REPRINT

IMPLEMENTATION OF AN INFORMATION GOVERNANCE PROGRAM

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

JAN-MAR 2015 ISSUE

risk & compliance
JAN-MAR 2015
www.riskandcompliancemagazine.com
Inside this issue:
FEATURE
The role of General Counsel and Chief Compliance Officer
EXPERT FORUM
Effective management of cyber security risks
HOT TOPIC
Implementation of an information governance program

www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

HOT TOPIC

IMPLEMENTATION OF AN INFORMATION GOVERNANCE PROGRAM

PANEL EXPERTS

Bas van Gils
Consultant
BIZZdesign
T: +31 (0)6 4843 2088
E: b.van gils@bizzdesign.com

Bas van Gils is a passionate and experienced consultant, trainer and researcher with a focus on strategic architecture and data management. He holds an MSc in information management and technology from Tilburg University, and a PhD in computer science from Nijmegen University. Mr Van Gils has been involved in a variety of projects, ranging from strategic redesign, building an architecture capability, building a data management capability and optimising a business intelligence landscape. He has published several academic and professional books and articles, and is currently also active as public speaker, researcher and lecturer.

Sanjay Bhandari
Partner
EY
T: +44 (0)20 7951 8370
E: sbhandari@uk.ey.com

Sanjay Bhandari is a partner in the Forensic Technology & Discovery Services Practice at EY in London. He is a qualified lawyer with over 25 years' professional experience and has a specific focus on information governance and e-discovery. Mr Bhandari has managed cross-border disputes including many disputes and investigations involving large scale document production. He has advised businesses in a wide variety of sectors and also advises clients on records risk management strategies, an area of increasing concern to businesses dealing with the risks associated with quickly expanding electronic records.

Chris Saunders
European Leader for Data and Information Governance
IBM Global Business Services (GBS)
T: +44 (0)782 451 8913
E: chris.saunders@uk.ibm.com

Chris Saunders is the European leader of Data and Information Governance for IBM Global Business Services. He has specialised in this area for more than 10 years, managing successful consultancy assignments with more than 30 companies across both public and private sectors, including financial services, oil & gas, utilities, telecommunications, automotive, industrial, retail, professional services, defence and treasury. Mr Saunders is a frequent author of white papers and speaker at international conferences on Data Quality Management and Governance. In 2010 he was responsible for the written submission which was awarded the global Data Governance Best Practice Award for his client the British Army.

Julian Cunningham-Day
Partner
Linklaters LLP
T: +44 (0)20 7456 4048
E: julian.cunningham-day@linklaters.com

Julian Cunningham-Day is a Linklaters partner with many years' experience working on multinational information governance projects including advising on confidentiality, privacy, bank secrecy, records management strategies and the implementation of binding corporate rules. In particular, he specialises in complex multi-jurisdictional compliance projects in highly regulated industries such as financial services and telecoms. He also has extensive experience in IT-related corporate transactions, telecoms, eBusiness and outsourcing.

Steven Zagoudis
Founder and CEO
MetaGovernance Solutions LLC
T: +1 (404) 593 1601
E: szagoudis@metagovernance.com

Steve Zagoudis is a co-founder of MetaGovernance. He has substantial corporate experience directing IT and information governance efforts at Standard Oil, BP Worldwide, Sequent, IBM, Goldman-Sachs and 7 of the 12 Federal Home Loan Banks. Mr Zagoudis' involvement with executive-level management puts into practice his passion of driving business and competitive advantage through the optimal use of an organisation's information assets.

RC: In what ways has the nature, volume and importance of information produced by companies evolved over the years? How has the associated risk profile changed?

Van Gils: Since the industrial age, there has been a slow but steady increase in the amount of information that companies use and produce. While manual, and often *ad hoc*, information management processes were sufficient in the past, in the modern technological era this is no longer the case. The introduction of the computer has made it easier for companies to store and reproduce data, the web has made it easier to share data, and currently we are experiencing the effects of big data and the internet of things. Companies are increasingly dependent on data and information. Without these key assets, many industries would collapse. Accordingly, the risks associated with information have changed drastically, both in terms of probability and impact. Perhaps the most discussed example at the moment is the privacy issues that result from large scale combinations of social and big data. There is wide recognition of this fact, given the amount of legislation around information quality and governance, the attention for data and information management processes and discussions about information valuation in academic and professional literature.

Bhandari: Information has become multi-faceted and is generated across multiple systems. The ease of generating information has led to an annual growth rate of about 40 percent in the enterprise, according to IDC. The importance of structured and unstructured information in the organisation has also increased significantly in terms of business intelligence, operational efficiencies and regulatory compliance. It is for this reason that information needs to be proactively managed. The associated risk profile of the information landscape has changed dramatically in terms of the challenges of managing a growing volume of data across multiple applications. That challenge is exacerbated by the often marked absence of appropriately evolved information governance practices. Information is also increasingly shared with third parties, can be transferred and processed in countries outside EEA and hosted in the cloud, which adds complexity to control and security.

Saunders: Just about any bog-standard presentation on corporate data starts with a quotation about the 'data explosion', how we are drowning in data and how it is increasing exponentially. Today there are three key elements regarding corporate data. The first is proper lifecycle management, so that companies have the right level of access to the right type of data and can comply with security and privacy legislation. The second is the effective and compliant use of big data. The third is dealing with unstructured as well as structured data, and gaining the right value from it while subject to internal and external requirements. The risk profile has changed, and with the sheer volume of data involved it is essential to take a risk management approach to data. Companies should think about a number of issues, including risks of loss, security breaches, costs of non-compliance, and, of course, the corporate reputation when data is misused. This is applicable for either an individual dealing with the company, or on a larger scale when the company's name hits the public domain.

