

The future of enterprise information governance



Preface

The future of enterprise information governance is an Economist Intelligence Unit briefing paper, sponsored by EMC. In April 2008 the Economist Intelligence Unit conducted a survey of 192 senior executives around the world on the benefits, challenges and risks associated with developing an enterprise-wide information governance strategy. The Economist Intelligence Unit wrote and executed the survey, conducted the analysis and produced the report. To supplement the findings of the survey, the Economist Intelligence Unit also conducted in-depth interviews with a number of business executives from leading companies. The findings and views expressed in the report do not necessarily reflect the views of the sponsor. Elizabeth Bennett was the author of the report, and Debra D'Agostino was the editor. Danielle Noble was responsible for layout and design.

Our thanks are due to all survey respondents and interviewees for their time and insight.

October 2008

Executive summary

Information is the lifeblood of any modern-day business. Companies succeed and falter based on the reliability, availability and security of their data.

A corporation's capacity to handle information depends upon a variety of factors, including engaged executives and a company culture that supports collective ownership of information. However, strategically created enterprise-wide frameworks that define how information is controlled, accessed and used are arguably the most critical elements in a successful information management programme. For the purposes of this report, those frameworks, and the mechanisms that enforce them, are referred to as information governance.

Are most companies properly governing how their information is used, shared and analysed? At first glance, it seems that firms have a solid handle on this. Worldwide, nearly 73% of respondents report that their company's overall ability to provide access to critical business information when needed is good or very good, and 65% say that their firm's ability to protect sensitive information is good or very good.

However, only 38% of all respondents say that their companies have a formal enterprise-wide information governance strategy in place. In fact, fewer than half of all respondents believe that information governance is important or very important to their company's success today. This suggests complacency among some companies about the true strategic importance of managing corporate information.

There are several reasons why proper information governance remains elusive, but the biggest challenge worldwide is identifying the cost/risk/return tradeoffs of managing information company-wide (40%). Enforcing policies company-wide (39%) and gaining support from department heads and line-of-business managers (35%) are also obstacles.

More positively, 77% of respondents expect information governance to be important or very important to their company's success over the next three years. As a result, many firms have begun building the foundation for information governance policies. A majority (65%) have defined policies around how information is to be stored and shared among employees and stakeholders. Furthermore, some organisations are forming formal governance bodies to create strategies, policies and procedures surrounding the distribution of information inside and outside the firm. This is a good start, but considering that 68% of respondents also expect that the complexity of their company's information governance issues will grow over the next three years, there is little time to waste.

Other findings from the survey include:

- Only 46% of respondents report that their company's organisational structure around information governance is somewhat or very effective. Furthermore, only 54% of respondents worldwide say that their firm regularly reviews and revises information backup and retention policies. Moreover, when asked about managing the cost of collecting, storing and securing information throughout its lifecycle, only 47% of respondents rate their firm's ability in this area as good or very good.
- As a result, sharing data across a company remains difficult. Only 43% of respondents rate their firm's



ability to integrate and share information across departments and necessary third parties as good or very good; 21% say that it is poor or very poor. This is particularly significant as it pertains to sharing customer information: 57% of respondents acknowledge that they do not have a single view of the customer.

- Those that have a formal information governance strategy report significant benefits. Eighty-one percent of firms with a formal information governance strategy in place report that “information can be better shared between departments, allowing for better decision-making”. Nearly half (47%) of respondents from these firms also say that “integrated information and business intelligence about our customers, products and resources can be leveraged for greater business results”.
- For firms without a governance strategy, the risks may be significant. Only 51% of respondents at companies that do not have a formal information governance strategy rate their firm’s overall ability to protect sensitive data as good or very good, compared with 85% for those whose companies have a formal strategy. Similarly, 92% of respondents at firms with information governance strategies rate their company’s ability to provide access to critical business information when it is needed as good or very good, compared with only 57% of companies that do not have governance strategies in place.



Who took the survey?

This survey, conducted by the Economist Intelligence Unit in April 2008, included responses from 192 business executives around the world. Thirty percent of survey respondents were located in North America, 30% in western Europe, 30% in Asia-Pacific, and 10% from Latin America, the Middle East and eastern Europe. Forty-four percent of respondents held C-level titles, and 46% hailed from companies with more than US\$1bn in annual revenue. The survey included responses from a range of business functions and industries.



Introduction: From information explosion to information governance

Despite the seemingly infinite ways in which technology is said to make sharing information easier, it is undeniable that processing, storing, protecting and analysing information becomes increasingly more complicated for companies with each passing year. Not only is the volume of information that businesses generate growing by roughly 60% each year, but regulatory requirements such as Sarbanes-Oxley and e-discovery laws in the US and elsewhere are forcing corporations to evaluate their ability to control effectively information and its flow between departments and third parties.

The Internet and other technology innovations have caused the pace of business operations to increase significantly. Consequently, workers are under more pressure than ever to meet tight deadlines and make faster, more astute decisions. To do so, they need reliable information delivered to them quickly. While technology has been the focus of information management initiatives for some time, companies are beginning to realise that the full value of information depends in large part on the policies and procedures that govern and control its use, access, analysis, retention and protection.

