Disposing of Digital Debris

Information Governance Strategy and Practice in Action

EDRM Information Governance Reference Model (IGRM)
CGOC (Compliance, Governance and Oversight Council)
2014

"It would be helpful if systems were in place to get rid of the junk. Part of the reason e-discovery is so expensive is because companies have so much data that serves no business need … Companies are going to realize that it's important to get their information governance under control to get rid of the data that has no business need … in ways that will improve the company's bottom line."

– The Honorable Andrew J. Peck

Authors

EDRM

- George Socha
- Tom Gelbmann

IGRM

- Aliye Ergulen – lead
- Reed Irvin – co lead
- Damian Durrant
- Quin Gregor
- Eric Killough
- Marcus Ledergerber
- Brian Tuemmier
- Nancy Wallrich

CGOC

- Derek Gascon
- Lynn Molfetta

With thanks to Dr. Herb Roitblat and Tracie McFadden Burns

"As a member of CGOC for many years, and someone who really believes in a holistic information governance strategy, I've spent most of my career as a records management professional building a program that is based on the IGRM model. I'm a true believer that it is not a 'one size fits all' approach. However, if you ignore the fundamental elements of what ties a program together – a strategy that brings all the relevant people and business processes together – you will find yourself hitting brick walls along the way."

Lynn Molfetta, Global Head of Records Management, Citigroup; the opinions expressed in this article are those of the CGOC Practitioner, Lynn Molfetta, and not necessarily those of Citibank or its affiliates.

Introduction

No one intentionally creates digital debris. We document decisions as we collaborate; we create files, backups, databases, and applications; and we store photos, music, digital training programs, logs and reports. We create that content at that moment and imbue it with value and purpose. However, as circumstances evolve, information can lose value as it loses currency.

In 2012, the Compliance, Governance and Oversight Council (CGOC) released survey results indicating that approximately:

- 1% of organizational information is subject to legal hold
- Only 5% is held pursuant to a document classification schema
- 25% relates to a business need
- The remaining 69% has no legal or business value

A survey conducted at the 2013 CGOC Summit showed that organizations are reluctant to eliminate digital debris because they:

- Do not know where to start
- Cannot bring all information stakeholders to the table
- Are unable to demonstrate the urgency
- Cannot clearly demonstrate negative cost and risk impacts
- Cannot build a compelling business case

Information Governance (IG) -- a critical, cross-functional discipline -- focuses on reducing an organization's data footprint in a controlled and defensible manner. The core of a successful IG program is the automation of repeatable and defensible policies and processes with supporting technology, and people accountable for the transformation. The need to have a coherent IG program and to begin deletion of digital debris is more pressing now than ever, as data continues to proliferate in volume, velocity, variety and variability.

Consider the following:

- Every day, we create 2.5 quintillion bytes of data and rising
- Storage locations can include on-site, off-site, cloud and Software as a Service (SaaS) deployments and appear in a variety of hybrid configurations
- Social media platforms such as *Twitter*, *Instagram* or *Facebook* combine large volumes of data with high intensity social habits, creating large volumes of potentially sensitive data
- IT infrastructure, burdened by the storage and management of excessive data, shoulders high hidden costs that impact its budget and degrade application performance and operations
- E-discovery processes result in the preservation of large amounts of data, including many duplicates that will be re-used as evidence in future litigation if not properly destroyed
- New regulatory requirements such as Dodd-Frank and privacy regulations increase the cost and risk of unnecessarily managing data debris

The question is no longer *why* but *how* to identify and dispose of digital debris.

To help organizations understand how to dispose of their digital debris, the EDRM Information Governance Reference Model (IGRM) and the CGOC explore in this white paper:

I. The Problem – Defining and Identifying Digital Debris

II. The Strategy – Leveraging the IGRM to Define a Successful IG program

III. The Practice – How to Put the Strategy into Action with Success

SECTION I: The Problem – Defining and Identifying Digital Debris

Most IT departments default to a "keep everything forever" approach to data as they attempt to ensure the organization's regulatory compliance and e-discovery readiness without guidance.

As a result, the amount of content created and stored digitally increases annually at an exponential rate. Organizations now commonly measure their data storage by the petabyte, or, *one million* gigabytes. At the same time, organizations increase the complexity and cost of managing this information by generating a growing array of data types. Additionally, data volumes are exploding with an ever-expanding number of internet-enabled devices, bringing with them all of the challenges associated with BYOD.

IT today must manage multiple data sources, including:

- Email messages and attachments
- Social media and blog posts (consumer and business)
- Text messages and instant messages
- Photos, videos and audio (multi-media, photos, videos, conference calls, voice mails, memos, etc.)
- Machine-generated data (log files, call detail records, etc.)
- Contextual data
- Structured data (database/transactional)

This data deluge impacts more than just the storage space of IT departments. Unchecked data growth degrades application performance as bloated storage devices slow read and write times and burden backup and recovery processes. As performance degrades and volumes bloat, so does the ability to track documents. This leads to the creation of more debris and to significant financial consequences, from both a risk management and an IT management perspective.

