SERIES FOUR

Information Governance Essentials for the Emerging Life Sciences Company

Information Governance (IG) is generally thought of as the processes, policies, and software solutions needed to manage data and content across a business. More formally, Gartner's IT Glossary defines it as "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."

Having these capabilities from the outset to manage an organization's information assets would seem reasonable and necessary, but an IG program is typically not high on the list of priorities for emerging life sciences companies. Data and documents are often acquired, processed, and stored without ample regard to how they will be controlled and managed in the future.

Given the weighty definition above, it's easy to understand why some may view IG programs as costly, complex, and/or resource intensive, or that their companies are not large or sophisticated enough to warrant a formal IG effort. But the reality is that governance becomes more complex and expensive to reign in the longer a growing company goes without it. While a large, full-fledged IG program is not needed initially, investment in a few foundational governance disciplines and practices and adds significant value by:

- *Reducing regulatory compliance risks and expediting preparation for PAIs.*
- *Ensuring controls are in place for data security and privacy.*
- *Streamlining clinical trials and submission processes.*
- *Integrating and managing data from partners and 3rd party providers.*
- *Increasing user productivity through better access to information.*

A "right-sized" IG program for the smaller company does not have to be expensive or intrusive and can serve as a foundation for more formal governance practices that can evolve over time in digestible, incremental phases.

The Common Scenario

Through its formative years, an emerging life sciences company's sights are rightfully set on research and development of its therapies. Creating a structured operating model (including IG) is less of a priority that tends to evolve incrementally as the company grows. During these early stages, most companies rely heavily on contracted third parties to

support research, clinical, pilot manufacturing activities and as well as corporate functions, including IT and HR. Companies in this stage are often engaged in partnerships that involve sharing of sensitive information and intellectual property with other organizations.

As a result, information assets are typically managed by multiple parties with a variety of platforms, often externally through vendor-provided point solutions (e.g., lab notebooks, clinical systems, document management, CRM) as well as internal shared drives, team rooms, and email systems. While some consideration may be given to future integration, the company's primary attention is on advancing the research and development where third-party point solutions and services provide adequate support.

As R&D progresses, the company builds out new functional areas and business processes to manage upcoming submissions and commercialization. New staff and vendors are onboarded in anticipation of the upcoming launch; activity rises to new levels and information volumes increase dramatically – as does the need to share information across a broader set of stakeholders, both internally and externally.

As R&D concludes and submission and commercialization milestones approach, the volume of data and information increases dramatically, along with the number of parties involved and the solutions and platforms in use. Business users across the company are faced with multiple challenges to create compliant, auditable submission dossiers; properly secure intellectual property and sensitive information assets; and ensure that critical assets within the growing volume of information are easily located, and readily available to the growing user base. Often, by this time:

- Departments have engaged and are exchanging information with multiple external organizations,
- Data and information assets are spread across multiple locations and platforms,
- Multiple copies and versions of information assets may exist in multiple locations,
- Inconsistent and/or inadequate methods are used to handle critical and sensitive data, and
- Standards for data security, privacy, quality, and integrity are either lacking or not enforced across the technologies and platforms in use.

Too often the growing amounts of information that the emerging company and its partners produce and consume during the development phase are not properly governed. As a result, businesses may experience sub-optimal productivity, quality issues, and/or increased exposure to regulatory risk. Although the need for governance policies, processes, and standards becomes readily apparent during this period, most would agree that it is a very inconvenient time to undertake a governance program given the added regulatory scrutiny and pressures that business users face in their day-to-day activities. Without basic governance capabilities in place (when they're needed most), meeting these challenges becomes more formidable (than they already are), and often lead to schedule delays and compliance risks.

A Little Goes a Long Way

With some attention and investment focused on establishing basic IG capabilities during its formative years, a company can easily weave sound information governance awareness and practices into its cultural fabric and alleviate many of the common issues that governance-deficient organizations face. A IG program can be initiated at any time, but incorporating a few governance fundamentals early in a company's evolution pays important dividends later in terms of information and data integrity, security, quality, risk management, and productivity throughout the organization.

While a basic IG program can help to minimize compliance risks, it also provides other benefits to a growing company by ensuring that all employees follow the same policies for managing the company's information assets in classifying, handling, securing, and properly storing information assets for sharing and future use. When exchanging information with third-party service providers, defining and following a few basic policies and procedures can ensure all vendors meet certain baseline qualifications that lessen the risks of compliance violations, security breaches, data loss, unauthorized access, and substandard quality. As activity spikes and new service and solution providers are hired, the company can be assured that vendors who handle company information have been properly vetted, enabling timely integration of their solutions and services to support the business' needs.