Cunningham-Day: Once it was only the fundamental components of a business that were committed to paper – at the time the only durable medium in which records were retained – now, virtually every minute aspect of a company's operation is recorded through some electronic process, whether it be the electronic communication channels we almost all use, or the system/building monitoring processes that we install. While statisticians may attempt to quantify the volume of this information, its value and risk is much harder to define, let alone predict, over the years that much of the information will remain in existence. As humanity grapples with recycling the explosive growth of physical waste on this planet, powerful analytical tools are increasingly deriving commercial and philanthropic value from the digital exhaust of our working lives. At the same time, these tools are increasingly being used by competitors, regulators and governments to defend their own interests and attack those they consider to be threats. Participating in the digital economy offers the opportunity to be successful at a speed and scale that was inconceivable even 10 years ago, but the risks are enormous too, with reputations and fortunes destroyed overnight through the power of social media.

Zagoudis: Two challenges emerge from the current state: mining the growing mountain of data through its various uses and lifecycle and transforming this mountain of data into accurate information that organisations can use for competitive advantage and decision-making. Increased automation in all areas of business, from manufacturing floor to online sales platforms has resulted in exponential growth in data. The push to digitisation and the 'internet of things' increases the risks of exposing data to outside parties through network breaches. The explosion of data within the organisation has resulted in sophisticated databases and reporting tools that can handle big data. Unfortunately, the adoption of new tools can be rendered ineffective if uncontrolled and undocumented. Stewardship models are needed to assign risk and accountability. Ensuring this proper accountability and lifecycle transparency for critical data will continue to be an imperative.

RC: In your opinion, are companies doing enough to address the challenges they face in managing the information they produce, store, handle and transfer?

Bhandari: Companies have tried different approaches to address the challenges they are facing and are in a state of flux. In the last few years, these challenges have often been seen as an IT issue and the approach has therefore been to invest in sophisticated technologies which have incurred significant investment and perhaps questionable value add. Increasingly, organisations are realising that in the absence of good information governance principles, these applications are difficult to implement and manage.

Zagoudis: Our experience suggests that companies are often solving only pieces of the problem, or their efforts are siloed in a department or division of the organisation. These disparate efforts fail to achieve the desired business objectives and don't move the organisation towards better profitability or competitive positioning. Most companies are still dealing with basic data plumbing issues. Very few are at the level of managing and leveraging their information assets. What's needed in the future is a more comprehensive approach that optimises information for internal usage, manages information through its lifecycle, and creates a path to continuous improvement. Information governance as a discipline is evolving within companies with various stages of adoption. Many related disciplines, including data governance, policy compliance, content management and security are operating under the umbrella of information governance, but without meaningful improvements in accuracy and accountability.

> **"It would be a brave company that stood up and said they were doing enough to manage their information."**
>
> *Julian Cunningham-Day, Linklaters LLP*

Cunningham-Day: It would be a brave company that stood up and said they were doing enough to manage their information. The level of understanding of the value and risk of a company's information footprint has moved swiftly up the global board agenda in most multinational organisations, with the appointment of chief information officers and chief data officers proliferating. Companies have been subject to legal or commercial imperatives to retain and protect various types of information for decades, such as accounts, contracts and payroll, and most sophisticated organisations have now developed local procedures to identify what needs to be kept, for how long and how to minimise the risks of losing the information. Most of these procedures were first developed in a business culture dominated by physical records and private communications; few have managed to develop holistic strategies that effectively manage the risks associated with the increasingly electronic, globalised, unstructured and replicated nature of modern business records.

Saunders: As any good consultant will always say, "it varies". Some companies have been doing this for a long time, whereas others have started only recently. Most firms are now at least starting to address it. Unfortunately, there are a lot of common traps into which companies fall. Some firms are being too formal and all-embracing, trying to get every aspect of information governance documented and agreed by senior management without actually doing anything. Secondly, a tick-box culture has begun to emerge: firms seem to think that, by sending out regular questionnaires to ask departments and process leaders if they are complying with corporate policy, they are managing information effectively. Thirdly, some corporates are ducking the 'ownership' issue: companies cannot manage information without effective business ownership of information, and a clear understanding of what this means. What is more, some companies seem unable to measure the quality of their data in a meaningful way which, in turn, means they will not be able to monitor whether it is improving or deteriorating. One still hears meaningless statements such as "data quality in my department is 95 percent".

Van Gils: No two organisations are alike and it is hard to make general claims about the way organisations deal with the risks associated with broken information infrastructures. However, we feel that the focus and effort that many organisations put forward in the management of data as an asset is insufficient. On the positive side, we see that many organisations are implementing policies, processes, standards and controls to get a grip on the complexity of data. Also, many business and IT professionals are increasingly aware of the issue. Many frameworks for enterprise architecture and process management deal with these types of issues. However, good intentions do not always have the desired effect. Many organisations forget or ignore their core principles about data-as-an-asset when the rubber hits the road in projects and programs. Worse, some organisations fail to even establish their core principles at all. Under the pressure of deadlines and budget constraints we see many steering committees choose more functionality for every dollar rather than investing in information. Clearly this is not a sustainable position – while systems are temporary, data is forever.

RC: Against this backdrop, to what extent has it become essential for today's businesses to design and implement an effective information governance program?

