

C-Level Guide to Covering Your Information Governance Assets

By Steve O'Neill, Esq.



SECURITY

THE DATA EXPLOSION

The management and protection of information assets increasingly represent both the greatest potential value and the greatest risk to the enterprise. Big Data and analytics are now being leveraged by companies well beyond Amazon, Facebook, Uber and Google. Beginning with the Enron scandal and the advent of penalties (civil and criminal) for the improper destruction of electronically stored information (ESI), the existential risk from the disclosure of corporate mistakes or malfeasance through investigation, litigation discovery, or hacking has increased on pace with the explosion of digital data. The reputational damage to Target, Sony, Home Depot and even the U.S. Office of Personnel Management is substantial.

Many organizations now report a literal doubling of stored data each year. The oft-heard anecdote that the hardware cost of data storage has decreased over time obscures the reality that the combined hard and soft costs of this explosion are enormous.



The exponential growth of new data combined with an ocean of unstructured legacy data can only increase management costs and litigation response costs / risks.

Too much data affects the bottom line in many ways. Multiple surveys report that employees spend excessive time searching for and managing information. In the age of Bring Your Own Device (BYOD/BYOT), completely loyal employees regularly leak organizational data (i.e., information assets) into an unmanaged "Shadow IT" system involving insecure personal cloud technologies like Dropbox, Box, Google Drive, and Evernote, as well as PST email archive files – so employees can have the information they need to accomplish their jobs.

Detailed document retention policies, created for legacy paper records and ostensibly applicable to digital information assets, are unevenly applied to digital records in the form of email, even if the policies so mandate. Most importantly for risk mitigation, records and documents are inconsistently disposed of as required by retention schedules. **This practice is not defensible.**

In the context of regulation, investigation, and litigation, it is now well known that upon notice or reasonable anticipation of a duty to preserve evidence, ALL relevant records and documents must be identified and preserved from alteration or deletion. Horror stories abound regarding the disruption and cost of these efforts. Indeed, these risks flow from several directions:

1. The risk of a "smoking gun,"
2. The cost of legal review of potentially millions of documents
3. The risk of court sanctions in response to destruction of electronic evidence

This “data explosion” is no longer just a problem for IT. It is a much broader challenge, involving more than technology; it includes risk management, corporate governance, organizational culture, employee training, and other disciplines. Organizations are increasingly recognizing that the management and protection of information assets are concerns of the board and C-level executive team.¹ This recognition will only increase as the benefits of Big Data and analytics become more widely available. **Without buy-in across executive-level, management of this geometric data growth will likely involve greater risks and costs.**

INCOMPLETE SOLUTIONS + UNEVEN IMPLEMENTATION = CONTINUED DATA GROWTH

Results and successes in efforts to manage digital data growth vary by industry sector and size. Logically, larger organizations in more regulated industries (e.g., publicly traded, life sciences, financial services) are further ahead along the solution continuum. However, survey data and interviews show that even large cap, highly regulated organizations are at best challenged by the data explosion, if not overwhelmed.²

In theory, there is a great business case to be made for robust management of information assets in terms of ROI and risk management. What is the status of these efforts? As children might ask on a long automobile trip, “Are we there yet?” And the answer would have to be, “No, the GPS isn’t working that well out here, the roads seem to have changed, and we are a little bit lost.”

IS INFORMATION GOVERNANCE THE SILVER BULLET?

With the stakes so high, tremendous efforts are underway to understand, measure and rationalize the data management processes and other drivers necessary to reign in this data monster in a legally defensible manner. Much work is being done under the relatively recently coined umbrella of Information Governance or IG. Various committees, organizations and thought leaders have created overlapping definitions for IG. Two influential definitions are:

| | |
|------------------------------|--|
| Gartner | “the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.” http://www.gartner.com/it-glossary/information-governance . |
| The Sedona Conference | “an organization’s coordinated, interdisciplinary approach to satisfying information legal and compliance requirements and managing information risks while optimizing information value. As such, Information Governance encompasses and reconciles the various legal and compliance requirements and risks addressed by different information focused disciplines, such as records and information management (“RIM”), data privacy, information security, and eDiscovery.” See The Sedona Conference Commentary on Information Governance . |

In addition to traditional records management organizations (e.g., ARMA) becoming heavily involved in developing the cross-disciplinary aspects of IG, organizations such as George Socha's successful EDM Group have proposed an infographic model known as the Information Governance Reference Model (IGRM).