Generally, the longer an organization retains a piece of data, the less value that data will have and the more risk it presents.

Examples of digital debris

Here are a few examples of retained information without apparent value:

Short-term reference files

- *SharePoint*, network drives, *Dropbox* and similar repositories used to enable sharing, transferring or temporarily storing files are rarely purged upon task completion.

- Logs, reports or dumps from applications and database systems all lose their value over time.
- "Work files" are rarely cleaned up at the end of the project or case.

Orphaned files

- Departing employees' data often remains in place and unmanaged. If not specifically reviewed and classified, this data becomes unreferenced, unused and forgotten.
- Mislabeled, misfiled documents (such as those not conforming to naming standards) will disappear from use but not from storage.
- Files from old or unsupported applications remain in place because their custodians do not feel empowered to delete them as they are unsure what the files represent.

Outdated or superseded files

- Outdated versions or draft copies -- major sources of near-duplicated analysis in electronic discovery -- expose the company to tremendous and unnecessary risk. While initially useful during creation, these files ought to be cleared up or specifically classified as a business record. If the draft has not advanced in 6-12 months, the chances of it doing so diminish.
- Draft or "old version" folders containing entire working sets of documents or drawings are often saved, superseded and then forgotten.

Systems upgrades, safety and litigation copies

- As systems are replaced or upgraded, the content of the old system is not adequately merged with the new system, causing massive duplication. Similarly, in anticipation of upgrade complications, extra copies are created but never destroyed.
- Files are often copied because of their importance at the time. However, even as their value decreases, the copies remain.
- Impending litigation demands that the parties either preserve their data in place or duplicate it to another area. Often, these efforts lead to terabytes of redundant, even superfluous, data. Once the litigation resolves, the parties move on, neglecting to dispose of these "litigation copies". Then, since they still exist, the same useless information is re-discovered in new cases. This can become a never-ending cycle.

Outdated storage technology

- The storage systems used to house data also age: from backup tapes to old disks to forgotten computer systems. Legacy systems in general are often a vast source of digital debris.

- In the ground-breaking case of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), the discovery of responsive but unprocessed emails on several undisclosed, eight-year-old backup tapes, led to a fine (later partially overturned) that exceeded $1.4B.

- A Fortune 100 company, performing an internal audit, located more than 33,000 items of abandoned storage media, Blackberry's, disks and computers. These legacy devices held very significant volumes of data -- none of it easily accessible.

Technical duplicates

- On average, 15% of duplicate files are necessary to their context and cannot be deleted without ruining the integrity of a larger set.
    - Examples are logo files that are embedded within other files, addendum or exhibits to compound documents, database configuration files, or externally referenced files in CAD engineering drawings.

- Technical duplicates are not debris, but they do increase the data set and cost and risk and have to be dealt with by an IG program.

- Duplicate files in existence at the establishment of a legal or preservation hold cannot be deleted. However, one benefit of an active IG program would be the identification and deletion of unnecessary duplicates *prior* to the preservation and resulting legal hold.

> *"An ocean of digital debris already overwhelms many companies … Unless cleanup becomes a directed, funded and systemic part of an information governance program, the clutter continues."*

Advantages of disposing of digital debris

Today, technology such as tablets, laptops, smart phones and other platforms provide a constant connection allowing employees to continuously create new business content, data and new demands for data storage.

Fortunately, new technology can also process, identify and classify data in batches or in real time – solutions not available a few years ago. These advances also enable mining of "big data" for critical business insight. These new technology-assisted possibilities for data analysis are most effective when the underlying data has been effectively governed and cleaned of digital debris.

If effective IG is in place, some of the many benefits of defensibly disposing of digital debris include:

- **Reducing both litigation and production costs:** In the 2012 RAND Report, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery,* a study of 35 cases showed the total costs for collection, processing and review of data were "generally around $18,000" per GB. Properly maintained data requires less searching and gathering by staff and less review by counsel.

- **Reduce employee costs:** The management of large data systems, which includes creating and maintaining on-site and off-site backups, takes considerable time. The nightly window available for disaster recovery backups shrinks as each successive gigabyte of debris is added to the ocean. In turn, this adds to increased complexity of performing and completing these tasks. Reducing the debris gives back these resources.

- **Reduce Total Cost Ownership (TCO) of storage and IT infrastructure**: The costs and time spent maintaining redundant servers and backing up digital debris, while supporting outdated applications can be reduced.

- **Reduce litigation and compliance risk**: With unnecessary information reduced and valued information managed, exposure to risk based on regulatory obligations decreases. Also, less data and hardware storage means less risk of cybersecurity breach.