A corporation's capacity to handle information depends upon a variety of factors, including engaged executives and a company culture that supports collective ownership of information. However, strategically created enterprise-wide frameworks that define how information is controlled, accessed and used are arguably the most critical elements in a successful information management programme. For the purposes of this report, those frameworks—and the mechanisms that enforce them—are referred to as information governance.

The information that companies are busily generating, collecting and mining offers a wealth of potential benefits. However, its use carries substantial risks. As a result, some organisations are forming formal governance bodies to create strategies, policies and procedures surrounding the distribution of information inside and outside the firm. This report seeks to understand better how companies are establishing cross-functional governance bodies to create strategies and policies around corporate information.

Companies are beginning to realise that the full value of information depends in large part on the policies and procedures that govern and control its use, access, analysis, retention and protection.

The upside of firm-wide frameworks

According to our survey, worldwide, respondents from organisations with enterprise-wide information governance strategies are more likely to review their company's relationship to information positively: 91% of companies with an existing information governance strategy said that their company's overall ability to provide access to critical business information when it is needed is good or very good. By contrast, only 58% of respondents at companies without a formal governance programme give the same rating. Moreover, while nearly 85% of companies that have implemented an information governance strategy rate their company's ability to protect sensitive information as good or very good, only 51% of those without a strategy in place offer a similar assessment. The findings suggest a correlation between a company's commitment to governing information and its capacity to mitigate risk and reduce cost, as well as getting more value out of its information assets.

Julia Boland, senior vice-president of the enterprise services and solutions group at Chubb Corporation, says that risk management was a top priority when her company—a US\$14bn provider of personal and commercial property and casualty insurance—began putting new information governance standards in place 18 months ago. In early 2007 the Warren, New Jersey, firm implemented new policies for assessing the risks that it faced when working with external vendors. "We're going outside for services more and more because the Internet enables us to do that," says Ms Boland. "We're sharing information and exposing systems outside the company in ways we hadn't done before."

Ms Boland's group created a centralised global sourcing department that partners with the information technology (IT) security and IT risk-management groups to create a standardised process to rate vendors and determine the risks of each business arrangement. That process establishes minimum security requirements based on the nature of the services being provided and the sensitivity of the information being shared, according to Ms Boland.

The group manages contracts and, perhaps most importantly, ensures that no business unit goes off on its own to hire a third party. "We had an evaluation process before," explains Ms Boland, "but never from a pure risk perspective, and never in a way that the entire organisation could benefit from". Chubb's standardised and centralised vendor-risk assessment process ensures that proprietary information will be properly protected when it is transmitted beyond the company's firewall.

Improved risk management is just one important benefit of an overarching governance strategy: firms that successfully implement such frameworks across the enterprise also benefit from improved data mining and business intelligence that leads to better decision-making. Seventy-two percent of survey respondents say that a company-wide information governance strategy leads or would lead to better information sharing between departments and 53% say that it allows or would allow for better decision-making.

That was the key driver behind Catholic Health Initiative's (CHI) four-year effort to centralise core business functions, such as payroll, procurement, contracting and accounting. Now nearing completion, the effort began with the creation of an information governance committee that comprised operations

“You can make much more intelligent or even life-saving decisions if you have good information.”

– Michael Rowan, CIO, Catholic Health Initiative

and technical representatives as well as experts from the clinical, financial and strategic groups, which developed standards for new processes and technology requirements. Chief information officer (CIO) Michael Rowan says that information flow improved dramatically at the US\$8bn not-for-profit organisation, which owns and operates 76 hospitals and 42 long-term care facilities in the US. The consolidation, he adds, saves the company US\$75m annually and improves the overall level of care that the organisation provides. “If a patient gets treated at different hospitals in our system and the doctors don’t realise that he or she has diabetes, they could put him or her on an ineffective course of treatment,” explains Mr Rowan. Since clinical information has been centralised, doctors can now track a patient’s history regardless of which CHI facility has treated them. “You can make much more intelligent or even life-saving decisions if you have good information.”

The business side has also seen tangible benefits. In the past CHI had no way to determine how much money its many facilities were paying for supplies and services. “The lack of information was costing us a lot,” says Mr Rowan. Today, all procurement and contracting data are maintained on a single technology platform that employees have access to across facilities.

CHI’s governance council sets and helps to implement strategies for regulating information flow. The group meets at least monthly to review plans and upcoming investment decisions and requests, such as tracking particular patient information. It must determine whether the request is in line with the expectations of the organisation as a whole. “It may be that that work doesn’t fall within the guidelines of our priorities,” says Mr Rowan.

An education in compliance

For the past decade, Air Products and Chemicals has been developing a global framework to tackle the increasingly broad and complex area of information governance. However, in the last few years new regulatory requirements and security threats have spurred stricter attention to risk management, and therefore the policies and procedures that surround the flow of information.

“Our global organisations and systems involve broader collaboration,” explains Cheryl Flannery, Air Products’ director of information technology (IT) planning, relationship and risk management, whose job it is to evaluate and develop strategic risk programmes across the organisation. “We’re running global business applications and using more third parties in our work,” which, says Ms Flannery, required changes to the existing frameworks and to the firm’s approach to information security.

Ms Flannery says Air Products’ security education and awareness programme is the essential line of defense against unintentionally exposing sensitive data, such as intellectual property or the personal information of employees or patients who use the company’s

healthcare services.

The multi-level programme starts when new employees are trained in how to use and distribute information. “We try to help employees think about the balance between the need for information and the risks that come with sharing it,” Ms Flannery says.

