, by providing a legal basis for rules on data protection for all activities within the scope of EU law (Article 16 of the Treaty).

³ http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

⁴ <http://ec.europa.eu/isa/>

⁵ http://joinup.ec.europa.eu/sites/default/files/towards_open_government_metadata_0.pdf

Recommendations

Effective data management is crucial for operational efficiency within public organisations, and can result in the generation of substantial benefits for its 'clients'. It is true that public bodies have been slower to recognise the value they can achieve from effectively harnessing the power of data they hold. The scale and range of public sector data is overwhelming, but not effectively exploited.

The electronic data management practices of European and national public administrations could be developed through investments in data analytics software, resources and processes. They would benefit from key capabilities in sharing and manipulating their own data (which could be culled from the web), and integrating diverse data from public administrations, and social and corporate databases. This could boost the efficiency of their services, for example by combating fraud through combining and analysing social and financial information.

Public services could also be improved if public administrations were to invest in social media. Social networks would provide a space to evaluate public opinion, obtain feedback on policies and communicate emergency information more efficiently. Social media provide public organisations with an opportunity to be more responsive to citizens. The effectiveness of social networks in facilitating citizen protest has demonstrated that governments can use the same networks to be more proactive in their engagement with the public. Governments are beginning to recognise the value of using social media to solicit feedback, share information and communicate with citizens.

European institutions could adopt and document a consistent strategy for overall data management: metadata, master and reference data. For example, Deloitte has demonstrated the value-added of business process management tools to support master and reference data management. This could also be applied to metadata management, to guarantee consistent data visibility and reporting.

Challenges and next steps

A fundamental characteristic of our age is the rising tide of data, which is global, diverse, valuable and complex. Applied to European public organisations, this leads to major challenges that need to be overcome if sound electronics data management capabilities are to be developed in this sector:

First, European institutions have to change their mentality of operating in 'silos' and learn to operate in a matrix model. Technical solutions should be re-designed accordingly in order to establish sustainable organisation-wide information management. Data quality and accessibility then become key challenges, since for some institutions, European or national, data is not easy to access and manipulate, and often available only in hard copy or stored in incompatible formats. There is also a frequent inability to source data from multiple systems, due to the lack of a seamless exchange of information assets. Furthermore, institutions are concerned about privacy and security when it comes to releasing large amounts of raw data to the public. Finally, the context of multi-stakeholders and multi-cultural contexts in an enlarging Europe adds complexity to the set-up of best practices such as metadata management.

Deloitte has an established framework that addresses the core aspects of an organisation's ability to manage its data and to deal with the recent challenges and rapid growth of information assets. The Deloitte Analytics Public Sector group has the industry knowledge and tools to address the unique challenges that public sector organisations face. Data mining and data analytics support better policy setting and decision making.

Data is a renewable resource, continually multiplying in volume. Fresh data is continually being collected and replenished, and existing data is being used in unforeseen ways, as new applications are to be developed. In an information-driven age, the ability of European and national institutions politicians to realise the opportunities associated with data management may make policy implementation more successful, empower institutions to govern more effectively, based on solid evidence, and lead the European economy to expand. The result should produce a vital asset that is flexible, reliable, efficient, cross-disciplinary and cross-border.



Banking and asset management players are increasingly considering electronic data management to be a strategic activity requiring operational efficiency

Financial services

Pascal Martino
 Directeur
 Advisory & Consulting
 Deloitte

Julie Chaidron
 Manager
 Advisory & Consulting
 Deloitte

Elias Pankert
 Analyst
 Advisory & Consulting
 Deloitte

Data management systems are an essential component of the business infrastructure of every banking and wealth management firm. Effective master and reference data management is crucial for operational efficiency in the entire value chain of companies and their service providers.



Although reference data is descriptive in nature (e.g. instrument/product, client, counterparty, book, corporate actions, calendars, etc.), it is shared and re-used across trades and transactions. It is often referred to as 'static data', but increasingly includes real-time data (e.g. external price and market data)⁶. In the financial sector, market data represents the largest share of data management-related costs, such as the purchase of market data from third party data providers and the corresponding cost of human resources required to manage and control the data flow and databases.

Almost all functional activities, from portfolio management in the front office to settlement and reporting in the back office, use data management systems as their main source of information to perform their daily activities. This is also true for other business-related activities such as CRM, risk management, compliance, investment restrictions control, internal and regulatory reporting, sales, investment restrictions, etc.

Scope of securities reference data



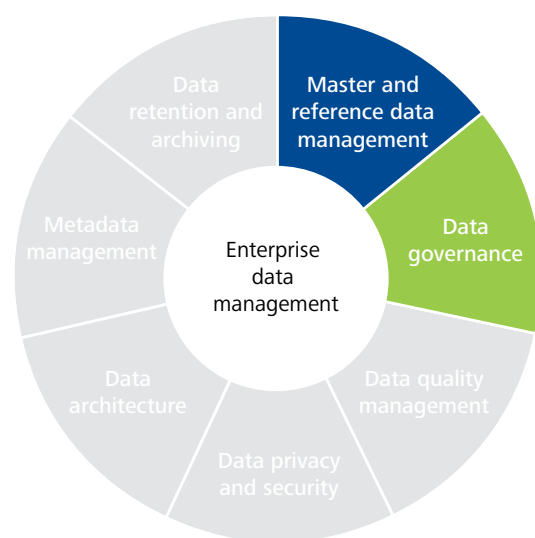
Effective data management supports



⁶ White paper: 'Growth, risk and compliance: the case for a strategic approach to managing reference data', Deloitte and Swift, 2012

To ensure a common vision among business owners, data management should be addressed at an enterprise level and not at a functional level. In order to implement this, a strategic approach should be designed, including cross-functional sponsorship, clear governance structures and budgeting across divisions.

To meet client and market expectations of data management (i.e. customisation and data reporting, quality of data and transparency, independence, quick data production through automated processes, etc.) and respond to the increasing volume of data, financial companies could design their strategic approach using the two main factors highlighted below:



Master and reference data management models

Co-existence of three models in data management—focus on the securities masterfile

Financial institutions choose the data management model that best fits their requirements according to the availability, consistency, timeliness and accuracy of data. It is possible to operate different models in parallel, depending on the category of data. The database model




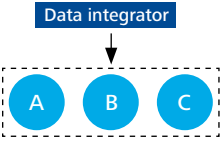
chosen for client or product data is not necessarily the same as the database for reference and market securities data. Whereas client data is often stored locally, financial services companies typically organise their securities master file according to one of three models:

- **Centralisation** of the securities master file with one centralised team in charge of management and monitoring of the securities master file at the group level
- **Centralisation with competency centres** with one centralised team in charge of creating and controlling most securities, and dedicated competency centres close to business teams responsible for creating or controlling securities requiring specific expertise. The aim is to leverage existing resources to provide the expertise required and allocate responsibilities across the institution as needed
- **Complete decentralisation** where there is no securities master file shared at the group level, but each individual entity has its own securities master file, and may have its own systems and processes. This model still exists for historical reasons, such as the merger or non-integration of systems. Generally, the volume of the securities master file does not exceed 50,000 active securities (consolidated at group level). With an increasing volume of securities and reference data fields to manage, financial institutions could rethink their data management model and governance to improve data quality and process efficiency, and reduce costs

The centralisation of the securities master file is the most representative model in the financial market in Luxembourg. This model enables companies to manage a large volume of securities and reference data fields (from 50,000 to 250,000 active securities) in an efficient way, avoiding duplication of tasks within the group (such as data feed, data searches, openings and controls) and minimising the cost of market data external providers.

However, the centralisation of the securities master file comes at a cost, because a system has to be selected, acquired and implemented. The business case has to be evaluated carefully. By centralising securities management, the reference data team increases both its standing and its bargaining power within the group. In general, centralisation of data management is coupled with automation of most of the underlying processes, including data workflow with external providers.

Some financial institutions have started to establish competency centres, which focus on conducting controls on specific securities or reference data fields. This, in turn, enables companies to significantly improve the quality of reference data by assigning control responsibilities where the expertise lies within the company. In the long run, the next step would be to allow competency centres to focus on both inputs and controls. Delegating some responsibilities to competency centres implies a number of advantages such as quality improvement, but there are some disadvantages, such as the loss of reference data controls and processes.

Models	Description and stakeholders
<p>1. Centralisation (HUB)</p> 	<ul style="list-style-type: none"> • One team responsible for the management and monitoring of the securities profile • Centralisation of opening and control tasks • Sharing of information with all group entities • One system • Discount rate on purchase prices of data • Economies of scale • Standardisation of the processes and associated system
<p>2. Competency centre</p> 	<ul style="list-style-type: none"> • One Centralised team responsible for opening and control for most securities • representatives in the local entities and in the business teams for opening and control of specific securities – Expertise located close to business interests • Distribution of data to all group entities • Leverage effect and synergies at group level • Strong value-added for the client of the various entities
<p>3. Complete decentralisation</p> 	<ul style="list-style-type: none"> • Each local entity has its own securities Master File and a dedicated team • No synergies • Multiplication of the costs • Weak power of negotiation with the main providers • Separate and sometimes different systems • Creation of a security duplicated through the different entities • Potential lack of consistency in the static information and price for a given security between the different entities (client impact)
<p>Data flow outsourcing</p> 	<ul style="list-style-type: none"> • SLAs to be put in place with counterparties • Declining balance for the purchase prices of data • High quality of information (scrubbing done by external data provider) • Internal controls targeted to check the quality of received data • Distribution of the data to all group entities • Solution lacks flexibility

Outsourcing of data flow: an opportunity for process and control optimisation

These three models could be coupled with the outsourcing of data flow to a data integrator (a company specialised in the integration of data or another financial institution that provides this service). By outsourcing all or part of the data flow, the financial institution can focus on controls rather than on data collection and input, and is able to limit the number of internal resources required to manage the securities master file. Again, outsourcing of data flows may be possible for data relating to the securities, but not for client or counterparty data.