- **Create more business value using big data and analytics**: With useless data minimized, the business can obtain more analytic and predictive value from their enterprise information and invest in more innovative areas.

Section III, below, will discuss methods of implementing an IG program in greater detail.

What are the roadblocks to achieving Information Governance and disposal?

In spite of the measurable cost and risk-reduction benefits of a properly executed IG program, many organizations still fail to adequately fund, empower or even to staff this function. Most organizations suffer from many of the following roadblocks to IG:

- **Difficulty in distinguishing digital data debris from useful data:** Good content hides data debris and vice versa. No one creates content intending to create debris but little content remains "good" indefinitely. Finding debris contained in a specific folder or file can take much time and effort, especially if hidden within sub-folders. Also what is useful today may become useless tomorrow.

- **Overwhelmed by the amount of debris:** An ocean of digital debris already overwhelms many companies. Daunted by terabytes or even petabytes of unclassified content and having no substantial roadmap towards its classification, these companies elect to keep

the problem on their back burners. Unless cleanup becomes a directed, funded and systemic part of an information governance program, the clutter continues.

- **Lack of awareness and responsibility:** How does someone determine when information is no longer useful? Every organization consists of departments comprised of individuals who often represent competing interests. In turn, each individual has needs for creating and managing information. Multiple stakeholders in the same information may not understand the conflicting priorities of their colleagues. Policies at an organization-wide level likely do not take all information needs into account. Moreover, the organization itself has needs that each individual may not understand in full and is often hampered by outdated, unclear or otherwise flawed policies and guidelines.

- **Data hoarders and futurists:** These two classes of department or employee can be very expensive for an organization:

    - Data hoarders are those custodians who consider all data "good data" (*see* http://ubm.io/1bwOFeo)
    - Futurists believe "we might need it for the future": this leads to the indefinite and unsustainable retention of everything.

- **Siloed information sources:** Independent or quasi-independent operations across the enterprise can result in a lack of coordinated responsibility for identification of information with business value, regulatory obligation, or litigation duty. What data exists in an organization? Where does it reside? How long must the organization retain it? Who owns it? Rarely understanding all of these questions, IT or RIM applies its own policies to data, not always based upon the dictates of litigation and regulatory duties, or in proportion to the data's actual business value.

- **Regulatory & Legal**: Increasingly complex and numerous regulatory requirements – HIPPA, PCI-DSS, GLBA, FINRA, FISMA, Dodd-Frank and similar – demand proper management and extensive oversight of data, especially for organizations whose data spans numerous regulatory bodies or who are international. Policies created outside of a coherent IG framework, even those well-defined on paper, may not satisfy these requirements, especially when they are competing. A disorganized or non-existent IG program exposes the organization to great expense and, potentially, great risk.

- **Risk aversion:** The financial consequences of indefensibly deleting data that could be subject to regulatory or legal obligations are significant, increasing the tendency to keep everything. When reasonable anticipation of litigation exists, organizations must retain any data potentially relevant in any action between the parties. While the "reasonableness" factor ensures that application of this principle to each case turns on its

own unique circumstances, certain efforts must be made. Organizations must issue and review written legal holds, conduct focused data collection, and preserve the data of key stakeholders. Too often, however, these efforts produce debris. The hold process itself produces debris when, driven by risk aversion holds are first applied too broadly and then are not released with explicit follow-up.

According to a recent eDJ Group survey, more than 96% of Information Governance professionals believe that defensible data deletion is necessary in order to manage growing volumes of digital information. The question is how.