Air Products conducts annual refresher training and special sessions with employees who have elevated access to sensitive information. Ms Flannery’s group also publishes news items on the corporate intranet about high-profile security breaches and related topics. “When that happens, my group determines how we would handle it if that kind of breach happened here,” Ms Flannery explains.

To stay abreast of trends in information governance, information security and other technology areas, Ms Flannery has embarked upon her own course of study. She meets regularly with peers in the chemicals industry to share best practices in cyber security and is a member of an executive council at the Society for Information Management, an association of IT professionals. The Advanced Practices Council looks at the latest technologies and where there is business value, Ms Flannery says. “Sometimes it’s tough to know when something is cost effective and when it’s the best time to implement it. Hearing other people’s experiences is extremely valuable.”



Deployment challenges

Despite the known benefits and centralised authority that a governance strategy can bring to an organisation, just 38% of survey respondents say that their companies have a formal enterprise-wide information governance strategy in place, and less than half of all respondents say that information governance is important or very important to their company's success.

Even when there is some foundation in place, such a sweeping project can be tough going. "Companies don't have a big appetite for information governance," says Richard Jhang, a partner in the advisory services practice of international consulting firm, PricewaterhouseCoopers (PwC). Organisations become overwhelmed when they start recognising the many risks inherent in information mismanagement. "Trying to address them all at once can feel like trying to boil the ocean," says Mr Jhang. Instead, businesses often address information risks incrementally and in a manageable fashion, he says.

As the survey results indicate, there are also cultural hurdles to enacting and enforcing information governance. Respondents say that two of the biggest challenges that they face when implementing an information governance strategy are gaining support from department heads and line-of-business managers (35%), and enforcing policies company-wide (39%). Karl Pomschar, CIO of Munich-based Qimonda, a US\$5bn supplier of data memory products, says that people tend to be resistant to change. "Many systems have been highly developed and do exactly what companies require," Mr Pomschar explains. "But now, with standard solutions, people are not willing to go for compromises."

Governance at home and abroad

Like many firms that grapple with making information available across international boundaries, Intel has invested considerable resources in developing a consistent framework across the more than 45 countries in which it operates. Understanding regional regulatory requirements is an onerous task, according to Diane Bryant, Intel's chief information officer.

For starters, keeping up with regional export control laws that govern how certain information technologies can be transmitted overseas or to foreign nationals is a priority at the US\$38bn semiconductor maker. With penalties ranging from fines to imprisonment, there is little margin for error when establishing, for example, the types of information that can flow freely in and out of China. "Those types of restrictions add a level of complexity to a corporate-wide infrastructure," Ms Bryant explains.

Intel used to have locally based information technology groups that served regional needs, but the company implemented a global

infrastructure group in 1993, making it easier to enforce information-sharing policies to comply with regulations, she says.

Then there are geographic challenges that highlight cultural variances and must be handled with nuance rather than unilateral policies. For example, summer interns employed by Intel offices in the US are considered to be temporary workers and therefore granted certain limited access to business-critical information. However, comparable college-age interns in Intel's Israeli locations are treated as full-time employees with higher permission levels to sensitive information. "We realised we were giving interns in Israel a whole lot more information access than our US interns, even though they were at the same level and had the same job expectations, based on the differences in how student interns are classified," Ms Bryant recalls. To remedy the situation, the access controls were adjusted to provide US interns with the same level of information as their Israeli counterparts.

While global consistency has been Intel's focus for some time, nimbleness and agility are parallel priorities. "Systems have to be able easily to accommodate modifications," says Ms Bryant. "They have to allow for regional differences."



When it comes to gaining enterprise support, part of the struggle is determining who is responsible for a governance body and its domain, says Peter Whatnell, CIO of Sunoco, a leading manufacturer and marketer of petroleum and petrochemical products. “Initially, there was some difficulty in establishing the ownership for the initiative,” he says of the company’s efforts to centralise information policies and procedures. The challenge, he adds, is that information governance crosses all organisational boundaries and touches so many people. “There was no existing protocol or precedent to guide us.” Sunoco eventually established a small oversight group chaired by a senior representative from the legal department, which has primary responsibility for compliance and related activities.

Once governance policies have been created, implementing and enforcing them is yet another issue, says Mr Whatnell. It took Sunoco nearly six months to define its information governance strategy, and the firm expects it will require as long as three years to put the automated controls in place. Once the systems are set, mandating new procedures will require time and finesse. “Getting several thousand people to change their work practices in a manner that doesn’t interfere with their needs is a big challenge,” says Mr Whatnell.



The business of balancing cost, risk and return

The survey suggests that executives struggle in other areas as well. Regardless of whether their companies have an information governance structure in place, 40% of respondents said that the biggest challenge they face in implementing a strategy is determining the costs, risks and returns of managing information company-wide. As director of IT planning, relationship and risk management at Air Products & Chemicals, Cheryl Flannery is acutely aware of how difficult it can be to quantify the success of information governance efforts. The US\$10bn manufacturer of industrial gases and chemicals operates in more than 40 countries and has made some important corporate-wide changes to the policies that govern information. Those changes have yielded benefits in the form of improved data protection and clearer accountability for how information is shared across the organisation. There are certainly challenges, however, such as balancing the need to protect sensitive information with the need to share it. Quantifying the benefits is tricky: “we look at how we’re reducing security incidents that interrupt operations and impact on the business,” Ms Flannery says, “but we haven’t worked through quantifying the dollar benefit”.

