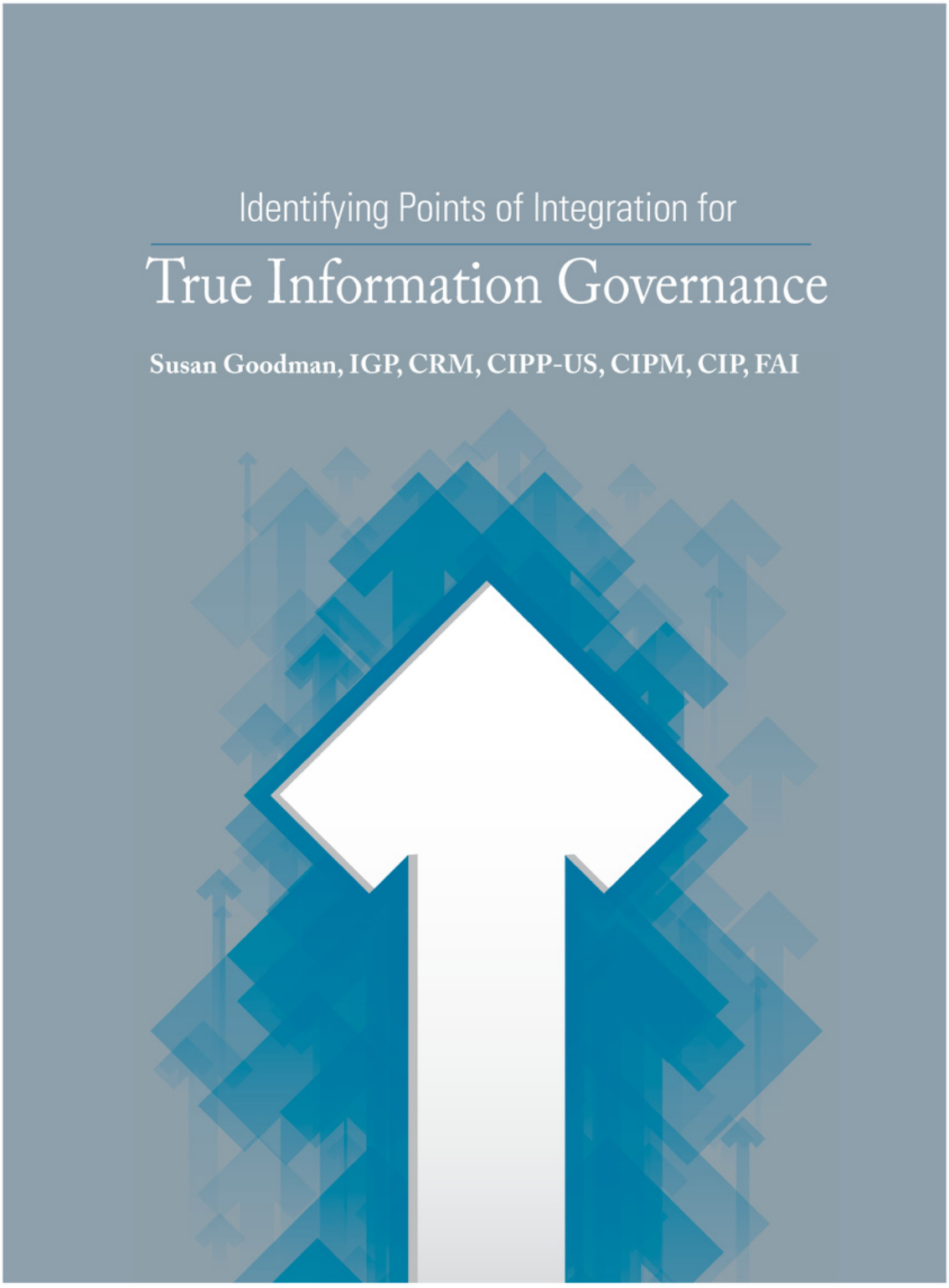
FELLOWS FORUM



True information governance (IG) integrates all applicable elements of its component functions – records and information management (RIM), legal/compliance, information technology (IT), information security, privacy, and business units – within the IG program's overarching structure.