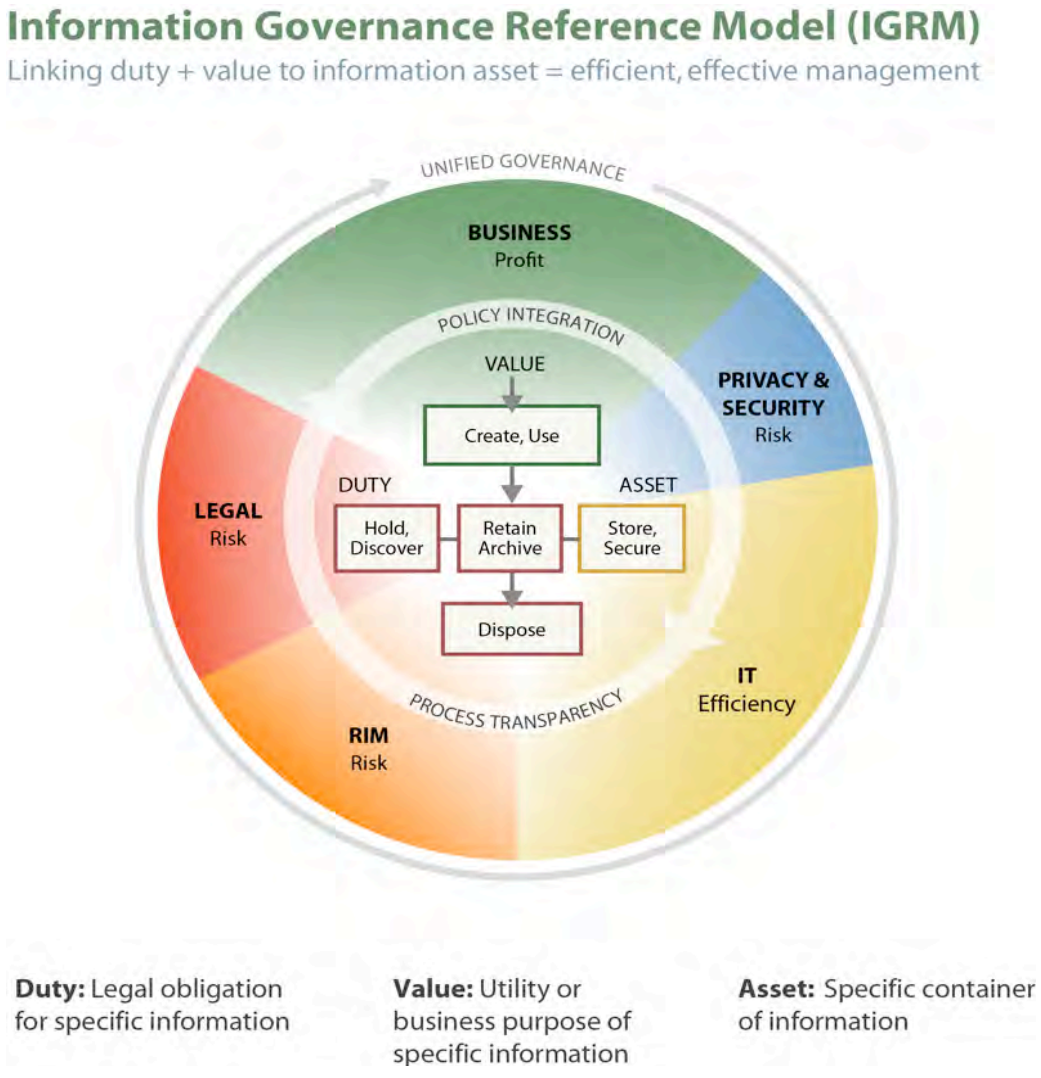
While this white paper cannot prescribe in detail an IG program applicable to all organizations, the next section will describe the IGRM framework as a foundation for the creation of an IG program to help an organization realize the benefits described above.

SECTION II: The Strategy: Leveraging the IGRM to Define a Successful IG Program

The most important step in cleaning up digital debris is to create a coherent Information Governance strategy. However, a recent Association of Information and Image Management (AIIM) report found that fewer than 10 percent of organizations have such a strategy in place.

The IGRM Model

The EDRM's Information Governance Reference Model (IGRM) helps organizations define an effective governance strategy. The IGRM systematically aligns information stakeholders and creates a unified approach to IG people, policy and process. Legal, IT, RIM, privacy, security and business unit stakeholders – all creators and consumers of information – must work together with integrated policies and transparent processes. A key building block is that the IGRM links the concepts of duty and value to data and its stakeholders.



As the model illustrates, unified governance requires stakeholders to make determinations about the duties and the values attached to their data assets.

By applying this model, organizations can reach across corporate silos to meet their legal responsibilities, maximize the value of data, efficiently store and secure required information, and defensibly dispose of digital debris.

An effective, defensible disposal program requires:

- **People**: Leadership and commitment to guide transformational change.
- **Policies & Processes:** Rules, regulations and procedures that link information duties and value to data assets; and information demand to infrastructure supply.
- **Technology:** Tools that enable IT to implement and execute IG policies and procedures.

With the following three-step approach, an organization can effectively begin to reduce both the risk and overhead costs associated with its risky retention of digital debris.

Step one: designate the Information Governance program leadership

Several groups usually share responsibility for an organization's data including: stakeholders from IT, legal, risk management, privacy, line of business, records, and compliance. Critically, to ensure defensibility, this should also include participation with outside counsel. Therefore, a vital first step in developing an IG strategy is to designate, fund and empower a task force, including representatives from each of those groups, to develop the IG program.

This task force should assess business requirements, priorities and practices to determine cleanup opportunities. Once this entity understands the breadth of data stored and the business drivers for its existence, it can define and communicate the criteria for retention or disposal of information. Then, the task force can draft unified protocols and acquire and implement technology.