Currently, players in Luxembourg that have a limited volume of reference data (from 5,000 to 30,000 active securities) are considering outsourcing their current process to an external provider. Apart from a solid business case, a major aspect in the decision to outsource data management is the issue of responsibility for the data quality. It is common practice that parts of data management are outsourced to third party providers without passing on the responsibility to the provider.

Data governance

Data governance is a critical function impacting all business activities. Developing a strong data governance policy can enable companies to achieve efficient data quality management.

Data governance requires a dedicated system based on reference data 'ownership' in order to give a sense of responsibility to business lines and IT professionals. It must cover the entire life cycle from reference data sources to reporting.

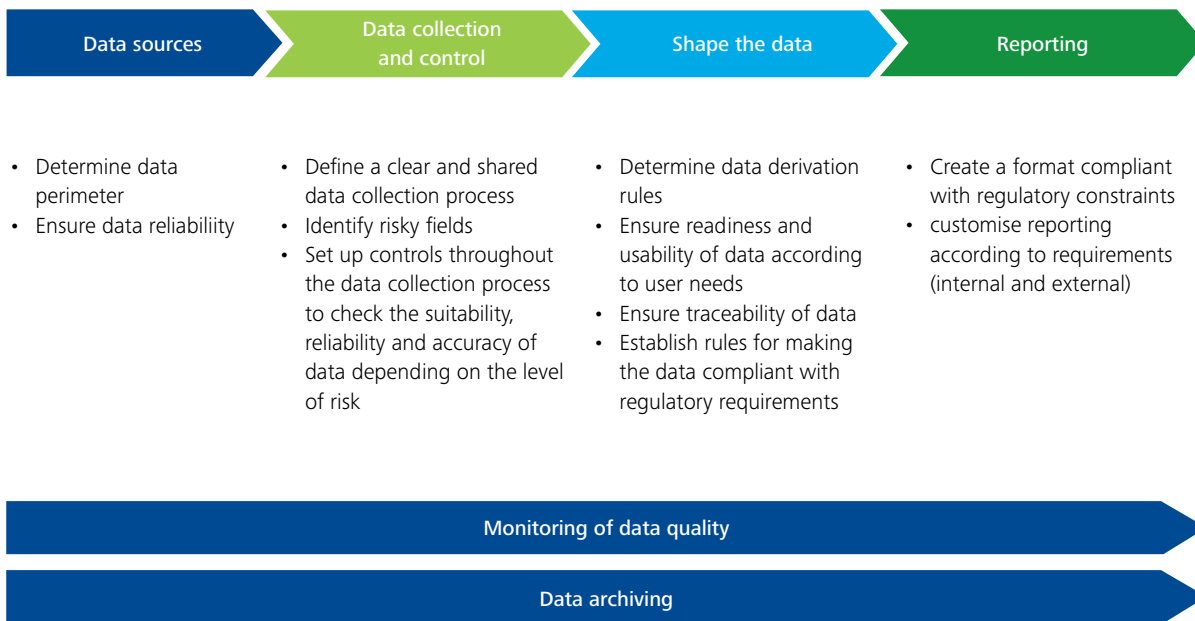
The Reference Data team should be able to answer the following questions:

- Who is using which data?
- Is all data included in my current securities master file being effectively used by the business?
- What are the key and more 'risky' fields?
- Should I accept any new requests from the business, or can we enter into discussions, propose alternatives, reject any requests?
- How should I monitor the quality of the data in my securities database?
- Can I become proactive and suggest new data and fields to the business, enabling the current quality of reports provided to customers to be improved?



Some financial institutions have started to establish competency centres, which focus on conducting controls on specific securities or reference data fields

Data governance should cover all the main stages of the data life cycle listed in the figure below.



Automation of processes strengthens the focus on controls

In line with the increasing volume of securities and reference data, the industry is progressively moving from manual processing towards automation. This shift is important as it allows for raising data quality and capacity to process ever-increasing volumes of transactions. By automating some processes, reference data management teams can shift their focus from reference data research and collection to controls, which has a direct impact on quality.

With respect to data controls, best market practice is to prioritise controls according to the importance level of the related reference data fields. Levels of importance are assigned to each reference data field, taking into account the potential impact of errors on clients, pricing and NAV, etc.

When opening a new security in the securities master file, most users prefer the 'full opening mode', which means that all reference data fields of the new security have to be filled in and validated before the opening of the new security can be completed. In general, the 'full opening mode' uses 50 to 150 reference data fields to describe one security. When there are more than 150 reference data fields, 'partial opening' can be used. In this case, only reference data fields considered as mandatory will be filled in and the others will be completed only when necessary. In the case of 'partial opening', the mandatory fields could change, depending on the profile of the user.

This amount could be significantly reduced by:

- Rationalising the number of reference data fields
- Challenging the needs of end-users
- Decreasing the number of data providers' workstations
- Optimising costs with data providers
- Centralising market data flows and business teams into a centre of excellence

Depending on the initial situation, the potential cost savings can range from between 10% and 20% of the total cost of the database.

Dedicated systems for data management allow for more flexibility and agility

For a securities master file with a large volume of securities (>50,000), we observe that financial institutions extract reference data management from their core banking system—or portfolio management system—to implement a dedicated system. This is aimed at giving the reference data management team more flexibility and taking advantage of mature market tools. When reference data management is serviced through a dedicated system, institutions are also able to deal with special requirements from internal and external clients, without having to consider specific constraints related to the core banking system.

Models of centralisation or competency centres are supported by one unique system shared by all the entities. By sharing systems, financial institutions further improve their operational excellence. Indeed, they benefit from cost sharing, synergies and economies of scale at the group level. They can also create a centralised and dedicated team for reference data management ('centre of excellence'), instead of integrating reference data management teams into other departments, which could decrease their visibility, bargaining power and flexibility. The decentralisation model is often a consequence of the various different operating systems implemented in each entity. As a result, entities cannot evolve at the same pace in terms of system developments, and are unable to share the costs or benefit from a centralised database, its securities and their related reference data fields.

Data governance requires a dedicated system based on reference data 'ownership' in order to give a sense of responsibility to business lines and IT professionals

The costs (i.e. cost of data, human resources and systems) related to the management of reference data is significant at the group level. On average, the associated cost means in terms of human resources and data purchase ranges between an estimated €80 and €120 per security. In the Luxembourg market, and on average, the total cost for a database of about 80,000 securities would be estimated at around €6.5 million and €8.8 million per year (including the market data purchase and human resources required to manage these).

Approach for operational excellence in data management

As stated previously, the quality of the reference data should be considered a key strategic aspect in operational excellence.

The first step in reaching operational excellence would be to diagnose your current situation in terms of data governance and management. This would enable you to identify potential room for improvement. According to your group priorities and resources, you will be able to prioritise and select projects to reach operational excellence.

By targeting operational excellence, you will implement an efficient model which can deliver the best value to your stakeholders, taking into account their requirements, such as customisation of data and reporting, data quality and transparency, independence from the IT function (for greater development flexibility) and rapid data production through automated processes.

Examples of operational excellence projects

Data models and governance

- Define the operating model for data management according to group strategy
- Define the data governance and escalation process to support the operating model
- Identify data owners in relation with their expertise and determine their responsibilities in terms of supporting operating model and data governance
- Define the value chain and processes that will support operating model and data governance

Data source	Processes	Systems
<ul style="list-style-type: none"> • Share data definition at all levels • Rationalise reference data fields according to end-users and clients needs/usage • Ensure traceability of data • Prioritise reference data fields according to their potential financial impact on business activities and on client • Reinforce controls on 'critical' reference data fields to improve data quality • Renegotiate contracts with data providers after rationalisation of data 	<ul style="list-style-type: none"> • Lean review and improve level of automation of processes such as: <ul style="list-style-type: none"> - Data collection - Data input - Data control - Reporting - Data archiving • Design processes to monitor controls throughout the data life cycle 	<ul style="list-style-type: none"> • Select a provider via RFP process and develop a dedicated system for data management to improve its flexibility

Organising for analytics in healthcare

Healthcare

Marco Lichtfous

Partner

Advisory & Consulting
Deloitte

Petra Hazenberg

Partner

Advisory & Consulting
Deloitte

Gunnar Mortier

Senior Manager

Advisory & Consulting
Deloitte

Ronan Vander Elst

Directeur

Advisory & Consulting
Deloitte

The growing thirst for information—reliably accurate information—is dramatically changing the healthcare industry in many ways. Externally, the government, industry groups, payers, employers and patients are demanding more insightful information, accountability and transparency. Internally, there is increasing demand for clinicians and leaders to improve service quality, patient satisfaction and clinical outcomes.

At the same time, healthcare providers are being constantly challenged to provide better results with fewer resources and at a lower cost. These external and internal forces can lead to greater performance risk, and are driving healthcare organisations to develop a better understanding of their clinical and financial outcomes. The table stakes have changed in the ‘new normal’—the ability to build enterprise information management and analytics capabilities that can provide new insights about patient populations that may be essential for organisations to thrive and ultimately, survive.

A key to promoting sustainable enterprise excellence can lie in the organisation’s ability to harness the potential of clinical systems that can produce insights that enable informed decision making. Organisations that have excelled at building information management and analytical capabilities (referred to commonly as ‘analytics’) have realised tangible benefits such as: improving clinical outcomes, reducing insurance denials, reducing avoidable re-admissions, and increasing the use of resources to help meet the growing demand for patient services—just to name a few.