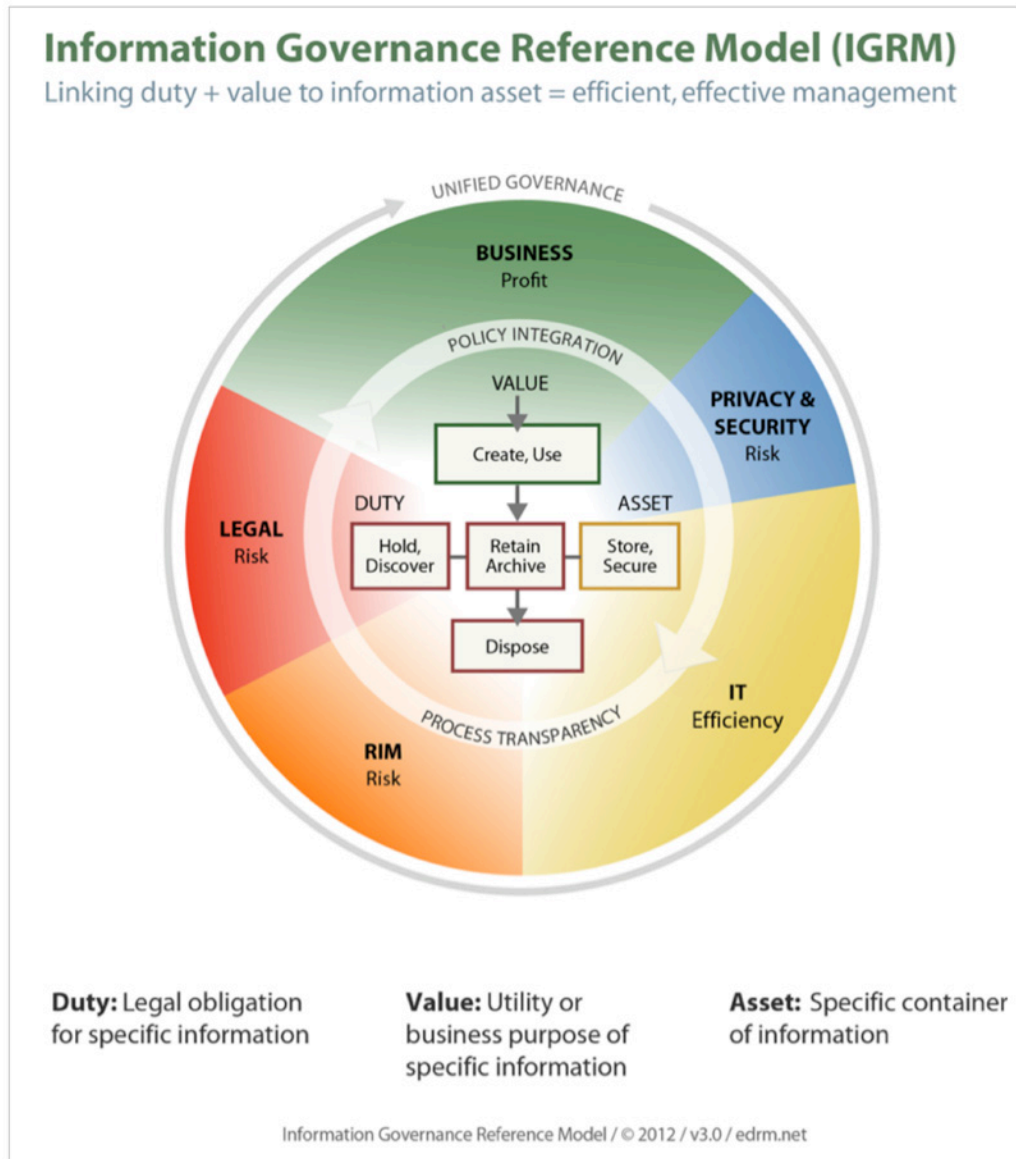


Figure 1 An Information Governance Reference Model

Being relatively new, and bridging numerous specialized disciplines with heretofore inconsistent native terminologies, IG can either be seen as a unifying principle (think: missing link; the Higgs boson) or as a bromide with limited practical utility for implementation (all hat, no horse). In fact, for people who have been dealing with electronic evidence and retention policies since the 1990s, IG is mostly the same old wine in a new bottle, involving the interrelationship among the traditional fields of Legal, RIM (Records & Information Management), and IT in the development of defensible document retention/destruction policies for large organizations, as shown in this decade-old infographic.

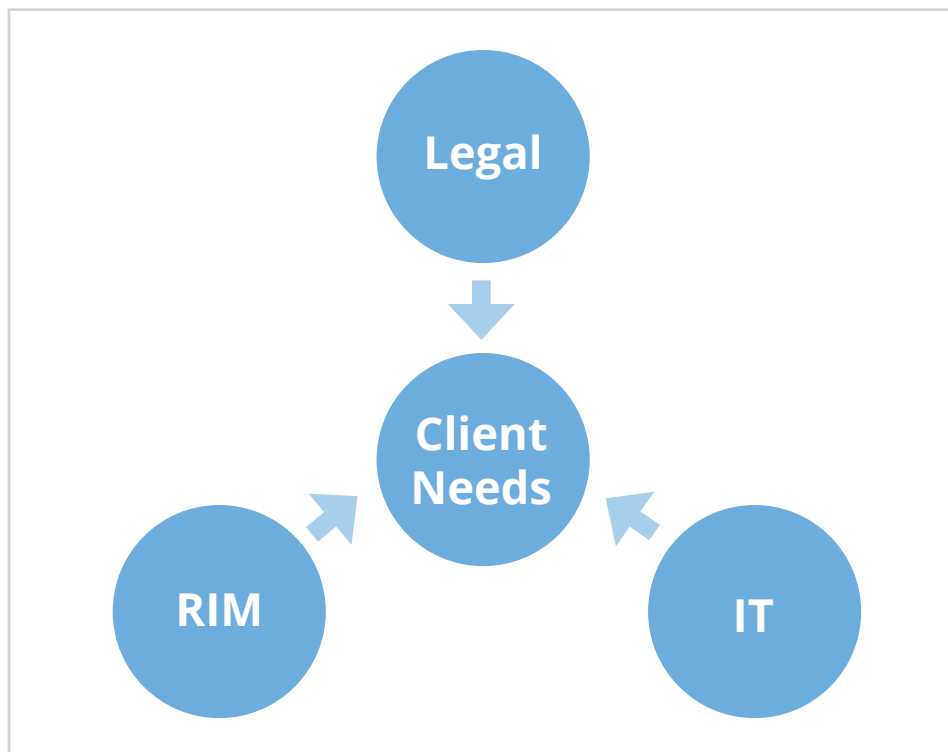


Figure 2 A Document Retention Policy Team, © Steven J. O'Neill, Esq. 2003

Conceptually, a successful IG program should involve and harmonize whatever factors a particular organization requires to maximize benefits and minimize risks. In a sense then, an IG program is better viewed as a “smoothie” where all the necessary ingredients are first identified and then blended together into the perfect mix.

With the questionable and yet unproven utility of adopting a generic IG rubric as a real solution to the data explosion, what should be done? Should organizations continue to make incremental improvements by investing in technology solutions without requiring effective, harmonized implementation? Is “Cloud Computing” the answer right now or does it present unexplored risks? Are there any “net new events” on the horizon or breakthrough technologies that will save the day? How should board members and C-Level executive teams address their fiduciary duties regarding the management of information assets, given the known risks?