Saunders: An effective information governance program is essential, but it does not need to be a huge overhead or a burden, and it will generate real benefits. Most companies are already doing something in this area, but it probably is not well organised, is failing to address the most pressing business issues, and is not measured and reported on.

Cunningham-Day: Most businesses now need to participate fully in the digital economy in order to survive. Those who do so without at least developing a high level understanding of their information estate, the pathways by which information leaves their organisation, and the risks associated with both the retained and the disclosed information, are jeopardising the future of their business. Designing and implementing a strategy to address these issues is necessarily an iterative process due to the rapid evolution of most businesses' IT systems and operational processes. For those developing a more centralised information governance model, it is often a question of 'needing to start somewhere' rather than being able to define a fully-fledged strategy at the outset. This may involve identifying key information risks and commercialisation opportunities in the short, medium and long term, and feasible steps to address them, then sequencing the steps in consultation with relevant stakeholders in IT and operations.

Van Gils: If we accept the premise that data is an asset, as many organisations claim to do, then we must also accept the consequence: data must be managed. In a sense, data is not much different from other capital intensive assets such as equipment or buildings. This leaves the question, how should we manage data? Examining information governance over the last 20 years shows that a continuous information governance program is the best way forward. Organisations require a program as a coordination mechanism, and this must be a continuous process given that information governance is not a one-shot effort. A way to draw the necessary attention to an organisation's information governance program is by putting data on the balance sheet. This is something several organisations are currently trying to do, and I expect many others to follow.

Bhandari: An effective information governance program is increasingly seen as critical to the success of managing the organisation's crucial information assets, ensuring compliance with regulatory requirements and managing operational risk. The benefits of a comprehensive information governance program include protecting and ensuring the integrity of data as a valuable asset, controlling data-related operational risks and associated costs, ensuring legal and regulatory compliance across national boundaries, an improved ability to respond to regulators' requests for information, the ability to apply retention schedules to the correct content types, improved management of content to prevent continued 'infoglut', reduced e-discovery costs, e-discovery readiness, better stakeholder management of information assets, timely data reduction and destruction, and management of access to sensitive categories of information.

Zagoudis: The need for effective information governance reaches beyond increased information volume, disjointed data architectures and individual departmentalised efforts. Expanding business in the context of today's competitive drivers and financial environments demands using information as a strategic asset. Financial assets must be put to work to enable development, expansion and creation of value. Information assets are no different. They must be leveraged to their maximum potential. There is no denying that governance controls and other risk and compliance techniques need to be deployed for regulatory compliance and sound business practices. With financial assets, the CFO, controller and treasurer working in harmony to obtain, maximise, control and protect financial assets. Effective information governance both forces and enables organisations to look at information assets in the same light as financial assets.

RC: How would you define information governance as an emerging discipline? What do you think the future of information governance promises for advancements in business efficiency and risk reduction?

Cunningham-Day: Information governance has undergone a significant vocational facelift in recent years. Previously it was hard to get traction from senior management when they picked up the phone and heard you were from the records or data protection department. Now it is widely understood that information governance for a multinational company is a key area of risk and opportunity extending far beyond archiving and requiring a broad skillset, including understanding IT systems, business processes, corporate governance, relevant legal and compliance requirements, and employee and customer behaviours. While the risks associated with poor information governance are becoming increasingly understood, understanding the benefits of good information governance is taking a bit longer to crystallise for management. This may be because organisations often have to take significant steps in implementing their information governance strategy before realising the benefits in areas such as process centralisation and de-duplication, customer profile augmentation and litigation/investigation response.

Zagoudis: Information governance becomes a competitive game changer when the focus is top-down, business-driven, technology-enabled, and integrated tightly into the value chain of the organisation. This framework provides a paradigm shift that moves governance from back-office risk reduction to boardroom revenue generation strategies and management execution. Data

governance traditionally focused on the quality, storage, management and procedures governing physical data assets. Information governance evolved by combining the previously disparate disciplines of records management, content management, privacy, legal oversight, compliance, risk and data security, extending the scope from inside the corporation out to partners, customers and service providers. While useful, the combining of these disciplines without an overriding framework fails to maximise the full potential of a comprehensive approach to information governance. Learning organisations realise how to treat information as a strategic asset. Information governance becomes the differentiator for organisations that survive the information age. Herein lies the future of information governance.

Bhandari: Information governance is moving from the basement to the boardroom. Historically, many organisations have equated information with records and have downplayed its importance. There is a growing realisation of the value of information and the importance of governing it appropriately. As a discipline, it is still in transition as governance touches so many parts of the organisation, and it can be a real challenge to create ownership of the problem. Information governance is a discipline that sits across the organisation including general counsel, records management, business units and IT. The information governance principles need to be understood by all employees and be an integral part of how information assets are managed across the business. Information governance will become increasingly critical to an organisation. It underpins the business process, ensures data quality, enables more effective business intelligence across the organisation and improved management of risk. Most importantly, the 'fashion' for big data initiatives is unlikely to be a passing fad. Organisations are going to want to get more and more value from their information. Big data initiatives work best where the greatest volume and variety of relevant data can be incorporated to generate insight. That requires a degree of control around the volume, variety and velocity of information sources.