Buttons: Power, Home, Back, Forward, Stop, Record, Print, ECG, MPR, Monitor, Patient, Pulse, Alarm, Silence, Stop

What is analytics?

Business analytics typically focuses on areas such as financial performance, reimbursement, productivity and utilisation. Clinical analytics focuses on areas that help providers deliver more effective and efficient clinical care (mortality and morbidity measures), increase patient safety (signal detection), and/or improve population care (public health programs, immunisations, market needs). Due to the complexity of healthcare, it can be challenging to find the desirable mix of business and clinical measures that convey a clear linkage between business or operational decisions and clinical outcomes. However, with an effective approach, an understanding of this linkage can often yield powerful insights. As a result, the growing importance of business and clinical analytics-driven process measures are becoming more prevalent as accountable care, shifting reimbursement models, and service-line strategies may demand a holistic view that combines clinical outcomes and financial and satisfaction measures.

Regardless of the terminology used, the objective should be to develop and implement a sustainable, adaptive analytics capability that handles the growing volume of data in a consistently reliable way and can yield insights to improve both patient care and business performance. To help achieve this, it is important to first recognise the potential barriers and roadblocks that cause many provider organisations to falter when tackling the complex opportunity that is analytics. Armed with this understanding, the path to implementing an effective analytics function can become clearer, more attainable, and a source of a new competitive advantage.

Business analytics typically focuses on areas such as financial performance, reimbursement, productivity and utilisation

What are the common pitfalls that healthcare organisations face today?

Several challenges need to be addressed in order to effectively deploy and embed analytics in the organisation's culture, decision making processes and operations. Aside from technical, data and skill considerations, there are political, cultural and organisational pitfalls that can slow or stall the implementation of the program. By anticipating and planning for these pitfalls, executives can be better prepared to build support and maintain momentum.

Organisational barriers

There are several reasons why executives may struggle with the question of where to place an analytics function in the organisation. First, the fact that the IT function often holds responsibility for the Enterprise Data Warehouse (EDW) and reporting causes some organisations to view IT as a natural owner of analytics. Second, in many organisations the Finance Department has historically been one of the largest users of analytics. Not only do they need information to support business decisions, they also can have a major requirement for risk management and compliance data. Third, clinical leadership requires clinical analytics insights and capabilities to compete in today's market. Finally, the emergence of genomics and translational research are closely aligned with care delivery and involve new complex data sets that hold the potential for clinical breakthroughs and new sources of revenue.

Territorial disputes over data

Many executives have learned how to work around fragmented data and inefficient processes to get the information they need to be effective. As a result, control and ownership of data can often be a very personal and highly political issue. Executives frequently make decisions within their own area of responsibility based on personal intuition and consensus, often because they lack access to good information or because it's easier to rely on what has worked in the past in other organisations. Overcoming the status quo to implement an enterprise analytics program usually requires a combination of strong leadership and a willingness to drive behavioural change in the organisation.

Unclear roles and responsibilities

As organisations struggle with implementing an analytics program, they realise that priorities and roles should be defined: what projects will be undertaken, how will project requests be prioritised, where will the skilled resources come from, what data is needed, how will that data be maintained, and how will results be measured? Addressing such questions frequently involves several departments, data sources, staff and conflicting priorities (e.g. when high quality analytics are wanted fast, and at a low cost, by multiple departments at the same time). In the absence of formal decision-making protocols, such situations can often lead to stalled projects, substandard results, and unsatisfied analytics customers. In other situations, departments who are frustrated with the inability to get things done at the enterprise level launch their own independent analytics efforts.

Competition for resources

It is rare to find a healthcare organisation that has sufficient staffing and skills to pursue all the analytics opportunities. Many providers are struggling to recruit and retain experienced managers and analysts who possess the combination of healthcare domain specialisation, data mining knowledge and experience with the vast array of analytics tools and methodologies. This resource constraint can apply to business and clinical departments, as well as the IT organisation where it is important to have access to the data architects, programmers and analysts who can work effectively with end-users. Conversely, functional departments face similar challenges in that the individuals who possess the specific skills and sector knowledge are often busy with their existing responsibilities.

What is the best way to organise for analytics?

Transforming an organisation to embrace an analytics culture can take a significant commitment on the part of executives, management and other stakeholders. The ability to implement an effective analytics program should depend more on leadership, structure, decision rights and behaviour change, than on the size and complexity of the infrastructure or the technical platforms involved.



Getting leadership to champion the analytics program

The model analytics strategy should begin with strong executive leadership capable of bringing together talented people with extensive experience in applying analytical methods to clinical and business issues. These leaders should take ownership of the deployment of their analyst talent to the best and most effective use that supports the organisation's mission and strategy. This means that jockeying for resources for pet projects, building 'shadow' analytics groups, or hiding strong analysts within a specific function should be discouraged. Instead, the team works together to identify and prioritise the particular analytical issues that the organisation will most benefit from addressing.

With the leadership on board, the analytics function can serve as the intersection of a company's business strategy, the data behind it, and the technology that delivers it—which together helps improve an organisation's performance. Once leadership has reached agreement on which areas are of highest priority to the enterprise, they should then motivate their staff to become analytics champions and participants. These champions should include management, clinicians, researchers, analysts, technologists and others. Building support for analytics needs leaders to work across silos to collaborate with each other.

Aligning analytics resources with enterprise priorities

It is important to establish an effective structure to help promote collaborative behaviours. However, this can typically prove challenging as organisations often base analysts within the functions they serve, creating silos that work against the enterprise analytics strategy. For example, financial analysts work on financial concerns, while clinical analysts focus on patient care issues. An organisation should answer this question: *“What is the leading way to align people so they are positioned to support the immediate and long-term needs of the enterprise?”* And alignment doesn’t mean just putting everyone in the same group as a centralised function, as discussed below.

Structuring analytics in silos can limit analysts’ abilities to collaborate on broad, strategic initiatives or complex issues involving multiple areas of the business. By organising resources so they can work across traditional boundaries, new insights can be obtained at the enterprise level that cannot be developed in isolation. The biggest challenge is in balancing the need to keep them working ‘close to the business’, while enabling them to work ‘closely with each other across the business’. By achieving this balance, organisations can achieve the synergy of leveraging its combined knowledge, skills, tools and information resources. Figure 1 illustrates three general approaches to structuring an analytics function.

Figure 1 – Analytics delivery models

	Description*	Strengths	Weaknesses
	<p>All analyst groups report to one function at the enterprise level, even if they are assigned to serve different departments or functions based on strategic priorities set at the corporate level. Resources may also be ‘engaged’ by operating units for specific analytics projects</p>	<p>This model enables an enterprise wide view of what is going on. This makes it easier to deploy analysts on strategic projects, reduces confusion, or limits competition for resources on functional initiatives</p>	<p>Reduced responsiveness to departmental needs. Potential to create distance between analysts and business users, especially if analysts are located in a central location. Risk of ‘shadow’ analytics groups arising to address unique business requirements. Model may falter without strong enterprise focus or leadership</p>
	<p>Individual analyst groups resides in departments that are strong consumers of analytics. While groups may provide limited reporting to other departments, their primary focus is on the needs of their individual business units</p>	<p>Easier to deploy resources to perform analytics within the department. Highly responsive to individual department needs</p>	<p>Difficult to set enterprise priorities, limited incentive to share best practices or resources, conflicting data. Often results in independent analyst groups, resulting in lack of communication, confusion, data integrity issues, duplication of effort, and unnecessary costs</p>
	<p>Analysts groups exist at the health system or enterprise level as well as in departments or business units that utilize analytics capabilities for their specific needs. Some common governance and standards to promote collaboration and knowledge-sharing among the community.</p>	<p>Promotes collaboration, knowledge-sharing while retaining departmental flexibility. Increased communication facilitates an enterprise view of project priorities and status while reducing risk of redundant projects and resources. Best model for bringing domain experts together to enterprise or complex analytics issues.</p>	<p>Requires a strong governance model in order to be effective. May take longer to fully implement. Conflicting priorities and resource issues may arise due to the informal nature or secondary reporting line relationship.</p>

Achieving this balance in a complex organisation with interrelated functions such as care delivery, research, and community services involves recognising that the needs vary greatly in different parts of the organisation. Some analytics applications function better in a centralised environment to serve specialised needs (e.g. research, data management) or infrequent analytics users, while other areas may likely benefit from a more distributed approach that brings together the leading talent and resources from across the organisation to achieve a strategic priority (e.g. promoting service line excellence).

An effective way to achieve this balance should combine centralised resources (e.g. skills, people, tools, and information) to help address strategic or commonly-shared needs, with a virtual community of highly skilled domain specialists who are not based within IT, but work closely with data and reporting specialists when needed. In other instances, organisations that have been previously highly decentralised may move to a centralised model to establish a common foundation of analytic specialisation that may then be redeployed in various areas of the organisation. Ultimately, the specific model will be the one that is better aligned with the organisation's overall enterprise strategy and business model.

Establishing clear roles and responsibilities to help enable effectiveness

Effective analytics projects should not begin with data and end with models; rather, they should begin with strategy and end with insights that lead to improved decision making and results. This paradigm shift begins with the tone at the top and is facilitated by an effective organisational model. But to be truly transformational, it requires a new understanding of the 'who, what and how' of decision making. To improve results, once the leaders are on board and the desirable structure is in place, a decision rights framework should be established to make the new analytics structure operational. This is the 'glue' that holds everything together.