The biggest challenge worldwide is identifying the cost/risk/return tradeoffs of managing information company-wide.

According to the survey results, scattered and decentralised systems are another challenge and still commonplace in many organisations. More than half (52%) of all respondents say that data silos are still an obstacle, although the problem is less prevalent among North American companies (40%) than those in Europe (58%) or Asia-Pacific (56%).

While not all firms have formal information governance structures in place, many have begun building the foundation for information governance policies. Globally, 63% of respondents—one-quarter (27%) of whom identified themselves as the chief executive officer (CEO), president or managing director—report that their company’s executive leadership understands the need for proper information governance. Most (65%) have defined policies around how information is to be stored and shared among employees and stakeholders, and 59% say that their firm has defined a policy for properly disposing of IT hardware that may contain sensitive information (this is more common among North American companies than those in Asia-Pacific and Europe).

However, the fact that 35% of organisations operate without defined policies regarding the sharing and storage of information begs the question of whether all organisations should implement such structures and how much they risk by not doing so. Steven John, global director of IT at H.B. Fuller, a Saint Paul, MN-based adhesive maker that operates in 32 countries, admits that his organisation risks making reputation-altering errors with the ageing information infrastructure that it is in the process of replacing. “Certain processes and decisions are more prone to error,” says Mr John

While the company makes do with manual methods of consolidating financial and product data from its 15,000 databases, Mr John explains that a lack of data standards can lead to inadvertent mistakes “when extracting information from disparate unvalidated sources”.



Establishing overarching governance

“As our business continues to grow, it’s harder to rely on human glue to get information to the right person.”

– Diane Bryant, CIO, Intel

Protecting sensitive data is an overriding concern for companies with or without information governance structures. For those without an information governance strategy, though, the risks may be significant: only 51% of respondents at companies that do not have a formal information governance strategy rate their firm’s overall ability to protect sensitive data as good or very good, compared with 85% for those whose companies have a formal strategy.

“Information and intellectual property are our crown jewels,” says Intel’s Diane Bryant, a 23-year veteran of the company and newly appointed CIO. The Santa Clara, CA-based maker of microprocessors has had formal policies in place for governing and protecting information for the last 20 years, according to Ms Bryant, but no overarching governance to enforce them or formal team to address new or changing issues.

As a result, Intel formed its information governance body in early 2007 as a corporate steering committee that includes the CEO, chief financial officer (CFO) and general managers representing each business group. High on the list of priorities was data security. Protecting data is an ongoing effort, as internal and external environments shift. For example, Intel is in the process of implementing a business intelligence system that will allow employees in all phases of the core business—product development, manufacturing and sales—to view the same product lifecycle information from a single software platform. Currently, this information resides in separate repositories, and some of it is disseminated through e-mails, phone calls and meetings. “As our business continues to grow, it’s harder to rely on human glue to

A regional comparison of information governance

Thanks to certain technologies, some aspects of today’s global business environment have been democratised and homogenised. Yet survey results indicate that geographic regions actually support different approaches to governing information.

For example, overall responsibility for information governance varies according to region. In North America, 40% of respondents report that the chief information officer (CIO) is responsible for overall information governance, followed by just 16% for chief executive officers (CEOs). In other regions of the world, though, respondents report that the CEO is more often the final decision-maker. In Europe and Asia-Pacific, for instance, the CEO is most often responsible (38% and 39%, respectively) for overall governance of information, followed by the CIO (30% and 23%, respectively).

Across all regions, CEOs are more likely to head information governance strategies at small companies (firms with less than

US\$500m in revenue) than large ones, where CIOs most often take the lead. This could imply that CIOs at smaller companies are not empowered to make decisions, or that these companies do not have a CIO.

Pranav Roach, president of Hughes Network Systems India, a New Delhi-based provider of broadband satellite products and services, says that CEOs in India are more involved than ever in information governance matters. Recent legislation, he explains, has shifted responsibility for data protection onto executives. “There’s a heightened level of accountability for executives here,” says Mr Pranav. “They are responsible for the networks and must-have rules that protect information and stop its misuse.”

Globally, responsibility for identifying risks associated with corporate information is split closely between the CEO (24%) and CIO (28%), although among large companies CIOs are far more likely to be responsible for identifying risks than CEOs. In North America, the CIO clearly leads this charge (26%), while the CEO (14%) is far less often involved.



get information to the right person.”

If one thing is certain, it is that workers who benefit from well-governed information often have to make compromises to see the gains. At Unisys, a global information technology consulting firm, consultants like to work in collaborative and less structured technologies, like wikis. However, it is incumbent upon them to make sure that the whole company benefits from the most valuable information. “They like the freedom,” says Alex Goodall, the firm’s principal knowledge management consultant. “But the expectation is that when there is corporate-quality and relevant material, that it gets to the right place,” meaning a structured information repository that other consultants can access.

Workers in all regions have to adjust to stricter information governance policies. For example, compared with workers in other Asian countries, Chinese workers are more likely to try to use personal e-mail accounts for work purposes, according to Thomas Goebel, an information officer at Evonik Degussa China, a subsidiary of a multinational chemical company based in Essen, Germany. The practice is strongly discouraged as it puts the company at risk. “When an employee leaves we have no access to his e-mails, and sometimes a customer may not even know the company they are dealing with,” says Mr Goebel, who is based in Shanghai. To address this and other types of risky behaviour, Evonik Degussa holds regular training and education sessions.

