Adrian Gregory

has over 25 years experience in data working across B2C and B2C in marketing and location-based services' applications. His current organization, DQM Group, formed in 1996, has grown to become the most trusted independent provider of Data Governance services to the UK marketing industry, working for over 80 per cent of leading commercial data owners and increasingly leading brands. DQM Group has won numerous industry awards, including Data Strategy, Data Service Provider of the Year for 2007, 2008 and 2009. In addition to his role at DQM Group, where he spends 50 per cent of his time on strategic data assignments for customers, he is Chairman of the Institute of Direct Marketing Data Council and the Direct Marketing Association Data Governance Working Party.

Data governance — Protecting and unleashing the value of your customer data assets

Stage 1: Understanding data governance and your current data management capability

Adrian Gregory

Abstract

Many organizations are waking up to the fact that customer data is a valuable corporate asset that needs careful protection and their value actively managed or 'governed'. An increasing number are also discovering the hard way that data can also be a significant liability. Zurich Insurance was recently fined a UK record £2.27 m by the Financial Services Authority (FSA) for losing details on 46,000 customers. This paper highlights the need for taking the utmost care with management of your customer data. It also makes the case for investing in, and actively developing, its value for much broader business benefit of increased sales, reduced operational cost, greater profits and long-term growth. It defines and details an emerging management discipline called data governance, explaining exactly what is meant by the term, and what people are trying to achieve by introducing data governance discipline within their organization. It's an important subject that's going to get bigger and more central to organizations in the future. The paper explains the strong links between corporate governance, risk and compliance and how data underpin all three, and how it too needs to be 'governed'. Without strong data governance the organization will fail to provide effective corporate governance and compliance, and will open the organization to significant risk of failure in both. Not least, without effective data governance the organization will fail to maximize the value of its data assets. With the case made for data governance, the second part of the paper focuses on how organizations of any size can understand their own current data capability using the powerful Data Governance Maturity Model approach first developed for IT Governance. You will understand how to develop your own ideal 'to be' state and what actions you need to take to get there. The approach is illustrated through a case study for a leading 'not for profit' organization that is embarking on a major data governance programme. Its aim is to

Adrian Gregory
Chairman, IDM Data Council
DQM Group
Tel: +44 087 0242 7788
E-mail: adrian.gregory@dqmgroup.com

help maximize the benefits (and avoid failure) of its investment in a substantial Customer (Supporter) Relationship Management (SRM) programme to create a single view of all its supporters. This paper is the first of a series on this important topic of data governance. Through the series, we will follow this not for profit organization as it develops a new data organization, a realistic data strategy and roadmap and makes its way towards establishing optimal data governance throughout the organization and the highest level on the Data Governance Maturity Model. This is to both achieve success with its SRM programme and to really unleash the value of its supporter data.

The need for this paper — Introduction

Customer data is a valuable asset

Customer data is a valuable business asset that has received less management attention, and fewer resources and business processes than are applied to other value-driving parts of the organization. Customer data can also be a significant liability. Personal, behavioural and transactional data used for marketing and marketing communications need careful management in order to be accurate, accessible, compliant and fit for purpose.

Strong need to raise professional standards

There is a strong need to raise professional standards in data management; help private and public sector organizations cope with growing regulation; help them organize to integrate disparate data sources to gain a holistic view of the customer, prospect and market; and unleash the full value of their data assets whilst avoiding the downside risks from data security breaches, data theft or loss and improper or inaccurate use of data.

The aim of this paper is to help you:

- understand the impact of inadequate data governance and data breaches in terms of direct costs, brand damage and missed opportunity;
- explain exactly what data governance is, and why it's important to your organization;
- understand fully your organization's current data capability. The paper details the Data Governance Maturity Model, which enables you to plot your position and monitor your progress as you strive towards 'managed' and even 'optimal' data management.

The paper starts by looking at the impact of poor data governance.

Part 1: The impact of poor data governance

Remember these data disasters? (Figure 1)

Theft of customer data is a common practice and very damaging

There are a number of issues related to data that create potentially significant risk for an organization. The key issues include:

- risk of data theft and loss;

Figure 1: Recent newspaper headlines highlighting some serious data breaches

• risk from breaches of data privacy and/or regulatory compliance;
• risk of damage from poor data quality.

Risk and impact of data theft

The risk

Do you know what time of day your sensitive information is most at risk? Between 3pm and 5pm on a Friday afternoon. This is when members of staff start planning their weekend, realize they are short of cash and decide to steal personal data for sale on the black market. While such actions by front-line staff in call centres have been well publicized, it is just as common among back-room members of the IT department.

According to Forrester Research,[1] 80 per cent of data leaks are created by staff. Current trading conditions that have led to increased redundancies have also led to an increased risk of data theft by staff. Only 12 per cent of sacked IT professionals would not abuse their access rights to take sensitive data out of a company if made redundant, compared to 88 per cent who would, according to a survey by Cyber-Ark.

Staff attitudes to data theft: New research on theft of customer data — The threat from within

New research from DQM Group supports the view that data theft is a common business practice, especially among departing employees. Most respondents in the DQM Group survey believed that employees often take customer data with them when they leave a company. Many didn't think this could be prevented — and didn't know that it is illegal.