Van Gils: In my opinion, information governance is what happens when we accept that data is an important asset to the company. This realisation may result in a deliberate, planned action that brings about the start of a data governance program and everything associated with it. In short, this could give rise to the introduction of data stewards, improved policies around data, and scorecards around data quality. However, this can also be a much more bottom-up process, with people on the work floor recognising the need to take care of data and changing their behaviour accordingly. In practice, we often see both. The best indicator for information governance gaining traction in an organisation is a change in culture. People know that faulty data may lead to serious issues 'downstream' in the process and therefore take their role as steward of the data seriously. These issues may suffer from an increase in look-up time, additional validation steps, or even faulty strategic decisions due to poor data quality. The promise of information governance, of course, is the inverse of these risks. Indeed, there is hard dollar value to be gained by getting this right. Even more, if companies are able to change their mindset and build an effective information governance program, then typically they also benefit from an improvement in agility and a transparency of decision making.

Saunders: Information governance still a young subject, so you will see a wide range of definitions. One which has served us well over many years is the notion that information governance has three elements. First is governance of the underlying data, including the architecture which turns the data into information. Second is governance of the wider range of information assets such as reports, strategies, definitions, policies, processes, standards and methods. Third is the matching of the supply and demand for information across the business, ensuring that the right capability is available to information consumers, in a controlled manner, to an agreed level of service.

RC: Could you outline the key elements of an information governance program? How does the interplay of corporate governance, information governance and data governance define the success of a program?

> **"The information governance principles need to be understood by all employees and be an integral part of how information assets are managed across the business."**
>
> *Sanjay Bhandari, EY*

Zagoudis: Effective information governance provides the linkage between business demands for information and the oversight of risk, compliance and quality of underlying information and data assets. This starts with an overarching framework that encapsulates data, information, reporting applications, controls and organisational stewardship into a trusted platform of information for business operations and disclosure. This needs to be initiated, supported and monitored at the corporate and board levels of the organisation. Corporate culture needs to embrace a shared vision of how information governance can provide business advantage through leveraging information assets. This vision gets executed through business and technology policies, standards and procedures to ensure integration with corporate governance. Navigating to the future of information governance requires continuous improvement processes based on feedback on actual current state, periodic definition of desired future state and a clear roadmap that is shared between board-level governance, management and operations.

Van Gils: In many ways, information governance is a means to an end. However, it goes further than policing a set of rules. Building data management capability is an integral part of data governance. If you look at governance in this way, then it is a broad and goal-oriented discipline. Organisations agree on goals, figure out which capabilities are needed, and then 'govern' their proper implementation and realisation. Ideally, the goals of the different governance disciplines are aligned. In practice, we often see conflicts of interest. For example, from a corporate or financial governance perspective we may arrive at the conclusion that it would be a bad idea for certain activities to be assigned to a single person. Organisations may hope for segregation of duties. At the same time, organisations may also arrive at the conclusion that, from a data and information perspective, it makes a lot of sense to create a single role to steward the data related to these activities. Arguably, the key to success in these cases is collaboration, which is the most important part of building an information governance program.

> **"It is the orchestration of people, processes and technology to ensure that data is managed as a key asset of the business."**
>
> *Chris Saunders,*
> *IBM Global Business Services (GBS)*

Bhandari: There are four key elements of an information governance program. The first is strategy – from the business executives' point of view, what impact is information governance having on realising the business strategy, facilitating compliance with applicable regulations, improving operations, managing risk and increasing revenues. Second is governance, which defines the information governance organisation and is responsible for the ongoing maintenance, administration and safekeeping of the information governance program. Third is operations – the infrastructure, systems and processes that make the information governance program operational. Finally, performance management means monitoring how well information governance is performing against the needs of the business and the expectations of the users. Corporate governance, information governance and data governance is the top down hierarchy of governance within the organisation. It is important to have all three limbs of governance aligned and operating effectively. Corporate governance ensures the organisation meets its regulatory requirements, including legal retention requirements, data privacy law and meeting information security standards. Information governance ensures the integrity and management of information assets in the organisation through its guiding principles. Data governance is the implementation aspect of information governance policies.

Saunders: When creating an information governance program companies need a clear, proven target operating model which includes a number of features. There must be well-defined roles and responsibilities, and a detailed explanation of how they interact with one another. Policies, procedures, guidelines and means of supporting compliance with them must also be set out. Companies should embrace the lifecycle management of their information, including security, privacy, definitions and business rules. Effective data quality management and remediation should be included. Further, there should be an approach to matching the demand for information with its supply. As far as the interplay of the various types of governance are concerned, these need to be understood carefully. Corporate governance establishes chains of responsibility, authority and communication to empower people via decision rights. Information governance is a core part of this – it is required to realise the full extent of business benefits derivable from a corporation's information management activities. Data governance is the cornerstone of information governance. It is the orchestration of people, processes and technology to ensure that data is managed as a key asset of the business.

Cunningham-Day: Effective information governance usually involves the coordination of a variety of disciplines within a large organisation, including information-specific functions such as records management, data management/security/protection, as well as the information interfaces with all of the customer-facing business lines and corporate infrastructure functions that make up the business. Some of the key procedural anchors for an information governance program include the development of a consistent global records taxonomy with an associated schedule of retention periods and other storage and recovery requirements, operating principles for dealing with unstructured or non-record data, as well as effective interfaces with the company's data- and business-functional architectures. As information governance affects every aspect of the business, the program must have a significant focus on corporate governance, change processes and stakeholder management – particularly at the implementation phase to drive engagement in what is often a disruptive process.

RC: Information security is a major issue in today's digital business environment. How should this be reflected in a good information governance program?

