WHITE PAPER

Governance, Risk and Compliance Series

- The Role of Data Management in Mitigating Risk

By Mike Ferguson
Intelligent Business Strategies
August 2010

Prepared for:

TABLE OF CONTENTS

AN INTRODUCTION TO GOVERNANCE, RISK AND COMPLIANCE

Corporate failures in that last five to ten years have resulted in a greater focus on GRC to raise the bar in striving to achiev higher quality business practices

In the last decade we have seen a significant number of major corporate failures in various countries around the world. Some of these failures have been have been due to poor management practices (also known as *governance*). This has resulted in new legislation, and *compliance* regulations being introduced in an attempt to force companies to raise the bar in terms of higher quality processes and business practices. In the last few years it has been the collapse of the financial services industry that has caught the attention of many. In this case, many of the banks that have collapsed have done so because of poor credit *risk management* practices. Lending money to higher-risk customers in the sub-prime mortgage market ultimately resulted in many of these customers not being able to pay their mortgages. As a result many banks collapsed or were taken over by governments or other banks.

The focus from all of this fallout has come down to three main areas that are closely related. These are:

- Corporate governance
- Risk management
- Enterprise compliance

Together these are known as governance, risk and compliance (GRC). Wikipedia provides an excellent diagram (see figure 1) of these three areas and how they are integrated. It also shows that a combination of strategy, people, processes and technology are needed to get the GRC problem under control.

Companies need a GRC strategy to help manage their business

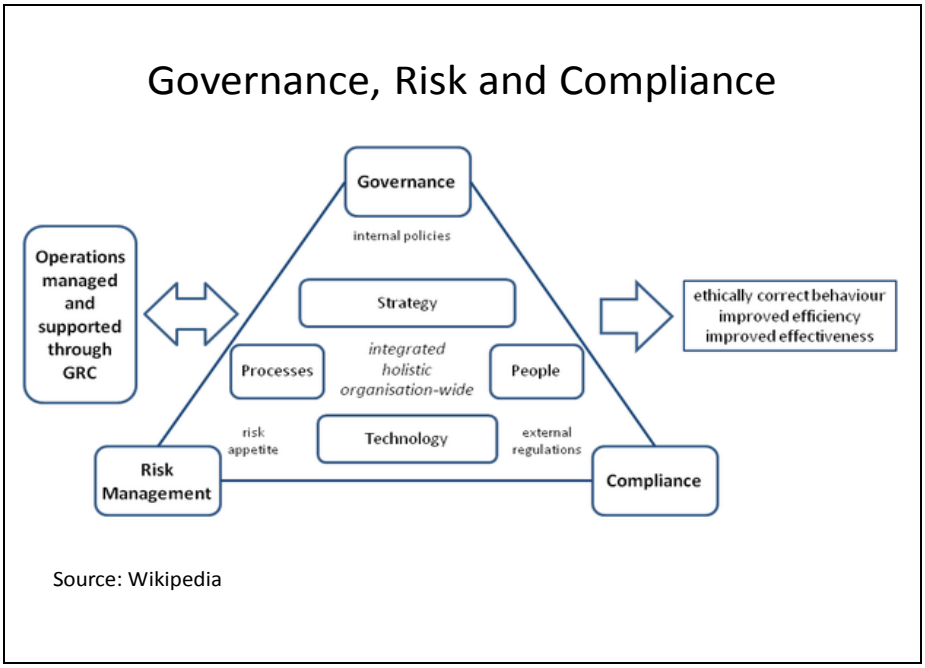

Figure 1

Governance is about accountability and control

Looking at this in more detail, **governance** describes the overall management and control of the entire organisation. Governance requires more use of control structures based on accountability and approval. It also requires standardisation

and integration of business processes as well as better use of management information made possible by corporate performance management and business intelligence.

Risk management is about improving the ability to mitigate risk

Risk management is the set of processes through which management identifies, analyses and preferably avoids risks that might adversely impact the organization's ability to meet its business objectives. It is also about being able to quickly detect risks that occur and respond in a timely manner to minimise the impact of these risk *events* on the business as a whole. Breach of legislation, non-compliance with regulations and credit risk exposure are key risk areas of concern in GRC.

Increasing amounts of business legislation and regulations have led many companies to focus on compliance

Compliance is about conforming to stated requirements. These requirements may be specified in legislation (e.g. the US Sarbanes-Oxley Act), industry regulations (e.g. the Solvency II regulation for the insurance industry) or even in corporate policies. Business analysis is needed to identify compliance requirements, assess the state of compliance in the organisation at present, and assess the risks and potential costs of non-compliance against the projected cost of achieving it. Implementation of compliance requirements can cause changes to business processes, reporting, event monitoring and organisational accountability.