True IG also enables the success of each of its component functions – and of the organization itself – because these functions are enterprise-wide and have overlapping, interrelated, and interdependent systems. By way of example, privacy goals related to compliant information lifecycle management (ILM) (e.g., collection, use, and disposition) and to data security are dependent on effective integration with legal, RIM, IT, information security, and the business units.

To get executive support for a truly integrated information governance (IG) program, IG professionals must be able to align the IG strategy to the organization's goals, depict the program's overarching structure, and describe the necessary functional integration. This article suggests the points of integration among the IG component functions for two areas: legal preservation/records holds and information lifecycle management.

This is why establishing a formal, well-integrated IG program is key to an organization's ability to:

- Enhance legal, regulatory, and policy compliance
- Reduce risk
- Increase cost effectiveness and efficiency
- Improve competitive advantage through optimally leveraged information assets

The IG Program Initiative

Garnering support from executives, management, and staff for an overarching IG structure can be challenging in organizations where an IG culture doesn't yet exist. This is because component functions typically have different reporting lines, separate budgets, and entrenched, insufficiently interfaced infrastructure elements for which substantial resources have already been invested.

Organizational leaders must believe in IG, understand and feel comfortable with the changes needed to institutionalize it, and make the initiative a priority for a true IG program to be successful. This means that IG professionals must be able to depict the overarching IG structure (i.e., what this will "look like"), describe the necessary functional integration, and define the requirements for the program.

When developing the IG program business case, charter, mission, project plan, budget, and communications, it is imperative, then, to explain the need and engender buy-in for an infrastructure that is integrated by design. Initiate the program by taking the following steps.

1 .Appoint a Leader

Some organizations have begun to establish the role of IG director or an equivalent title; this could be the person to lead the initiative. Whatever the title, the person leading this effort should embody the description of a certified Information Governance Professional (IGP): a person who – according to the IGP certification material – "has the strategic perspective and the requisite knowledge to help an organization leverage information for maximum value while reducing the costs and mitigating the risks associated with using and governing this important asset."

The leader should actualize the IGP competency of "Establishing IG Business Integration and Oversight" by aligning the IG strategy and program to the organization's goals, needs, and objectives. This requires, according to the competency description, working closely with business units to determine the steps for implementing the IG program in their divisions, as well as regularly monitoring and auditing their performance to confirm compliance and to ensure that the IG program isn't impeding the organization's business goals. The leader also must ensure the needed integration among all the IG functions mentioned above.

2. Choose Team Members

Establish a cross-disciplinary IG team to promote, guide, oversee, acquire resources for, and otherwise support the IG initiative and arrange for necessary work to be conducted. Configure the team in a way that makes the best sense for the organization, but include – at minimum – decision-making representatives from all IG component functions: RIM, legal/compliance, IT, information security, and privacy.

Business units could have direct representation on the team, too, through liaison relationships with team members, for example, in which case it is advantageous to choose business liaisons who have responsibility for one or more IG functions in their business unit.

3. Determine Areas for Integration

The IG team must reach consensus on the desired IG target state, as well as strategies for planning, designing, developing, operationalizing, and sustaining an integrated IG program.

Use the IGP DACUM chart (available at *www.arma.org/docs/igp/dacumchart1012.pdf*) as a core resource. Consider the key program elements within each component IG function (and business equivalents affected by them) for integration. Include, for example:

- Risk and compliance management
- Strategic planning
- Governance (structures, processes)
- Budgets (for functions, departments, and the enterprise)
- Policies, procedures, and process/information flows
- Staffing expertise and resources
- Accountability (roles and responsibilities)
- Technologies (functionality, interfaces) to support IG
- Relationships (intra- and inter-departmental, direct, and dotted line)
- Training (content and routines)
- Communications/messaging
- Monitoring, audit, enforcement, and reporting
- Methods and processes for IG program design, development, and implementation (e.g., systems and process analysis, project approval, management, and change management)

The following sections focus on points of integration for two areas that have particular relevance for all IG component functions: legal preservation/record holds and ILM.