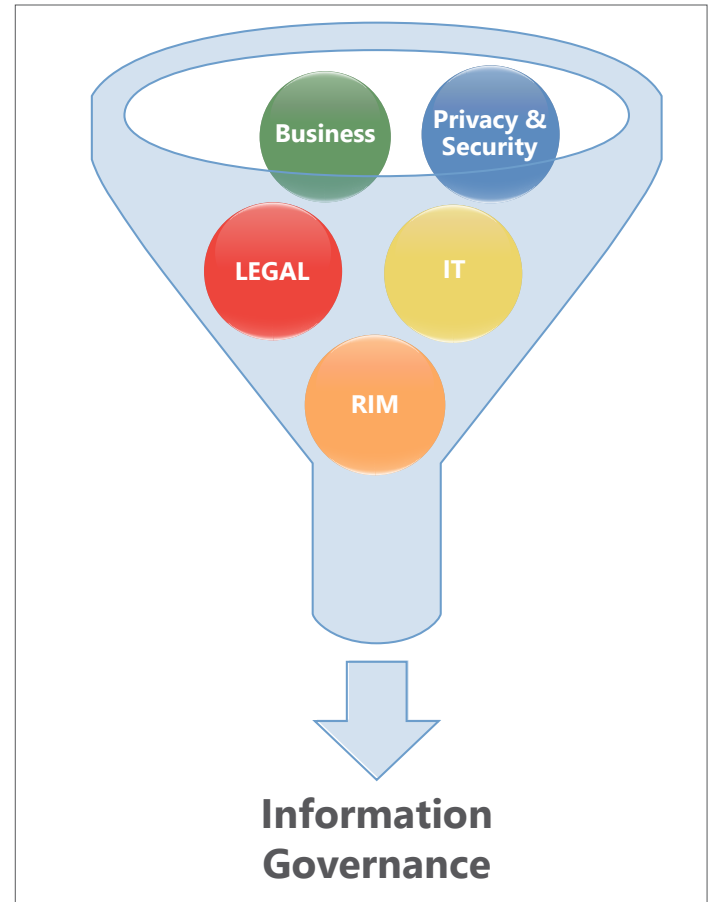


Figure 3 The IG Blender

A MODEST PROPOSAL – START WHERE YOU CAN MAKE REAL PROGRESS

There is really no precedent in history for this data explosion. The lure and concomitant danger of Big Data, together with the apparent lack of an easy technological fix, indicates that we are a bit lost. According to research conducted in 1999 at the Max Planck Institute for Biological Cybernetics in Tuebingen, Germany, it is actually true that people tend to walk in circles when lost in either the desert or the forest. Before unmanaged data doubles and then doubles again, business leaders need to figure out what can be used as a basis for navigation and try to avoid walking in circles. To strain a metaphor and paraphrase Lao Tzu, the journey of a thousand miles begins with a single step . . . in the right direction! Notwithstanding the enormity of the uncertainty and the gravity of the potential risks, to be successful, all organizations must undertake the journey.



Where to begin? For most organizations buried by the data explosion, a good (i.e., good faith from the perspective of being legally defensible) single step in the right direction will involve implementing currently existing and emerging technology that provides the following minimum functionality:

1. Ingestion of new and legacy data
2. Deduplication of multiple copies
3. Preservation of metadata
4. Ability to identify documents for implementation and release of “legal hold”
5. Ability to apply retention / destruction schedules
6. Audit controls
7. Automated deletion / destruction at end of data life cycle (unless data is still subject to a legal hold)

NEW FEDERAL RULES REVISIONS – A GAME CHANGER FOR DEFENSIBLE DELETION

This proposal is workable based on existing information technology but not without blending in the other important elements such as legal, RIM, privacy, security, and change management. **This proposal is timely because the Federal Courts are scheduled this year to begin a pivot away from one of the main sources of eDiscovery uncertainty – the imposition of severe sanctions for the loss of electronically stored information relevant to dispute resolution.** The pivot is a “net new event” for IG because it involves the first significant changes to the Federal Rules of Civil Procedure (FRCP) since 2006, when the concept of Electronically Stored Information (ESI) was expressly recognized and treated by the Rules – including the (mostly unsuccessful) attempt to create a Safe Harbor for the inadvertent destruction of ESI in Rule 37.