• over 76 per cent of respondents believed it is common practice for sales and marketing staff to take customer contact data with them when they leave an organization;

80 per cent of data leaks are created by staff
Source: **Forrester Research**

- most worryingly, over 80 per cent of respondents felt that staff should be able to take customer data with them to their next job;
- data theft can be easily prevented. Seventy-five per cent of respondents in sales and marketing said that theft would drop significantly if false contacts 'seeds' were added to the data to catch thieves and monitor all use of the data.

Research method

DQM Group surveyed directors, senior managers and customer-facing staff in over 500 major organizations during May and June 2010. Respondents were asked about their views on staff taking data (such as customer and prospect details) from one company to another. Full details of the DQM Group survey can be found at www.dqmgroup.com.

The impact of data theft and loss

Forrester Research[1] estimates that following a data security lapse, 10–20 per cent of customers will be lost in any given year. The most recent Ponemon Institute survey indicated that 74 per cent of survey respondents lost current customers as a direct result of a security breech.[2] In August 2010 the FSA fined Zurich Insurance a record £2.27 m for losing the details of 46,000 of its customers; this followed multi-million pound fines to Nationwide and HSBC. The infamous TK MAXX data breach in 2007 is estimated to have cost the company £800 m.

References are given at the end of this paper for obtaining further information on the research quoted.

Risk and impact of data privacy or regulatory breaches

Consumers have also woken up to the issue of data privacy. Data breaches put them at risk, through the possibility of financial threat or fraud right up to identify theft. This is turning into a growing anxiety about what personal information is held by organizations and how secure it is.

According to a global survey among 9,200 consumers in 14 countries carried out by Nokia Siemens Networks:

- 82 per cent of respondents see privacy as an important topic;
- 76 per cent are concerned about privacy violations;
- 45 per cent feel they lack control over their personal data.

The Information Commissioner (ICO) has new powers

When consumers start to be concerned about an issue, regulation is sure to follow. In the UK, new powers have been granted to the ICO under the Coroners and Justice Bill 2009. As well as providing power to audit without prior notice, the ICO will be able to impose fines on companies in breach of the Data Protection Act of up to 10 per cent of turnover. Further regulation currently in the consultation process with the ICO could lead to company directors facing 2 years in prison for their role in data losses.

This has given rise to the use of Privacy Impact Assessments as a method for understanding the extent to which data subjects are exposed by the capturing, processing, storage and movement of personal information. Alongside this, the ICO has called for 'Privacy by Design', foregrounding the need to build in controls and remediation in the event of a breach or loss.

With the burden of regulation increasing, organizations will undoubtedly have to apply more resources than before to the area of data governance. David Myddelton, Professor Emeritus of Finance and Accounting at Cranfield University School of Management, highlights that 'the compliance costs to a business often amounts to five times as much as the direct costs. The hassle factor can also be a serious cost to a business although it is harder to quantify'.

Risk of poor-quality data

Over 50 per cent of Customer Relationship Management (CRM) programmes fail due to poor-quality data *Source*: **Gartner Group**

Poor-data quality is another common problem that often has a significant impact on an organization's efficiencies and consequently its performance.

According to Gartner Group, over 50 per cent of CRM and data warehouse programmes fail or do not achieve business case benefits due to poor-quality data. This is costing organizations tens of millions pounds in direct investment, management time and lost opportunities.

Larry P. English,[3] in his book *Information Quality Applied* (2009), identified 122 organizations in Europe and the USA that together had wasted over $1.2 trillion due to problems created by poor-quality data. He estimates that between 20 per cent and 35 per cent of an organization's operating revenue is wasted in recovery from process failure and data scrap and rework.

The benefits of good data governance

Improves brand perception and builds consumer trust

Good data governance isn't just about reducing business risk. It often delivers substantial benefits in its own right.

Instead of seeing data governance as an extra cost of business, however, it should be recognized that brand values and perceptions can be positively impacted. Not least, it should be seen as an investment in an important asset, which should have a significantly positive impact on business profits and growth.

Significant consumer trust can be built through a clear, fair and positive approach to the collection and management of their data, as well as through proactive data security measures and a clearly demonstrated commitment to preventing data loss. An instance of data loss will often have a profoundly negative impact on consumer trust, and can cause irreparable brand damage.

Good data management enhances an organization's ability to cross-sell and up-sell to its customers. According to 2006 sales figures, 35 per cent of Amazon's sales are done through its recommendation system, which automatically suggests products to customers based on their previous purchases.

A major insurance company successfully reduced errors in application from 34 per cent to 4 per cent of policies by reviewing and simplifying its data error process, leading to savings in data entry costs estimated at over £1.5 m. The organization also significantly reduced policy cancellations and cut claim overpayments by over £2 m through better data management.

There are many other examples that make the case for investing in good data governance.

What is data governance and where does it fit in the organization?

What is data governance?

‘Data Governance is the business practice that defines and manages strategies for people, processes, and technologies to ensure that valuable data assets are formally protected and managed throughout the organisation’

People often have different understandings of the term data governance. To some it's all about privacy and regulatory compliance. To others it's more about security or data quality. In fact, it covers all of these key topics and much more. It's an important subject that's going to get bigger and more central to organizations in the future.

Gwen Thomas[4] from The Data Governance Institute defines it simply as 'the exercise of decision-making and authority for data-related matters'. A more detailed and encompassing definition is as follows:

> 'Data Governance is the business practice that defines and manages strategies for people, processes, and technologies to ensure that valuable data assets are formally protected and managed throughout the organisation'.

