What is information governance and how does it differ from data governance?

Susan Bennett, Principal, Sibenco Legal & Advisory and Co-founder, Information Governance ANZ

- The terms 'data' and 'information' are often used interchangeably however they are not the same.
- Information governance provides a strategic framework for organisations seeking to control data and information.
- To derive value from information, companies need to invest in technology and systems that can be used to gain a competitive advantage and deliver benefits directly to the bottom line.

As information governance and data governance becomes increasingly important for organisations seeking to control and secure information, it is important to understand what each one does and achieves.

What exactly is their purpose, and how do they differ from one another?

Information governance is a fundamental part of good corporate governance. Its mission is to maximise the value of information while minimising the costs and risks of holding it. Data governance is a key subset of this model. It aims to control information at the data level, ensuring the maintenance of accurate and high-quality data through the implementation of appropriate systems and processes.

This article looks at the roles information governance and data governance play within an organisation and how they are interlinked.

Data and information

While the terms 'data' and 'information' are often used interchangeably, they are not the same. Data consists of bits and bytes — a collection 0s and 1s which are processed by computer systems. Information comes from data, after the data has been organised, analysed and presented in a context where it can be used. Traditionally, the concept of information has been understood as 'the act of informing', usually in the context of conveying knowledge. In other words, information is data with context.

Table 1 illustrates the difference between data and information, and how the information then enables decisions to be made to improve outcomes.

As the above examples illustrate, data is the recording of the occurrence of the event(s). The data analysis process occurs once the data has been organised and cleaned, which then enables trends, insights and information to be produced. This in turn enables relevant decision-makers to enhance improve processes, products or services to improve outcomes.

Figure 1 shows how information extracted from data analytics can be used to ultimately deliver on an organisation's strategic goals. It also demonstrates that the value of data is not inherently in the data itself — instead, it is derived through the creation of a data set or sets, the data analytics process and from the information that is derived, which is then used to make better decisions and deliver improved outcomes. See Figure 1.

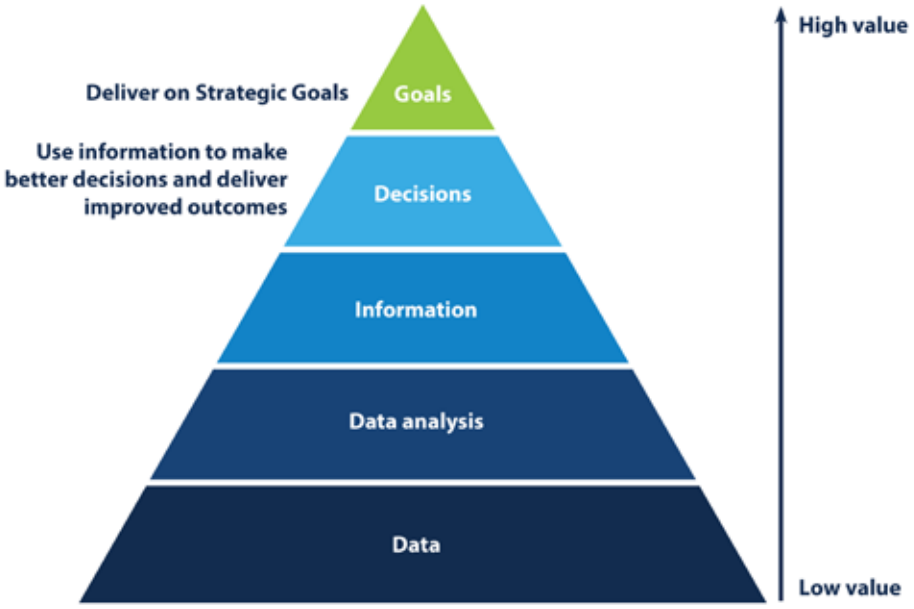
Big data and information

Big data describes the exponentially increasing volumes and variety of data held by corporations and governments that cannot easily be processed or manipulated with ordinary tools. The

Table 1: The difference between data and information, and how they can be used.