The revised Rule 37(e) governing sanctions for destruction of electronic evidence and other changes to the discovery rules were approved by the U.S. Supreme Court earlier this year and will go into effect on December 1, 2015 governing all current and new litigation, unless Congress acts to limit or amend it, which is almost universally not expected.

The revised sanctions rule provides a game-changing “green light” to organizations to *defensibly automate* the deletion / destruction of unneeded legacy and other data in accordance with a reasonable document retention policy and retention schedule. In the simplest of terms, by properly implementing currently available software, every single record and document that is not covered by a legal hold and is slated for destruction under the retention policy and schedule, can disappear forever.

Where the revisions to Rule 37(e) really matter is in the event that an organization mistakenly deletes / destroys records or documents that are later deemed to be relevant in a civil litigation.

Under the 2006 rule, there was a split in the Federal Circuits, where for example the 2nd Circuit (NY, CT, and VT) allowed very severe sanctions to be assessed against a party and its attorneys for loss of evidence resulting from levels of negligence. In contrast, other circuits required a bad faith or intentional loss of evidence to trigger severe sanctions. Worse yet, some circuits left the decision of sanctions to each U.S. District Court trial judge under the doctrine of the inherent powers of the court. Consequently, under the 2006 FRCP, organizations fearing that they might be involved in litigation in an unfavorable circuit for sanctions would seek to protect themselves by over-preserving data in anticipation of litigation. Naturally, given that the sanctions included dismissal of a case or the shifting of the burden of proof with an adverse jury instruction, the risk of the impact of this driver on litigation directly contributed to the current data explosion.

LEGALLY DEFENSIBLE AUTOMATED DELETION / DESTRUCTION

The data explosion discussed above coincided with a public and private data reporting explosion in the wake of the Enron and WorldCom scandals. The advent of “good governance” and corporate transparency rules such as Sarbanes-Oxley together with the rise in the importance of electronic discovery in civil and criminal litigation created an onerous recordkeeping and reporting regime. As noted above, the risks created by this expansive regime cut several ways; keep too little – wrong; keep too much – wrong again.

The “Green Light” provided by the FRCP revisions is really the first break large organizations have had





since the paradigm shift to creating virtually all information in digital form. There are some legal commentators who have complained that the Advisory Committee on Civil Rules favored large organizations over individual litigants such as employees, personal injury plaintiffs, and product liability plaintiffs where the cost and reach of civil discovery is asymmetrical. The revised FRCP Rule 26 adopts the “proportionality” concept first publicized by [The Sedona Conference](#), which promulgated early best practices concerning eDiscovery and continues to be relevant with guidance on IG. The fear among the plaintiff’s bar is that the proportionality concept will unfairly limit civil discovery in asymmetrical cases (where the cost and burden of discovery is onerous only for the corporate defendant). The fear among the corporate defense bar is that the proportionality concept is a Trojan Horse, which will invite plaintiff-friendly judges to continue to over-sanction. However, the official Commentary from the Rules Committee responsible for drafting and presenting the revised rules to the U.S. Supreme Court for approval, expressly states that judges are no longer permitted to utilize inherent powers or state law to impose the severe case-killing sanctions. Before such sanctions can be assessed, the revised FRCP Rule 37(e) requires a finding that a party destroyed relevant information with the intent of depriving its opponent access. Subject to the usual caveat about the hazards of litigation, this is a high hurdle to clear.