Data governance encompasses the people, processes and technology required to create a consistent and proper handling of an organization's data across the enterprise.

It encompasses *all* aspects of data management and not just data quality, data security and regulatory compliance.

Tony Fisher[5] says in his book *The Data Asset*, 'Data Governance is a methodology and philosophy for benefiting from your data. It is not a programme or a technology that will "fix" a problem. It is much more than just having a strategy. Data Governance is a mindset. It's about establishing a culture where quality is achieved, maintained, valued and used to drive the business'.

Certainly, without effective data governance the organization will fail to maximize the value of its data assets.

The link to corporate risk and compliance

If your organization has an IT infrastucture, it has data. If it has data, it needs data governance. It is also a process that has to be enacted in day-to-day business activities every time personal information or sensitive data are being handled.

This means that data governance is both corporate and individual. Every employee needs to understand and conform to stated policies and regulations. The organization needs to be able to audit that

understanding and demonstrate to regulators that it is maintaining best practice.

The enormity of the collapse of the banking sector in 2008 even surpassed the numerous corporate failures that have taken place over the last decade such as the Enron and MCI (Worldcom) frauds.

It has placed an even greater focus from politicians and legislators on how organizations are managed, or not, which has often proven to have been the case. The Enron case led to major legislation in the form of Sarbanes–Oxley in 2002. No doubt more will follow.

Such Corporate failure and legislation has created a new management discipline known as Corporate *Governance*, which today is at the top of every Board Agenda — a key responsibility of every Director and a driver to reduce *Risk*. Both are closely related to *Compliance*. Together Governance, Risk and Compliance is known as GRC.

Corporate Governance, Risk and Compliance (GRC) depends on effective data governance

Underpinning GRC is a dependency on data. As Mike Ferguson[6,7] highlights in his publication 'Governance, Risk and Compliance — the Role of Data Management in Mitigating Risk', data is crucial to effectively governing and managing an organization (see the Integrated GRC in Figure 2).

Data itself must be 'governed' so that it is accurate, complete, trusted and understood and can be used to help govern the organization, greatly reduce risk and achieve compliance.

Integrated governance, risk and compliance

Goal of data governance is to add value and reduce risk

The goal of GRC and data governance is a shared one — to add value to the enterprise while mitigating risk. This is what attracts support and investment from the Board and makes data governance a sustainable activity.

For any organization with a focus on performance improvement and a significant data resource, the objective should be to progress its data governance capability.
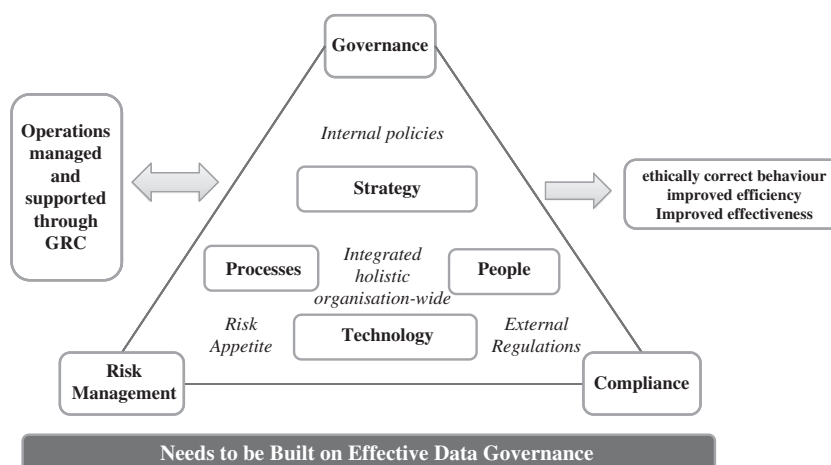
Figure 2: The relationship between corporate governance, risk and compliance
Source: Racz *et al.*[8]

Part 2 of this paper outlines a proven approach to understanding and measuring your current data management capability and monitoring progress on an ongoing basis as you move towards the ideal state of an optimized set of processes aligned with your corporate vision and business goals.

Part 2: Understanding your data governance capability

Understanding your organization's current data capability is the first task when embarking on a data governance programme.

Initial investigation and risk assessment

Priority 1: Identify your Data Risks

On starting a data governance programme, a priority is to identify quickly any key risks to which the organization is exposed, before looking at your overall capability and opportunities to grow value.

An important step in highlighting where data may be at risk is to carry out a risk assessment and data audit. Using an interview-style approach, an organization can gain insight into, for example, what its current level of data security really is and the level of risk it is exposed to. That indicates where cultural changes or enhancements may be necessary, especially across the supply chain.

Such an initial investigation or audit will 'run the ruler' over the business to measure where areas of concern are to be found. Rather than leading to increased red tape in order to ensure compliance, however, it offers a pathway towards an enabled business that has an assured, fully compliant data asset at its heart.

The Direct Marketing Association DataSeal is an important new data security standard for managing customer data

As a starting point for a data governance programme, a thorough investigation will examine your existing policies around data security and compliance in relation to current legislation, such as the Data Protection Act. It should generate a gap analysis which compares your organization to external data governance standards, such as DMA DataSeal and ISO 27001.