Legal Preservation/ Records Holds

Departments that issue legal preservation/record holds (holds) typically rely on RIM, IT, business units, and other support functions to ensure that the holds are placed, maintained/managed, and released in all locations (e.g., servers, active file areas, electronic directories, third-party custodians). Assuming a well-established RIM program is in place, centralizing within RIM the enterprise-wide responsibility for ensuring compliance with hold requirements is the ideal way to forge a well-integrated, consistent, and compliant process. In the suggested scenario below, RIM would work under the direction and guidance of the issuer (e.g., the attorney responsible for the matter), who has legal accountability for holds.

RIM

RIM works with the hold-issuing entities to review and update policies that pertain to holds (e.g., legal discovery protocols, business policies) for inter-departmental consistency and currency. RIM also works with business units to document their step-by-step procedures.

> . . . hold-issuing department's policies should require that all hold notices be transmitted to RIM, in addition to custodians of potentially relevant data.

The policies (e.g., discovery protocols) and hold management instructions of each hold issuer (e.g., legal department) ensure that RIM and other affected parties are appropriately and consistently engaged. For example, each hold-issuing department's policies should require that all hold notices be transmitted to RIM, in addition to custodians of potentially relevant data. This enables RIM to ensure compliance.

RIM works with hold-issuing departments to establish clear criteria for hold release. Holds related to litigation, for example, can often be linked to a period of time after case settlement and exhaustion of statutes of limitation related to appeals. Release of holds related to regulatory inquiry/investigation can be more complex to determine. When effective hold release procedures for attorneys are in place, legal can issue release notices quickly, notifying affected business units and RIM so RIM, IT, and business units can perform their duties related to ILM.

Information security and privacy's policies, procedures, and responsibilities should document their:

- Review of retention schedules and inventories to identify and document personally identifiable information (PII), protected critical

infrastructure information (PCII), and security classifications

- Responsibility to provide RIM, legal/compliance, IT, and business units the privacy and information security requirements for managing PII during the legal hold and production processes

RIM's policies, procedures, and responsibilities should reflect the same.

RIM and Hold-Issuing Departments

Concurrent with the above, RIM and the hold issuer (e.g., legal) work together to refine the hold requirements using RIM-provided record retention schedules for descriptive information. Legal should also provide additional context for each hold (e.g., other responsible attorneys, locations affected, date range for the information – including whether future data is to be held).

RIM, Legal, IT, and Business Units

As dictated by the issuing attorney, RIM (through records liaisons) sends additional instructions to IT and the business units that are holding information relevant to the hold. Each has responsibility for placing, managing, and releasing the information upon official notice from the hold-issuing party.

Hold-Issuing Departments

Hold-issuing departments' policies should require that a formal hold (with a new matter number) be placed for each new matter that requires data preservation; it must not rely upon existing holds to serve that purpose, as this makes releasing the existing hold nearly impossible and too resource intensive.

RIM and IT

RIM and IT should assess technologies related to the hold process to identify hold metadata collection, functionality, and application interfaces to optimize information leveraging, reduce risk, and increase efficiencies.

They should also work together to customize the RIM software's hold module, if needed, so it interfaces with legal's matter management system's preservation notice module and with the applications the business units use to track holds. Using an integrated package, rather than separate applications for hold management, would be ideal.

These changes typically require a major culture shift, but many litigating attorneys welcome enhanced processes that will make their jobs easier.

IT, RIM, and Business Units

IT, RIM, and business units interface to identify the systems and applications containing data subject to the hold to enable IT (and business application owners) to implement and manage the hold and RIM to track it. This may require integrating metadata about systems (e.g., IT application directories) with departmental records inventories and retention schedules to glean needed information efficiently.

For instance, IT needs information from legal and RIM about the departments/functions that are affected by specific holds and where the relevant data may be found (e.g., applications that manage specific electronic content and the departments with which they are associated).

Policies and procedures in RIM, IT departments, and business units should reflect their collaboration and use of records/data inventories and technology/application inventories to pinpoint relevant data systems and locations.

RIM and IT should assess technologies related to the hold process to identify hold metadata collection, functionality, and applicaton interfaces...

All Affected Departments

Affected departments should have processes in place to provide RIM with reports on hold compliance. RIM should aggregate this data, measure it against metrics, and report all data needed to the hold issuer (e.g., legal) and the IG team.