Getting Started

The IG early program has the best chance for success if it is lightweight, relatively inexpensive, presents minimal disruption for business users, and can demonstrate results in a critical problem/risk area. The initial IG program centers on developing a core set of IG disciplines, practices and processes. Getting the program started involves forming a working group or "core team," defining core IG policies and SOPs, and identifying appropriate information domains for initial governance – usually critical ones that present compliance, productivity, or quality risks.

The IG Team

A common challenge in initiating the IG program is determining who will be involved. Because of its information-centric nature, the IT function is typically most suited to drive the initial IG effort. Leadership from an experienced IT resource is essential in the early stages. An experienced resource provides critical understanding and technical perspective of the regulations and complexities involved in architecting and implementing the necessary data security, privacy and compliance processes and solutions. The smaller, emerging company that doesn't have an IG-experienced resource on its IT staff should consider engaging consultants who can fill this role to coalesce the initial working group, kickstart the effort, and provide guidance as the program evolves.

The cross-functional nature of the IG program requires participation across the company. Ideally, the initial IG core team consists of members from IT, compliance, and legal along with representatives from business areas involved in the initial effort. While the IT resources can guide the effort and advance it from the architecture and technical perspective, the legal, compliance, and functional business areas provide the business context and perspective that drive IG policies and procedures. Initially, resources from the business groups assist in identifying and classifying information assets, specifying who should have access to information, and defining appropriate IG-related policies and SOPs for information management.

Executive sponsorship is critical to the success of the early program. The executive can help align the IG program to corporate initiatives, champion the program across organization, provide guidance to the core team, secure resources, and assist in resolving escalated issues when needed.

IG Policies and SOPs

High-level policies required for the basic IG program address regulatory compliance (from an IM perspective), information classification and security, data privacy, and CSV. Along with these policies, standard operating procedures (SOPs) can then be developed that describe methods and requirements for ensuring adherence to guidelines set out in the policies. The SOPs define processes, roles, and responsibilities for both company-wide and department-specific levels and serve as the basis for more detailed work instructions.

A full suite of policies and procedures is not required at the outset. The scope of the initial policies and SOPs can be limited to those that are necessary for privacy and compliance; addressing requirements related to 21 CFR 11, GDPR, and HIPAA is often a good starting point.

New policies and SOPs are not always necessary. In some cases, IG-specific considerations can be incorporated to the company's existing policies and SOPs that may already be in place for general corporate governance, IT operations, and GxP compliance. For example, an SOP for contracting third-parties may be augmented to include provisions for verification of adherence to CSV, security, and privacy requirements.

Foundational policies for the emerging life science company (or IG provisions in existing policies) may include:

- GxP data management
- Data privacy
- Vital records management
- Electronic information exchange
- Transparency and disclosure
- Appropriate use
- Records management
- Business continuity

Likewise, examples of foundational company-wide IG SOPs that should be developed early in a program include:

- 21 CFR Part 11 compliance
- Information classification
- Data security monitoring
- 3rd party integration standards & security
- Issue / incident management
- Employee onboarding for IG policies
- Naming and filing standards
- Computer systems validation

Once the policies and SOPs have been developed, it's then a matter of building awareness throughout the company and providing training to employees on their IG-related roles and responsibilities. The roles and responsibilities essentially constitute the beginnings of the company's IG organization and stewardship model that eventually includes role-based accountability for data integrity, security, and privacy, and processes for monitoring, auditing, and ensuring compliance.

Identifying IG Focus Areas

In addition to developing the policies and SOPs early in the program, the core team must also identify the initial set data and information domains that will managed under the IG program. The foundational IG program typically revolves around a specific business area or macro process such as clinical and regulatory submission, manufacturing, supply chain, or commercial distribution and reimbursement.

The initial set of domains for the early stage company are typically comprised of the key information assets that support GxP business processes where auditable lineage, integrity, and security are critical to ensuring regulatory compliance. Domains that should also be considered during the initial phases of the program include those deemed to be highly confidential and sensitive such as intellectual property, trade secrets, financial data, and personnel information.

As a pre-cursor to determining key areas for initial IG focus, companies often conduct a data and information discovery and mapping exercise that produces a categorized inventory of assets and identifies issues, gaps, and potential compliance, security, or integrity risks. Prior to conducting the discovery and mapping exercises, the IG core team should establish rudimentary definitions for data classification and meta-data tagging so that results of the discovery may be better analyzed for potential gaps or risks. For example, producing a list of sensitive assets residing on a certain server that are used for FDA submissions would be useful in determining if that information is properly secured, auditable, and compliant with 21 CFR 11.