Van Gils: A recent study has shown that information security is the third biggest threat for business continuity. Therefore, a well-organised information security program is of paramount importance. It makes sense for organisations to invest in risk assessments and define and implement measures to be 'sufficiently safe'. The responsibility for information governance should lie with senior business management, because management has to understand and deal with the risks their organisation is facing. The objective of a good information governance program is to assess the relationship between business risks and information security measures, in order for management to make meaningful decisions.

Saunders: Most companies are already doing something in terms of developing their information governance programs, and information security usually falls into this category. It needs to be included, along with other external legal and compliance requirements such as privacy. The question is whether you should move existing functions under the wing of a new information governance capability or leave them where they are. The answer will depend upon the individual circumstances, but certainly information governance should include information security: whether or not there already is a policy, whether this policy has been properly implemented, and whether compliance with it is being checked on an ongoing basis.

Bhandari: Information security is driven by the information governance policies enabling the

organisation to manage access to its information assets down to a lower level within the organisation – content type, role, jurisdiction, age profile, and so on – rather than at an application level. Information security sits at the centre of the information governance policy framework to ensure confidentiality, integrity and availability of information assets that are unauthorised or inappropriate use or disclosure. This is achieved by defining and strictly enforcing a security policy, processes and procedures to cover data access, data classification, acceptable data use, data protection, detailed information security and data handling procedures. The security policy can only be applied down to a data and document level if an effective information governance policy is in place across the organisation.

Cunningham-Day: A key first step for any holistic information governance program is to determine how the various parts of the organisation's policy and procedural architecture fit together. Data security is an important example of this as it is typically addressed in a number of areas. These include HR policies for employee screening, use and monitoring of information resources and IT systems; sourcing policies regarding initial and ongoing due diligence on service providers, as well as contractual information security requirements; and technical information security procedures, such as access controls and storage and transmission controls for technical personnel. It is becoming increasingly clear to companies that the IT team cannot combat the proliferation of information security threats on their own, and that behavioural controls on the rest of the workforce are at least as important in reducing the potential impact on the organisation. As a result, effective incorporation of information security into the program requires all of these stakeholders to be engaged early and work together to ensure that their collective concerns can be addressed in a way that is workable for everyone.

Zagoudis: Managing information security starts with an effective data and information classification program with the aim of identifying information based on the potential risks to the organisation. This needs to be coupled with well-defined information governance principles and enforcement rules regarding management and retention of information, and underlying data, that extends to all storage devices. Information governance also requires clear, undisputed and timely knowledge of the source and use of information both within and outside of the organisation. Due to the ever-changing organisational landscape, this source and use awareness needs to be maintained within a dynamic governance framework using technologies that provide the knowledge base and the ability to monitor information through its lifecycle and distribution paths. The information governance implications of policies related to security, privacy and compliance need to be factored into corporate educational programs. Theoretical governance without enforceable standards is of little use to an organisation.

RC: Given that technology provides the platform on which companies manage their information, how do issues such as cloud computing and 'bring your own device' complicate information governance?

Saunders: Issues like these create complexity in the areas of security and privacy. They do not so much complicate the governance as extend the scope of the appropriate policies. These policies need to be properly drafted, agreed, implemented and monitored for compliance.

Cunningham-Day: Managing information effectively across a global workforce on a multitude of internal systems and individual service providers was complicated enough before BYOD and the cloud came along. Now, it is difficult to satisfy the demands of staff and customers for access to a huge range of the organisation's information at any time and from anywhere, and from the same devices that they use to manage their personal lives, without the introduction of these innovations. The economies of scale and processing power that they offer are increasingly compelling, but they demand difficult compromises in terms of information management and security. Most cloud providers will not make definitive commitments about where the organisation's data will be stored and accessible from, while the use of cloud-backed personal devices at work could mean that the organisation's information becomes distributed across myriad different platforms. Without stringent sourcing and usage controls, this proliferation represents a fundamental challenge to conventional organisational approaches to data protection, client confidentiality, records management and e-discovery.

Zagoudis: The struggle between openness and control is difficult to manage. The fundamental issue is that organisations have little awareness about where information physically resides and are at the mercy of technology and security implementations. The need for such 'blind trust' in the technology can easily keep an astute compliance and risk officer awake at night. However, governance rules must be designed so as not to negate the business value for choosing these technologies. Both mobile and cloud technologies remove the physical protection boundary of having information within the confines of the organisation, therefore requiring additional due diligence. Maintaining 'source and use' awareness requires new governance technologies that provide the ability to look at business impact across the complete value chain. The balance is between protection and accelerating business momentum.

Bhandari: Having information governance policies in place should be a prerequisite for cloud-based solutions and Bring Your Own Device (BYOD) policies to ensure the integrity and security of the data. Of course, the cloud and BYOD both add complexity as they further separate ownership of information from ownership of the technology assets upon which the information is stored. BYOD has the added complexity of mixing personal and sensitive personal data on the same device as the organisation's data. The ownership of, responsibility for and access rights to the data therefore need to be clearly articulated to all stakeholders with appropriate information security wrappers.