Underpinning GRC is a dependency on data. Data is needed to govern and manage a business, to manage risk, and to help the business remain compliant. Data itself must be governed so that it remains *correct, complete, trusted* and clearly *understood*. Without this a GRC initiative cannot be built on a solid foundation. In the context of risk, data must be secured, access to it managed, and sensitive data masked to uphold privacy. In the context of compliance, the data and the policies around that data must be defined, maintained, managed and be auditable through common processes.

Companies need a GRC strategy

Looking at figure 1, an integrated, holistic, enterprise wide approach to GRC is needed and this is possible via strategy, people, processes and technology. Given that a company's ability to implement GRC is dependent on data, we also need to apply strategy, people, processes and technology to data to get the foundation right for GRC.

People, processes and technology are needed to implement GRC

In this **second** paper in the GRC series, we look at how data management can help companies mitigate risk and how that feeds into GRC from a business perspective. One more paper in the series will follow to look at how compliance applies to data.

WHAT IS ENTERPRISE RISK MANAGEMENT?

Publicly quoted companies are now evaluated on their ability to manage risk

In November 2007, Standard and Poors(S&P) issued a new Request for Comment on Enterprise Risk Management Analysis For Credit Ratings Of Nonfinancial Companies. Their intent was to establish an enterprise risk management (ERM) framework to be able to rate non-financial companies in addition to existing rating mechanisms for evaluating risk management in financial institutions. In fact, what they publish could also apply to financial institutions. The reason why this was important is that it really turned the spotlight on risk management in any industry to see how well companies can identify risks and manage them. Since then S&P have gone on to create their own risk management evaluation mechanisms that can reflect badly on stock prices if a company is marked down on this important area. Note also that ERM is the 'R' in GRC. It is therefore not stand-alone. Its relationship to compliance is that risks need to be avoided in order to remain compliant. Similarly the relationship between risk management and governance is reflected in risk adjusted corporate performance management (CPM).

Enterprise risk management is a key component of any GRC initiative

An inventory of all major risks and their impact on the business is a fundamentally important

The most obvious question in enterprise risk management is does your company have an inventory of all major risks that may impact on the company's ability to remain solvent and trade confidently? Is there somewhere you can go to see what risks the company has identified, the potential business impact of these risks and what is being done to manage them? There are many different kinds of risk. S&P published this example set in their 2007 document:

Environment risks	Financial risks	Supply risks	Management risks
Business continuity	Capital availability	Commodity prices	Corporate governance
Business market environment	Credit/counterparty	Supply chain	Data security
Environmental	Financial market risk		Employee health and safety
Liability lawsuits	Inflation		Intellectual property
Natural disasters/weather	Interest rates		Labour disputes
Pandemic	Liquidity		Labour skills shortage
Physical damage			M&A/restructuring
Political risk			Managing complexity
Regulatory/legislative			Outsourcing problems

Source: Standard and Poors

You could easily take this high level categorisation of risks to a much lower level. For example, the data security risk mentioned above can be broken down into data privacy, secure data access, data recoverability and data defects. Whatever the risks you face, they need to be documented. However ERM goes much deeper than this. The 2007 announcement by S&P was clearly aimed at being able to understand and evaluate the whole risk management issue from end to end in publically quoted companies. The S&P ERM document includes:

- Risk management culture and governance
- Risk controls
- Emerging risks
- Strategic risk management

Key risk indicators (KRIs) are used to measure the success of a risk management program

Risk management culture and governance is about implementing an ERM program. This program needs to include a vision on risk management, statements on policy towards risk, statements on risk tolerance, identification of staff responsible for risk management, staff reporting structure for risk related issues and risk management reports that go to executives and auditing bodies. It should also include details how the company measures success of its risk-management program using key risk indicators (KRIs). Furthermore it should state how KRIs affect management remuneration and how risk management integrates with corporate performance management and budgeting. This latter point is known as risk adjusted performance management.

Risk controls help to manage and prevent major risks ocurring

Monitoring KRI thresholds allows companies to trigger actions to minimise business impact of a risk when tolerence levels are breached

Risk controls are associated with how the company identifies and controls each major risk. To mitigate risk, companies need to understand what the major risks are, the risk limits are for each major risk and what controls are in place to enforce these limits. These controls may be in the form of approval processes and other checks and balances. KRIs are typically used to monitor and control major risks. KRI thresholds must be also documented to make sure that risk limits are known and not breached. Risk management also needs to be integrated into business processes and risks intelligence needs to be shared with senior management. If risks occur, then there needs to be a process to manage losses and manage changes to ERM procedures to avoid the same loss happening again. These changes also need to be monitored and be auditable.