Having integrated, comprehensive, and effective policies, procedures, and technologies for holds, per above, provides valuable data and enables metrics to be used to enhance compliance and reduce risk and costs for legal holds and discovery. Additionally, aggregating details about specific matters related to which information was determined to be relevant/valuable (and which information was not) can increase the effectiveness of the discovery process for future matters, thus creating potential advantage (e.g., litigation wins, reduced fines) for the organization.

Information Lifecycle Management

Effective ILM – from creation or collection/receipt to use, management (e.g., transfer, storage), and disposition (i.e., transfer for long-term protection or destruction) – is dependent on all organizational entities applying the relevant IG policies, procedures, standards, and guidance. Because these processes are non-linear, iterative, and complex, especially for electronic data, there are many points of integration that will provide maximum benefit.

The hold responsibilities mentioned above, especially the release of holds, are intrinsically connected with the ability to oversee and perform ILM. This is because when information is not disposed of after its retention requirements have been met, risk and cost are typically increased. For example, the cost of litigation increases because all relevant information must be produced for discovery even if it could have been disposed of legitimately prior to legal discovery.

The following scenarios represent several recommended points of IG integration for ILM.

RIM, Privacy, and Information Security

As mentioned above, privacy reviews all RIM processes and retention schedules to identify PII. Information security provides security classifications for listed records – including PCII. These, and specific requirements, are reflected in RIM's retention schedules. Conversely, privacy and information security procedures reference the records retention schedule, which addresses privacy requirements and considerations. When there are conflicts in retention requirements, privacy and RIM reach consensus about the appropriate disposition and document it for defensibility, in order to reduce risk.

RIM and IT

IT needs information from RIM to know when it is permissible to dispose of data. This should be a welcome collaboration, as disposing of obsolete data supports an IT goal to increase operational cost-effectiveness through: reduced back-up requirements and the need to purchase additional servers; increased efficiency in managing data for backups, migration, e-discovery, and other processes; and more strategic use of IT capacity and expertise, which also provides competitive advantage

RIM and Business Units

The enterprise is reliant on business units to implement records disposition and on RIM to enforce it.

RIM puts processes in place for organizational entities (businesses, internal oversight, and support teams) to identify potential secondary and additional uses for information assets they maintain, are responsible for (including third parties), or could collect as part of their work.

RIM also captures recommendations for enhanced data collection and use during inventory and retention scheduling processes for ILM.

RIM, IT, and Business Units

Business units must know what information exists within the department and across the enterprise that could create new business opportunities if it were shared. For instance, results of surveys conducted by one business unit could provide valuable marketing information for another business entity. These potential opportunities are reliant upon RIM, IT, and their business inventories and directories to provide this information.

IT, therefore, ensures that the systems they develop and administer include requirements (e.g., fields, data analysis capability, reporting, interfaces with other applications) to enable organizational entities to better leverage information assets.

All IG Components

All IT applications and business projects are reviewed to determine if PII is included in any stage of the business process and, if so, undergo a thorough privacy review to ensure compliance with privacy requirements. Similarly, information security reviews IT projects to ensure compliance with all information security requirements. Finally, all stakeholder IG functions review and approve information security questionnaires (or equivalent) and vendor responses.

All of these processes should be consistently documented across applicable functions and – to the extent possible – automated.

The IG Professional Imperative

IG professionals have a responsibility and opportunity to provide leadership in establishing and sustaining a truly integrated IG program – one that reflects collaborative efforts among all IG component function across the enterprise. Success begins with their ability to demonstrate to executive leadership the value of having an overarching IG structure that supports and contributes to the optimal success of each IG function, to business units, and to the organization as a whole.

About the Author: Susan Goodman, IGP, CRM, CIPP-US, CIPM, CIP, FAI, is the chief privacy officer of the City of Seattle. She has directed and had other key leadership roles in IG, RIM, and privacy programs across diverse industry sectors, in-house and as a consultant. She is a frequent speaker and author and former RIM adjunct faculty member. Goodman can be contacted at *suegoodman.infogov@gmail.com*. Note: The views expressed in this article are the author's and do not represent those of her employer.