KPMG

cutting through complexity

Information Governance – The Growing Complexity

IT ADVISORY

kpmg.com/cn

The information that an organisation possesses and uses is its most valuable asset.

As data becomes more complex in today's digital era, it is ever more important that information usage and protection be transparent.

Information governance aims to provide a management framework for an organisation's information based on its business value and associated risk. If applied appropriately, information governance can provide a mechanism to generate fast, high-quality information to help leaders make vital business decisions. In addition, it can provide customers and regulators with insights into how the data has been collected, used, transferred, stored and/or destroyed.

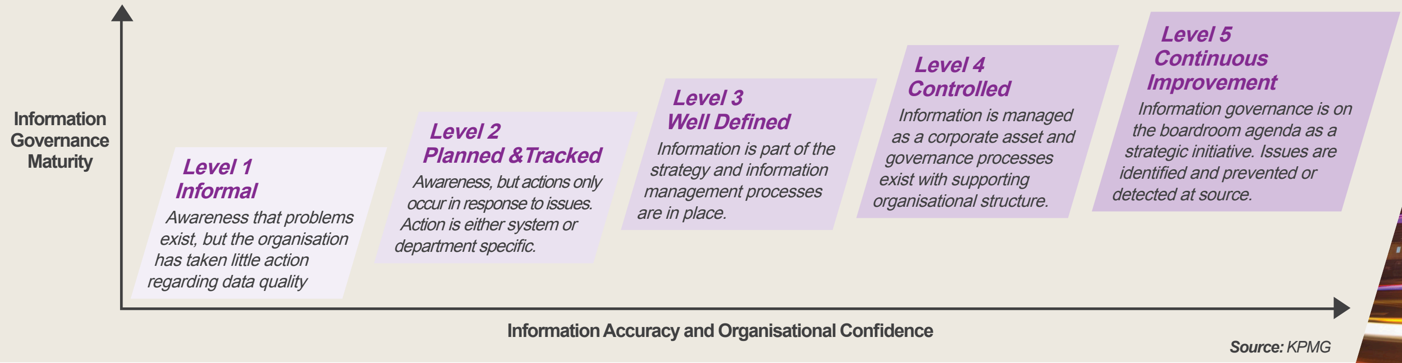
[Differing regulations, in conjunction with the increased focus on information risk and customer data confidentiality, means information governance should have a firm place on the boardroom agenda.]

As organisations grow, managing information assets becomes much more complex. Data security breaches now appear to be headline news almost on a weekly basis. The consequences can be disastrous as organisations' bottom line and reputation are impacted.

Differing regulations regarding State secrets, personal data protection laws and cross-border data transfer are becoming more complex. In conjunction with the increased focus on information risk and customer data confidentiality, this means information governance should also have a firm place on the boardroom agenda.

Pressures on information governance

Information management and protection is undoubtedly moving in keeping with organisational changes. A planned governance structure for information allows organisations to support business expansion, while meeting regulatory and personal data protection laws. An example of an Information Governance Maturity model is illustrated below, which clearly outlines the link between information accuracy and confidence in an organisation. Companies with higher-level maturity models tend to have clear leadership commitment embedded in their business, which includes common governance processes and structures.


Information Governance Maturity
Level 1 Informal
Awareness that problems exist, but the organisation has taken little action regarding data quality
Level 2 Planned & Tracked
Awareness, but actions only occur in response to issues. Action is either system or department specific.
Level 3 Well Defined
Information is part of the strategy and information management processes are in place.
Level 4 Controlled
Information is managed as a corporate asset and governance processes exist with supporting organisational structure.
Level 5 Continuous Improvement
Information governance is on the boardroom agenda as a strategic initiative. Issues are identified and prevented or detected at source.
Information Accuracy and Organisational Confidence

Source: *KPMG*

One of the main reasons structured information management is needed is the increasing obligation to assure customers about how data is handled. The challenges of protecting client data confidentiality and strict personal data protection laws have meant the handling of customer data should be completely transparent and have clear accountability.

Information governance reduces the risk of accidental and/or deliberate breaches of client information, employee data and/or intellectual property. By classifying and identifying critical data elements and understanding its location and flow, organisations can have improved control over their information assets. Strong governance ultimately supports brand protection and increased enforcement of policies both internally and with third parties. In a world where data loss is heavily publicised and penalised, getting this right is proving financially significant, both financially and from a reputation standpoint.

Why is it important?
The China and Hong Kong Landscape

China tends to focus on enforcing its numerous local requirements for data protection. The restrictions regarding data leaving China are board issues, and the data may be incriminating if it relates to State secrets. The Hong Kong Security Bureau continues to develop policies for the protection and handling of confidential government information.