The first step in establishing a decision framework for analytics includes identifying the stakeholders that should be involved in making the key analytics decisions. Typically, this means the CEO and senior management. But it is also important to build on the strengths of the existing operating model and engage the local or departmental leaders who will be responsible for implementing the decisions that drive results. Then, once the 'who' has been decided, the 'what' needs to be identified. This requires agreement on the decisions that matter in enterprise analytics and the resources to be allocated.

To establish a framework to achieve such agreement, a commonly used tool is the 'RACI' matrix, which outlines who is Responsible, Accountable, Consulted and Informed for each important analytics decision. Figure 2 illustrates examples of important decisions and the RACI matrix that could support an integrated enterprise analytics function.

Typically, the IT department will remain the custodian on issues of data quality and data standards. The finance and clinical functions—the largest data producers and analytics consumers—can have a major influence on data quality, business and care delivery issues, and other functions such as marketing, quality, regulatory, internal audit and compliance may be important stakeholders.

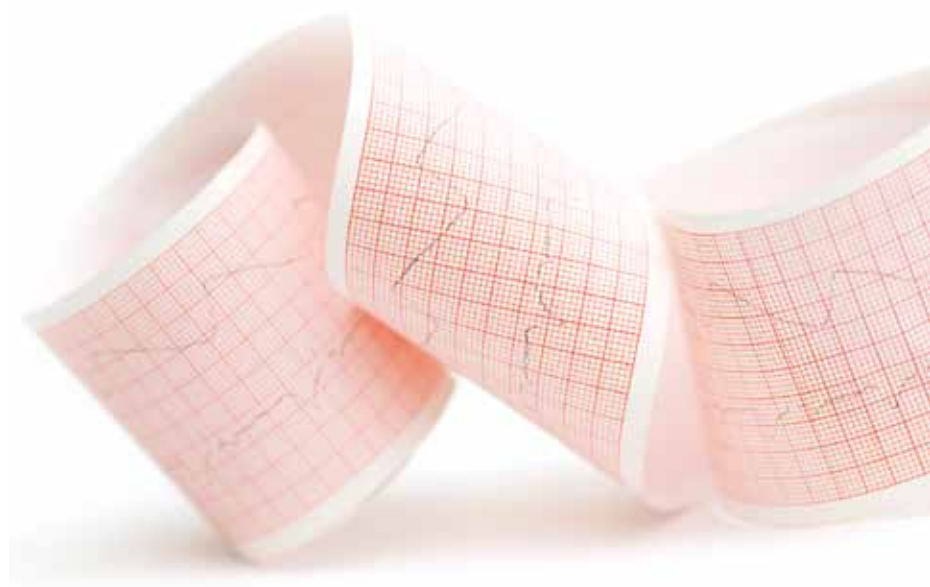


Figure 2 – Sample decision rights RACI framework

Decision	Roles				
	Health System Leadership	Enterprise Analytics Group	Clinical	Finance	Technology
Set health system analytics goals and metrics	A	R	C	C	C
Set and maintain data standards for health system	I	I	R	R	A/R
Determine clinical outcomes to be measured	C	I	A/R	I	C
Determine analytics projects to be resourced	A	R	R	R	R
Allocate analytics resources	I	A/R	C	C	I

Key

- R** = Responsible for ‘doing the work’ and participating in decision making
- A** = Accountable for the work product or outcome of the decision and for ensuring the decision is made
- C** = Consulted by the ‘responsible’ stakeholders to provide input but not directly involved in the work or decision making
- I** = Informed about the decision after the decision has been made but not involved in the work or decision making

Note: A clear decision rights framework can provide the foundation for an enterprise analytics function by defining what role each party plays in decision making. When all stakeholders share a common understanding of the decision making process, they can have more trust that the projects being deployed are in the enterprise’s best interest, and that the data and insights are correct. The sample above shows only five of the many decisions that need to be clarified in the new analytics organisation.

The final step in the establishment of the decision framework for analytics should be to focus on the ‘how’ of decision making. This involves an assessment of the existing cross-functional governance committees and a decision on whether to establish a new analytics governing body or whether an existing leadership team is

to manage and monitor analytics decisions and processes going forward. Either way, a clear charter setting out meeting frequency, voting rights and protocols should be put in place to ensure that the new decision framework for analytics operates smoothly over the long term.

Promoting a culture of analytics

Structuring an effective enterprise analytics function can ultimately provide vital resources that help enhance and accelerate decision making, enabling the organisation to operate as an effective and successful integrated enterprise. But just establishing the core components of a good analytics function may not be sufficient to transform the organisation—a culture shift also needs to take place for the power of analytics to be fully realised.

One tactic to help support behaviour change is to develop and execute a change management and communication campaign to help the organisation understand the nature of the changes and the benefits that will be achieved. It can be helpful to tailor the campaign to the needs of physicians and other stakeholders to keep them engaged with and committed to the program. This can 'brand' the analytics effort, illustrate the new behaviours that are needed for results, build momentum and get people excited about dedicating time and effort to analytics projects. Another tactic for building support for new organisational behaviours is to identify pilot analytics projects and help build effective teams by pulling together resources from multiple areas and achieving a visible 'quick win' that they can promote to other parts of the organisation.

Analysts working across all the functional areas can become ambassadors for change and begin to educate their peers and leaders on the real benefits and possibilities of analytics. These individuals can be supplemented with others with specialised sector experience, complex problem-solving skills and the ability to combine logical and intuitive thinking in each situation.

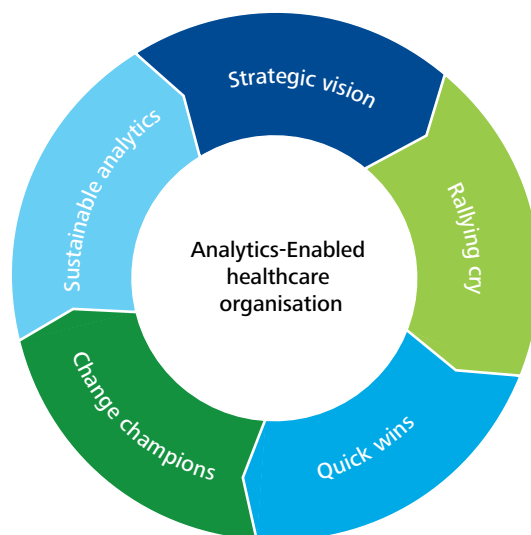
Effective analytics projects should not begin with data and end with models



So where should you start?

Leaders should first agree on a direction that clearly and directly supports the organisation's mission and strategic objectives and links to the analytics program. Once the objectives and priorities have been established by the leadership, a structured approach that leverages leading practices can help accelerate the analytics program. Figure 3 illustrates several important actions that have demonstrated results in real-world situations for other healthcare organisations.

Figure 3 – Steps to help create an analytics programme



Action 1: define the strategic vision—promote alignment by beginning with a clear vision of how analytics can help the organisation. Suggested approaches to doing this should involve engaging with industry peers, conducting a leadership retreat with subject matter specialists, or reviewing other effective programs. Once foundational awareness has been achieved, the leadership can formulate a clear statement of purpose for strategy development.

Action 2: develop a rallying cry—once the future is defined, then communicate the details that will get everyone on board and engaged. Create an analytics strategy that helps identify specific stakeholders, use

cases, resource requirements (data, skills, experience) and expected benefits. During this process the vision can be translated into an actionable strategy that addresses staffing, skills, data, technology and other requirements. Finally, a phased roadmap with specific milestones and checkpoints can be helpful to segment the journey.

Action 3: nominate change champions—identify a core group of champions who share the commitment, experience and passion to launch the program. At this time, it is important to promptly identify the governance and decision-making protocols needed to help implement, maintain and refine the analytics program from inception and as it is extended to other areas of the organisation.

Action 4: create momentum with quick wins—select a pilot project to help gain experience and establish momentum: nothing breeds success like success... Picking a project that offers the opportunity for a quick win allows the organisation to begin building a knowledge base of experience, tools and methods that can be leveraged in future analytics projects. In addition, it can offer a valuable opportunity to develop an experienced core group that can be used to 'seed' other analytics 'Tiger Teams', groups of technical specialists selected for their experience, energy and imagination.

Action 5: sustain enterprise analytics—lessons learned and leading practices should be used to formulate a sustainable analytics strategy. This strategy should address integration with other specific functions such as business planning, data governance, clinical outcomes, finance and IT. Finally, to continue momentum, the analytics function should include structured processes such as intake, project management, communications and planning to maintain alignment between the efforts of the group and the priorities of the organisation.

It is important to understand that developing an effective analytics program should be an iterative process that can yield new lessons with each project. To expedite this process, the checklist in Figure 4 highlights several important questions to be considered.

What are the benefits of getting it right?

Once the analytics program is implemented, the organisation should have a much better capability for analysing, monitoring and addressing the circumstances that impact clinical and business performance. The process of implementing an effective analytics program involves a review of many areas ranging from the quality of data sources to the way in which the information is organised and presented to decision makers. As a result of this process, many lessons can be learned that will contribute to the organisation's mission of delivering high quality, cost-effective care that improves patient and community health.

One thing is certain in healthcare—significant industry change is upon us for the foreseeable future. Through capabilities such as predictive modelling, simulation and data mining—decision makers and analysts can explore various scenarios to determine the likely future impact of their decisions in any of the equally plausible future scenarios. The resulting insights will enhance clinical, business and process management, regulatory compliance and overall competitiveness. This may also help prepare for the eventuality of reported clinical data coming under the same level of scrutiny and certification as financial data. Where an analytics program was once considered a luxury involving statisticians and actuaries, it is rapidly becoming an imperative for doing business and managing the complexity of today's healthcare environment.