DATA	INFORMATION	OUTCOME
Date and employee IDs for employee sick days	Dates of employee sick days before or after long weekends	Identify employees and take appropriate action e.g. conversation with employee, adjust work rosters
Dates and times of pick-up and delivery of packages	Length of time taken to deliver to different areas and/or different days of week	Adjustments to logistics, e.g. control time of departures to maximise efficiency in time and costs
Blood pressure readings and dates	Sally Smith's blood pressure reading and dates	Adjustment of medication for Sally Smith
Number of caesareans in 2016 in NSW	XYZ Hospital caesarean rate for 2016 in NSW	Review why rate of caesareans was statistically different to previous comparable period and/or other hospitals

Figure 1: How information extracted from data analytics can assist an organisation's strategic goals



UK Information Commissioner's Officer March 2017 report, entitled 'Big data, artificial intelligence, machine learning and data protection' [at para 11] describes the connection between big data, artificial intelligence (AI) and machine learning as follows: 'AI can be seen as a key to unlocking the value of big data; and machine learning is one of the technical mechanisms that underpins and facilitates AI. The combination of all three concepts can be called 'big data analytics'.

Big data analytics — using modelling, AI and machine learning — enables insights and information to be derived from these big data sets. The information can then be used to deliver improved outcomes for both corporations and governments. For example, in the corporate sector, the insights may lead to the development of new or improved products or services, which can provide a competitive advantage and ultimately deliver improved results to the bottom line. In the government sector, big data analytics can lead to better decision-making, such as more efficient allocation of resources or an increased ability to direct resources to improve outcomes overall.

In other words, there is big value in the information that can be extracted from data for both the corporate and government sectors. In December 2015, the Australian Government released its Australian Government Public Data Policy Statement as part of the National Innovation and Science Agenda, recognising data as 'a strategic national resource that holds considerable value for growing the economy, improving service delivery and transforming policy outcomes'.

Information governance

Information governance provides a strategic framework for organisations seeking to control data and information. It recognises the value and opportunity of data as a strategic resource or 'the new oil' and identifies the risks and costs involved in the event of non-compliance with legal requirements and the consequences of a serious data breach. See Figure 2.

Information governance is defined by the Information Governance Initiative (a think-tank and community of IG professionals) as, 'The activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs.'

In other words, information governance encompasses the systems (including policies, processes, and technology) by which information is used, processed, controlled and secured.

Organisations should consider information as an asset and measure both the value and costs of the data and information they hold. This means quantifying the financial benefits of data

Figure 2: Information governance

as well as the costs (and subsequent savings) resulting from risk management investments.

To derive value from information, companies need to invest in technology and systems that can be used to gain a competitive advantage and deliver benefits directly to the bottom line. This includes the implementation of data analytics to improve or develop new services or products, or data sharing systems to enhance, for example, the allocation of resources for the delivery of health services in the public sector.

Reducing costs and risks of holding information

Minimising the risks and costs of holding information is one of the main objectives of an information governance program. Further strategic investments are needed to achieve this, specifically in technology, processes and people.

Organisations incur significant costs in holding information that is either required for the running of the business (RIM) and/or by law. Legal requirements include:

- record keeping obligations
- data protection and privacy obligations
- document/data production in litigation — ediscovery.

Well managed organisations have an active defensible disposition of records program, which eliminate documents no longer required by law and governs the ongoing removal of redundant, outdated and trivial documents (ROT) from the business.

Decreasing data storage costs can be counterproductive, because it encourages data retention. Large data volumes can create a significant financial burden — especially when the following are considered:

- the costs of holding large volumes of data including additional resources (personnel) and storage costs
- the costs of 'back ended' services — for example, analytics services to find documents, information audits and other forensic services that may be required from time to time
- the cost of producing documents/ data for litigation and regulators — ediscovery — which has grown into a $10 billion per annum global industry due to the exponential rise in data volumes held by organisations.

Minimising data breach costs in the event of a cyberattack

An effective information governance program can also help mitigate the costs of a serious data breach, which include:

- business interruption costs
- costs of data breach notification. From February 2018, government agencies and businesses covered by the *Privacy Act 1988* will be required to notify any individuals affected by a data breach that is likely to result in serious harm
- costs of responding to regulators
- ongoing lost revenue and profit due to brand and reputation damage where personally information is disclosed, such as customer and employee information
- costs of litigation including class actions
- share price dips
- C-suite executive departures.

A comprehensive information governance program that ensures an effective response to a potential data breach includes:

- a privacy framework with policies and processes aligned with the information governance program, protecting personal information and upholding a culture of privacy through training and auditing
- ensuring the implementation of appropriate cyber incident reporting, both internally and to external regulators, as required under mandatory notification breach legislation, cyber incident response and business continuity plans
- training of all relevant personnel (including it, privacy and legal) to equip them to respond quickly and adequately in the event of a data breach.

Data governance

Data governance is a key subset of information governance. Its objective is to control data at the data level and to ensure integrity through appropriate systems and processes.

An effective information governance program can also help mitigate the costs of a serious data breach.

