5 STEPS TO JUMPSTART YOUR IG INITIATIVE

GUIDANCE SOFTWARE is now

opentext™

OVERVIEW

Information Governance (IG) is a broad topic and an emerging market with decision structures and authority figures being defined across organizations and industries. IG includes the integration of people, products, and processes to understand and extract value from information, while minimizing the associated risks and costs. While it may be challenging to define the differences between information and data governance, or between content and data management, we do know what information governance is not. Information governance is not a product, market, or industry that simply serves the requirements of legal, compliance, and risk teams alone.

In many cases, technology is developing faster than organizations can create, or update, necessary policies. Much of the technology that drives information governance stems from e-Discovery, which can be considered quite mature, particularly in the U.S. Shifting this technology from a more stringent and highly scrutinized, court-examined process to a proactive solutions-based process - in a less scrutinized manner - has helped accelerate this transition. Interestingly, organizations are no longer waiting for their internal data governance policies to be fully established before considering these emerging technologies. In many cases, the advent of information governance software is not only helping organizations recognize their problems, but is serving as a 'policy-enabler' of sorts.

Alongside the evolution of software technology and internal data governance policies, the decision-making process and accountability structures within organizations – or the 'people' – are concurrently evolving. We are witnessing what has traditionally been a Legal or IT responsibility maturing into a mix of IG committees or steering committees, C-level executive accountability, and the inclusion of external stakeholders. In this whitepaper, we will cover the apparent barriers to IG adoption, the evolution of IG decision-making, and how organizations can align their resources to successfully advance their information governance initiatives.