Each group will offer a unique and invaluable perspective on IG:

- **Business units**: To assess the value of the data, the business perspective is essential. Employees created this information, so their input is critical in determining the original and ongoing business need for it. Challenges to defensible deletion within the business units stem from dual tendencies to hold on to everything indefinitely while emphasizing the importance of recent data.
- **Information Security, Privacy and Compliance**: IS and compliance perspectives should guide an access and vulnerability assessment. Both high value data for retention and debris for disposal must be evaluated from a privacy perspective. Security must

persistently audit employee access levels and privacy obligations. An IG policy that does not include IS contributions will not succeed.

- **Privacy:** The privacy group has policy requirements for protecting access to certain types of data based on the organization, the industry and on regulations governing the data. The privacy assurance team must understand each of the other groups' governance policies so that they can balance accessibility with security.

- **Legal**: The legal department must assess risk and identify content that may be harmful to the organization if it is not preserved or protected appropriately. Also, the legal department must provide legal hold visibility to other information stakeholders, in order for them to do their job while minimizing legal risks. Targeted content deletions can effectively preserve litigation content while reducing costs, headaches and complexity, if the input of legal stakeholders is heeded.

- **Records Management**: Since Records Management (RM) usually owns the corporate schedule for retention and deletion, a natural extension of their role would be management of the IG calendar. They can expand the existing schedule to include all ESI along with paper. The schedule could include descriptions of the business value of each asset, so that it is transparent to stakeholders. Also, RM can suggest and implement naming conventions, retention categories and de-duplication procedures.

- **Information Technology**: IT has the responsibility for maintaining the infrastructure to store all data (including digital debris) and the cost of managing it. If defined, this includes executing agreed upon IG policies covering retention and disposal. Therefore, IT must be given all the visibility and access it needs to determine where in the new framework a data asset falls. And finally IT needs to vet any technology needed to implement IG prior to its purchase to ensure it can deliver, execute and support**.**

Step two: create or improve Information Governance processes

The IG committee should review all existing policies and procedures concerning the disposition of data. This in itself is often a major task. In order to understand the challenges and to communicate a solution, the task force must first ascertain what already works within the information ecosystem and what does not. For instance, this committee should look beyond departmental verbiage and habits to identify common classification and data retention models already in place.

After examining these workflows and the data habits of business units, the committee should then begin the process of writing policies and procedures that govern this content going forward.

An example might be to start with policies and procedures to perform data triage for high value and risk content. For example, the preservation of prior art, used as a source of content for patent creation and future defense thereof. Other examples might be contracts, critical business agreements and present high value business initiatives. High risk data might include that previously the subject of discovery in litigation. Also, it is often it is easier to put in place forward-looking plans and implement these first, before stepping back to deal with the existing digital debris.

Throughout this step, the task force should keep in mind its central goal: the automation of repeatable and defensible processes for defining legal, records, and business information retention schedules.

Ideally, identifying technologies that support auto-classification of data and automation can help ensure the maintenance and proper securing of data required for litigation and regulatory obligations, while the organization keeps its data stores nimble and accessible.

Step three: put technology in place to support the initiative

Most organizations have records management policies in place, but only on paper or on a public website. Unless organizations go beyond simply publishing policy and instead actually implement it, no defensible disposal program can progress.

It is important to note that within this framework, step three regarding technology is step three for a reason. Often an organization's default behavior when facing data overload, is to throw technology at the problem, before there is an understanding of the overall problems to be solved. With IG, it is critical the stakeholders first identify priority content and then determine how they want to protect or dispose of this. Technology solutions that can support these requirements should then be identified.

Leveraging the growing wealth of technology available today, organizations can automate legal holds, records retention, de-duplication, storage tiering, and deletion of data with no business, legal or regulatory value. To simplify overall implementation, it is desirable to use technologies that support a number of these capabilities within a single platform.

Ideally, the chosen technology platform must also provide a central catalog itemizing the classes of and sources of data of end-users. Policy makers in legal, records, business and compliance must be able to view, understand and share this catalog.

With the people, policies, processes and technology in place, the organization must execute. In Section III, we provide an overview of the CGOC framework and discuss how to use it to operationalize such an information governance program.

"As a member of CGOC for many years, and someone who really believes in a holistic information governance strategy, I've spent most of my career as a records management professional building a program that is based on the IGRM model. I'm a true believer that it is not a "one size fits all" approach. However, if you ignore the fundamental elements of what ties a program together – a strategy that brings all the relevant people and business processes together – you will find yourself hitting brick walls along the way.

To give a real life example that illustrates the importance of this statement, there was a time that I presented an ILG strategy to the head of Technology that focused on reducing the volumes of data that had exceeded its retention obligations and had no business reasons to keep. I stressed the importance of storage capacity reaching insurmountable levels, the risks associated with keeping more information than was required for legal and regulatory reasons and, most important, the significant cost reductions that can result in this effort. Suffice it to say, the strategy was approved instantaneously and we set out to achieve this goal. What I did not realize at the time was that the support I received from a very senior executive sponsor of the Company was only the beginning. In fact, every senior executive who was either a stakeholder or an enabler needed to buy in to the strategy – not just nod their heads in agreement, but actually agree to collaboratively work on a set of objectives and deliverables to achieve this goal.