It is important to have tested procedures in place to deal with disasters

Emerging risks are about what processes and procedures a company has in place to mitigate risk and to prepare for a disaster. There could be several potential 'disasters' defined, each with their own severity. Companies need to identify and rank disasters in order of importance, stress test each of them and put any necessary contingency plans in place to be able to respond in a robust way if they occur. In particular, a company must understand the impact of risks on its liquidity and have liquidity risk management practices in place to monitor this. In that sense a company needs to monitor external events and trends as well as internal events and trends to anticipate the emergence of so-called disasters.

Risk adjusted corporate performance management is important to make sure that risk is taken into account when making strategic decisions

Strategic risk management involves the development of strategic plans that may include risk/reward analysis when allocating resources (e.g., capital, talent). This also includes reflecting risk in strategic decision making, pricing, and performance measurement. It is no accident that risk management is considered the flip side of performance management when it comes to strategic decision making. This is sometimes referred to as risk adjusted CPM where strategic level CPM scorecards include both Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs). It should be possible to see an overview or risks on a CPM scorecard with detailed drill down on risks supported. This is because risk management affects financial decisions and must be taken into account.

Given this definition of enterprise risk management it is obvious that implementing it successfully depends on data. For ERM to work well, this data needs to be trusted and secure. Understanding the data issues associated with risk management is therefore important because these issues may increase the possibility of risks occurring that may have a detrimental business impact.

DATA ISSUES THAT CONTRIBUTE TO BUSINESS RISK

Poor data quality and data privacy violations increase risks in the enterprise

With respect to risk management there are a number of data related risk issues that need to be managed in a GRC program to prevent data problems contributing to the occurrence of business risks. These include the risks associated with:

- Data quality
- Data privacy
- Unauthorised data maintenance
- Data synchronisation
- Data recovery

Let's look at each of these in more detail

DATA QUALITY RISKS

We have already said that trusted data is needed for ERM. With respect to data quality, there is no doubt that data defects can cause business risks to occur. For example in insurance, poor-quality customer, insured risk and/or claims data fed into 'propensity to lapse' predictive models could result in incorrect or too many customers being flagged as likely to lapse. This means that underwriters may seek to obtain renewals on high-risk customers and marketing budgets set aside for customer retention may become poorly targeted. This result is an increased risk of driving up claims and damaging loss ratios.

Data defects can increase the risk of process delays and unplanned operational costs

In manufacturing, incomplete and/or inaccurate order data can cause production planning errors, which in turn impacts production schedules causing manufacturing errors and shortages or over manufacture of finished goods. Over-manufacture would drive up energy and material costs which are the top concerns of many manufacturing CFOs. This problem can also be caused by erroneous data on available stocks.

While IT is not responsible for what business users enter into databases and applications it nevertheless IT that is often burdened trying to keep data quality accurate and complete in underlying data stores. It does this by making use of data profiling and data cleansing technology to help identify and clean up poor quality data or to prevent poor quality data getting beyond data entry. In addition, business owners need to monitor data quality in their business areas to make sure that it is not deteriorating. Data quality monitoring technology can be used to help with this task.

Data ownership is an important factor when managing 'at risk' data

A key question however is who is responsible for what third parties can see? For example, if business owners and data stewards inside the enterprise monitor the quality of data used internally, then who is responsible for the data available to customers, partners or suppliers? Ownership and quality of externally facing data is also important. It is therefore somewhat short sighted to restrict ownership of data to a specific system. It is much more effective to associate data ownership with a master data entity (e.g. customer data) or a transaction type (e.g. orders) because this type of ownership is enterprise wide.

DATA PRIVACY RISKS

Sensitive and cofidential data needs to be protected from data privacy breaches

The challenge in data privacy is to share data while protecting personally identifiable information. Data privacy becomes a risk management issue when sensitive data gets 'into the wild'. This kind of problem is known as a *data privacy breach* and is of particular concern when customer data is exposed and gets into the wrong hands. Some employee data is also sensitive. Companies need to plan for data privacy breaches and do everything possible to prevent them from happening. Data privacy breaches can lead to fraud, major customer dissatisfaction, loss of business, liability lawsuits and regulatory penalties. They can also significantly damage a company brand and corporate reputation.

Masking sensitive data in test and production ebvironments is important

Redundant copies of sensitive and confidential data must also be taken into account

Data privacy goes well beyond a data breach with sensitive data getting into the wrong hands outside the enterprise. It also coves exposure of sensitive data to unauthorised personnel inside the enterprise. There are a number of surveys that indicate that data theft and many data breaches have been attributed to internal malicious employee actions. To counter this problem, there needs to be a way of identifying and masking sensitive data so that it is not seen by unauthorised business users and IT developers. In the latter case of IT developers, it is often test data that can be the problem. Many companies create test data sets from full copies of production data. This is because quality assurance testing often requires production data to be able to accurately test real world scenarios. The problem with using production data to create test data sets is that it introduces a potential exposure risk when sensitive data is involved in the testing. If several test data sets are created from production data then there will likely be multiple instances of sensitive information stored in various test environments. This increases the chances of sensitive data theft by a malicious insider.