Conclusion

As firms large and small begin to think more strategically about how information is used and conveyed, they will have little choice but to invest time and resources in a qualified cross-functional group to create a standard set of policies and procedures for governing information. In fact, 77% of survey respondents say that enterprise information governance will be very important or somewhat important to their company's success in three years, compared with just 49% today.

Most information governance bodies address their work from the perspective of protecting information. However, as those bodies gain a firmer grasp of data security, they will have to look at the ways in which controlling and distributing data can improve operations, decrease costs and even increase the bottom line. They will also have to adjust and alter strategies based on shifts in the external environment, some of which will add additional complications. To that end, 68% of respondents expect their company's information governance issues to become more complex over the next three years.

The future of information governance will hinge on continually evaluating policies and adapting them as business priorities and market conditions evolve. Just as an effective corporate governance strategy can yield competitive advantages, effective information governance can turn information into a more consistent generator of business value. For now, those implementing or seeking to strengthen an information governance programme should consider the following:

- Be clear at the outset about roles, responsibilities and accountability across the organisation. Establish a central governance body with decision-making authority and cross-functional and geographic representation. Committees should plan to meet regularly and be sufficiently small and empowered to make decisions swiftly.
- Top-down support is critical to the success of any information governance strategy. Senior management and the board should be briefed regularly on projects and progress related to information governance.
- Establish a formal and ongoing education programme to make employees aware of new policies and procedures and the reasoning behind them. Develop training sessions and annual governance refreshers to ensure that the entire organisation is in line with the frameworks.
- Enforce standards with flexibility. While some policies and procedures should be universal, certain business units and regions may need some leeway when it comes to process particularities. They should be free to determine the best course of action within the overall governance boundaries.
- Stay abreast of trends in information governance by joining professional organisations, attending conferences and reading up-to-date research. Reach out to counterparts in firms that have already established information governance frameworks.

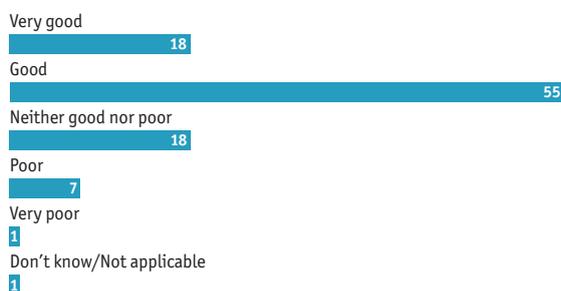
Globally, responsibility for identifying risks associated with corporate information is split closely between the CEO (24%) and CIO (28%), although among large companies CIOs are far more likely to be responsible for identifying risks than CEOs. In North America, the CIO clearly leads this charge (26%), while the CEO (14%) is far less often involved.

Appendix: Survey results

In April 2008, the Economist Intelligence Unit conducted a global online survey of 192 senior executives from various industries. Please note that not all answers add up to 100% because of rounding or because respondents were able to provide multiple answers to some questions.

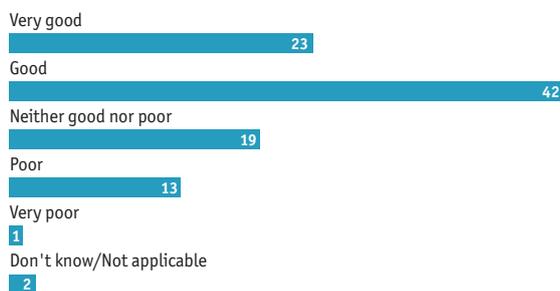
How would you rate your company's overall ability to provide access to critical business information when it is needed?

(% respondents)



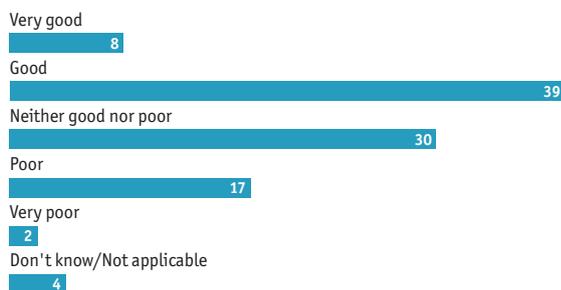
How would you rate your company's overall ability to protect sensitive information?

(% respondents)



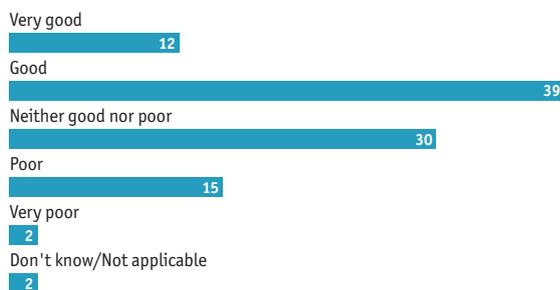
How would you rate your company's overall ability to manage the cost of collecting, storing, and securing information throughout its lifecycle?

