Information Governance
Starting an Effective Program

Also from our online service:
Confidential Witnesses in Securities Cases pg. 34
Class Action Settlement Agreements pg. 16
ITC Investigations Post-Suprema pg. 44
Information Governance
Establishing a Program and Executing Initial Projects
A principle-based approach to information governance (IG) can help an organization address data issues as they arise in a way that benefits the organization and IG stakeholders, and outweighs any costs associated with the initial investment. By understanding the components of a successful IG program, counsel can champion IG strategies that minimize risk and maximize the value of a company’s data.
This article provides an overview of the components of an effective IG program and common IG projects, focusing on:
- The benefits of IG.
- The groups within an organization that are most involved in IG.
- Steps to take to implement an IG program.
- How to prioritize and execute IG projects.

**BENEFITS OF IG**
The hallmark of IG is managing information effectively and efficiently to gain the greatest advantage possible while protecting against negative exposure. An IG program enables companies to achieve, for example:
- Comprehensive, streamlined approaches to business policies and processes affecting information.
- Collaboration within and across business functions to address institutional data challenges.
- Clear decision-making processes that promote enterprise-wide strategic planning.
- More efficient use of organizational resources dedicated to records and information management (RIM), data privacy, information security and litigation responses.
- Greater use of automation to streamline workflows and reduce bureaucratic burdens on end-users.
- A better holistic understanding of company data.
- A dedicated business function focused on the analytical capabilities and opportunities available to extract business value from company information.
- A dedicated infrastructure that is ready to respond to incidents regarding the improper disclosure or management of company information.

Additionally, IG guards against:
- Potential liability stemming from inconsistent company policies and processes regarding data management.
- Siloed approaches to resolving institutional challenges, which do not account for the needs of all business stakeholders and ultimately waste enterprise resources.
- Failures to properly escalate serious issues that require executive-level attention.

**IG STAKEHOLDERS**
Effective IG brings together stakeholders from across the organization. The departments that are typically involved in IG, though to varying degrees, include:
- **RIM.** The RIM department is responsible for proper declaration, maintenance, retention and disposition of company information to comply with applicable statutory and regulatory requirements (see Box, Common Legal and Regulatory IG Standards). RIM personnel may support the legal department with litigation responses and e-discovery. Although it is an essential stakeholder and participant in an organization’s IG program, the RIM function has a narrower focus and should not be expected to carry out an IG program on its own.
- **IT.** The IT team ensures that the systems and devices that employees need to do their jobs are operational. Additionally, IT is responsible for the systems that maintain an organization’s electronically stored information, while other groups own the information itself.
- **Legal.** The legal department is responsible for an organization’s litigation response protocols and leads e-discovery efforts, both of which rely on understanding an organization’s IT infrastructure and RIM policies. The legal group also advises generally on the privacy and confidentiality aspects of data management and oversees contract management.
- **Information security.** Because data breaches and threats from both inside and outside an organization are rising in number, information security is a paramount function for any company with sensitive or confidential data. The information security department:
  - secures information repositories against unauthorized access;
  - provides guidance to employees about optimal practices to prevent misappropriation of company information; and
  - guards against internal threats.

Bad actors within the organization that threaten the company’s security and reputation.
Unidentified deficiencies in company practices regarding RIM, data privacy, information security and litigation responses.
The accumulation of vast amounts of legacy data of questionable value.

IG guards against siloed approaches to resolving institutional challenges, which do not account for the needs of all business stakeholders and ultimately waste enterprise resources.
Common Legal and Regulatory IG Standards

An IG program must account for an organization’s legal and regulatory influences, which vary based on the vast differences in requirements within and across industries and jurisdictions. Some of the most commonly applicable laws and regulations include:

- **The Sarbanes-Oxley Act of 2002.** Auditors of financial statements for securities issuers and investment companies must retain certain records for seven years. This includes working papers and other documents that form the basis of the audit or review, and other documents that were created, sent or received in connection with the audit or review, and contain conclusions, opinions, analyses or financial data. (18 U.S.C. §§ 1519-1520(a); 17 C.F.R. § 210.2-06.)