UNAUTHORISED DATA MAINTENANCE RISKS

Data access security must also be managed to prevent unathorised maintenance of sensitive data by employees

Following on from the issues related to data privacy is the unauthorised access and maintenance of sensitive data by employees. Because subset copies of data occur across operational systems and multiple departments, this problem is often much more difficult to manage than it may first appear. It requires security privilege co-ordination across multiple portals, applications and database technologies. It is further complicated by that fact that many applications, even today, have their own 'baked in' proprietary authorisation models. In addition, the data that you may be trying to protect may be known by different data names in the different underlying systems that underpin a company's core business processes. Although many companies are gradually moving towards common authentication and authorisation mechanisms (e.g. corporate LDAP directory), they are still in a 'hybrid' state with a complex authentication and authorisation landscape. It is this kind of complexity that leaves to door open to data access security breaches.

A common authentication and authorisation mechanism simplified management of data access security

All kinds of risks can stem from these kinds of breaches. They include fraud, process delays due to data defects, unplanned increases in operational costs and customer dissatisfaction to name a few.

DATA SYNCHRONISATION RISKS

Data synchronisation errors increase the risk of process delays, unplanned operational costs and customer dissatisfaction

Lack of data synchronisation can cause major disruption in any business operation. For example, customer data is needed in sales, marketing, service, finance and distribution. Product data is needed in product development, planning, manufacturing, stores and e-commerce. Many of these business functions are supported by separate application systems and keeping data synchronised is therefore a major issue. For example in customer data, a simple name change or a change in a group of companies' hierarchy is a common requirement. Making sure those changes ripple across all systems in the enterprise that need to remain synchronised is often much more complex. In the past this task has been tackled on a system by system basis with piecemeal synchronisation jobs managing point-to-point synchronisation between two systems. There has been little in the way of a common approach to doing this.

Lack of synchronisation can increase the risk of process delays due to data defects, unplanned increases in operational costs and customer dissatisfaction. It may also cause increases in credit risk, and result in erroneous data to be made available to third parties (e.g. product data being made available to retailers and electronic exchanges) and decision makers.

DATA RECOVERY RISKS

Being able to backup and recovery master data and transaction data entities irrespective of location of the data acrosss the enterprise would significantly reduce risk

The issue with data recovery is obvious. If data is not recoverable it can have a massive impact on the company's ability to operate. Processes can break and come to a halt which can severely impact costs, revenue and customer confidence. While this may seem a straightforward issue to solve, it is often complicated by the fact that subsets of master data (e.g. customer, product, asset, etc.) and transaction data (e.g. orders) may have proliferated across departments and application systems as business processes execute. Therefore guaranteeing integrity and recoverability of certain types of data may be far more complex than originally anticipated. Maintaining data relationships and data integrity across all systems in the enterprise is critical to continuous operation. It follows that so called 'enterprise backup' and 'enterprise recovery' may be needed in the most severe cases. Being able to backup and recover master and transaction data irrespective of the location of that data is therefore desirable. While this is not typically happening today, there are most certainly aspirations in many companies to be able to do this as it would significantly simplify current practices while also reducing risk. The challenge is to be able to identify where all the data (and corresponding data relationships) are located in the enterprise.

USING DATA MANAGEMENT FOR RISK MITIGATION

Data management technologies can be used to identify and manage data at risk

In the last section we identified types of data risk that can be contribute to business risk. In order to reduce the possibility of these types of data risks occurring, data governance and data management can be introduced. We have already discussed how to implement data governance in the first white paper[1] in this GRC series. In this paper we will look specifically at the how people, processes and data management technologies can be used to identify and manage data at risk.

CULTURAL AND ORGANISATIONAL ISSUES

Accountability breeds ownership and lays the foundation for control

A risk prevention methodology and tested risk recovery procedures helps to breed confidence

Data risk management is very much a part of enterprise risk management (ERM) which in turn is a key element of GRC. Slipstreaming an ERM or GRC initiative and any associated executive backing related to that initiative is often the way to gain awareness that data management matters. Awareness breeds interest but making people accountable breeds ownership and introduces control. Having a risk prevention methodology that can identify and classify data risks together with fully tested risk recovery procedures breeds confidence. It also provides the guard rails needed to get data risks under control. It is also important to recognise that the insider threat is real and dangerous when it comes to data breaches. By integrating email records management, e-discovery and auditability into risk management procedures it becomes possible to breed a culture that of a safe, well managed data environment. It also creates a culture where self-disclosure is encouraged. Adding a data governance council[2] that also deals with data security adds even more weight.