The Personal Data (Privacy) Ordinance is not new to Hong Kong, though the Amendment was passed in June 2012 and the first phase came into effect in October 2012. This has had significant impacts on all those handling personal data in Hong Kong. Organisations that collect, process and use personal data now have tighter, more refined Data Privacy Principles to follow. Organisations using personal data in direct marketing, and/or transferring data to those engaging in direct marketing will have even more obligations to protect data privacy. For example, if an organisation intends to use personal data in direct marketing, it must inform the data subject (the person the data is related to) in writing regarding the kind of personal data, which will be used, and the classes of 'marketing subjects' it relates to. The data subject must be given a free response mechanism whereby he/she can swiftly give consent. This consent mechanism also applies to the transfer of personal data to another organisation.

Understanding how information is governed in an organisation is the key to compliance and, increasingly, the market brand. It also helps to address the growing need for data quality when engaging customers on a personal level, to analyse spending behaviour and internet browsing patterns, and to study synergies in cross-marketing between integrated product (brand) offerings.

> **The Personal Data (Privacy) Ordinance is not new to Hong Kong, though the Amendment was passed in June 2012 and the first phase came into effect in October 2012. This has had significant impacts on all those handling personal data in Hong Kong.**

Whose problem is it?

Historically, establishing robust information management was considered an IT challenge. The chief information officers were expected to deliver the appropriate technology to support critical data reporting, while the chief information security officers, who are mostly aligned with IT functions, were expected to protect it. As the regulation of data usage has significantly tightened over recent years, the approach to information management has been forced to shift so that a cross-functional approach to governance is now required. The business needs to be involved as they own the data, not the IT.

> **Organisations often find it difficult to establish the cross-functional collaboration they need to appropriately manage and tackle this broad information management challenge.**

Business leaders are now accountable. Inadequate control over information can directly impact the organisation's reputation and its top line, and breaching any regulation or legislation can result in possible personal liability for these leaders. However, organisations often struggle to obtain the necessary information to help them decide on what action to take to manage this exposure in a cost-effective way.

For organisations to consider all aspects of information governance, they now need input from experts in the various areas of information use and protection. This includes Privacy (Legal, HR), IT Security (Technology, Business Continuity), Management Reporting and Analytics (Business Units), Operations (COO), and Forensics and Regulatory Compliance (Risk and Compliance). Organisations often find it difficult to establish the cross-functional collaboration they need to appropriately manage and tackle this broad information management challenge. Although this type of silo mentality across the business increases cost, it is often considered acceptable so long as the small cogs operate effectively, produce reports, and protect data in systems. IAs such, information governance can provide standardisation, help with cost control and can help organisations react effectively to reporting and compliance requirements. It also contributes to a number of the business objectives shown below.

BETTER

- Reduces errors & mishandling
- Enhances project management
- Increases process efficiency
- Sustains compliance
- Assists cultural change/accountability

CHEAPER

- Reduces litigation costs
- Lowers audit costs
- Lowers IT infrastructure costs
- Decreases cost of control
- Reduces error costs
- Lowers insurance premiums

FASTER

- Reduces processing time
- Increases information sharing & availability
- Fosters effective communication & cooperation between business units
- Integrates key processes
- Streamlines acquisitions

MORE SECURE

- Strengthens processes/ controls
- Increases information ownership
- Provides controls by sensitivity
- Reduces number of vulnerabilities
- Offers controls across lifecycle
- Provides controls designed for risk
- Reduces incident costs

Approaches vary but standardisation is key

Information governance approaches should provide standardisation for information management, and should focus on finding the most suitable personnel, processes, technology and controls that address compliance requirements, while also protecting the most important information assets.

Information LifeCycle Management (ILM) can be used to align the business value of information, and comprises policies, processes, practices and tools. In this way, organisational support from all levels is inherently required to promote proper information governance, such as promoting awareness through training.

A robust approach should cover the complete governance lifecycle, enabling organisations to choose the appropriate focus they require to achieve their specific business needs. At a high level, the KPMG approach supports organisations across the following key areas:

Privacy

The handling and protection of personal identifiable information (PII) that individuals provide in the course of everyday transactions, electronically or otherwise, across territories and jurisdictions.

Data classification

The process of dividing data sources, e.g., documents, applications, databases, into groupings to which defined levels of controls, protection and policies can be applied to support business objectives.

IT security

The process of protecting data from unauthorised access, use, disclosure, destruction, modification, or disruption across multiple jurisdictions.

Third-party management

The process of managing external entities that may process or store information owned or originated by an organisation, e.g., Cloud providers.

eRecords management

The planning, controlling, directing, organising, training, promoting, and other managerial activities related to the creation, maintenance and use, and disposition of electronic records; this is typically managed through data ownership, governance structure and committees.