- **The Securities Exchange Act of 1934.** Registered broker-dealers must keep extensive records related to their financial statements and business communications for various time periods depending on the record at issue. Electronic records must be stored in a non-rewriteable, non-erasable format. (15 U.S.C. § 78a; 17 C.F.R. §§ 240.17a-3, 17c-4.)


- **Data breach notification laws.** Forty-seven states, the District of Columbia, Puerto Rico and the US Virgin Islands have security breach laws that require entities to notify individuals of data breaches involving their personally identifiable information. (See National Conference of State Legislatures, Security Breach Notification Laws (June 11, 2015), available at ncl.org.)

- **Charter of Fundamental Rights of the European Union.** Among other fundamental rights delineated in this charter, the EU recognizes that everyone has the right to the protection of their personal data. Article 8 of the charter states that data must be processed fairly for specific purposes with the consent of the person concerned or some other legitimate interest pursuant to law.

- **Directive 95/46/EC of the European Parliament and the Council of the European Union.** This directive, applicable to EU member states, is aimed at protecting an individual’s right to privacy. Article 7 of the directive outlines the circumstances under which the processing of personal data is acceptable.

- **Data privacy.** The data privacy group helps organizations navigate the myriad laws, regulations and directives that dictate how to handle the personal information of customers, constituencies and employees. Data privacy requirements go beyond the disclosure of personal information and also apply to the processing, transfer and maintenance of personal information.

- **Compliance.** Larger or highly regulated entities may have compliance functions to ensure employees adhere to company policies and procedures, as well as externally imposed requirements. The compliance department monitors employee performance and practices and aggregates its findings to provide benchmarking snapshots of adherence to company policies. Compliance also directs remediation efforts when deficiencies are identified.

- **Human resources (HR).** Employee training, on-boarding and off-boarding are all functions typically managed by HR. These processes present critical opportunities to inform, review and enforce IG policies and procedures. Evaluating these processes through analytics and metrics can identify potential improvements to IG policies and procedures.

- **Business representatives.** Representatives from key business units should be consulted when developing, deploying and enforcing IG policies and procedures, including when, for example, major IT upgrades are contemplated, laws or regulations change, or an organization is standing up its operations overseas.

- **Analytics.** To the extent an organization relies on data analytics to enhance products, services or business offerings, the analytics function drives the strategic direction of an IG program. Harnessing the value of information is one of the foundational purposes of IG, but an IG program also must balance the goals of analytics against information risks and retention requirements.

- **Audit.** The audit department assesses various aspects of the enterprise’s performance against a set of defined standards. Audit findings demonstrate areas where the organization is meeting its goals as well as areas where the organization can improve. This information is valuable to an IG program because it can drive strategic decision-making and resource allocation.
**Finance.** The finance group is charged with accurately maintaining the organization’s accounting books and records, which implicates several core aspects of IG, including RIM, data privacy and information security. Finance can provide important perspectives on how IG program policies and procedures impact the organization’s operations, which ultimately affects customers, constituencies and employees.

**PREPARING TO IMPLEMENT AN IG PROGRAM**

There are several ways that the need for IG may come to the attention of an organization. In many cases, an adverse litigation event, a regulatory fine or a significant data breach acts as a wake-up call. These types of “black swan” incidents create conditions that trigger both an immediate tactical response and a longer-term strategic plan to implement IG solutions. Other times, the idea originates in the upper levels of an organization as a preventive measure, to be implemented using a top-down approach. Alternatively, personnel in the business levels of an organization may come together to engage in IG activities and layer their efforts onto existing projects until appropriate resources are allocated and a more formal IG structure can be achieved.

**GAINING SUPPORT FOR IG CHAMPIONS**

The ideal way to implement an IG program is with both upper management support and broad-based participation from the various business functions most concerned with IG. Organizations should consider appointing an executive-level IG champion who holds ultimate responsibility for the IG program. In some organizations, this individual could be named the Chief Information Governance Officer (CIGO). A CIGO could be a stand-alone position or an additional title for an existing C-level executive with other responsibilities. Not every organization is large enough or complex enough to warrant a stand-alone CIGO position, but every company should have a senior-level employee who coordinates IG efforts (see below Creating a Corporate Governance Framework).