Leadership

- Do leaders share a common vision of the future analytics model and have the right incentives in place to operate as one?
- What leadership roles and capabilities are needed to effectively execute enterprise analytics?
- If these capabilities do not currently exist within the organisation, will they be developed internally or acquired from outside?

Organisation structure

- What is the current operating model and organisation design? What is the vision for the future? What gaps exist?
- What analytics capabilities are needed in the future?
- What integration model will best support teamwork and collaboration?

Decision rights

- Are major stakeholders such as physicians, hospital administrators and technology leaders included in the decision rights structure?
- Is there clear agreement on who is accountable for each major decision?
- Do decision makers have easy access to current data, information and analyses?
- Is the mix of collaborative and consensus-driven decision making appropriate?

Behaviour change

- How has this organisation previously reacted to major transformations?
- How will change impact different stakeholders?
- To what extent is there a shared vision and alignment of goals across the organisation?
- What communication channels are most effective for engaging with the various stakeholders who should be involved in the journey?
- What organisational culture will be promoted? Does the capacity to adopt a new culture currently exist?

The impact of Solvency II on data management in insurance

Insurance

Jean-Pierre Maissin
Partner
Advisory & Consulting
Deloitte

Ronan Vander Elst
Directeur
Advisory & Consulting
Deloitte

In recent years, the Luxembourg insurance industry has been under the ever-growing pressure of regulations such as Solvency II. In a nutshell, Solvency II impacts the way insurance companies manage their risks and has consequences across the entire company, e.g. capital, governance, processes and systems.

Consequently, data is an important and wide-ranging topic in Solvency II. Furthermore, data is directly targeted by Solvency II, as it is required to be accurate, complete and appropriate—not to mention traceable. Unarguably, this is easier said than done: especially as the regulators will most likely impose strict penalties. For instance, insufficient data quality will result in an insurer being forced to build and maintain additional capital in order to provide a cushion in the event of errors in the calculation of capital requirements. As a result, the prerequisites for meeting the Solvency II requirements are data governance and data control.

Most insurers are facing the same challenges. Actuaries and risk managers often use a mix of IT extracts from heterogeneous operational systems and various business-managed end-user computing files, causing reconciliation challenges, knotty problems and many other issues. Many manual adjustments are performed, often in a decentralised form, causing important losses of traceability. Data quality checks—when performed—are usually informal and data is not stored in consistent sets, making the reuse of a given input set extremely difficult. Furthermore, insurance companies have to contend with

increasingly heterogeneous data sources, both internal and external, and given both data pushing and pulling.

Nevertheless, Solvency II is far from being the only driver for data management, and neither is it the oldest one. Top-line growth (revenue generation) has always been a concern and a challenge for insurers. Although these days the insurance market appears to be mature, providing limited opportunities for growth at first sight, experience shows that insurance firms still have great potential for improving customer value. To effectively and efficiently benefit from this potential, the starting point should be to identify which customers create and destroy value, and to what extent they do so. This requires excellent insight into key customer information, such as profitability, churn and loyalty drivers. The second step, i.e. customer segmentation, should be performed on quantitative characteristics, to differentiate customers from each other and group them into business-meaningful clusters. These characteristics include—but are not limited to—product ownership, sales channel preferences, socio-demographics and transactional data. If required, the third step for improving the customer value curve should involve the concept of selective retention, i.e. retaining valuable



customers, while letting go of non-profitable ones. The main challenge in this process is that it requires the cross-referencing of different data sources, e.g. customer relationships, and operational and financial databases.

Along with top-line growth, bottom-line growth (cost reduction) is another essential driver for data management. Bottom-line growth, once the top-line is fixed, relies mostly on the reduction of operational costs. And experience shows that the greatest operational cost linked to data management lies in the duplication of extracted data. In many companies, the IT department is bombarded with numerous and repeated requests for data extracts from all departments. Hence, multiple duplicates are created and spread across the company causing consequent losses of ownership. For that matter, increasing automation in data management is key to reducing errors and correction costs, spotting inefficient cost centres and rationalising the interfacing with data repositories.

Finally, there is one other data management concept that is ideal for meeting the requirements of Solvency II: data centralisation. Building up an Enterprise Data Warehouse (EDWH) in an insurance company is the best way to gather all corporate data at a single point and with a single version of the truth in a unique and standardised format, and to make it available for all departments.

As a result, the prerequisites for meeting the Solvency II requirements are data governance and data control

This is where Solvency II can play the essential role of an enabler. Implementing Solvency II is unarguably a heavy investment, and so everyone's goal should be to reach an acceptable level of compliance at the most reasonable cost. However, this should not be quite the end of the story. Indeed, considering Solvency II in terms of a constraining regulation only would be a huge missed opportunity. We believe Solvency II is an extremely powerful springboard for implementing an EDWH and revising data governance, based on a two-step roadmap:

- 1) Identify your dashboarding and reporting needs and
- 2) Identify among these needs quick wins with Solvency II data requirements

The whole idea is very simple: Solvency II—given the heavy and mandatory investment it requires—must be used as a lever for implementing data management mechanisms and building an EDWH. Through revenue generation and cost reduction, these will make a major contribution to business growth by enabling you to implement and benefit from the latest data exploitation techniques, such as business intelligence and analytics.

Do you DLP?

Maximising the business value of your Data Loss Prevention (DLP) solution

Data security

Roland Bastin

Partner
Advisory & Consulting
Deloitte

François Barret

Senior Manager
Advisory & Consulting
Deloitte



Data can be both an asset and a liability. As organisations grow, the volume and complexity of data required to support the business increases. All organisations store sensitive data that their customers, business partners, shareholders and the Board expect them to protect against theft, loss and misuse.

The intrinsic and contextual value of data and associated ownership risks vary throughout the data life cycle. The business value of information assets—gains on process and function performance, revenue and margin contribution—is a function of:

- Inherent value
- Contextual value
- Enterprise context
- Associated risk
- Cost of ownership

Data can be managed like any other enterprise asset, subject to the same net business value calculations balancing value, risk and total cost of ownership.

Figure 1 - Enterprise data lifecycle

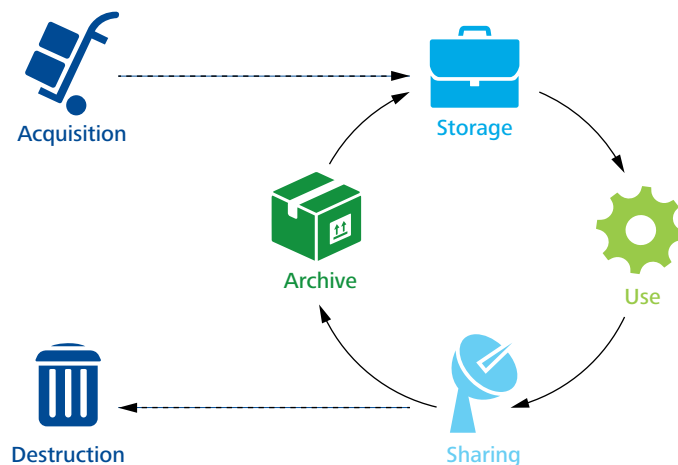
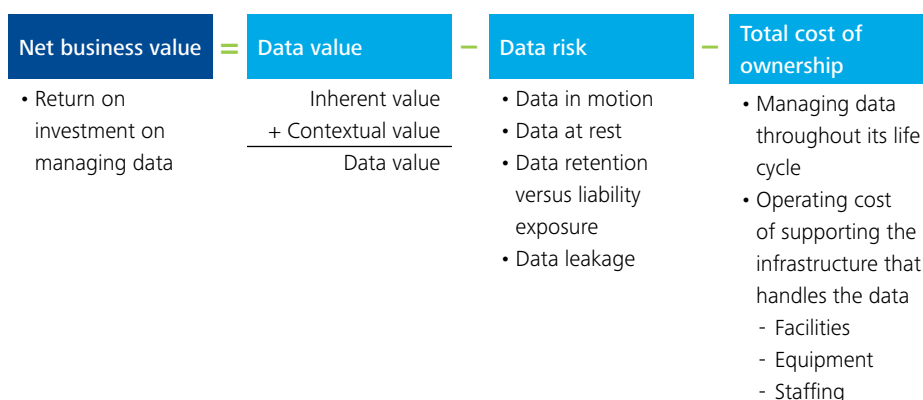


Figure 2 - Analysing data assets



When managed data and information has a negative net business value, the enterprise has several options, including:

- Increasing the value
- Reducing risk
- Discarding the data

Despite data management, high profile security breaches involving personal and corporate data continue.

What is data loss?

Data loss can be defined as the movement of an information asset from an intended state to an unintended, inappropriate or unauthorised state, representing a risk or a potentially negative impact to the organisation.

Data can be categorised using the following criteria:

1. Form:

- Structured—hierarchical, relational, network: XML files, relational information (databases), files with detailed attributes, transactional information
- Unstructured—free form (80% of potentially usable business information): email, blueprints, audio, video, images

2. Type:

- Personal: credit card number, social security number, social insurance number, name and/or address, financial information, medical information, date of birth
- Corporate: strategy, legal, intellectual property, intelligence information, financial information, sales information, marketing information

3. The type of threat data is exposed to:

- Insider: disgruntled employee, ladder climber, petty ID thief, contractors, outsourcers, business partners/vendors, fraudsters
- Outsider: spies and industry espionage, gangs, ideologists, cyber terrorists, scammers (e.g. phisher), social engineer, script kiddies

Data loss can come in many forms, and may compromise various types of personal or corporate information. Data is being targeted by both internal and external groups.