Once the initial risk assessment is complete and any immediate issues addressed, you can focus on really understanding your broader data governance capability.

Three key areas of data governance capability

When assessing your current data governance capability your focus should be on three core areas:

- People
- Process
- Technology

Data governance concerns the whole organization. Not just another 'IT problem'

People

Data should be central to the whole organization. They create challenges that affect every employee; it's not just another problem for 'IT to sort out'. In fact, leaving data to IT, with its many other priorities, is highly unlikely to deliver a data asset that truly supports the demands and opportunities of the business.

Crucial to success is executive level backing, with a properly funded team focused on delivering high-quality, secure and compliant data that are fit for purpose for all business users. Senior management will need to embrace the value of data, and promote a 'vision' and positive data culture through the organization.

Process

Effective data governance is an ongoing, long-term process

Data management is never a one-time programme, but very much an ongoing process. Similarly, it cannot be tackled all at once. You need to recognize that your organization needs to make step changes to develop its data to be successful; this process must be evolutionary, taking many small, achievable, measurable steps to achieve your longer-term goals.

Adopt a 'lifecycle' approach

We recommend a 'lifecycle' approach to ongoing data development comprising five phases:

Phase 1   *Data investigation and discover;*

Phase 2   *Design: creating a single data model, data rules and processes;*

Phase 3   *Employment: working to the now universally agreed rules;*

Phase 4   *Maintenance: the ongoing job of keeping the data accurate and fit for purpose;*

Phase 5   *Redundancy: in line with good business practice (not least the Data Protection Act), the often difficult decision to archive and store redundant data that is no longer of value to your organization.*

Technology

Technology can and in fact needs to play a significant role in developing data that are fit for purpose, in reducing risks and in growing data value over the longer term.

It will bring significant benefits around standardizing data and improving data quality generally, for monitoring and reconciling data, managing risk and implementing a much more secure data culture throughout your organization.
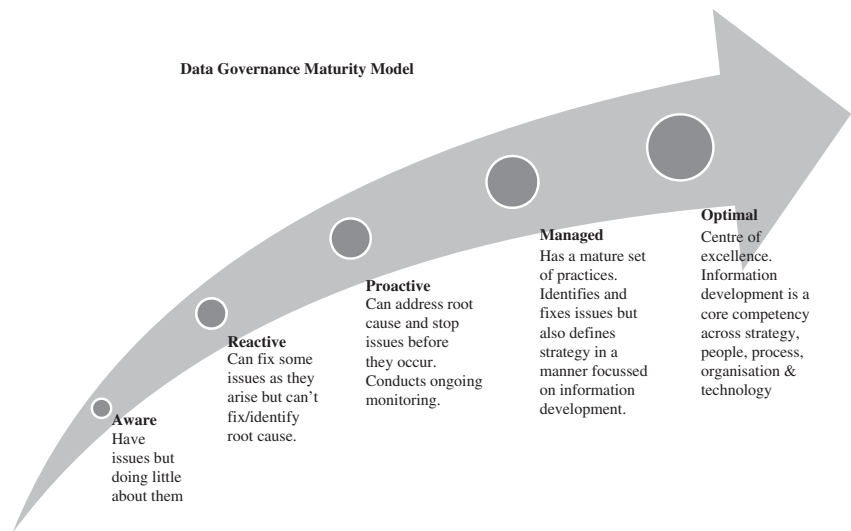
In addition, the right technology tools will enable data to be more efficiently accessed and used throughout the organization.

Your success in developing the data asset your organization needs will depend on people issues, your processes, and the technology your organization employs to support them and data management.

Understand your data governance maturity

Measure your 'data governance maturity'

When assessing your data governance capability, which will address people, process and technology matters, a good approach is to use a Data Governance Maturity Method, which categorizes capability into distinct stages as shown in Figure 3.

Data Governance Maturity Model

Aware
Have issues but doing little about them

Reactive
Can fix some issues as they arise but can't fix/identify root cause.

Proactive
Can address root cause and stop issues before they occur. Conducts ongoing monitoring.

Managed
Has a mature set of practices. Identifies and fixes issues but also defines strategy in a manner focussed on information development.

Optimal
Centre of excellence. Information development is a core competency across strategy, people, process, organisation & technology

Figure 3:   The Data Governance Maturity Model

This paper outlines the DQM Group approach, which is based on the proven MIKE2.0 Method developed for information management and strategy.[8] Other organizations including Dataflux and IBM have developed similar Maturity Models for Data Governance.

As your data governance capability matures, you will enjoy the benefits of higher-value data, such as increased sales. You will also reduce the risks of data breaches that can do so much damage.

Improving your data governance maturity level is hard and will take time. It is a long-term process that must be addressed in small, careful steps.

To start, this paper takes you through the characteristics of each stage of the Data Governance Maturity Model.

Stage 1: Aware
Your data management is undisciplined. You have issues but are doing little about them.

Some 40 per cent of the organizations we assess fall into this first category

Data cost is an overhead, not a strategic investment. Data is managed in 'silos' with redundant data in each one. There are few defined data rules and policies. There is little or no senior management oversight. Sales and financial systems do not synchronize.

Sound familiar? Some 40 per cent of the organizations we assess fall into this first category!

Characteristics of the Aware Stage

- duplicate and inconsistent data;
- unable to adapt to business changes;
- localized data management;
- IT-driven projects;
- technology addresses specific problems and needs.