(% respondents)



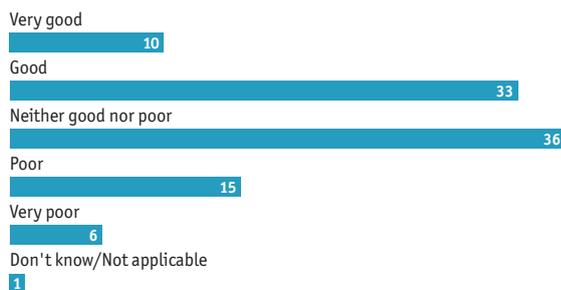
How would you rate your company's overall ability to create business value from its information assets?

(% respondents)



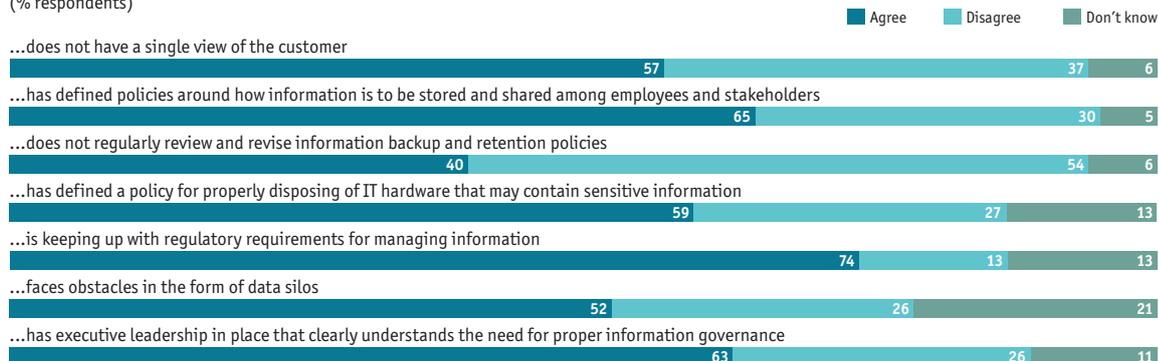
How do you rate your company's overall ability to integrate and share information across departments and necessary third parties?

(% respondents)



Do you agree or disagree with the following statements? My company...

(% respondents)



In your opinion, what are (or would be) the greatest benefits of an enterprise-wide information governance strategy at your company? Select up to three

(% of respondents)



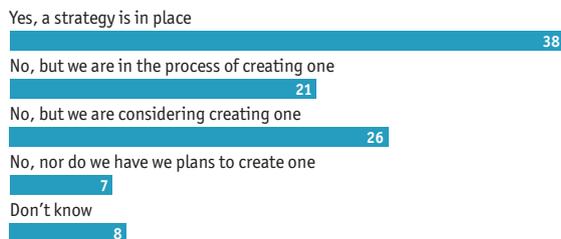
In your opinion, what are (or would be) the greatest challenges in implementing an enterprise-wide information governance strategy at your company? Select up to three

(% of respondents)



Does your company have an enterprise-wide information governance strategy?

(% respondents)



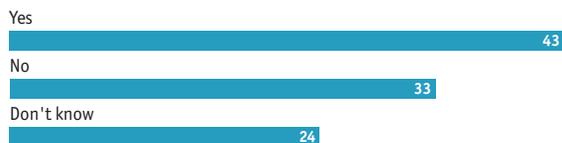
What was the primary catalyst for your company's decision to develop an information governance strategy?

(% respondents)



Would your company consider, or has it sought assistance in developing and implementing an information governance strategy from an outside organisation?

(% respondents)



Who in your company is responsible for identifying the risks associated with the information your company owns?

(% respondents)



Who in your company is responsible for identifying the additional business value that can be created from the information your company owns?

(% respondents)



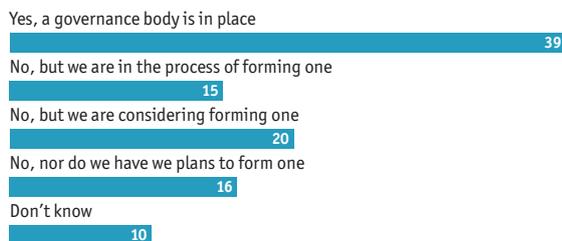
Who in your company is responsible for the overall governance of the information your company owns?

(% respondents)



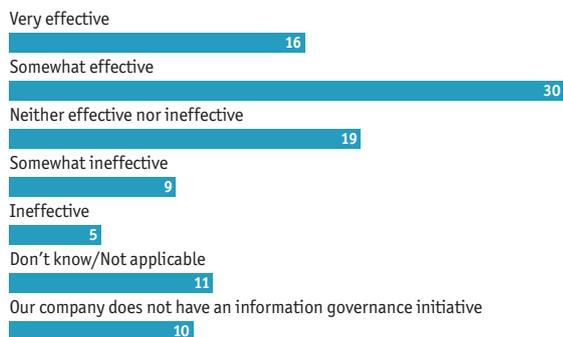
Does your company have a formal information governance body to set and enforce policies?