A number of factors are driving organisations' data loss prevention needs: globalisation, varying regulations, varying customer expectations, customer privacy sensitivity, brand risk, advances in technology, mobile devices, advanced persistent threats (APT), extended enterprise, third party service provider risk, regulation and compliance (anti-money laundering, breach notification, PCI-DSS, GLBA, etc.) and data growth.

The data explosion

There has been massive growth in data volumes in recent years. Almost 3 trillion gigabytes of information was created and replicated as of 2012, compared to over 1 trillion in 2012 and 130 million in 2005. There are several factors driving this data growth and the associated challenges, including:

- **Globalisation:** *"70% of economic growth over the next decade will come from emerging markets, with China and India accounting for 40% of that growth"*⁷
- **Organisation:** *"40% projected growth in global data generated per year vs. 5% growth in global IT spending"*⁸
- **Consumerisation:**
 - *"On an aggregate, 56% of companies say yes to consumerisation and allow employees to use their personal devices for work-related activities"*⁹
 - *"31% of the mobile devices connecting to the corporate network are owned by the employees: 66% are laptops, 25% smartphones and 9% are tablets"*¹⁰

The rise in data volumes is forcing organisations to re-evaluate and refocus their information management practices to better integrate and leverage data in core business processes.

Sensitive data such as personal and financial information and intellectual property moves horizontally across organisational boundaries, including vertical business processes. Organisations commonly do not have a good understanding of the movement, proliferation and changes in their data leaving them susceptible to data loss.

Additionally, organisational boundaries are changing as enterprises become more virtual, blurring the distinction between internal and external. Perimeter-centric security often hinders business growth and brings a false sense of security when it comes to data protection.

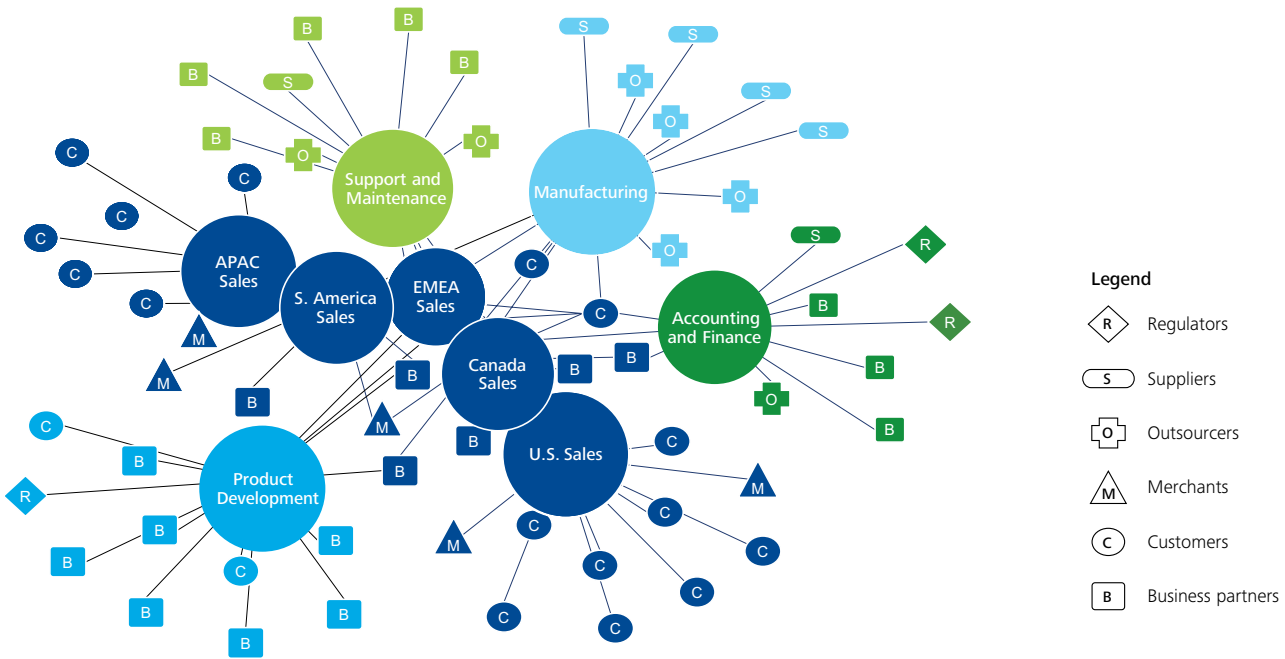
⁷ World Economic Outlook Database, International Monetary Fund, UNWTO World Tourism Organisation

⁸ McKinsey Global Institute—Big data: The next frontier for innovation, competition, and productivity

⁹ Trend Micro Consumerization Report 2011

¹⁰ Trend Micro Consumerization Report 2011

Figure 3 - Blurred organisational boundaries



How data loss can happen to your organisation

Sensitive data can be lost or compromised in a number of intentional or unintentional ways, due to 'threat agents' (employees, users, hackers, etc.) acting in a malicious or innocent manner. Some common data loss scenarios are:

- Data in use (i.e. 'What is the agent doing with it?'):
 - Disgruntled employees copying files containing personal or confidential information to portable devices (e.g. flash drives)
 - Users printing sensitive data to equipment in common areas which can be accessed by others
- Data in motion (i.e. 'Where is the data going?'):
 - Users sending sensitive data to personal webmail accounts in order to work at home
 - Personal and confidential information being shared with third parties for valid business purposes using insecure transmission protocols
 - Malicious insiders transmitting personal and confidential information outside of an organisation's network

- Data at rest (i.e. 'Where is sensitive data located?'):
 - Business users innocently placing personal information in insecure storage locations where access is not administered by IT
 - Database administrators storing (unencrypted) backup copies of sensitive data in unapproved locations

The intrinsic and contextual value of data and associated ownership risks vary throughout the data life cycle



Data loss can come in many forms, and may compromise various types of personal or corporate information

Data loss proliferation

Data is growing at an exponential rate, as is the number of incidents in which data has been lost.

More than 1600 data loss incidents occurred¹¹ last year (See Figure 4).

Incidents involving digital media and hacking are most common¹² (Figure 5).

Data loss is occurring across industries, affecting organisations of varying sizes and different types of information assets¹³ (Figure 6).

The variables to take into account when calculating the cost of a data loss incident are:

- Brand impact:
 - Media scrutiny
 - Loss of customers
 - Loss of business due to critical intellectual asset loss
- Regulatory impact:
 - Independent audit fees
 - Regulatory fines
- Financial impact:
 - Notification
 - Lost business
 - Response costs
 - Competitive disadvantage
- Operational impact:
 - Diversion of employees from strategic initiatives to work on damage limitation
 - Need to implement comprehensive (additional) security solutions

Figure 4 - Number of data loss incidents over time

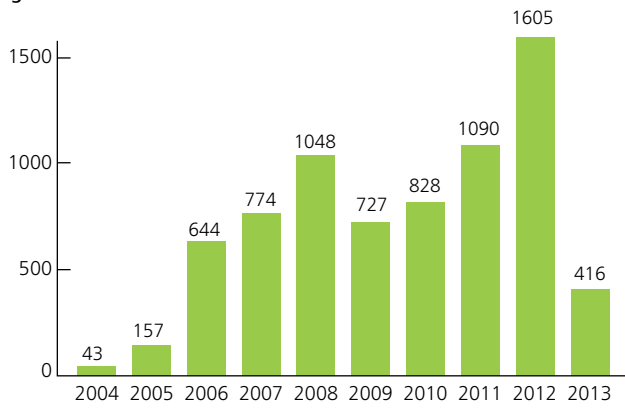


Figure 5 - Types of data loss incidents

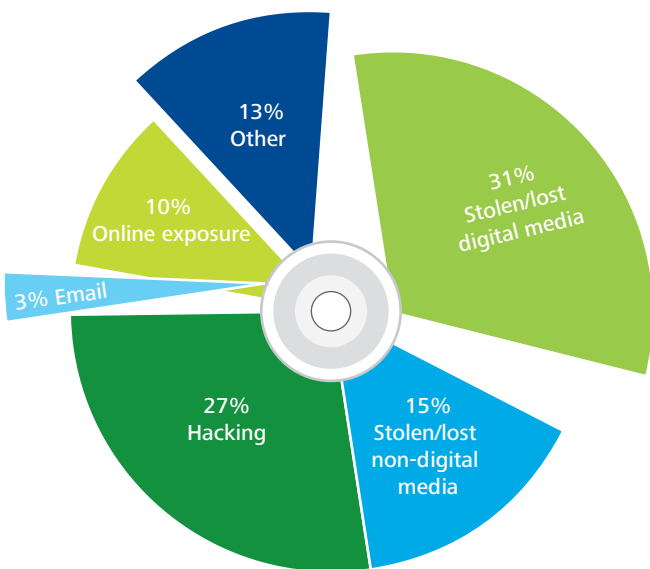
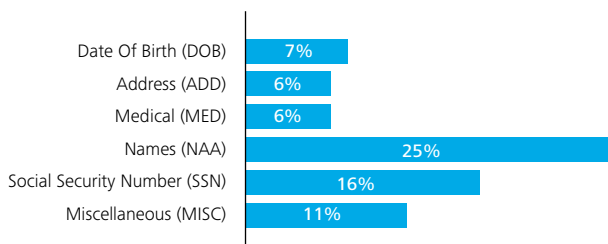


Figure 6 - Types of data loss



Moreover, a recent study by the Ponemon Institute¹⁴ shows that the cost of data loss is steadily increasing.