After realizing this important step, we regrouped applying the same strategy and set of business processes with assigned resources, executive sponsorship and a commitment to work together toward the end goal.

If I can share one bit of advice, it's this: Don't try to boil the ocean. Go after one area at a time. The area you pick will be based upon a number of factors evaluated by your own organization. What works for one company, might not work for another, but overall, the end goal is the same for everyone!"

- *Lynn Molfetta, Global Head of Records Management, Citigroup;* the opinions expressed in this article are those of the CGOC Practitioner, Lynn Molfetta, and not necessarily those of Citibank or its affiliates.

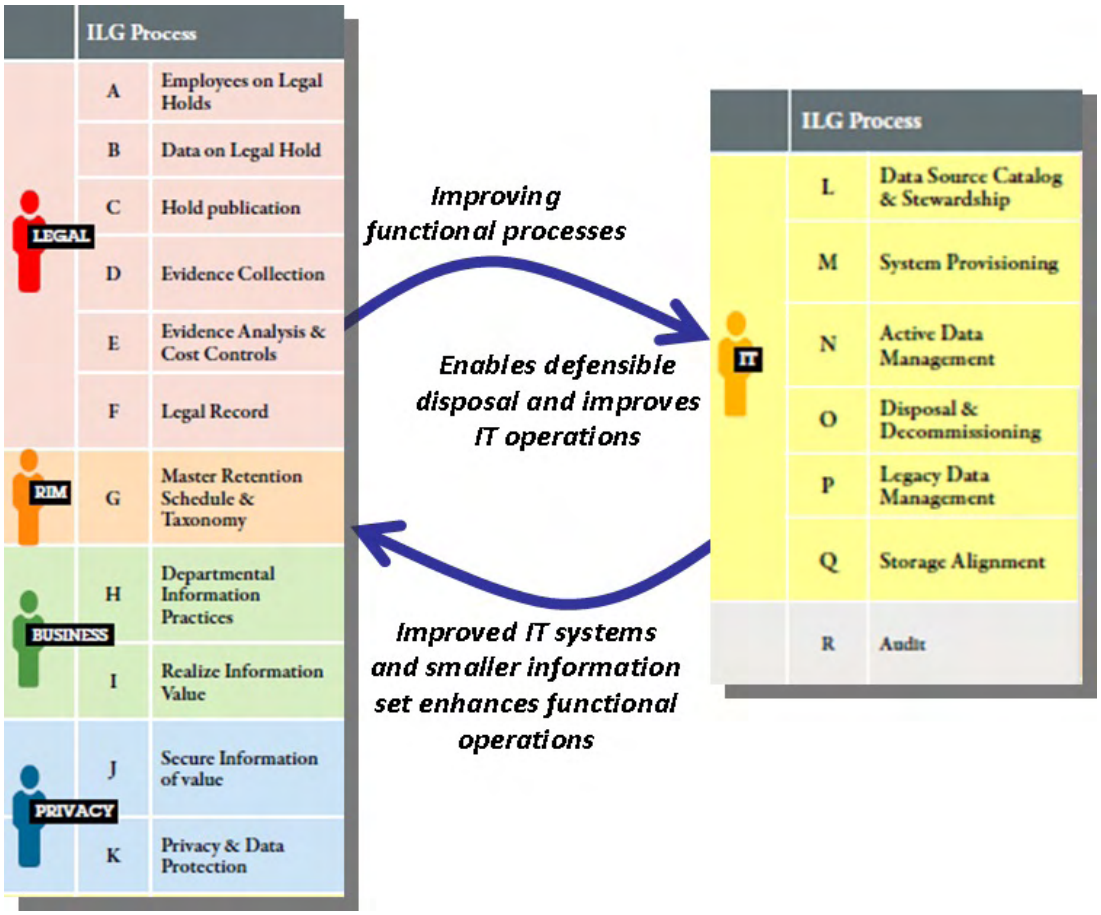
SECTION III: How to Put the Strategy into Practice with Success

The journey to implementing effective information governance begins with a detailed assessment of the maturity of the organization's existing governance processes. From there, it can identify the steps necessary to achieve its IG end state.

Integrating people, process and technology

The CGOC corporate practitioners adopted the IGRM model as the strategy and leveraged it to further detail how to operationalize an IG program. The CGOC community developed the Information Governance Maturity Model (IGMM) to substantiate the processes necessary for a robust governance system that crosses the primary set of stakeholders. These processes are integral to the quality of governance operations and impact the functional roles of legal, records, IT, privacy and business units.

Evaluating how these processes are currently addressed surfaces gaps that help the IG program team understand areas where operational and financial efficiencies can be realized. Assembling the cross-functional team with the full support of an executive champion is of utmost importance to its success. The chart below outlines the characteristics of a program's level of maturity based on the CGOC IGMM.