Van Gils: The underlying theme here is 'loss of control'. In the old days, companies had full control over the entire 'stack'. From hardware and software to the data itself, however, this is no longer the case. With the cloud, organisations no longer control where their data is stored – someone else does. Furthermore, with BYOD, firms no longer control what hardware is used. This poses a major risk for many organisations. From an IT perspective, these trends make perfect sense. Why bother controlling expensive hardware, if people want to use their own iPad? Do we really care which hardware is used? The answer, of course, should be that we don't care, provided we are able to

> **"The information governance implications of policies related to security, privacy and compliance need to be factored into corporate educational programs."**
>
> *Steven Zagoudis,*
> *MetaGovernance Solutions LLC*

keep our data sufficiently safe and secure. This is where information governance comes into play. Organisations need a strong assessment of the impact on data security when data is moved to the cloud or when they institute a BYOD policy. Based on this risk assessment, it is crucial to work with business management to define what risk level is acceptable, and with enterprise architecture and the information security office to define appropriate risk mitigation strategies.

RC: What is the role of technology in implementing a sustainable information governance program? What are the critical success factors that applied technology solutions must get right in order to be effective?

Bhandari: Technology is an important part of implementing a sustainable information governance program. However, a sustainable information governance program constitutes governance, people, process and technology elements. These four elements are complementary and it would not be possible to achieve the objective of an a sustainable information governance progra' on their own. Increasingly, core applications enable the enforcement of information governance policies through the classification of types of information asset, retention schedules and controls based on different levels of access control. However, these information governance policies are applied and managed within each individual application across multiple systems, multiple data centres and multiple jurisdictions. Today there is an influx of information governance tools offered, each with a slightly different interpretation of what information governance means. However, there is not one tool that will resolve the information governance issue, but rather a combination of tools. The information governance 'toolbox' would consist of at least four functionalities. First, an information governance tool that would enable the organisation to create and actively enforce corporate policies across organisational and jurisdictional boundaries, IT systems, content repositories, cloud-based applications and paper archives. This would ensure a consistent approach across all information assets within the organisation enabling a more effective information governance and risk mitigation. Second, automated indexing would enable the classification of each information asset refining the content type and topic and thereby enabling a more accurate classification of each asset. This is particularly effective for less structured repositories and in most cases each tool focuses on particular type of repositories. Third, metadata management within core business application where the corporate classification schema will be applied. Finally, an intelligent archiving platform classification whereby content is indexed on ingestion and duplication of data avoided. The critical success factor required to make a technology solution effective is to have the functionality that enables the application of information governance policies, processes and procedures. Organisations face a significant challenge when implementing technology solutions to govern its information of how to deal with legacy data to ensure compliance with regulatory policies. It is at this point that the four information governance tool options need to be considered.

Van Gils: A 'technology first' mindset is very dangerous in the realm of information governance. Unfortunately, companies often have at their disposal the best of the best in terms of tools – be it data profiling tools or meta-data tools – and yet still encounter serious data issues. There is a reason that we often hear "a fool with a tool is still a fool, making disaster faster". This is a tricky puzzle that has a lot to do with the maturity of the data management and data governance capability of the organisation. Data governance is, in many respects, quite similar to enterprise architecture. Both disciplines regard the enterprise as a whole, and have a major impact on the way organisations do things. Duplication of knowledge in different tools will make life harder, not easier. Think, for example, about two tools for storing business meta-data, such as definitions of key entities. This is a violation of the DRY principle – don't repeat yourself – and will surely cause trouble if we are not careful.

Zagoudis: Maintaining effective information governance without technology equates to managing an organisation's books and records without a general ledger system. The relationships are too complex, too dynamic and too extensive to manage without enabling technology. Technology plays a critical role in providing continual, automated monitoring of data assets to ensure the accuracy and appropriate use. Critical success factors include enterprise awareness, integrated controls and targeted stakeholder distribution of issues, incident management and clear delineation of responsibility. Effective information governance technology delivers trusted enterprise information within a fully encapsulated governance and control framework. This umbrella captures the information landscape of the organisation, along with the relationships to business process, data, application and technical architecture. Included is the mapping of governance roles designating accountability, delegation and usage between business units and information. Without effective technology, information governance becomes a theoretical exercise that is not directly connected to business operations.

Cunningham-Day: With the exception of certain critical legal documents, legislation around the world is increasingly facilitating the migration to an electronic-only information governance model. This means that technology is at the heart of most of the inputs and the outputs from the information governance process. A key success factor for enabling technologies in information governance is to strike the right balance between manual intervention and automation at the right time. Enhanced search capabilities and 'privacy by design' concepts had led many to assume that inherently fallible manual processes could soon be dispensed with, and information governance could now be left to manage itself once the necessary systems and processes had been designed. However, for many of those currently involved in the daily conflicts and inconsistencies of managing a global operation's information governance processes, it is clear that the path to a fully digitised business is a gradual one. As a result, the technologies most likely to get widespread traction today are those that can support information owners to manage disparate systems and processes more effectively and consistently, rather than seeking to reinvent the information governance process entirely.

Saunders: There are claims out there along the lines of "implement our software and all your information governance problems will be solved". Companies should not believe a word of it. Technology is an enabler in a wide range of areas – data quality issues management, profiling, scorecards, KPI measurement and monitoring, data cleansing, data dictionaries and directories, and indeed the whole architecture which takes data from the operational systems and provides business information. IT obviously has a key role to play in this too. It is often the IT function which kicks off an information governance program, but it has to be properly owned by the business if it is to succeed. If you ever hear "data quality is an IT problem" then there's a lot of 'hearts and minds' work to be done.

RC: When creating and rolling out an information governance program, what are the benefits of a top-down approach? Is it also important to consider a bottom-up approach?