Data flow analytics

The process of classifying and managing the flow of information assets within an organisation and to its third parties, creating value out of big data and understanding its sensitivity.

We have extensive experience in assisting clients with their information governance and information protection needs. Our approach is to help balance value preservation with value creation to deliver the desired results, based on the organisation's specific needs.

KPMG
cutting through complexity

TECHNOLOGY RISK CONSULTING

Information Risks Today

Embrace or Deny?

A Board member's guide to today's information security and risk revolution.

www.kpmg.co.uk/security

DATA LOSS BAROMETER

Insights into lost and stolen information / November 2010

KPMG's Data Loss Barometer shines a light on the latest trends and statistics for lost and stolen information in 2010

Key Findings:

- Overall downward trend (25%) in reported data loss incidents
- More records are lost or stolen within Financial Services than any other sector
- The 'Malicious Insider' is a continuing threat
- 12% growth of data loss incidents in Healthcare
- Portable media are still largely unencrypted
- More people affected by Hacking than any other cause of data loss
- Incidents involving a third party is more commonplace in the Government sector

KPMG
cutting through complexity™

THE METHODOLOGY

The Data Loss Barometer analyses data loss incidents reported around the world since 2005. This data is freely available in some countries thanks to legislation that requires full disclosure of data loss incidents. In other countries, information is obtained via KPMG's global network of independent member firms.

Key information sources include the media, internet searches and independent news or data feeds. Care is taken to use data only from reputable and independent sources. Availability, consistency and accuracy of information can vary between sources, countries and by type of incident.

A complete list of the information sources used is too large to include here but particular thanks should go to the Open Security Foundation who have provided invaluable support and information.

For more information, go to www.datalossbarometer.com

KPMG

China Boardroom Update
New Guidance from the Privacy Commissioner

ADVISORY

Issue 4 – August 2010

There would be little disagreement that privacy is a significant issue for both business and consumers alike in the Hong Kong market place. 90% of respondents in a recent KPMG survey stated privacy concerns as an issue for the adoption of mobile and Internet based initiatives. But what can be done by business in order to gain the trust of the consumer and reduce this level of concern?

Privacy Commissioners Guidance:

- Privacy Impact Assessments (PIA)

Further KPMG reading material on privacy and data loss related issues:

- Data Loss Barometer
- Privacy Bulletins

Updates from the Privacy Commissioner

The Hong Kong Privacy Commissioner for Personal Data has recently released new guidance on how organisations should obtain assurance that they are protecting the information of their customers and staffs. The guidance dictates how organisations are responsible for the personal information they maintain and that they should perform regular Privacy Impact Assessments (PIAs) as part of their projects to limit their exposure to privacy risks.

In an associated media release, the Office of the Privacy Commissioner is quoted as saying:

"Although PIA is not a requirement under the Personal Data (Privacy) Ordinance, I always advise organisational data users to conduct a PIA before embarking on a project which involves the handling of a substantial amount of personal data. A PIA will not only serve to indicate the privacy risks the project may involve but also helps data users to build data protection into the design of the project."

The guidance comments that PIAs are a systematic tool that can aid organisations to make informed decisions when implementing new projects, which could impact personal information. By integrating the assessment within the project's delivery, early warnings can be provided where legislation may not be enforced or where the risks to personal information are not being adequately addressed.

The PIA process is defined as having four key steps:

1. Analyse the data processing cycle against the six data privacy principles.
2. Analyse the risks associated with the information in question considering the volume, nature and activities of the data subjects and users.
3. Assess the mitigating activities that have been implemented to address any concerns that have been identified.
4. Provide a report that gives a summary of the project for context and the results of the previous three stages.

AUDIT • TAX • ADVISORY

The need to identify, classify and control transactional and customer data is growing. Once these initial steps have been established and data ownership has been standardised through information governance, other aspects should increase. These include the ability to provide data management and loss prevention, sustainable information for management reporting, and cost-effective compliancy with privacy laws. Otherwise, mind the gaps.

If you require further information, or you would like to arrange a discussion, please contact:

Hong Kong

Henry Shek
Partner
Consulting

henry.shek@kpmg.com
+852 2143 8799

Alex Skilton
Senior Manager
Consulting

alex.skilton@kpmg.com
+852 2847 5025

Mainland China

Philip Ng
Partner
Consulting

philip.ng@kpmg.com
+86 (10) 8508 7093

Wesley Wang
Director
Consulting

wei.wang@kpmg.com
+86 (21) 2212 2850

KPMG
cutting through complexity

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.