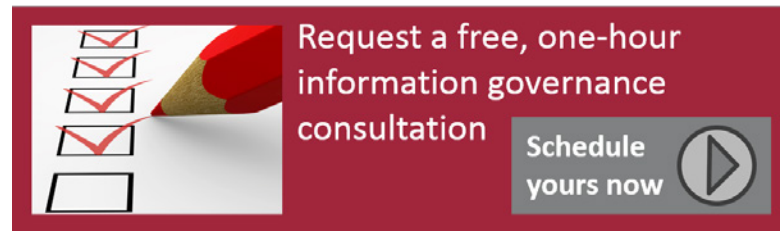
For now (meaning after December 1, 2015), a good faith reading of the elements necessary to issue sanctions combined with the type of reasonable and consistently followed document retention / destruction policy blessed by the U.S. Supreme Court in the 2005 Arthur Andersen case and a robust legal hold procedure, should provide a legally defensible basis to adopt and implement substantial data remediation measures – including automated deletion.

CONCLUSION


Information assets, whether in the form of intellectual property, personal and corporate information or Big Data, are critically valuable to every organization. The exponential growth of organizational data in the form of email and other unstructured data is costly, risky, and unsustainable. Boards and C-Level executive teams are increasingly compelled to understand and provide guidance and direction in order to mitigate legal and reputational risk, and of course, increase efficiency and profitability. The emerging field of Information Governance (IG) is a useful conceptual tool in that it expressly recognizes that data management requires a cross disciplinary effort blending expertise in the legal, records & information management and IT disciplines. However, IG provides an approach and not a solution. It does not provide guidance as to the best first steps to take because each organization and each industry is so different.

In the face of geometric data growth, purchasing more storage year after year is no longer a prudent option. Doing nothing at all would probably not comply with the reasonableness required by the corporate “business judgment rule.” The Modest Proposal for a first next step to mitigate the data explosion is applicable to organizations in most industries. It can be done with currently existing technology and the ROI can be demonstrated. By using existing and emerging software tools to identify, ingest, deduplicate and categorize legacy data into “big buckets” for automated retention / destruction, an organization can stop hoarding unneeded data (data remediation) and create business oriented “day-forward” policies for data stewards and employees alike. The real beauty of such an approach is that the workflows and change management required to “bite off a big piece of the problem” such as email, can be leveraged by then ingesting and processing other organizational data stores into the software solution, including Cloud Computing data.

[Click here to schedule a free consultation with Attorney, Steve O’Neill.](#)



Request a free, one-hour
information governance
consultation

Schedule
yours now 

ABOUT STEVE O’NEILL

Steven J. O’Neill is a business and technology attorney with more than 23 years of litigation, arbitration and legal counseling experience. Steve focuses on helping organizations manage their email, document retention and destruction policies to enable them to significantly reduce and control both costs and risks, in a legally defensible manner.

Steve was previously a litigator and eDiscovery attorney with an AmLaw 100 firm and later chaired an eDiscovery and retention policy compliance practice area at a major New England law firm.

Steve has written numerous articles, taught Continuing Legal Education seminars and lectured nationally on electronic evidence discovery (eDiscovery), retention policies, information security and the legal impacts of technology. Steve is a member of the eDiscovery Committee of an AmLaw 100 firm and former partner eDiscovery practice area chair at Thelen Reid.

Please contact Steve O’Neill at soneill@attorneyoneill.com or call 888-766-3455.

¹Big Data and analytics is not a new concept but over the past few years, public company ‘boards and their management teams have been paying more attention to it and the value it can add to company strategy and risk assessment.’ Currently, according to the survey, overall 33% of companies educate their boards on big data and 48% do not. However, a full 48% of large cap companies already provide this training. ‘Big data is structured and unstructured data generated from diverse sources in real time, in volumes too large for traditional technologies to capture, manage, and process in a timely manner.’ (Deloitte Survey 2014, p. 55)

²Surveys available at www.arma.org.