According to the Data Governance Institute, Data governance is defined as follows:

> 'Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.'

In April 2017, ISO/IEC 38500 was released, titled 'Information technology — Governance of IT — Governance of data.' The introductory section refers to the advent of cloud computing, the realisation of the potential of the 'internet of things' and the increasing use of big data analytics. It states:

'This flood of data brings with it an urgent requirement and responsibility for governing bodies to ensure that valuable opportunities are leveraged and valuable data is protected and secured.'

The American Health Information Management Association (AHIMA) provide the following explanation:

> 'Data governance is the sub-domain of information governance that provides for the design and execution of data needs planning and data quality assurance in concert with the strategic information needs of the organization. Data governance includes data modelling, data mapping, data audit, data quality controls, data quality management, data architecture, and data dictionaries. DG collaborates with EIM in functional components essential to the enterprise plans for information organization and classification.'

The ISO/IEC 38500 sets out the principles, model and aspects for good governance of data. This includes the 6 principles for good governance of IT as they relate to data include:

1. Responsibility — for the organisation's use of data including the whole lifecycle of data
2. Strategy — data strategy that aligns with overall strategy, including plans for data use, covering all parts of the data accountability map
3. Acquisition — by collection or purchase or as a by-product of business activity of data
4. Conformance — relevant performance metrics, including conformance to external obligations and internal compliance to appropriate internal policies
5. Human behaviour — identifying and properly considering human behaviours for example, policy to govern the acceptable use of data and devices across the organisation.

Section 9 of the ISO/IEC 38500 sets out the governance of data-specifics aspects this includes:

- quality — the measure of how accurately it encapsulates the facts it is trying to represent
- timeliness — which will depend on the decisions being made
- context — applying context to data allows information to be obtained from it
- volume — a large amount of consistent data may increase the confidence of a trend of prediction
- risk management — including data classification schemes and security of data
- constraints — including legislation, regulations, contractual obligations to access, use, store or distribute the data; as well as societal concerns about how date is used and how decision are made from that data.

Figure 3: Definition of information governance

Data derived from the Information Governance Initiative 2014 Annual Report.
More info at www.iginitiative.com. © Information Governance Initiative.

The purpose of data governance is to implement effective data management, ensuring that data is of high quality, accurate and reliable. Data governance programs rely on the implementation of specific data policies and processes within an organisation, where the management, cleansing and storing of data follow strict standards and procedures.

Increasingly data governance is managed by a chief data officer (CDO) or equivalent who is responsible for setting data governance policies and procedures and implementing and monitoring systems to ensure that data is reliable and of high-quality.

The relationship between information and data governance

Barclay T Blair, Executive Director of the US-based think-tank Information Governance Initiative (See Figure 3 for their definition of information governance) explains the difference between information governance and data governance as follows:

'The two are executed in different parts of the company, by different people, with different tools, with different practical goals. Whereas information governance is mostly concerned with risk mitigation, Data governance is mostly concerned with things like data quality, master data management, and dashboards enabled by a common schema. Of course, in concept both disciplines encompass both risk and value, but in practice this is what it typically looks like.'

Typically, information and data is managed by various owners throughout an organisation including:

- data — chief data officer
- privacy — chief privacy officer or general counsel
- cybersecurity — chief information security officer
- risk & compliance — chief risk officer
- records — rim manager
- ediscovery — ediscovery counsel or general counsel

In recent years, a new role of chief information governance officer (CIGO) for overall responsibility of information has emerged to ensure information governance and organisational objectives are met. See Figure 4.

Whether the leader is an information governance steering committee, a designated C-level executive within their current existing role or a CIGO, the task is to successfully align information governance systems including technology, processes and people to meet the organisation's overall strategic business objectives.