- Your technology is likely to be:
  - salesforce automation;
  - database marketing system, although often many organizations in this stage outsource their marketing databases.

Stage 2: Reactive

In the Reactive Stage you can fix some issues as they arise but can't identify/fix root cause.

We estimate that 30 to 40 per cent of organizations in the UK are in the Reactive Stage

Reactive organizations struggle to achieve regulatory requirements. Data is not governed by the organization as a whole. Data sharing is rare. There is little data quality deployment. Data is still 'siloed'. Action is usually driven by crisis, for example, a failing CRM programme. Often failure of CRM triggers focus on data.

The Reactive Stage is the most difficult to progress beyond. It requires top level support, clear vision, goals and defined strategy that is adequately resourced. We estimate that 30–40 per cent of organizations in the UK are in the Reactive Stage.

Characteristics of the Reactive Stage

- line of business influences IT;
- little cross-functional collaboration;
- high cost to maintain multiple databases and applications;
- usually IT gets the blame for failure of systems;
- odd successes due to 'heroes'.
- Technology employed is likely to be:
  - data warehouse;
  - CRM.

Stage 3: Proactive

In the Proactive Stage the organization can at last identify and address root cause and stop issues before they arise.

You will be analysing and monitoring your data, for example for accuracy, on an ongoing basis.

We estimate that 10 and 15 per cent of organizations in the UK are in the Proactive Stage

There will have been a major culture change. The organization will view data as a strategic asset across the enterprise. You will have 'Data Stewards' or Champions and clear rules, processes and policies.

Data will be recognized as adding real value to the organization. We estimate that 10 and 15 per cent of organizations in the UK are in the Proactive Stage.

Characteristics of the Proactive Stage

- needs committed 'do-ers' experts (Data Stewards/Champions) who understand needs of business and have IT experience;
- business and IT groups work together;
- data are seen as a corporate asset;
- it is likely that the organization will now truly have a single, unified customer view.

- Technology employed is likely to be:
  - ◦ Customer Master Data Management

Stage 4: Managed

By the Managed Stage you will have a mature set of data processes. You can identify issues as they arise and can define strategy in a manner focused on data development.

You believe that power and most value are delivered from sharing data. You will have mastered the use of CRM, Enterprise Resource Planning (ERP) and Data Warehouse technology.

You will be employing company-wide data definitions and business rules designed for data consistency. We believe that less than 10 per cent of organizations in the UK have reached the Managed Stage.

Characteristics of the Managed Stage

- reaching the Managed Stage does not mean replacing current systems or buying one solution that claims to meet all needs;
- it is about understanding where you are and what is needed to improve current systems.
- Technology employed is likely to be
  - ◦ automated data security and compliance management technologies addressing people issues.

Stage 5: Optimal

Your organization is a centre of excellence in Data Management.
Data and data development is a core competency across people, process and technology.

A key goal now is to enforce best practice and consistently codify data across the organization.

Executive sponsorship is a given, as is a team approach between users and IT.

Focus becomes more about business process integration than about the data themselves. Very few organizations in the UK have reached the Optimal Stage on the Data Governance Maturity Model.

Characteristics of the Optimal Stage

- repeatable, automated business processes;
- business requirements drive IT projects;
- personalized customer relationships;
- optimized business operations;
- unified data governance strategy;
- comfortable adding external data without fear of corrupting internal data.
- Technology employed is likely to be:
  - ◦ Business Process Automation;
  - ◦ Master Data Management.

We believe that less than 10 per cent of organizations in the UK have reached the Managed Stage

Very few organizations in the UK have reached the Optimal Stage on the Data Governance Maturity Model

Having read about the key characteristics of each stage of the Data Governance Maturity Model, you will have a good feel for where your organization sits.

Depending on the size and complexity of your organization, you might wish to have a much more measured approach, which you can repeat as you progress with your data governance strategy.

Data governance in action — A current example of an organization aiming for optimal data governance

Background

Data Governance Case Study

Note: All values quoted in the case study have been changed

In 2008, a leading Not for Profit (NFP) organization began a 5-year transformation programme planning to invest in excess of £20 m in a major SRM programme designed to create a single supporter view. Its aim was simply to place its supporters at the heart of its vision and deliver business benefits over £80 m.

Two years in, the programme is stalling badly due to poor and inconsistent data held on its multiple databases across the organization and with third-party partners. Data formats, standards and rules, where available, vary widely. Access is often difficult, slow and rarely in the form required. (Note that this is normal: according to research from Gartner Group, over 50 per cent of CRM programmes fail due to data quality issues.)

Data governance and data issues must be addressed for success in customer relationship management and to turn customer data into a valuable corporate asset

It was clear that while supporter data is recognized as core to the success of NFP, it is not consistently approached as an asset. Key challenges exist, including a lack of single focus and vision for data; a lack of appreciation of the implications and risks to NFP if data are not treated as an asset; and an organizational structure that does not easily enable access to data by key business user groups to support their activities.

NFP recognized that a step change in its approach to its supporter data is required if all the benefits of its SRM programme are to be achieved. This step change is required urgently and the organization appointed DQM Group in August 2010 to lead a focused, clearly defined programme of work to quickly but thoroughly assess NFP's data capability, map out the target state and define a clear roadmap to enable NFP to move from its current position to the target state.