In addition to designating an executive-level IG sponsor, IG stakeholders from across the enterprise should be involved and consulted at the outset of an IG program (see Box, Identifying the Stakeholders: The IGI RACI Matrix). Appointing an executive-level IG sponsor and establishing an IG steering committee requires upper management support, but some organizations do not have that executive-level sponsorship at the outset. In those situations, the business-level employees interested in advancing IG should identify opportunities to demonstrate the value of efficiently addressing multiple organizational issues simultaneously.

Grassroots IG champions should consider organizing an informal IG steering committee, which can then approach executives in the organization about formally establishing an IG program and steering committee. If sponsorship is not possible, these IG champions should find at least one senior-level executive who supports their efforts. An informal IG steering committee can be formed before launching a successful grassroots IG initiative, but it may be easier to gain executive-level support once the committee can point to demonstrative IG success.

For example, an organization looking to decommission a legacy document management system and establish a new system can gather IG champions across the organization to accomplish more using fewer resources. In conjunction with implementing the new document management platform, the IG champions and steering committee can demonstrate the value of an IG model to members of upper management by:

- Remediating information in the legacy system that is eligible for destruction before migrating content to the new system.
- Updating policies on the use of company document management systems to proactively manage the creation of information in the new system.
- Evaluating opportunities to use auto-classification tools to support ongoing records management and e-discovery in the new system.
- Training employees on company records management policies.

Each of these supplemental activities presents an opportunity to leverage an existing project to achieve a greater return on investment for the organization at a lower cost than pursuing the projects independently or reactively.

**BUDGETING TIME AND RESOURCES**

The time and resources needed to implement an IG program generally depend on the size, complexity and maturity of the organization. Larger organizations operating in a complex information environment may create a CIGO position and establish an IG program with dedicated full-time IG employees. By contrast, smaller organizations may charge existing employees with IG responsibilities in addition to their other responsibilities.
Companies that appoint a CIGO or an equivalent executive-level individual and hire full-time, dedicated IG employees need a separate budget for the IG program.

Companies that build an IG program using existing resources may fund the IG program using a small percentage of each stakeholder’s budget in the form of an IG tax.

Some companies may choose to fund each IG project individually.

The IG steering committee should consider which approach works best for its organization.

**PRIORITIZING AND EXECUTING IG PROJECTS**

Once an organization has gathered an initial team of IG stakeholders and secured senior-level support, the next task is to identify and prioritize a set of defined projects. The IG steering committee should be responsible for drafting, budgeting, prioritizing and executing project plans, while keeping the executive IG stakeholders (CIGO or otherwise) informed. As project plans are developed, an organization may identify additional stakeholders to be involved in the IG program.

After developing the IG project plans, the next step is to start executing on the identified projects in order of priority. These projects may include:

- Defining and implementing a corporate governance framework for IG.
- Developing and updating IG policies and procedures.
- Defensibly disposing of data and implementing litigation hold tracking.
- Establishing a comprehensive legacy data clean-up system.
- Conducting analytical procedures on company data.

*(IGI 2014 Annual Report, at 30.)*

**CREATING A CORPORATE GOVERNANCE FRAMEWORK**

A corporate governance framework for IG should outline the roles, responsibilities and reporting structure of the committees and individuals involved in the IG program (see Box, Identifying the Stakeholders: The IGI RACI Matrix). The number of committees and individuals depends on the size, complexity and maturity of the organization. For example, a localized organization of fewer than 200 employees has different IG needs than a multinational corporation with over 20,000 employees.

Although the exact corporate governance structure varies within and across industries, certain basic components serve as the foundation of any IG program. Key roles include the following:

- **Head executive IG stakeholder.** This role typically is filled by a singularly focused CIGO or a high-level executive with responsibility for an organization’s IG program in addition to other executive duties. The executive must be high enough in the organization to have authority and control, and ideally should have a background in one of the central areas of IG, such as legal, IT or RIM.