Figure 7 - Average cost per record by cost activity

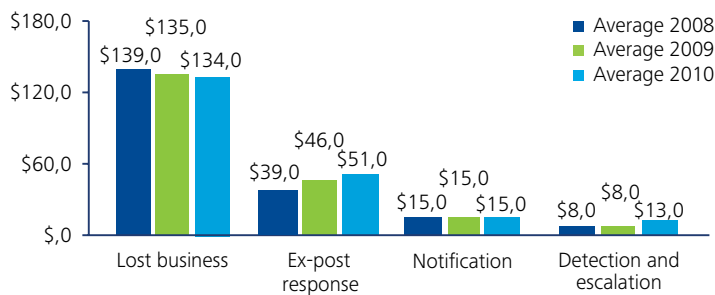


Figure 8 - Cost per record of direct and indirect costs



The cost to organisations occurs at each stage of the incident response life cycle—detection, notification, post-response—leading to the cost of lost business.

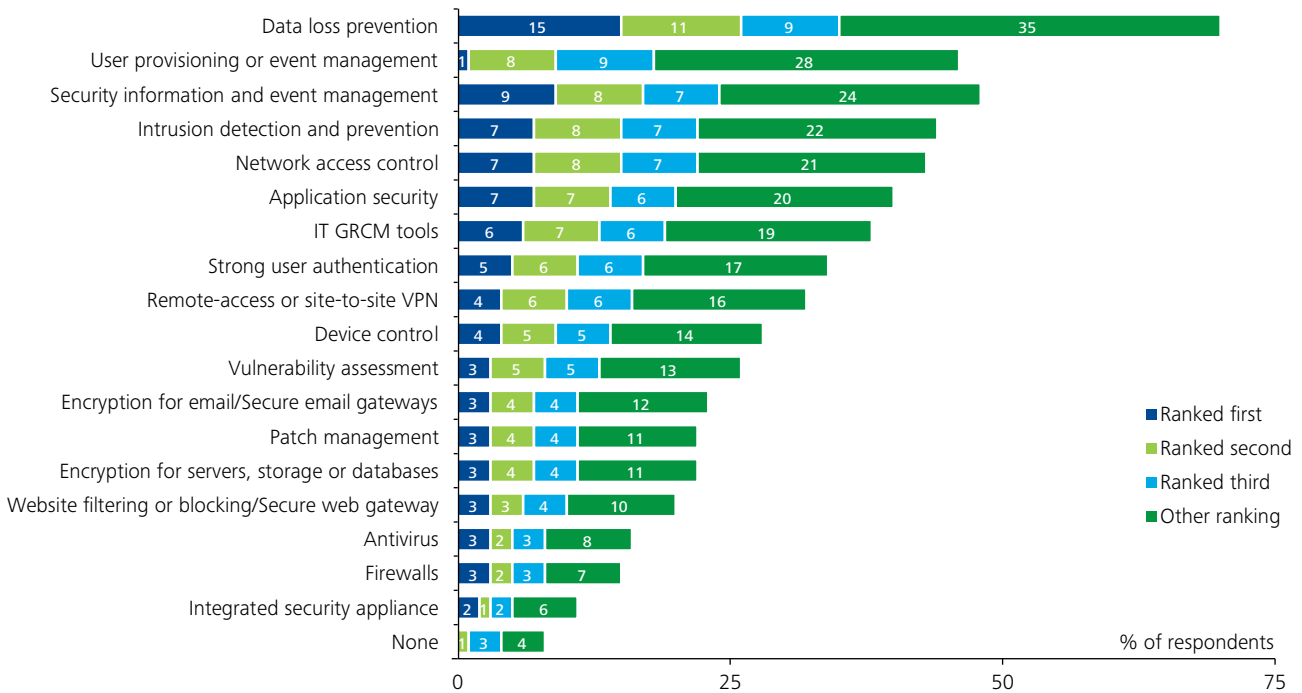
The cost of lost business has remained relatively stable last four years, and now averages US\$135 per record compromised, or 63% of data breach costs

Data loss can have a significant impact on an organisation's bottom line, which is why organisations are increasingly turning to data protection measures in order to prevent data loss.

Data protection is a general term that encompasses a number of measures, including:

- **Data encryption**—this refers to a method of modifying data so that it is meaningless and unreadable in its encrypted form. It must also be reasonably secure, i.e. it must not be easy to decrypt without the proper key
- **Data obfuscation**—this is when data is rendered unusable by some means, but it is not considered a reliable form of encryption (obfuscating the data with a simple substitution cipher is not considered encryption)
 - Substitution, which replaces a value in the column with fictional data
 - Randomisation, which replaces the value with random data
 - Shuffling, which switches column values between records
 - Nullifying, which replaces column values with NULL
 - Skewing, which alters the numeric data by a random variance
 - Encryption/decryption, which employs reversible scrambling
- **Data masking** is a method of hiding sensitive data in a way that the clear text cannot be reconstructed from the displayed data. This is useful in situations where it is only necessary to display a portion of the data
- **Data generation** is a method of creating fictional data following certain patterns to completely replace the original data set with the intent of being fully displayed
- **Data redaction** is a method of locating unstructured data in the document, indexing it using OCR, and masking or obfuscating as appropriate
- **Data loss prevention**, which according to a recent Gartner survey, is the top priority for organisations implementing security technologies

Figure 9 - DLP implementation trends



What is DLP?

Data Loss Prevention (DLP) should be part of an overall information risk and data protection/privacy strategy. It starts with understanding what your assets are. Not all data can be protected equally—you must first understand what needs to be protected the most.

DLP involves tools that monitor, identify and protect electronic data as it moves to, from, and through an organisation. Typically, data can be described as being in a state of use, motion or rest:

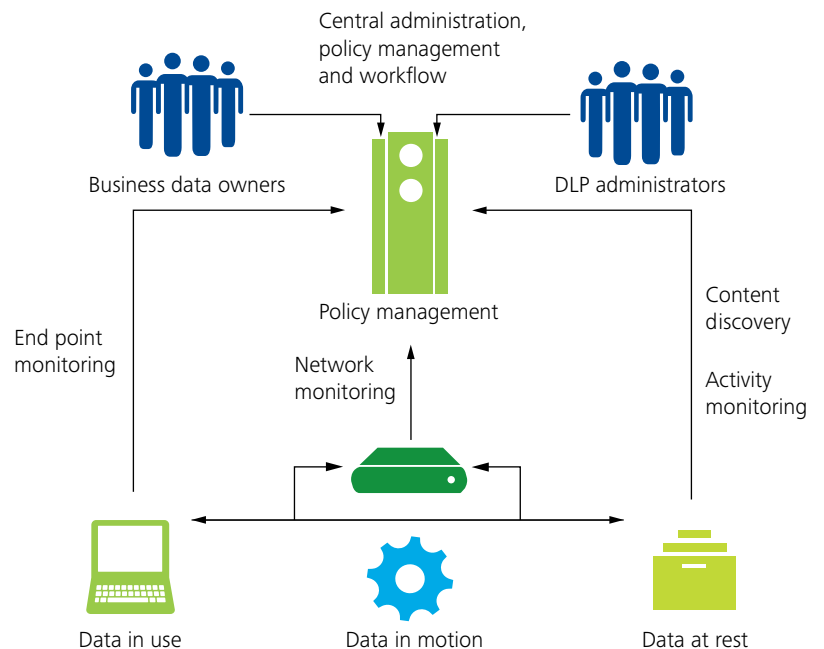
- **Data in use:**
 - Monitor user interactions with data to identify, for example, attempts to transfer sensitive content to a USB drive and apply policy
 - Common controls include disabling Copy, Print, Print Screen, Open, Paste, Save, Save As, and Notification

- **Data in motion:**
 - Analyse data traffic over the network to identify sensitive content being sent via email, IM, HTTP or FTP, and apply policy
 - Often requires integration with mail transfer agents, network components and other infrastructure
 - Common controls include Allow, Audit, Quarantine, Block, Encrypt and Notification
- **Data at rest:**
 - Scan and inspect enterprise data repositories to identify sensitive content and apply policy accordingly
 - Common controls include Encryption, Obfuscation, Quarantine, Deletion, and Notification

DLP tools typically consist of the following components:

- **Policy Management and Enforcement Servers:** a central platform for defining, deploying and implementing enterprise-wide DLP policies across various DLP components. Management servers are also used for incident response workflow management and reporting
- **End-point agents:** located within end-user devices such as desktops, laptops, etc. These agents discover and collect data on Data in Use activities performed on the device and are responsible for enforcing DLP policies on the device and reporting back to the Policy Management and Enforcement Server(s)
- **Network components:** can monitor network communications and restrict the flow of Data in Motion as necessary. Network components provide real-time monitoring and reporting of policy breaches to the Policy Management and Enforcement Server(s)
- **Discover components:** together with end-point agents, these components perform discovery activities for Data at Rest. Data discovery is based on the policies defined in the Policy Management and Enforcement Server(s)