Objectives and deliverables

The key objectives for the programme were to:

- thoroughly assess NFP's existing supporter data capability;
- clearly define the target state;
- provide a clear roadmap to enable NFP to move efficiently from its current position to the target state.

The objectives and deliverables were defined and agreed clearly at the outset

On completion of the review, DQM Group was asked provide a clear and detailed statement of what NFP needs to do to develop its supporter data into a valuable business asset that will make a

substantial contribution to the organization achieving its key objectives and vision.

The deliverables for the programme were to:

1. define NFP's current supporter data capabilities and its target capabilities in 3–5 years;
2. produce a roadmap detailing the route from the current position to the target state;
3. identify the specific initiatives and sub-projects that should be started now and in the next 12 months to make progress towards the target state and that will deliver tangible benefits as quickly as possible;
4. develop sufficient supporting materials and timetable to enable the organization to benchmark, measure and dashboard its progress towards the target state on an ongoing basis;
5. detail a new organizational and data governance structure for effectively managing its data assets, which fits within the NFP organizational structure;
6. recommend an approach for valuing NFP's supporter data as a business asset.

DQM Group approach

With a tight time frame DQM Group worked in two stages:

1. investigation and discovery;
2. planning and scheduling.

Subsequent stages, namely around implementation of the agreed Plans and Roadmap, fixing issues and addressing risks, will be managed by NFP internally. For us the importance of data to all organizations is such that we believe they should own responsibility for fixing issues and be accountable for ongoing data governance. For both of the DQM Group stages (and subsequent stages) the focus would be on the three key areas:

- People
- Process
- Technology

People

Working largely on-site, the initial priority was to undertake a very thorough investigation of NFP's current position with respect to people and its organization — how data is currently managed and how it is needed to support the SRM programme and the organization in the future. In parallel, we wanted to gain as thorough an understanding of the organization and its needs as possible.

We then embarked on a 'requirements study' by interviewing all stakeholders who have need for accurate data from within the

organization. These came largely from the Supporter Marketing Group, but other areas of the business as well. Overall, DQM Group conducted face-to-face interviews with 50 people, with varying roles, responsibilities and needs/uses of NFP's supporter data.

We built a full picture including (not in order of importance):

Many questions need asking to a broad audience across the organization

- Who needs data for what?
- Who 'owns' the data?
- What is the 'vision' for data?
- What sort of data is needed?
- What data attributes are important?
- What does the data need to support in terms of the organization, supporters' expectations and regulatory demands?
- What would it mean if data were not available to users?
- How easy is it to access and source data currently?
- What service levels are needed?
- Can NFP produce consistent performance numbers?
- Are there clear definitions (and understandings), for example, what is a supporter?
- What data risks is NFP exposed to?
- The current capability? What's covered? Where are the gaps?
- What has already been addressed? What are the priorities to be fixed?

Process

A thorough understanding of the customer data and data processes is needed

Another priority for us was to gain a thorough understanding of NFP's data itself and how it is used in, and by, the organization. We audited its key databases for:

- coverage (records and fields);
- quality (again at record and attribute level);
- consistency;
- availability;
- overlap.

We also needed to understand how data flows around NFP, its third-party processors and supporters, from data capture, to management, maintenance and distribution. Equally important were the rules (or lack of them) that are in place and whether they are being adhered to or ignored.

The longer-term aim will be to move to a single data structure and single set of rules that are rigorously applied.

Technology

The third aspect of our investigation was to understand NFP's current technical infrastructure for data management and support, and, importantly, the functionality of its new SRM system and implementation plans (not least when ideally the single data structure needs to be available).

We looked for gaps in the technology infrastructure where complementary technology could be used to help automate data governance processes and help improve data quality, compliance and measurement on an ongoing basis.

Establishing the current position on the Data Governance Maturity Model

NFP Data Governance Maturity Model

In addition to the face-to-face qualitative interviews, DQM Group targeted several versions of its Data Governance Maturity Model questionnaire comprising up to 200 questions to some 140 senior managers, business stakeholders, marketers and data professionals across NFP. This quantitative research was to give a precise current position on the Data Governance Maturity Model and highlight key areas that need addressing to enable NFP to improve its data capability on an ongoing basis.