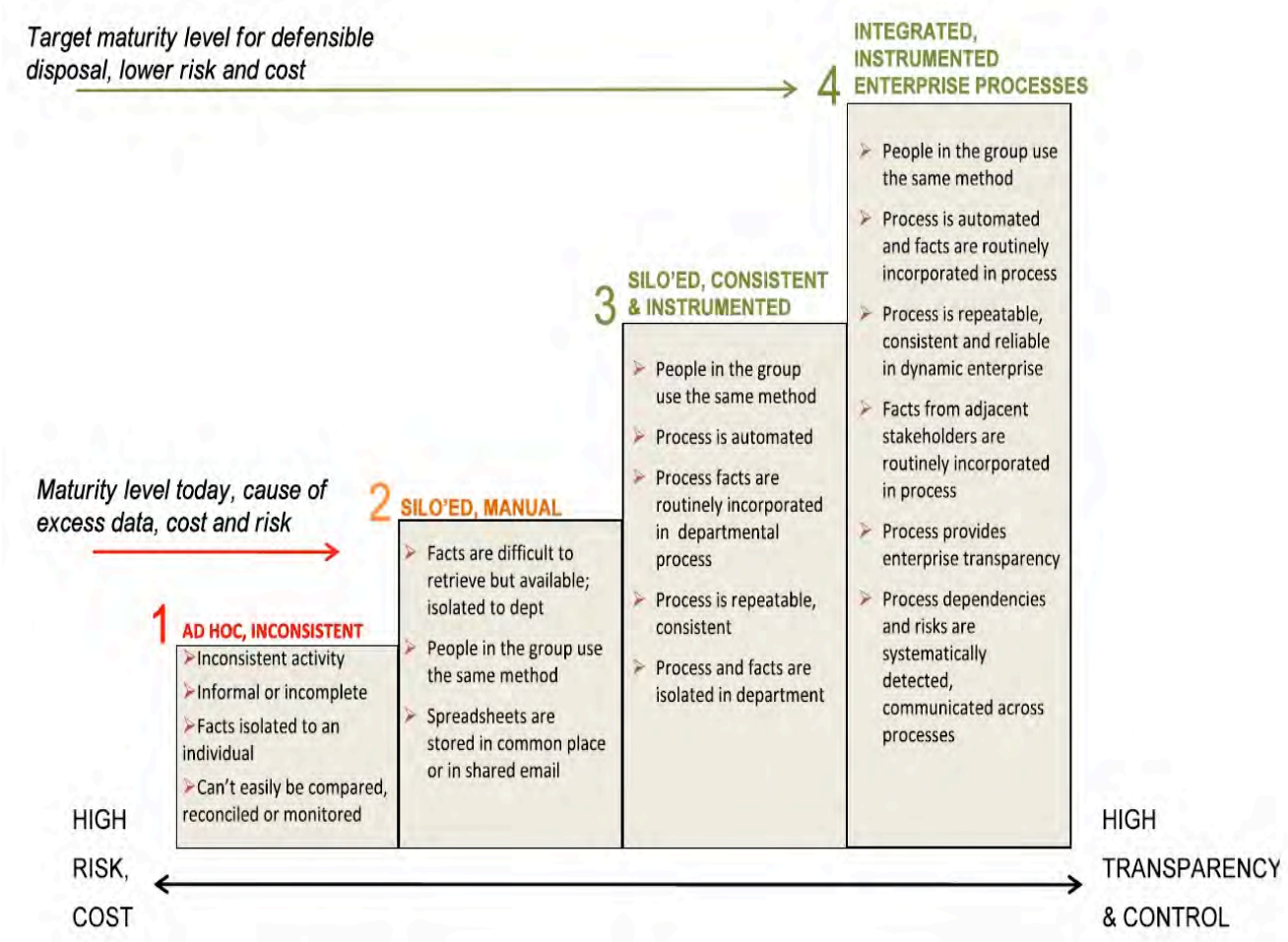
Highlighted are eighteen essential Information Lifecycle Governance (ILG) processes, which affect one or more stakeholder groups and provide a means of facilitation of an IG program. (More details can be found at CGOC.com)

There are four levels in the maturity model:

- **Level 1:** The least developed organizations practice only ad hoc processes. These are inconsistently implemented and create significant risk and costs in response to regulatory audits or litigation.

- **Levels 2 and 3:** More mature organizations demonstrate some consistency in managing information. The two levels are differentiated from one another by whether or not their processes are automated or spreadsheet driven. They are differentiated from Level 4 by the degree to which they are siloed within individual departments or lines of business.

- **Level 4:** The most mature IG programs take an enterprise view and effectively work across stakeholder groups through integrated processes, systems and communications.