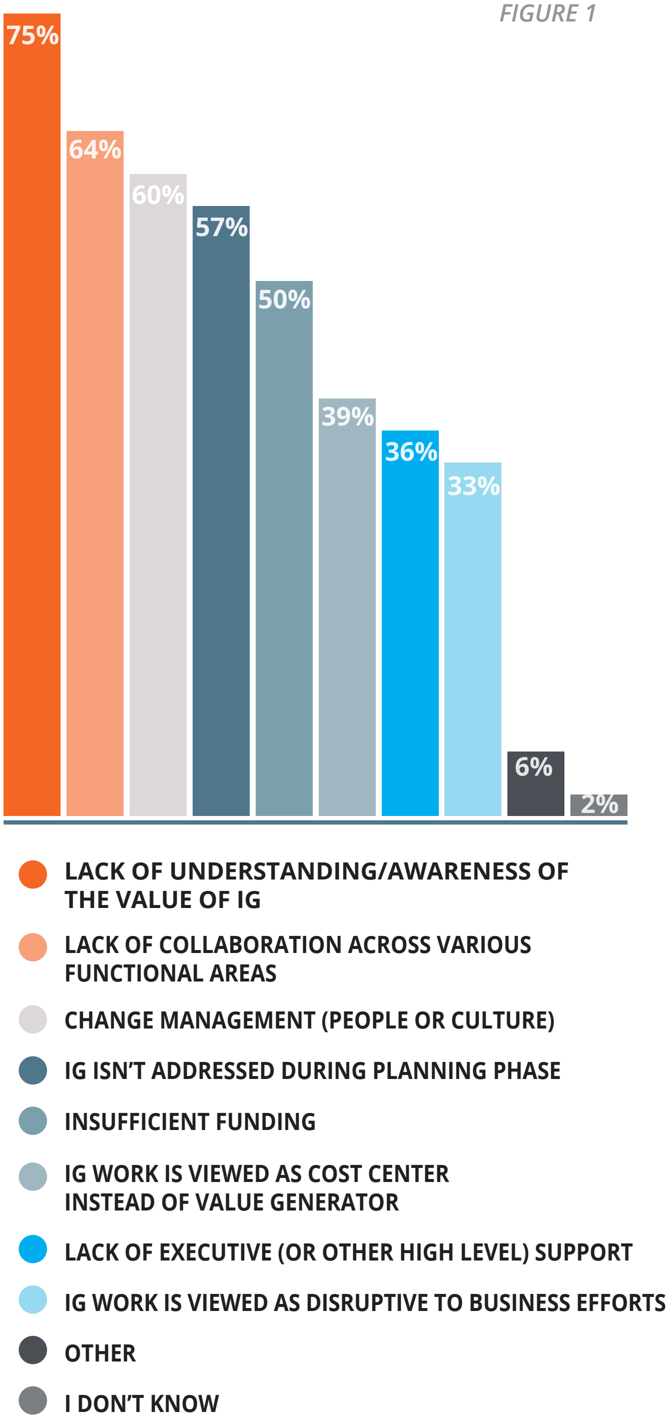
CHALLENGES TO IG ADOPTION

The exponential growth of electronic data, and especially sensitive information, presents unique challenges. Due to the sheer volume, Information Security teams often struggle to understand the data they are mandated to protect (e.g., what it is, why they have it, whether they should have it, what value it has, and what risk it poses to the organization, if any). Gartner predicts that by 2020, "60% of digital businesses will suffer major service failure due to the inability of IT security teams to manage digital risk."[1] IT personnel are often banned from deleting significant amounts of data due to a 'hoard-everything' mentality common to legal teams. In turn, legal departments struggle to manage rising e-discovery costs, and compliance stakeholders struggle to ensure agreement with both internal and external data privacy regulations at the risk of fines or sanctions. There are also increasing expectations that IG strategies not only address the aforementioned issues, but also proactively position data and content for more effective business intelligence and use.

Identifying and classifying sensitive data across the entire enterprise is a daunting and difficult proposition - especially in light of Shadow IT, data sprawl, and other data-related challenges. 41.6% of organizations say they are unable to classify sensitive data with existing technology.[2] It is clear there is a growing need for purpose-built information governance solutions.

In their 2015-2016 annual report, the Information Governance Initiative cited a lack of understanding or awareness of the value of IG as the number one barrier to IG progress. Other significant barriers include lack of collaboration across various functional areas, change management, and the lack of adequate planning [3]. See Figure 1. This supports the view that the challenges go beyond technological hurdles. Greater internal appreciation and collaboration around information governance is needed as well.

FIGURE 1



[1] Gartner Newsroom, Gartner, Inc. June 2016.

[2] "Can We Say Next-Gen Yet? State of Endpoint Security." A SANS Survey. March 2016

[3] "Information Governance Initiative Annual Report 2015 – 2016." Information Governance Initiative. 2015

5 STEPS TO JUMPSTART YOUR IG INITIATIVE

The following 5 steps will help address many of the challenges mentioned above and favorably position your organization for success.

STEP 1:

EDUCATE YOUR ORGANIZATION ON THE VALUE OF IG

Clearly communicate the benefits of a sustainable information governance program that will proactively manage your most sensitive data with a unified and systematic approach. It will be important to demonstrate this value from a practical perspective and to reinforce the idea that using content and data more effectively is not just the responsibility of a single individual or team. Rather, it is the responsibility of all stakeholders that have some level of interest in improving business intelligence, ensuring compliance, and mitigating legal, business, and security risks.

A comprehensive information governance program can do the following:

IT OR DATA BENEFITS

- Drive evidence-based decisions around technology upgrades, data architecture, divestitures, migrations, etc.
- Reduce storage and operational costs by systematically deleting data that has become stale or has no additional business value
- Migrate data to more cost-effective archives or secure repositories
- Improve the accuracy and reliability of data

SECURITY BENEFITS

- Proactively safeguard sensitive data from security breaches, insider threats, lost devices, or human error with the systematic identification and categorization of sensitive data
- Reduce the surface area of errant sensitive data risk via deduplication, deletion, migration, and other control actions

COMPLIANCE OR LEGAL BENEFITS

- Provide insight into how sensitive data is used and stored across geographic boundaries to address possible international cross-border data privacy issues (e.g., General Data Protection Regulation, US EU Privacy Shield, etc.)
- Determine where your information resides to better prepare for litigation involving international regulations
- Comply with regulatory statutes like HIPAA (Health Insurance Portability and Accountability Act) and PCI DSS (Payment Card Industry Data Security Standard)
- Execute on defensible disposition policies to reduce downstream e-Discovery costs with fewer files to review and redact