IDENTIFYING DATA AT RISK AND THE BUSINESS IMPACT

Companies need to identify 'at risk' data

Having a shared business vocabulary makes it easier to identify 'at risk' data

In order to manage data at risk, we first of all need to define the master and transaction data used in the enterprise and then highlight 'at risk' data items within this. We saw in the data governance white paper[3] in this series that this is done by creating a shared business vocabulary (SBV) of common data names and data definitions. This includes data integrity constraints. The SBV is built incrementally by focussing on specific master data entities and transaction data types.

Once master and transaction data items have been defined within the SBV, we then need to identify what data items in the SBV are considered to be 'at risk'. 'At risk' data can then be associated with threats that indicate what could go wrong with it. The table below show at risk data items and associated risks:

'At risk' data can be associated with threats to indicate what could go wrong with it

At Risk Data	Potential Data Risk (Threat)
Data items manually entered via the keyboard	Data quality defects
Data items considered sensitive or confidential	Breaches in data privacy
Data items considered restricted	Unauthorised access

[1,2,3] "*Governance, Risk and Compliance - The Role of Data Governance in GRC*"

Data items used in multiple applications supporting a core business process	Synchronisation errors
Data items considered critical to business operation and decision making	Recovery failure

For example, customer data may be considered sensitive and therefore potentially 'at risk' in terms of a data privacy breach or unauthorised access. Similarly, employee data items like Social Security Number and Salary may be considered confidential. It may also be the case that customer data is susceptible to poor data quality due to data entry errors occurring via the keyboard in the front office or by customers and partners over the internet.

Understanding the business impact of data risks helps prioritise risk management efforts

It is also important to understand the business impact of data risks. For example is the impact financial? Is it operational and if so what resources are needed to fix the problem? Does it result in regulatory compliance violations or does it impact the company brand and reputation?

Defining Policies To Manage 'At Risk' Data

Having identified data at risk, the next step is to define the policies needed to reduce the possibility of data risks occurring. Several types of risk mitigating data policies may need to be defined for each 'at risk' data item. These include:

Policies need to be defined for each 'at risk' data item so that data risks can be managed

- Data quality validation policies
- Data privacy policies
- Data lifecycle policies around who is authorised to
  - Create
  - Read
  - Update
  - Delete
- Data synchronisation policies
- Data backup and archive policies

These policies may also be restricted by *scoping limitations* to limit their risk management capability, e.g. to allow certain data policies to be set for data in a specific application used in a specific business process by people in a specific organisational area. However if data spans organisational units and systems then enterprise wide common policies should be enforced.

Determining Where 'Data At Risk' Is Located

Data 'at risk' needs to be located if risks are to be successfully managed

Having identified the data items in the SBV that are considered at risk, and defined policies to be applied to those items to reduce data risks, the next challenge is to identify where that data actually resides in the enterprise. This includes identifying all redundant copies of it whether they are in production systems or test systems. This is necessary because if we don't know where data is located, we cannot eliminate the possibility of data risks occurring. We need to locate the data and then map it back to the SBV in order to determine:

- How good the data quality is
- Whether or not data privacy is enforced on confidential and sensitive data items
- If authorised access to restricted data items is enforced across the enterprise

- If data synchronisation is working across all systems where that data is used and if the synchronisation is complete
- If critical data is recoverable across all systems that use it

We also need to know how much data we are dealing with at each location.

Data discovery technology helps to locate 'at risk' data quickly

The key point here is that a data discovery *and SBV mapping* exercise is needed to find 'at risk' data across the enterprise. This task may be done manually or automatically. If done manually the discovery task will be expensive and very time consuming. Therefore data management platforms that include an automated data discovery tool to locate data and data relationships across multiple systems in the enterprise offer a distinct advantage. By automatically mapping located data to the SBV, it becomes possible for these tools to locate data items flagged in the SBV as sensitive, confidential, business critical and also to determine if data quality policies are enforced.

PREVENTING DATA RISKS

Having identified where the 'at risk' data is located across the enterprise, the next step is to make use of people, data governance and data management processes and technologies to prevent data risks from occurring.