Deploying the IG Program

With the definition of foundational policies and SOPs, the core team of stakeholders, and the set of focus areas in place, the IG program can commence with its initial deployment. One of the first steps in the initial deployment is to develop materials that build awareness for the program's purpose, policies and procedures. Materials should include basic training for corporate-level and department-specific SOPs so that personnel are familiar with general company guidelines and policies for managing information as well as the specific accountabilities and stewardship procedures within their business area.

The initial deployment should focus on ensuring that basic capabilities and practices are in place. Users should be familiar with and following procedures for:

- Data privacy and security policy
- Handling sensitive assets
- Exchanging information with 3rd parties
- Classifying and storing information
- Managing copies and versions
- Requesting access to information
- Logging an issue or incident

A set of materials may also be developed may also for third parties that include policies, procedures, and guidelines for data interchange, architecture standards, security, privacy, and other IG-related requirements. These materials are often in the form of contract appendices or exhibits.

Along with building internal user/stewardship competencies and procedures for third parties, the initial deployment may also include remediation of issues identified during the information discovery and mapping exercise. Remediation is typically IT-oriented and can involve relocating or migrating files from shared network drives to new platforms or updating access rights to ensure that information is appropriately protected against unauthorized access or misuse.

Evolving the IG Program

The initial IG deployment provides the company with a foundation that can be built upon and expanded as it is applied to additional business areas and information domains throughout the company. Leveraging the knowledge and experience from prior deployments, the IG core team can continually refine the methods, materials, and tools used for roll out and ongoing management of the program.

IG Organization

As the number of business areas and stakeholders increase, the IG organization will naturally evolve to include additional members, along with more detailed definitions of specific roles and accountabilities. During the early stages of the program, individuals often assume responsibilities and duties for multiple roles. As the company continues to grow, duties and roles can be delegated and reassigned to more appropriate individuals within the organization.

The early IG core team can eventually take on a multi-level structure and grow to consist of a formal governance council, dedicated IG teams for R&D, commercial, and manufacturing functions, as well as various tactical teams and working groups. Tactical teams may be formed to oversee specific domains. For example, a team may be formed to just oversee governance of HCP and HCO master data.

IG Processes

As the IG program evolves, many of the existing informal governance process may become more structured and institutionalized. Issue management is a critical process for an effective governance program. While a rudimentary process may put in place for the initial IG deployment, the process can be enhanced in later phases with better tools for managing issue triage, delegation and escalation, as well as periodic analysis of issue types and resolution. Understanding the trends and nature of common issues may give rise to new processes and strategies to efficiently resolve or proactively manage certain types of challenges related to regulatory compliance, data quality, access rights, or availability.

Realizing the Benefits

A small investment in establishing IG capabilities and practices during the early stages of a company's evolution can reap dividends throughout the life of the company. An initial, "right-sized" IG program can be started at any time but establishing IG capabilities prior to submission and commercialization activities provides several key benefits.

- IG practices and capabilities help reduce regulatory compliance risks associated with information quality and integrity which may result in schedule delays. Governance information (often referred to as metadata) can also expedite preparation for regulatory audits and inspections.
- Foundational IG capabilities can help ensure that information requiring security and privacy is identified and that appropriate controls and access rights are specified and in place.
- Governance processes help streamline critical processes such as clinical trials and regulatory submissions. Business users can readily find and access information. Issues are managed and resolved more effectively and efficiently.
- Data integration and information exchange with parties and third-parties is more easily controlled and managed with IG architecture standards.
- Overall user productivity is increased – users spend less time locating data and more time leveraging it in their day-to-day work.

Next Steps

Companies that have not begun the IG journey should consider doing so by first forming a small working group to look at the short and long-term benefits that can be realized through an IG effort within their organization. As discussed earlier in this paper, a key element to the success of an initiative is having IT leadership with IG experience. Companies that do not have an experienced resource in that capacity or lack the bandwidth to undertake an IG effort should consider engaging consultants who can play this part initially and provide ongoing guidance as the company's organization and processes mature.

About Series Four

We focus on Information Governance services and solutions that help companies:

- Identify and mitigate compliance risks
- Ensure data security, privacy, and integrity
- Improve operational efficiencies
- Drive value from your information assets

Our solutions and services are tailored to the needs of emerging and mid-market pharmaceutical and biotechnology organizations and based in years of experience in architecting and implementing Information Management solutions the Life Science industry.

For more information, visit **www.seriesfour.net** or contact **info@seriesfour.net**

About the Author

Vic Stambaugh is Founder and Managing Partner of Series Four, LLC. He has worked with life sciences companies for over 25 years providing senior-level consulting service to C-level client executives in IM strategy, information architecture, analytics, and data governance. His experience spans for R&D, regulatory, and commercial business functions.