BUSINESS BENEFITS

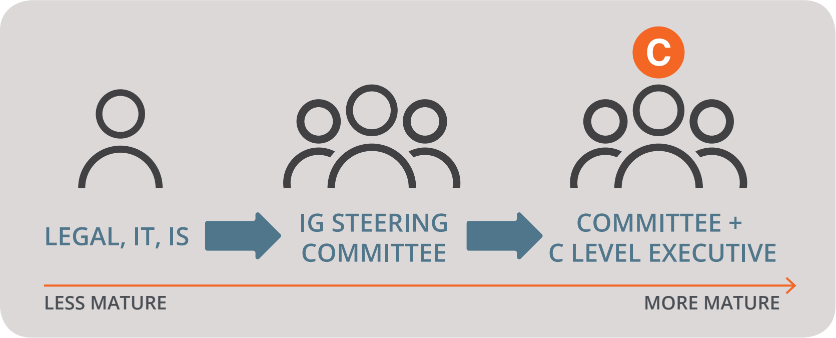
- Build trust and promote a culture that appreciates the business value of data security and privacy
- Align risk reduction metrics with business objectives in a traceable manner to measure privacy and security contributions
- Create privacy-led business models that drive new revenue and growth

STEP 2:

CREATE AN IG STEERING COMMITTEE

IG is not limited to serving the needs of legal, compliance, and risk teams alone. While less mature organizations may assign IG strategies to a single department or person, more advanced companies will have IG steering committees with representative stakeholders from across the organization - including, but not limited to, the lines of business, technology, security, legal, marketing, operations, and risk.

Enterprise architects should also play a key role in helping the committee balance competing projects, align business priorities with the technology agenda, and garner support from C-level officers. The most mature IG steering committees will have C-level executive oversight and accountability. The executive sponsor will encourage all stakeholders to carefully anticipate future directions in IG, both in technology and in the business use of that technology, and empower the Committee to make important decisions on key areas of corporate or technology governance.



The diagram above illustrates the evolution of the IG steering committee.

STEP 3:

THINK ABOUT THE EXTERNAL STAKEHOLDER

Customers, prospects, and partners have higher levels of awareness and expectations when it comes to protecting their sensitive and private information. They demand that organizations handle their sensitive data responsibly, in accordance with applicable laws and regulations and with an ethical sense of corporate and social responsibility. Information governance initiatives must address the needs of its users and partners by having data appropriately shared, used, preserved, and/or safely remediated. Organizations can no longer make assumptions about who curates what information, where and how it is processed, and whether data protection standards have already been met.

Having consistent IG standards and complying with privacy and data protection laws build trust with both customers and business partners. Third-party entities, like law firms and vendors, need to be compelled to disclose their security, storage, and disposal policies to ensure they meet or exceed data privacy standards aimed to protect personally identifiable information or other proprietary data. As data custodians of sensitive information, they can easily become targets for hackers looking for corporate intelligence or customer data. Having consistent IG principles that span across all business partners will also demonstrate good faith with auditors and regulatory authorities.

Data breaches or leaks, due to inadequate IG execution, can cause significant reputational damage which can consequentially result in lost business, decline in share value, or regulatory fines. Conversely, having a strong privacy-compliant IG strategy has the potential to not only mitigate security and regulatory risks, but demonstrate how privacy contributes to real business value and growth.

Organizations must therefore make an effort to understand how prospects, customers, partners, or regulators want to be served, facilitate better communication with all internal and external stakeholders, and focus on areas that build trust and transparency.

STEP 4:

CREATE A NEW KIND OF BUSINESS CASE

Establishing a business case for proactive IG requires both a quantitative return on investment (ROI) analysis as well as a qualitative examination of corporate priorities. Organizations that recently failed an audit or face litigation due to a data breach or privacy violation may be open to investing in technologies designed to manage their compliance practices. Under these circumstances, an IG program can get funded as a 'reactionary' measure; however, in order to make a business case for a proactive IG solution - somehow measuring what doesn't happen - organizations need to create a new kind of business case centered on both quantitative and qualitative analysis.

Quantitative Analysis

STORAGE AND MAINTENANCE COSTS

Some estimates show that poor data quality can cost organizations as much as $14.2 million annually[4]. However, when electronic information is maintained through proper data hygiene, organizations can realize almost immediate return by reducing the storage costs (de-duplicating files) and downstream e-discovery efforts (e.g., less data to process, review, redact, and produce). It is important to note that while enterprise data continues to grow - 60% annually (insurance, medical, legal as high as 120%)[5] – and the cost to store this data becomes cheaper over time, maintaining this data will still incur costs related to staffing, backup, migration, and restoration.