Cunningham-Day: For a global business that has commercial or regulatory imperatives to become more streamlined and coordinated in the way it conducts its operations globally, having a top-down component to the strategy is vital. If the business is looking to condense its datacentre footprint, rationalise business lines or start to deliver enterprise-wide services in new areas, then it is critical that these aims are fed into the strategy for the program so that consistent solutions can be developed that support these globalising initiatives. Having a top-down approach also gives the program the important initial strategic direction and impetus that is often dissipated or frustrated by a lengthy bottom-up approach. Getting detailed buy-in from stakeholders within the relevant business units is of course vital, but at the right time and in the right way. This may be by contributing to the initial 'as is' view

of the information landscape, then through stress-testing the proposed 'to-be' model with the realities of day-to-day operations in their specific area.

Saunders: You need to look at both a top-down and a bottom-up approach. A fully centralised approach may be too remote to affect the business at the right level, which is where the data is being created and amended, whereas a fully localised approach is not real governance. For example, you can't manage data quality entirely at a local level because a fix in one area may cause bigger problems in another. Equally, there's no point in centralising issues which relate purely to a particular business function or geographical area – provided, of course, you have first checked that the issue really does only have a local effect.

Zagoudis: There is intrinsic value to a top-down, bottom up and middle-out approaches working in unison to build an effective information governance program. Top-down provides the budget, communicates the importance of the initiative to all the stakeholders, and sets expectations for cooperation and for timelines. Top-down frames the context. The 'middle' refers to those responsible for implementation and ongoing support of the program, which include information governance administrators, technical staff and committee or working group representatives. This core team gathers input from all constituencies and communicates policies and procedures to the organisation. The core team provides detailed awareness of process and communicates status and plans to the organisation. This component is typically the missing element with most information governance initiatives. Bottom-up provides the reality of where the information meets the business processes and makes sure that the efforts are supported and adapted at the line level of the organisation.

Bhandari: A top-down approach to implementing an information governance program can better maintain adherence to new practices in managing information in the organisation – which is often driven by regulatory requirements – and to create the agility to adjust programs to the adoption of emerging technology, particularly to tools for communication and collaboration which are fluid. The bottom-up approach is also important to ensure that information governance principles are being applied and improved with feedback from the ground floor.

> **"Equally, the presence of 'nerdy suits', people who are able to comfortably move in the world of business and strategy as well as the world of data and IT, can also be extremely advantageous."**
>
> *Bas van Gils, BIZZdesign*

Van Gils: It seems that a top-down approach is most common for information governance. Top-down governance means the clear definitions of goals for information governance at the enterprise level. After a business case phase, organisations should start a program to implement an information governance capability in alignment with existing management processes and frameworks. This will provide firms with the usual or expected benefits – increased grip on information and data, higher ROI on IT, increased agility of the information landscape, improved process agility, and so on. There have been several case studies and handbooks that highlight these benefits. One thing that is often overlooked, though, is the power of local initiatives. This can be classified as a bottom-up approach to information governance. Typical examples are local groups that are fed-up with re-work and data quality issues, and, in order to deal with these issues, they start to develop local practices and procedures. This happens more often than you would expect. This type of approach does have its advantages. Local practices have been tried and tested and can slowly be adopted by the rest of the organisation.

RC: What about the people behind the technology? What individuals within the company need to be involved in the information governance process? What roles and responsibilities should companies look to assign, and how can they minimise problems arising from 'internal politics'?

Zagoudis: The concept of governance and data stewardship must be clearly understood. Commitment is required from all levels of the organisation – board, management and staff. Effective information governance requires a resourcing strategy that provides the content and context knowledge and a shared vision from which to build the program. A governance architect can assist during the start-up phase to manage the initial project, build consensus with the required stakeholders and develop the process and technology infrastructure that will support the governance initiative. Representation must be included for all process and domain stakeholders within the organisation on a governance committee, including operations, compliance, legal and security. Specialists in the various aspects of governance need to be trained, with time allocated to the program to provide for departmental engagement. Technologists will need to implement and manage the technology side of an information governance program.

Van Gils: No two organisations are alike, so it is hard to come up with a one size fits all answer. One thing to note, though, is we need both the 'nerds' and the 'suits'. Equally, the presence of 'nerdy suits', people who are able to comfortably move in the world of business and strategy as well as the world of data and IT, can also be extremely advantageous. Typically, these are business-minded architects, and data stewards. Desirable skills for an individual occupying this role include political and organisational sensitivity, change management and the usual data management skills. Organisations may utilise a formal top-down or a more bottom-up approach to information governance. Depending on the style of the approach, the maturity of the organisation and the maturity of the information governance capability, different roles and processes will be needed. As a general rule, though, the key success factor is accountability. Someone in the board, perhaps the CFO, should be accountable for information and data. This will help avoid some of the issues that arise from internal politics and help steer the information governance program in the right direction.

Bhandari: Good information governance is about people, process and technology – in that order of importance. The success of the policy is ultimately down to the people understanding, articulating and implementing the policies at every level of the organisation. Key stakeholders in articulation and implementation of the information governance policies and process will be general counsel, CIO, CTO, records manager, head of storage infrastructure, and business unit stakeholders. Those stakeholders may team as an information governance board chaired by a member of the board of directors. Success of policies may depend upon board responsibility. Ultimately, all staff are involved as data custodians in executing the policy on a day to day basis. An information governance council should be appointed with representatives from key stakeholder groups. The council needs to meet on a regular basis to manage and review its policies, processes and procedures in line with regulatory requirements and standards and to monitor emerging practices, especially around communication and collaboration.