This can be done by

1. Applying data governance and data risk management policies to discovered at risk data items to reduce data risks
2. Identifying the source or cause of each data risk and making changes to reduce the chances of further occurrences
3. Monitor data risks to see if mitigation policies and procedures are working

Applying Data Risk Management Policies

Tools in a data management technology platform can be used to apply and enforce risk management policies

Looking at these in more detail, the first is the application of data risk management policies to discovered 'at risk' data. The way this is done is to share metadata between tools in a data management platform. Figure 1 shows that data management platform highlighted in the data governance paper in this GRC series[4]. What is different here is that some additional data management tools have been added over and above those discussed in the first paper. These include a data privacy masking tool, a data backup and recovery tool and a data security management tool to manage authorisations across multiple systems. The tools needed to apply policy to 'at risk' data are highlighted in red.

The data management platform is a suite of tools that access shared metadata

[4] "*Governance, Risk and Compliance - The Role of Data Governance in GRC*"

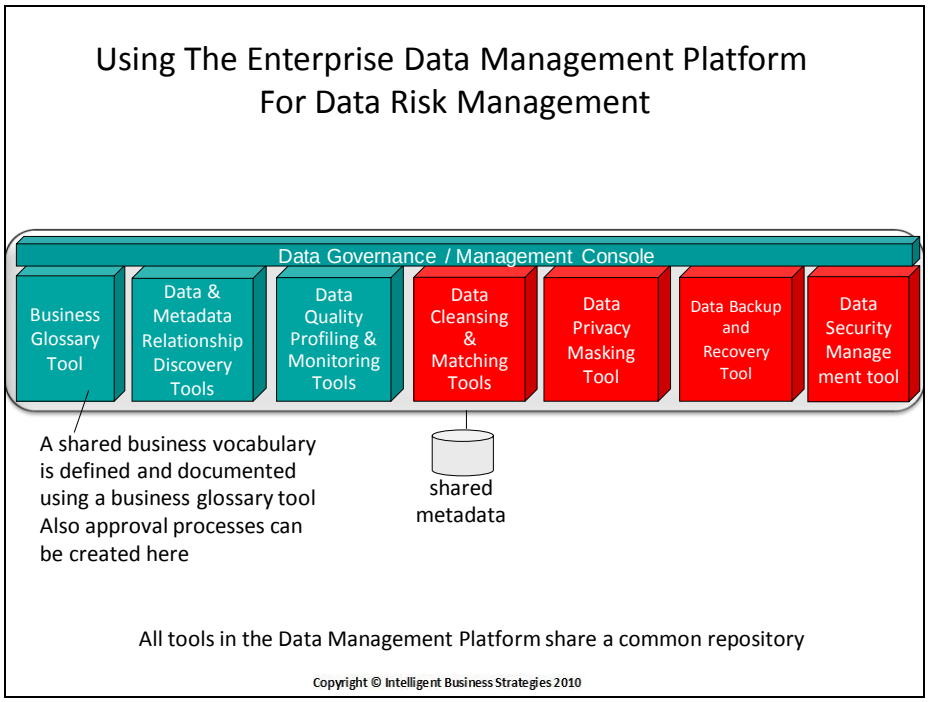

Figure 1

The key to this is the metadata sharing between the data discovery tool and the highlighted data management tools in the data management platform.

Automated data discovery seeks to find complete data entities across heterogeneous systems e.g. customer

Automated data discovery seeks to find complete business data entities across heterogeneous systems. An example of such an object is customer. This means identifying all customer data and data relationships across the enterprise irrespective of location. This is shown in Figure 2