An organization does not simply follow a straight line from a state where facts are difficult to obtain and groups use different methods for governance (Level 2) to a state that is automated, consistent and provides ready access to facts (Level 4). Processes and systems will require iterative review and update. Many organizational habits will need to change. The process and workflow integration in the IG program provides a basis for assessing the effectiveness of the overall governance solution.

The assessment process will reveal the interdependencies of the individual stakeholders and requires them to learn to work together to solve this shared problem. Armed with the awareness gained from this exercise, the organization can design a complete a detailed plan that can be executed with defined protocols of measuring performance.

The metrics used will depend on the organization and its culture. Some will be primarily interested in cost and time reduction, for instance, while others will be more interested in measuring risk. All organizations will benefit from the resulting integration of people, process and technology.

Collaborating with and across each of the IG stakeholder groups is critical to enabling the disposal of data in a defensible manner. Integrating key processes and information flow in Legal, RIM, Privacy and lines of business with IT allows a shared view of data policy, ownership and management. With this integration, the IT team can more effectively protect information and respond to legal, regulatory and business demands.

With the improved visibility provided through these revised practises, defensible disposal of digitial debris becomes possible, delivering efficiency in IT. This, in turn, transfers to other stakeholders as a reduced, high-quality data set ready for e-discovery, lifecycle management, analysis and business use.

A central data store that includes records and legal policies, as well as an inventory of IT systems where data is kept, provides the necessary openness while also enabling more robust audit trails needed to defend any disposition. As we integrate people, policies and processes, technology should support these efforts to automate. Technologies exist in the market space today which can help.

For more information on how organizations can reach their information governance program goals, we suggest readers should look into what their peers are doing by visiting the CGOC site, www.cgoc.com

A benefit of the holistic approach – recognizing stakeholder interdependency

The key here is that no one stakeholder can do this alone. All IG stakeholders can benefit and contribute to this holistic approach:

- **Records management** can provide IT with a master retention schedule and taxonomy for important organizational data. Access to policies defined in the master retention schedule

gives IT an understanding of the type of data to be retained and identifies how to classify unmanaged or legacy data according to the taxonomy. Determining the business value of data will vary across organizations, industries and individual business units, as will governmental rules and regulations.

- **Legal** is able to review content narrower applicable data sources without prolonged searches, identify data for legal hold, publish notifications and then begin the process of collection. Legal can provide a list of employees placed on legal hold to IT allowing it to identify the relevant data sources and prevent changes to or deletions of the data.

- **Line of business** users can identify the information it creates and its value and make it visible to IT, with clearly designated retention schedules from the Line of business viewpoint. Once the business stakeholders have identified and classified data important to their business needs, it becomes possible to ensure this data is managed based on their individual policies. In return, lines of business can access information on demand and apply big data analytics to gain a competitive advantage.

- **Privacy and security** can now ensure requirements are met with regard to organizational, industry and regulatory obligations. The privacy assurance team can better understand each of the other groups' governance policies so that they can balance accessibility with security.

- **IT**: With this improved visibility from all stakeholders, IT can finally manage information based upon business value and duty, whether legal or regulatory and defensibly dispose of digital debris. With these insights, IT can effectively manage its infrastructure environment across the enterprise and make quality information available across the enterprise.

This is the win-win picture for everyone in the digital era.

Conclusion

Organizations are drowning in digital debris. Employing EDRM's Information Governance Reference Model (IGRM) in conjunction with the CGOC's Information Governance Maturity Model (IGMM), organizations can define their information governance strategy, initiate an information governance leadership program, improve processes, deploy technology, and put the strategy and technology into practice.

With an effective information governance program, companies can link information value and duty to information assets, get rid of digital debris, and improve information and litigation economics. Only an information governance program that is in operation can enable companies to maximize the business value of their "Big Data" and defensibly dispose of digital debris.

About CGOC (Compliance, Governance and Oversight Council)

CGOC is a forum of more than 2600 legal, IT, records and information management professionals from corporations and government agencies. CGOC conducts primary research, has dedicated practice groups on challenging topics and hosts meetings throughout the U.S. and Europe where practice leaders convene to discuss discovery, retention, privacy and governance. Established in 2004, it fills the critical practitioners' gap between EDRM and The Sedona Conference. For more information, please visit https://www.cgoc.com.

About EDRM (Electronic Discovery Reference Model)

EDRM creates practical resources to improve e-discovery and information governance. Launched in May 2005, EDRM was established to address the lack of standards and guidelines in the e-discovery market. In January 2006, EDRM published the Electronic Discovery Reference Model, followed by additional resources such as IGRM, CARRM and the Talent Task Matrix. Since its launch, EDRM has comprised 269 organizations, including 173 service and software providers, 68 law firms, 3 industry groups and 24 corporations involved with e-discovery and information governance. Information about EDRM is available at http://www.edrm.net.