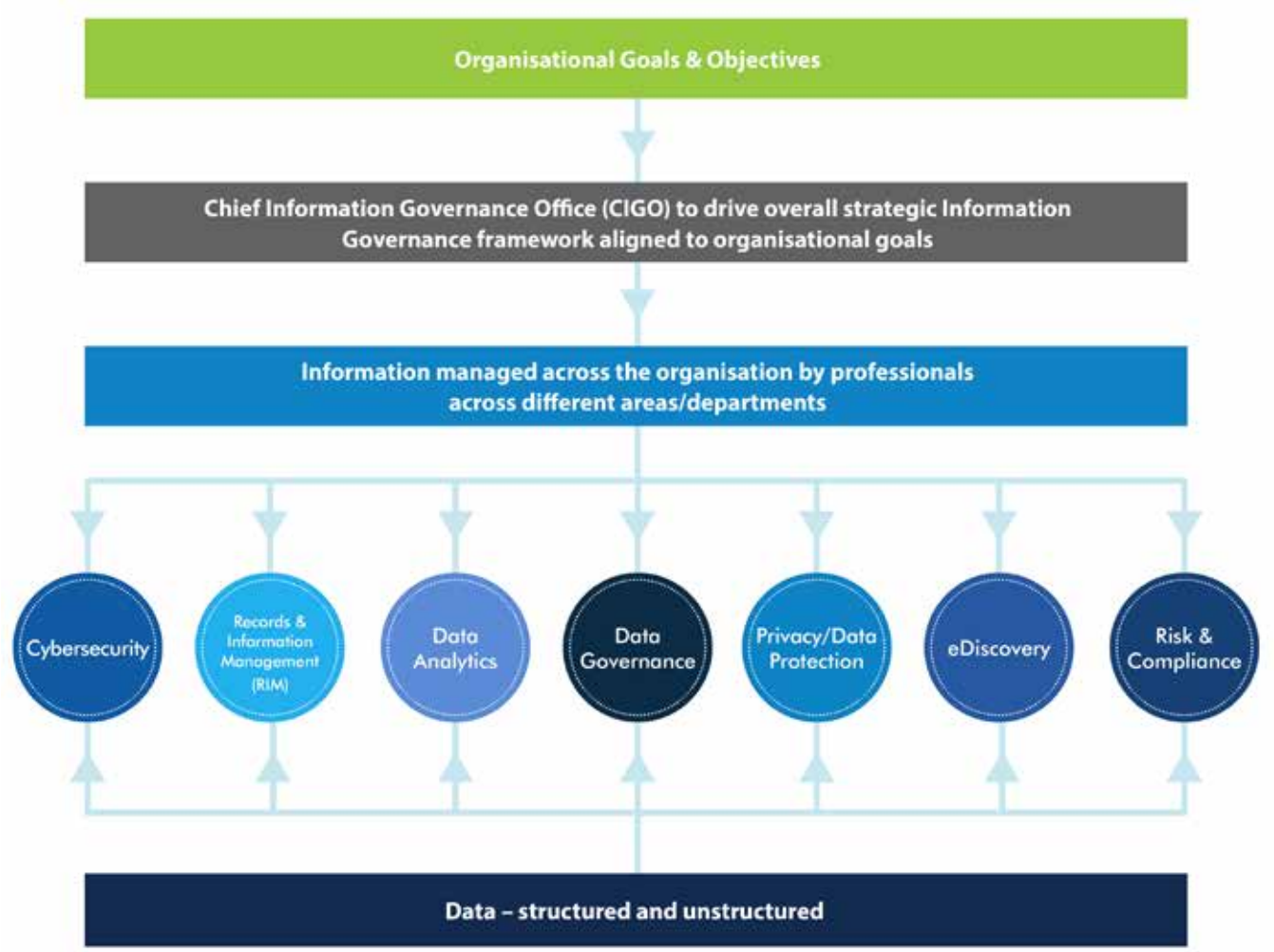
Information governance requires top down leadership. Boards and senior management are responsible for ensuring that an appropriate information governance framework, systems, and policies for information management activities are in place and being adhered to. The information governance framework and program includes: IG charter; data governance policies and procedures; privacy policies and procedures; information security policies and procedures; records retention and disposal policies and procedures; and legal hold policies and procedures.

It also requires those responsible for information across the various silos to work collaboratively to ensure that information strategic objectives are met and risks managed appropriately. The role of a dedicated CIGO who is able to work across the various organisational silos provides an effective mechanism for ensuring that data and information is controlled and secured, as well as minimising risks and maximising opportunities to derive value from information held by organisations.

In summary

Information governance and data governance are both increasingly important as the volumes and variety of data held by organisations continue

Figure 4: Organisational goals and objectives



to increase at exponential rates. It is important to keep in mind that the responsibility is not just for big data sets, it is for all data held and for all data in respect of which the organisation is responsible.

If the organisational focus is on data governance then all potential risks and costs will not be effectively minimised and the opportunity to leverage the data to better utilise the information it yields may not be maximised. An overall information governance framework will ensure that the information and data strategy is coherent and aligned throughout the organisation to enable strategic organisational goals to be achieved.

Effective information governance ensures that the business value of information is maximised and the risks and costs of information are minimised while an effective data governance program ensures that the data being held is accurate and reliable. ◪

Susan Bennett can be contacted on (02) 8226 8682 or by email at susan.bennett@sibenco.com.