(% respondents)



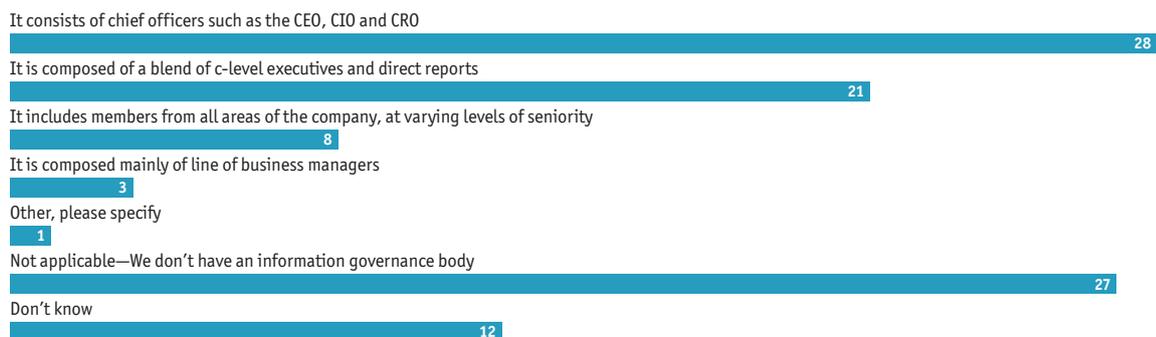
How effective would you say your company's information governance initiative has been to date?

(% respondents)



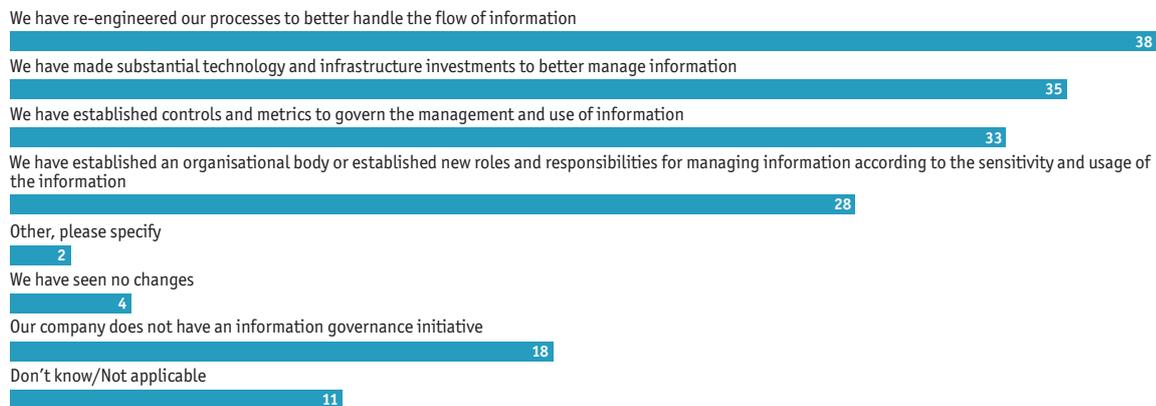
How is your company's information governance body composed?

(% of respondents)



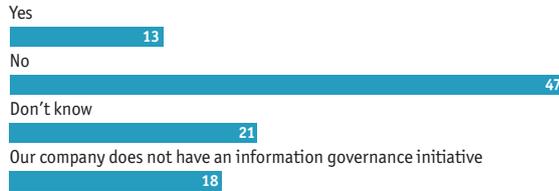
What corporate changes have taken place as a result of your firm's information governance initiative? Select all that apply.

(% respondents)



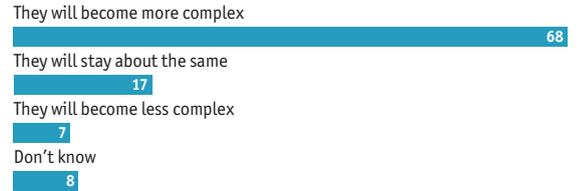
Does your company have a formal process by which it determines the ROI from your information governance initiative?

(% respondents)



How do you expect the complexity of your company's information governance issues will change over the next three years?

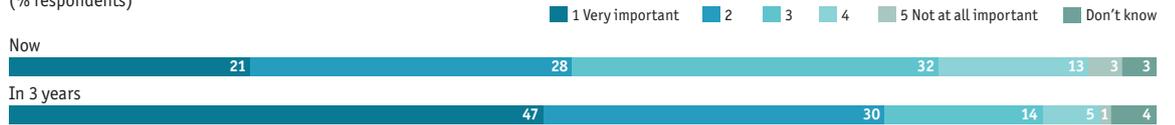
(% respondents)



How important is enterprise information governance to your company's success today? And how important do you think it will be in three years?

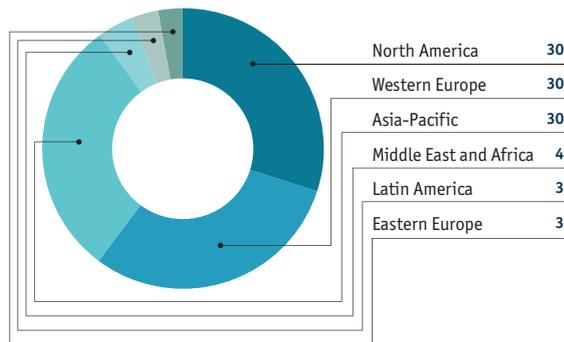
Rate on a scale of 1 to 5 where 1=Very important and 5=Not at all important.