Sample questions from the Data Governance Maturity Model questionnaire

- Is there a common definition for a customer in the organization?
- Is customer data trusted across the organization?
- Are common data models consistently governed and managed within the organization?
- Are data quality measures consistently recorded and compared?
- Is a common approach used to communicate issues, processes and updates regarding data governance?
- To what extent does the organization use formal processes to manage data capture?
- Are processes and practices deployed to define executive accountability for data?
- Does the organization deploy data standardization practices in a consistent way?
- Do business users ever build their own databases locally?
- Does the organization consistently identify and manage data issues?
- Is a Master Data Management process or method employed in the organization?
- Are data risks and issues consistently managed within the organization?
- Are privacy practices and processes consistently adopted?
- Does your organization focus on business processes?
- Does the organization commit proper resource to data quality, compliance and security matters?
- Do the group or divisional leadership teams consider data management process changes (rather than delegate to lower line levels)?
- Can business users quickly retrieve information about specific customers when they need it?
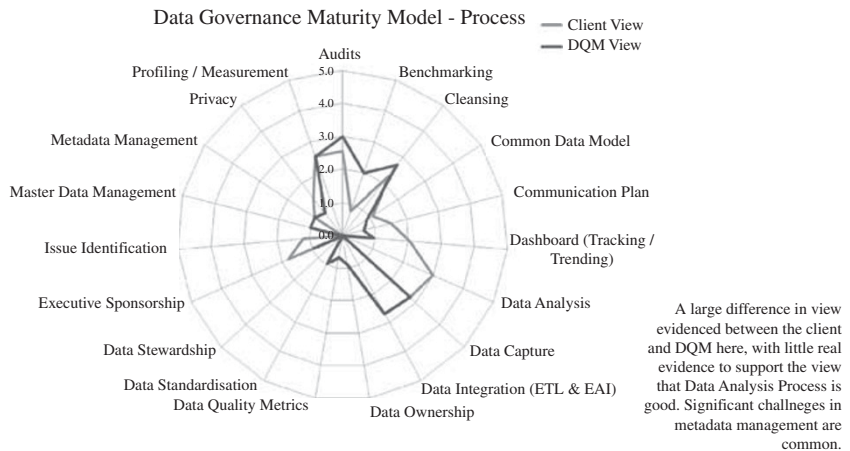
Your score and presenting the results

The detailed questionnaire approach will produce your precise point on the Data Governance Maturity Model at a given time. The answers should also generate useful 'spider diagrams' showing your score against a range of dimensions as a summary and by People, Process and Technology. These are invaluable for helping to understand where to focus your attention.
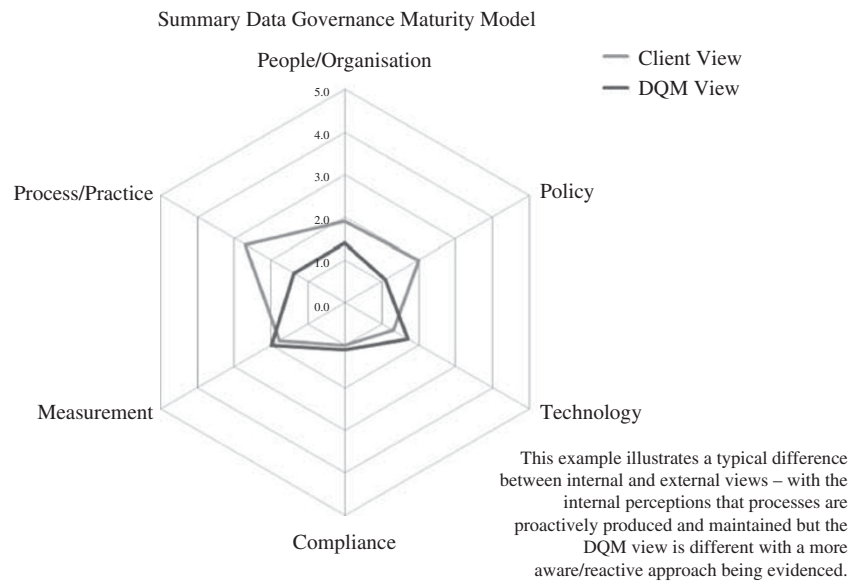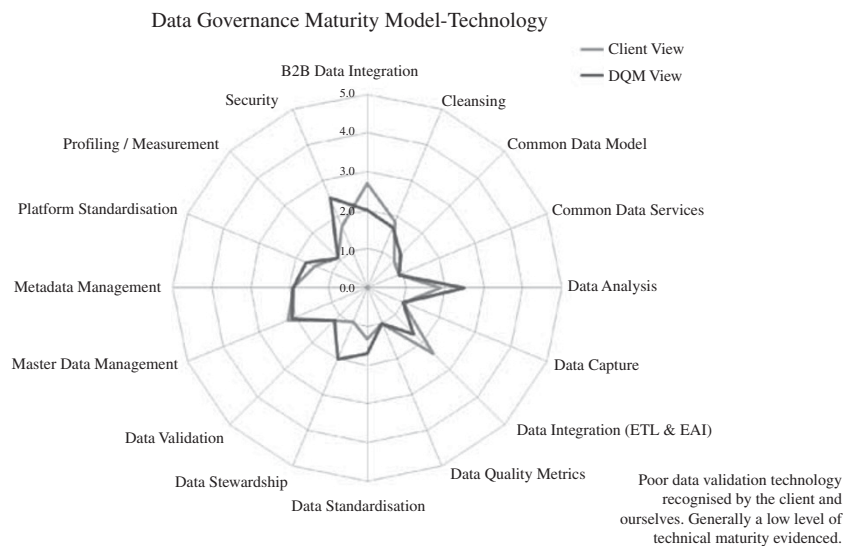