Figure 10 - DLP solution conceptual model

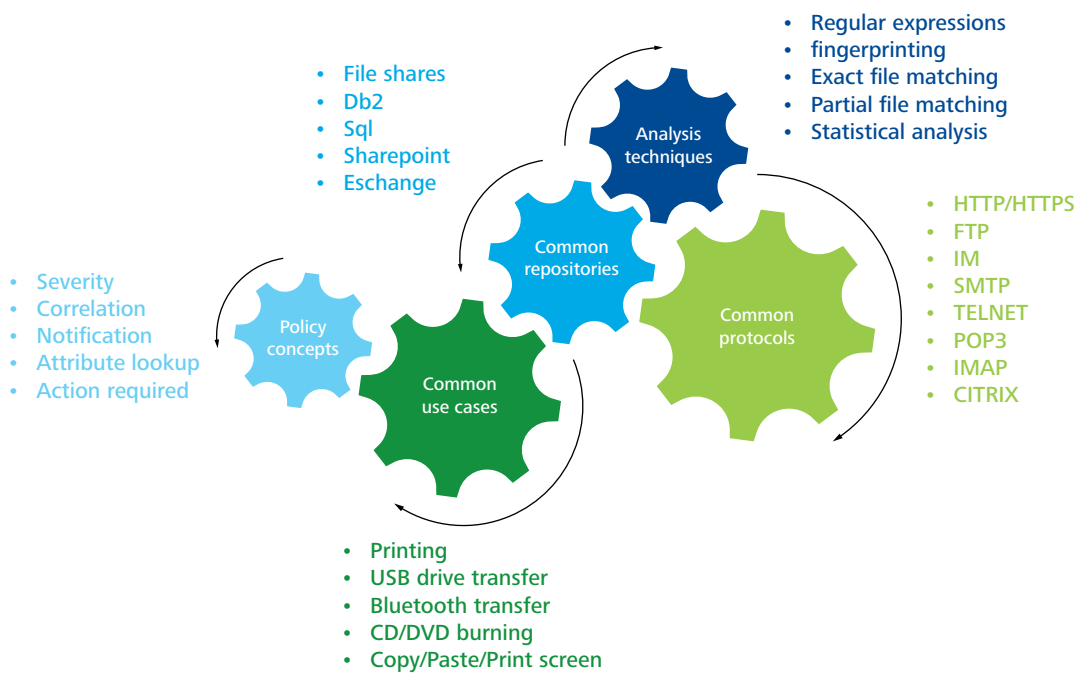


More than 1600 data loss incidents occurred last year

DLP tools vary significantly in their capabilities and have different strengths and weaknesses. However, there are some key capabilities and concepts that are generally applicable to most DLP tools, as summarised below:



Figure 11 - DLP key capabilities and concepts



Common DLP deployment challenges and their root causes

DLP solutions often do not achieve full business and data loss mitigation due to a number of common, but preventable challenges and root causes, including:

Challenges	Root causes
Business and IT sponsor frustration with the speed at which the solution becomes functional	<ul style="list-style-type: none"> Lack of a DLP strategy provides no clear vision and direction for the solution Poorly defined requirements cause work to be repeated, with a related cost 'Big Bang' approach vs. proof of concept, pilot and phased implementation DLP vendor marketing promises fail to materialise
Complaints from executive stakeholders that they don't understand the value the solution offers	<ul style="list-style-type: none"> Poorly defined or lack of DLP metrics and success criteria Inability to collect and report on metrics
Business community pushback due to a lack of communication or transparency	<ul style="list-style-type: none"> Poorly defined or lack of a training, awareness and communications plan
Inability to correlate and report upon DLP and other types of security incidents and associated risks	<ul style="list-style-type: none"> Lack of integration between DLP and Security Information and Event Management (SIEM) solutions Lack of integration between DLP and Governance, Risk and Compliance (GRC) solutions
Advanced capabilities such as deleting, blocking, encrypting and quarantining are rarely implemented	<ul style="list-style-type: none"> Lack of processes for business use case analysis and approval Policies defined based on content vs. contextual analysis Lack of processes for enabling efficient recovery of blocked or quarantined information Lack of processes for managing encrypted messages/transmissions/files
Data in Use capabilities are rarely implemented, if at all	<ul style="list-style-type: none"> Lack of processes for deployment and management of thousands of agents Endpoint technology limitations or incompatibility with vendor solutions
Incidents are not responded to in a timely manner or at all, or all incidents are treated as "equal"	<ul style="list-style-type: none"> Poorly defined or lack of incident severity levels and response workflows/procedures Roles and responsibilities not clearly defined Insufficient training and resourcing of incident response team(s) False positives caused by 'loosely' defined policies
High volumes of false positives lead to support team frustration, or legitimate business processes are blocked	<ul style="list-style-type: none"> Lack of processes for business use case analysis and approval Policies defined based on content vs. contextual analysis Lack of sufficient testing and fine-tuning of policies over time before full-scale deployment
Sensitive personal and confidential information is consistently found in unanticipated/undesirable locations and detected leaving the organisation's network	<ul style="list-style-type: none"> Poorly defined or lack of data classification policy Policies defined to monitor/search for minimal data elements and/or files Lack of an inventory of network egress points, storage repositories and end points Lack of business process re-engineering Poor communication with business users regarding security expectations and their responsibilities Poorly defined or lack of disciplinary measures and enforcement

Our approach

In our experience, a successful DLP solution/program must be approached holistically, focusing not just on the technology, but also on the people and processes needed to support and interface with the system(s). The approach we propose is as follows:



This approach integrates people, processes and technology. It allows DLP solutions to be aligned with business drivers and value



Key considerations for a successful approach

Below are some key considerations that should be taken into account as a first step towards a successful DLP tool selection and subsequent implementation:

Domain	Key considerations
General	<ul style="list-style-type: none">• What information or data elements present the most risk?• What locations or business units present the most risk?• What are our mitigating controls?• How robust do we need our governance structure and incident response workflow to be to support our goals and mitigate our risks?• What type of resourcing do we need to support management of the tool and the incidents it generates on an ongoing basis?
Data at rest	<ul style="list-style-type: none">• What types of data repository does the solution need to be able to scan?• What do we plan to do with the data once it is found?
Data in motion	<ul style="list-style-type: none">• Do we care about outgoing transmissions only, or incoming and internal transmissions as well?• What protocols do we need to monitor and protect?• Do we need to block or encrypt traffic?
Data in use	<ul style="list-style-type: none">• What platforms does the solution need to support?• What do we want the tool to accomplish when users are not on the network?

Conclusion

Approaching DLP in a more holistic manner and treating it as a program to drive organisational change, minimise business risk and realise full business value, as opposed to treating it as a technology “plug and play” type of solution, will bring some of the following key benefits:

- Clearly articulates the DLP program vision and strategy
- Helps prevent the cost of repeating work through clearly defined scope and requirements
- Demonstrate business value through ‘quick wins’
- Maintains stakeholder support through clearly defined metrics and success criteria
- Helps to prevent business community and end-user outcry through well designed, planned and delivered training and communications
- Enables the use of advanced system capabilities that can help prevent significant legal, regulatory, compliance and brand issues
- Improves incident response capabilities, helping the organisation to respond more efficiently and effectively in the event of data loss
- Helps prevent business interruption through advanced search/monitor policy definition that consider not only content but context
- Facilitates advanced incident correlation and reporting on governance, risk and compliance issues through integration with other security technologies

Contacts

Operational Excellence



Basil Sommerfeld
Partner - Operations & Human Capital Leader
+352 451 452 646
bsommerfeld@deloitte.lu



Pascal Martino
Directeur - Strategy & Corporate Finance
+352 451 452 119
pamartino@deloitte.lu



Julie Chaidron
Manager - Strategy & Corporate Finance
+352 451 454 807
jchaidron@deloitte.lu

Advisory & Consulting



Benjamin Collette
Partner - Strategy & Corporate Finance Leader
+352 451 452 809
bcollette@deloitte.lu



Petra Hazenberg
Partner - Strategy & Corporate Finance
+352 451 452 689
phazenberg@deloitte.lu



Filip Gilbert
Partner - Human Capital Advisory/Transformation
+352 451 452 743
fgilbert@deloitte.lu



Patrick Laurent
Partner - Technology & Enterprise Application
+352 451 454 170
palaurent@deloitte.lu



Jean-Pierre Maissin
Partner - Technology & Enterprise Application
+352 451 452 834
jpmaissin@deloitte.lu



Roland Bastin
Partner - Information & Technology Risk
+352 451 452 213
rbastin@deloitte.lu



Laurent Berliner
Partner - Business Risk
+352 451 452 328
lberliner@deloitte.lu



Marco Lichtfous
Partner - Capital Markets/Financial Risk
+352 451 454 876
mlichtfous@deloitte.lu

Audit



Sophie Mitchell
Partner - Audit Leader
+352 451 452 481
somitchell@deloitte.lu

Tax



Raymond Krawczykowski
Partner - Tax Leader
+352 451 452 500
rkrawczykowski@deloitte.lu

EU Institutions and Supranationals Industry



Joël Vanoverschelde
Partner - EU Institutions and Supranationals Leader
+352 451 452 850
jvanoverschelde@deloitte.lu

Bank and Credit Institutions



Martin Flaunet
Partner - Bank and Credit Institutions Leader
+352 451 452 334
mflaunet@deloitte.lu

Healthcare



Luc Brucher
Partner - Healthcare Leader
+352 451 454 704
lbrucher@deloitte.lu

Insurance



Thierry Flamand
Partner - Insurance Leader
+352 451 454 920
tflamand@deloitte.lu

Investment Funds and Hedge Funds



Johnny Yip
Partner - Investment Funds and Hedge Funds Leader
+352 451 452 489
jyiplanyan@deloitte.lu

Technology, media and Telecommunications - Public Sector



Georges Kioes
Partner - Technology, media and Telecommunications and Public Sector Leader
+352 451 452 249
gkioes@deloitte.lu

Deloitte is a multidisciplinary service organisation which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

Due to the constant changes and amendments to Luxembourg legislation, Deloitte cannot assume any liability for the content of this leaflet. It shall only serve as general information and shall not replace the need to consult your Deloitte adviser.

About Deloitte Touche Tohmatsu Limited:

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/lu/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's approximately 200,000 professionals are committed to becoming the standard of excellence.