Saunders: I'm not sure there's such a thing as an 'information governance process'. There are one-off change processes that need to be carefully designed and executed in order to put information governance in place, and there are business processes that will be affected – and hence business process leaders and functional department heads need to be involved. Some of these may not be directly involved in the early stages – if the data they use and the processes they own are not included in the initial stages of rolling out information governance, for example – but commitment will need to be obtained from all people at this level. The IT department will also, of course, have a key role to play in enabling effective information governance. There are a number of key roles within the business which help to define information governance. First are data and information owners, where the 'buck stops' for all aspects of data and information quality, security, privacy and lifecycle management. Domain data stewards are experts in individual domains of data, and are often in a many-to-one relationship with data owners. The stewards maintain the definitions, know where the data is used in the business and know what 'good quality' looks like. Information asset owners also play an important role – they have a responsibility for the quality of individual information assets. These are business people and may be in a matrix relationship with data and information owners, because an individual information asset may contain data from many different domains. Functional – or process – data stewards also play a particularly important role. These stewards know a specific functional area or process inside-out and, accordingly, will know and understand the pain caused to that area or process – bearing in mind that this may include many different subject areas of data. There is therefore a many-to-many relationship between domain and functional data stewards. The functional data steward is the go-to person for anybody who works in that area or process who thinks they may have a problem with data quality. The functional data steward is the person who works with other functional data stewards to support the investigation of, and agree the priority of, data quality issues. The names here are not important – some organisations are sensitive about the use of the word 'owner' or may use 'steward' to mean something else – it's the roles, clearly defined and with clear relationships between them, which are important. The question of 'internal politics' is partly about an effective change management process, and partly about ensuring that the names used for these roles are 'politically' acceptable.

Cunningham-Day: For some information governance programs, managing internal governance occupies as least as much time as researching and structuring the deliverables for the program. What tends to work well is to have a core project team tasked with driving the program forward who have strong links and representation from the key constituents for the project, including the COO and CIO, IT, legal, compliance, company secretarial, risk and audit, HR, finance, CRM and archiving. Strong project management from individuals that have extensive experience with the business is also key. This core team will usually need to report into a steering committee with representation from similar constituents, which will be used to endorse strategic direction and increase traction within their respective teams. The key to ensuring initial adoption and ongoing adherence is for senior management to 'get' the critical importance of the project and ensure the required changes in process and behaviour are sufficiently prioritised within the organisation.

RC: In your opinion, if an active information governance program has been executed correctly and is functioning well, what overall benefits should a company expect to derive?

Van Gils: The best way to measure the effect of an information governance program is to try to assess its impact on the bottom line. Hard dollar value is something that all business stakeholders will understand. In practice, however, this is hard to asses. Frequently we see organisations work the numbers to report "reduced impact on..." or "improved control over..." in relation to key factors such as risk, compliance, and so on. This is unsatisfactory. Before starting an information governance program, organisations must try to figure out which issues are on the management agenda in order to define clear KPIs and goals for the information governance program to achieve. These can be close to technology and data, or more in business terms for more mature organisations. An example of the former would be "reducing the number of errors for key data sources by 25 percent over the next two years". An example of the latter relates to such things as improved business continuity, or improved business agility through more effective decision making.

Saunders: There are both quantifiable and non-quantifiable benefits to be derived from an active information governance program. The main quantifiable advantages are reduced data cleansing effort, fewer customer complaints, a removal of duplicated information retrieval and creation processes, savings from centralised contracts with third-party data and services suppliers, and a reduction in effort for urgent, last-minute requests from regulators which cannot easily be met. From a non-quantifiable perspective, but still with a number of hard benefits, companies can expect a greatly reduced risk of compliance failures; this will be particularly beneficial for organisations that might be subject to financial penalties. Equally, companies can profit from better, timelier decision-making, which in turn will lead to improved business effectiveness. An enhanced external reputation, leading to greater customer retention and increased sales and improved staff morale, will in turn lead to better staff retention.

Cunningham-Day: The benefits of an information governance program will evolve over time. Early wins may include greater global dialogue between those creating the information within the organisation, those tasked with managing it and those requiring regular access to it. Early on, the program should also provide greater corporate awareness of the key data exfiltration risks for the organisation as well as the 10-20,000 data retention laws and regulations that a globally regulated business is typically subject to. This will allow prioritisation of longer term goals, such as greater centralisation and interrogation of data, more streamlined global processes, reduced storage costs and improved regulatory reporting and litigation readiness.

Bhandari: Key benefits of a functional information governance program include meeting regulatory compliance requirements, improving operational efficiencies, achieving storage and other cost savings, improving data integrity, reducing regulatory and other risk, improving business intelligence such as big data initiatives which may be focused on identifying revenue-generating opportunities, and leveraging competitive advantages and making more informed decisions.

Zagoudis: Information governance is all about maximising the business value of information by delivering relevant, accurate and timely information for making business decisions. As in any well-run manufacturing facility, effective information governance optimises throughput from the organisational information factory, while simultaneously reducing operating costs and risks. There is tremendous business opportunity in transforming raw data into meaningful information. Unfortunately, the bounty of this harvest will be lost if the focus is solely on risk, compliance or technology. In his groundbreaking work, *Mind and Nature*, Gregory Bateson defined information as "differences that make a difference". Effective information governance enables organisations to render meaningful information from the data chaos, or noise, that exists and be able to see differences in information patterns or trends. This turns noise into news that can make the difference between effective and ineffective business decisions. This is how transformation through a comprehensive information governance framework adds business value. R&C