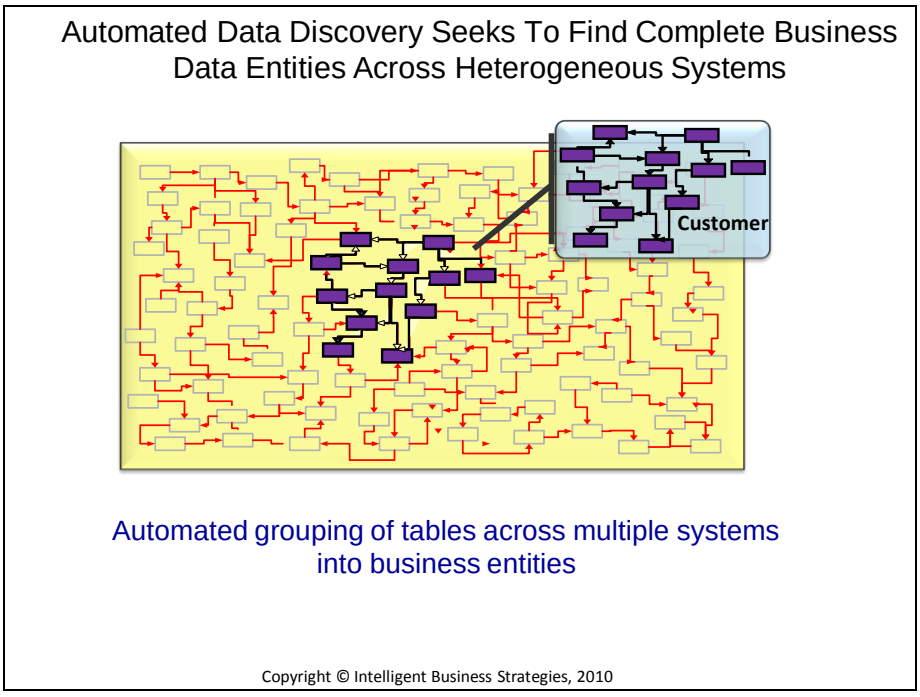

Figure 2

This means that it becomes possible to know where all 'at risk' data items associated with a discovered data entity are located

By finding complete business data entities (e.g. customer, product, order) it becomes possible to manage data risks at the entity level irrespective of where the data is located. For example, customer data quality, customer data privacy, customer data backup, customer data access security, customer data recovery, customer data synchronisation. This is because data discovery has already identified where the data is and by mapping it to an SBV it becomes possible to identify data risk management policies (quality, privacy, secure access etc.) that are 'in play' for a particular data entity.

Therefore by sharing metadata generated during data discovery with other data management tools it becomes possible to apply already defined policies to manage data risks. This is shown in Figure 3.

In terms of preventing data quality risks, metadata about poor quality data items can be shared with data quality tools so that data quality can be enforced. Similarly with respect to preventing beaches in data privacy, metadata about discovered sensitive and confidential data items can be shared with data privacy tools to allow them to mask this data in the systems where they are located and also to manage the generation of test data sets. With respect to data backup and recovery, it becomes possible to back up and recover complete data entities irrespective of location because data discovery has identified all data items and data relationships across heterogeneous systems in the enterprise.

By sharing the location of all 'at risk' data with other data management tools, it becomes possible to apply risk management policies to data across the enterprise

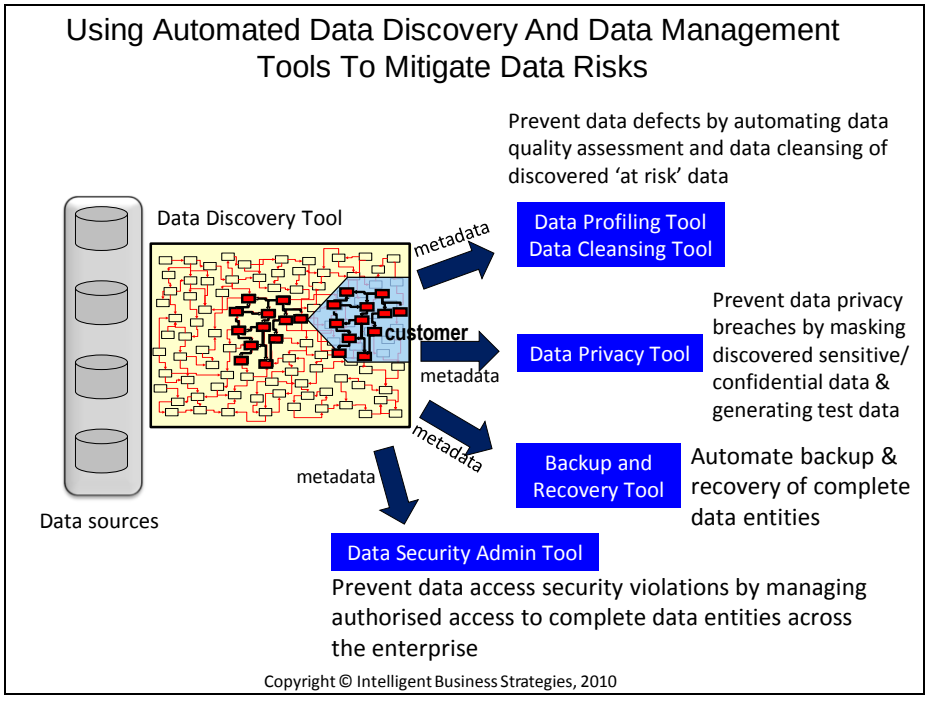

Figure 3

Sourcing Data Risks

In addition to being able to apply data governance and data management policies and controls to manage data risks, it is also very important to be able to determine the source of data risks to prevent future occurrences of these risks. The source (cause) of data risk events can be an employee, an external user (e.g. customer, partner, supplier), an application or script running inside the enterprise or an application or script running outside the enterprise, e.g. in the cloud, or on a customer or partner system. They can also be caused by natural disasters.