(% respondents)



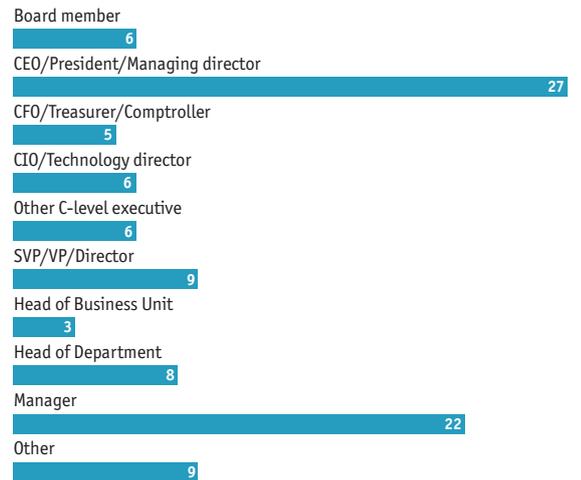
In which region are you personally based?

(% respondents)



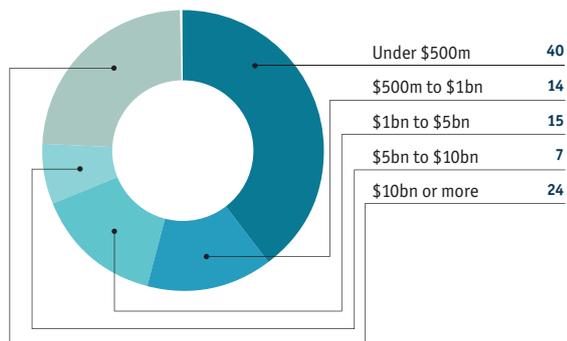
Which of the following best describes your job title?

(% respondents)



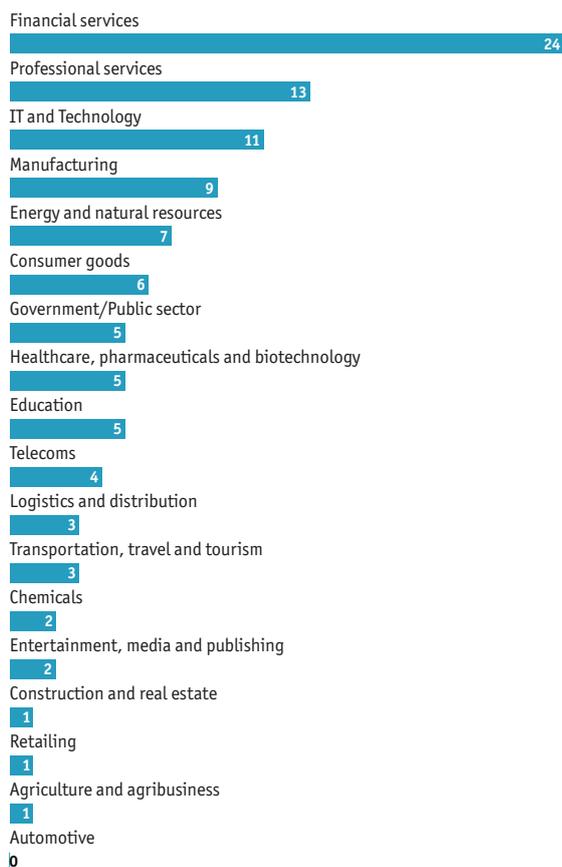
What is your organisation's global annual revenue in US dollars?

(% respondents)



What is your primary industry?

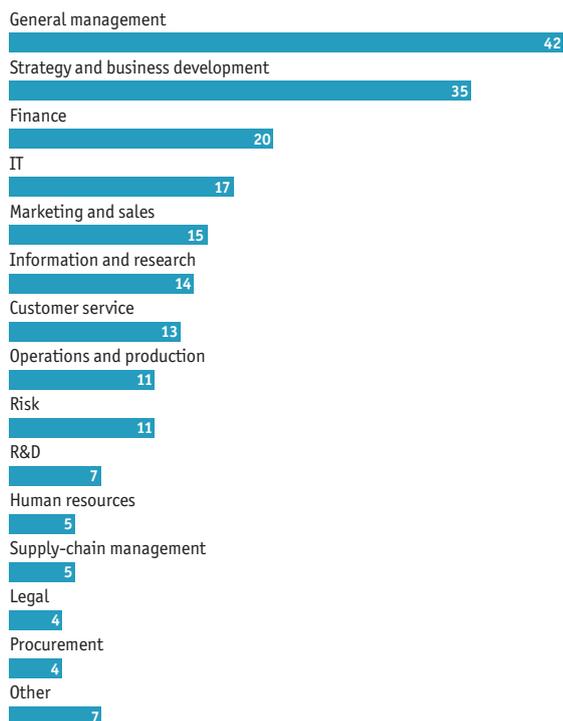
(% respondents)



What are your main functional roles?

Please choose no more than three functions.

(% respondents)



Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

LONDON

26 Red Lion Square

London

WC1R 4HQ

United Kingdom

Tel: (44.20) 7576 8000

Fax: (44.20) 7576 8476

E-mail: london@eiu.com

NEW YORK

111 West 57th Street

New York

NY 10019

United States

Tel: (1.212) 554 0600

Fax: (1.212) 586 1181/2

E-mail: newyork@eiu.com

HONG KONG

6001, Central Plaza

18 Harbour Road

Wanchai

Hong Kong

Tel: (852) 2585 3888

Fax: (852) 2802 7638

E-mail: hongkong@eiu.com