Figure 4: Summary Data Governance Maturity Model diagram showing NFP position as viewed by its staff and the DQM group view
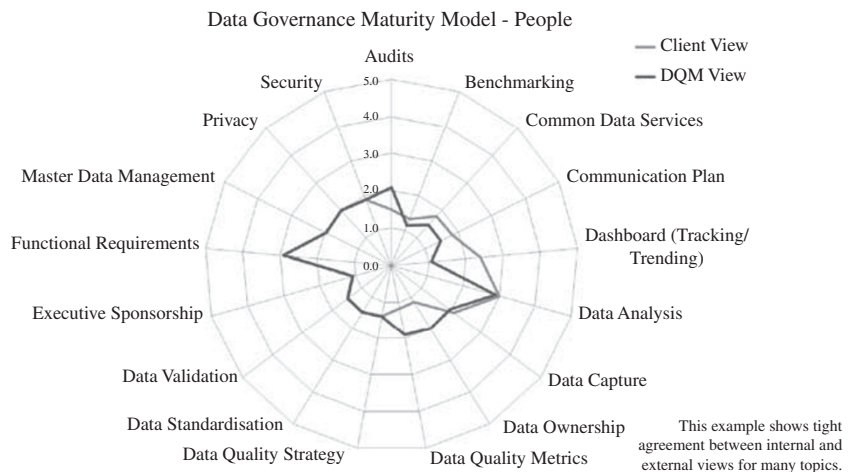
Figure 5: Data Governance Maturity Model diagram showing NFP position relating to people issues as viewed by its staff and the DQM group view

Data Governance Maturity Model - Process

A large difference in view evidenced between the client and DQM here, with little real evidence to support the view that Data Analysis Process is good. Significant challnges in metadata management are common.

Figure 6: Data Governance Maturity Model diagram showing NFP position relating to process issues as viewed by its staff and the DQM group view

Data Governance Maturity Model-Technology

Poor data validation technology recognised by the client and ourselves. Generally a low level of technical maturity evidenced.

Figure 7: Data Governance Maturity Model diagram showing NFP position relating to technology issues as viewed by its staff and the DQM group view

Figures 4–7 give illustrative spider diagrams for NFP driven by the 200 questions asked at the outset of its data governance programme in the initial Data Capability Assessment.

Results of stages 1 and 2

Reveals what needs to be done and the priorities for action

The DQM Group Data Capability Assessment gave the organization a clear picture of where it is and what it needs to do to improve its data, and to achieve the defined Business Case Benefits of the broader SRM programme. A new data organization was defined with clear roles and job descriptions defined. Thirteen work streams were designed to address and fix all the key issues over a realistic 24–30 month time frame. Remodelling and re-scoring the organization, with it having successfully completed these 13 work streams, would move it into the 'Managed' Stage and well on the way to optimal data governance.

Summary key points

Data must be 'governed' to minimize the risk of data breaches and to create long-term value for the organization. It's a challenging, long-term process but one that will deliver considerable success

- There are potentially significant risks for an organization associated with managing customer data. These include a real risk of theft or loss, damage from poor quality and breaches of data privacy. All can lead to substantial financial loss, from fines, and rework damage, to costly brand damage.
- Data governance is the business practice that defines and manages strategies for people, processes and technologies to ensure that valuable data assets are formally protected and managed throughout the organization.
- Data itself *must be governed* so that it is accurate, complete, trusted and understood and can be used to help govern the organization, greatly reduce risk and achieve compliance.
- The Data Governance Maturity Model is invaluable for giving you a precise measure today, and in the future, as you embark upon a data governance strategy to improve your data management capability.
- Once people and process factors are addressed, technology, especially for automating processes, should add value and move your organization towards achieving the Optimal level (Level 5) on the Data Governance Maturity Model.
- At this point, your customer data will be a significant asset to your organization that will truly help you drive sales, reduce costs, increase profits and achieve long-term growth.

Plus there is lots of data about data

Further reading

1. http://www.forrester.com/rb/Research/calculating_cost_of_security_breach/q/id/42082/t/2.
2. http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf.
3. English, L.P. (2009) *Information Quality Applied: Best Practices for Improving Business Information Processes*, Wiley Publishing Inc, Indianapolis, America.
4. Thomas, G. (2010 *The DGI Data Governance Framework*, The Data Governance Institute, Orlando, FL.
5. Fisher, T. (2009) *The Data Asset. How Smart Companies Govern their Data for Business Success*, John Wiley and Sons, New Jersey.
6. Ferguson, M. (2010a) 'Governance, risk & compliance series — The role of data governance in GRC Intelligent Business Strategies, July'.
7. Ferguson, M. (2010b) 'Governance, risk & compliance series — The role of data governance in mitigating risk Intelligent Business Strategies, August.
8. Racz, N., Weippl, E. and Seufert, A. (2010) 'A frame of reference for research of integrated GRC'. Bart De Decker, Ingrid Schaumüller-Bichl, ed., *Communications and Multimedia Security*, 11th IFIP TC 6/TC 11 International Conference, CMS 2010 Proceedings, Berlin, Springer, pp. 106–117.
9. http://mike2.openmethodology.org/wiki/What_is_MIKE2.0.
10. http://www.datameasures.com.
11. http://www.computerworlduk.com/news/security/3442/tk-maxx-data-breach-costs-could-hit-800m/.
12. *The Economist*. (2010) 'Data, data everywhere'. A Special Report on managing information, February.
13. DQM Group. (2010a) 'Turn your customer data into a strategic business asset — A Directors' briefing.
14. Abai, M., Adelman, S. and Moss, L. (2005) *Data Strategy*, Addison-Wesley, USA.
15. Dyche, J. and Levy, E. (2006) *Customer Data Integration: Reaching a Single Version of the Truth*, John Wiley and Sons, Canada.
16. DQM Group. (2010b) 'Customer data — The threat from within — A Directors' briefing'.