Data risks can be sourced and changes made to reduce risks even further

Once the source has been identified, changes to processes, training and testing procedures may be needed to help reduce data risks. It might even warrant taking out insurance against a data risk happening, if the cost of recovering from it is very severe. For example, it may be necessary to change processes in order to invoke data privacy services and data cleansing services on demand as data is entered via a keyboard, or on an event driven basis. It may also be the case that an information security council is introduced with a formal approval process to govern data access security so as to tie this to internal controls.

Monitoring Data Risks

Risk monitoring helps companies stay in control

The final step in data risk prevention is being able to monitor data risks to see if any problems are arising. This means being able to have access to risk indicators to highlight the frequency and severity of data risks. Data risk management reports and dashboards widgets are needed to allow business data owners to monitor data risks in their area of responsibility. It is likely that these risk monitoring capabilities can be added to already existing data quality monitoring dashboards to allow everything to be monitored off the one dashboard.

RECOVERING FROM DATA RISK EVENTS

In addition to being able to use technologies to manage risks, it must also be the case that there are procedures in place to recover from risks if they occur. For example, it should be possible to identify fraudulent activity that results from a data privacy breach and to easily locate the data risk (e.g. unmasked sensitive data). Metadata lineage is often important in helping to make this possible. Companies have to be confident in risk recovery which means that it must be possible to quickly identify the source of the risk, know where your data is, repair, mask and/or secure access to that data and be able to report on all recovery related activity.

Tested risk recovery procedures help companies act quickly to minimise business impact

Recovery procedures should be documented, communicated widely and automated where possible. A key element in risk recovery is to have thoroughly tested any controls and recoverability. This breeds confidence in ability to act quickly to minimise the business impact. It is also important to connect things like e-discovery into any recovery processes to be able to retrieve all related communications that may have taken place before and after the event occurred.

CONCLUSIONS

Data governance and data management have a significant part to play in mitigating risk

There is no doubt that data governance and data management has a significant part to play in mitigating risk. Above all there needs to be risk management strategy and a methodology for managing and preventing data risks. In addition it is paramount that you know where your data is and what it means if you are ever to stand a chance of identifying data at risk, classifying the risks and defining policies to manage these risks.

A shared business vocabulary allows you to systematically define data items, signal at risk data and define risk management policies

Having a shared business vocabulary (SBV) data is a critical starting point. The existence of an SBV allows you to systematically define master and transaction data and any associated risk management policies to be applied to that data. By making use of data discovery tools in a data management technology platform, commonly defined master and transaction data can be located across the enterprise and mapped to the SBV. Once this is done, it is possible to see 'at risk' data right across the enterprise. At this point you can determine if risk management policies (and any other data governance policies) are being enforced in the underlying systems that house the discovered 'at risk' data. If not, it then becomes possible to apply policies, source the causes of data risks and make any necessary changes to prevent re-occurrence. Given that data management software technology platforms provide much of the tooling to do this, it is difficult to see how or even why companies would not want to invest in them.

A data management platform helps you define and apply policies to manage 'at risk' data across the enterprise

Finally establishing organisational accountability and data ownership means people are responsible for monitoring data risks. This together with tested risk recovery procedures should breed confidence that the organisation is in control of and executing its risk management strategy

This paper has focussed on risk management in a GRC program. In the next paper in this series we will look at compliance.

ABOUT INTELLIGENT BUSINESS STRATEGIES

Today, successful companies are those that can absorb new information technologies and use them effectively in their businesses. But faced with so many new technology developments how can IT and business users possibly keep up? Intelligent Business Strategies is an IT research and consulting company whose goal is to help companies understand and exploit new developments in business intelligence, analytical processing, data management and enterprise business integration. Together, these technologies help an organisation become an *intelligent business*.

Mike Ferguson is Managing Director of Intelligent Business Strategies Limited. As an analyst and consultant he specialises in business intelligence and enterprise business integration. With over 29 years of IT experience, Mike has consulted for dozens of companies on business intelligence, data management and enterprise business integration. He has spoken at events all over the world and written numerous articles. Mike is a resident expert on the B-EYE-Network, providing articles, blogs and his insights on the industry. Formerly he was a principal and co-founder of Codd and Date Europe Limited – the inventors of the Relational Model, a Chief Architect at Teradata and European Managing Director of Database Associates. He teaches popular master classes in Operational Business Intelligence and Performance Management, Enterprise Data Governance, Master Data Management and Enterprise Business Integration

Intelligent Business Strategies
Springfield House
Water Lane, Wilmslow
Cheshire SK9 5BG
England
Telephone: (+44)-1625-520700

Internet URL: www.intelligentbusiness.biz
E-mail: info@intelligentbusiness.biz

Governance, Risk and Compliance Series
- The Role of Data Management in Mitigating Risk