COST OF A SECURITY BREACH

In 2016, the Ponemon Institute reported that the average cost of a single compromised record is $158[6]. This cost primarily stems from remedial measures like providing customers with credit monitoring services and reimbursement for actual damages, but also include declining sales due to loss in consumer confidence. On average, the total cost of a single data breach is now $4 million. It will be important to calculate the quantitative financial impact from a possible security breach from malicious hackers, rogue employees, and lost or stolen devices.

COST FOR REGULATORY NON-COMPLIANCE

Organizations can mitigate some of the risks related to regulatory non-compliance by adhering to their document retention and data governance policies; however, the truth is, many organizations struggle with the technological capability to effectively and accurately execute these policies. In today's highly regulated environment, the high cost of regulatory non-compliance can include possible sanctions, fines, and lawsuits. Organizations can start by measuring the cost of potential fines for data privacy violations. For instance, organizations in violation of the EU General Data Protection Regulation (GDPR) after May 2018 can be fined up to 4% of global revenue. It is worth mentioning that the Ponemon Institute reported that the cost of non-compliance is actually 2.65 times higher than the cost of compliance.[7]

Qualitative Analysis

FOCUS ON CORPORATE PRIORITIES

A business case solely grounded on the value proposition of cost reduction and risk mitigation is insufficient. A well-established IG strategy must also include considerations that include factors like improving the customer experience, gaining business insight, promoting corporate ethics, and competitive differentiation.

In a January 2016 survey conducted by Guidance Software, 46% of respondents claimed that protecting sensitive and private data was a top three initiative within their organization . Securing funding is easier under these circumstances; but, for those without explicit IG priorities, it may be necessary to strategically align the business case with existing corporate priorities. For instance, if the goal is to enter into new markets or boost incremental revenue, show how IG will help attain those goals. For example, IG can help address data privacy issues when entering new markets, or IG can create new privacy-led business models to boost sales.

[4] "The State of Data Quality: Current Practices and Evolving Trends." Gartner, Inc. December 2013
[5] "How Fast Is Our Data Volume Growing?" Storage Strategies, Inc. 2009.
[6] "2016 Cost of Data Breach Study: Global Analysis." Ponemon Institute LLC. June 2016
[7] "The True Cost of Compliance: A Benchmark Study of Multinational Organizations." Ponemon Institute LLC. January 2011

STEP 5:

AUGMENT TRAINING WITH TECHNOLOGY

Develop a data governance program or reevaluate existing ones and test for efficacy to identify areas for improvement and training to increase user awareness and empowerment. Proactively safeguard sensitive data by training employees to only retain what is absolutely necessary. The Federal Trade Commission, for example, encourages data minimization, or "limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely." Today, the sheer volume of data that a typical office worker receives or generates has grown exponentially; so rather than purchasing more storage space, companies should focus on enforcing their records retention and data governance programs.

While it is incredibly important to encourage employee responsibility, humans are still prone to make mistakes. Whether sensitive data is accidentally leaked, laptops are lost, or passwords left in plain view, you simply cannot solve these problems with training alone. It is equally, if not more, important to implement technology to gain transparency into sensitive data to help make evidence-based business decisions, and then automate those decisions going forward. There is simply too much data for human beings to process without the help of technology.

CONCLUSION

Information Governance includes a broad range of activities and technologies employed to maximize the value of information while minimizing associated risks and costs. The need to control private and sensitive data should be continuous and not treated opportunistically when there is pending litigation, an annual audit, or after a security breach. This continuous and systematic identification of risk within organizations will require a thorough evaluation of policies and technologies, training and automation, and the various types of corporate, financial, and social benefits that align with business objectives. The organizations that do this well will find the most success in implementing and jumpstarting an effective IG program.

[8] "Data Risk and Privacy Survey." Guidance Software. January 2016

[9] "Internet of Things. Privacy & Security in a Connected World." FTC Staff Report. January 2015

GUIDANCE SOFTWARE™

ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.