**Organizational IG steering committee.** As discussed above, the IG steering committee, which reports to the head executive IG stakeholder, is responsible for developing and implementing IG policies and procedures, and executing IG projects. IG steering committees vary in number of members depending on the size, complexity and industry focus of the organization. In most cases, the committee includes senior-level representatives who have decision-making authority, from the legal, IT, RIM, HR, compliance, analytics, data privacy, information security and finance areas of the business. The committee also should have members from key business units that represent the organization’s purpose or focus. For example, if an organization’s main business is designing and manufacturing a product, representatives from the design and manufacturing areas of the business should be included on the committee.

**Business unit IG committees.** Business unit IG committees, which are comprised of employees within various business units of an organization, identify issues, gather information and assist the organizational IG steering committee in executing IG projects. Like the IG steering committee, the number and size of business unit IG committees depends on the size, complexity and industry focus of the organization. If the company is small and narrowly focused, it may need these committees in only the central areas of IG, whereas business unit IG committees for a large, complex organization should reflect all of the areas represented on the IG steering committee.

The IG steering committee can identify additional roles that an organization may need by focusing on areas where more input or expertise can help solve IG challenges as the committee moves forward in its work. Roles can be permanent or temporary depending on the nature of the challenge.

**DEVELOPING FOUNDATIONAL POLICIES AND PROCEDURES**

An organization may choose to develop multiple IG foundational documents or create one overarching document that encompasses all of the principles, standards and reporting relationships for IG. Agreeing on content for the foundational documents is a good initial exercise for an organizational IG steering committee. The
documents should be consistent with other enterprise-wide governance documents and should:

- Outline the purpose of the IG program.
- Establish IG principles and standards.
- Clearly delineate IG roles and responsibilities.
- Outline reporting relationships among IG stakeholders.

When defining an IG program, an organization should consider its internal culture, the jurisdictional requirements of the countries in which it operates and its business needs. The organization also must update its existing policies and procedures and continue to do so on an ongoing basis. In some cases, the organization must rewrite existing policies, while in others it must draft policies from scratch. Associations or consortiums focused on RIM or IG may have templates or sample policies available to their members.

At the outset, an organization should consider drafting an:

- Organizational IG steering committee charter.
- IG organizational chart.
- IG responsibility assignment matrix, also known as a RACI matrix (see Box, Identifying the Stakeholders: The IGI RACI Matrix).

Further, as part of implementing an IG program, an organization should create or update the following policies and procedures:

- IG policy. This policy describes the principles and standards of an organization’s IG program and outlines its approach to creating, maintaining, using, protecting and disposing of information. The IG policy may take a high-level approach and charge the business functions with developing specific interpretations, or a more prescriptive approach that specifically describes how information will be managed in the organization.

- IG program charter. This procedural document outlines the roles and responsibilities of the individuals and committees on which an organization relies to execute its IG program. The IG program charter should describe the mission and goals of the IG program and address the escalation of non-compliance incidents. Additionally, some organizations may choose to include information about the organization’s IG governance model or RACI matrix in the charter.

- Bring your own device (BYOD) policy. Employees increasingly are using their personal devices for work-related activities. A BYOD policy describes the circumstances under which employees may do so. It is important to address this behavior in an official company policy designed to meet the organization’s obligations related to litigation, regulatory requirements, information security and data privacy. Additionally, organizations should examine “shadow IT” practices constituting employees’ use of available online applications (for example, Google docs) and private communications networks to determine if supplemental employee guidelines are warranted. (For a sample BYOD policy, with explanatory notes and drafting tips, search Bring Your Own Device to Work (BYOD) Policy on Practical Law.)

- Data privacy policy and procedures. These policies and procedures address an organization’s obligations concerning the privacy of its customers and employees. Implementing an IG program presents an opportunity for an organization to review data privacy requirements in a holistic manner and ensure that company policies and procedures are aligned with applicable requirements. (For a sample internal-facing privacy policy to protect personal information, search Personal Information Policy (Internal) on Practical Law.)

- Information security procedures. These procedures govern the levels of protection an organization employs to prevent unauthorized access to, or use of, its information. Because organizations cannot have uniform security practices for all of its information, some types of data need higher levels of security than others. An IG program allows an organization to assess those relative needs comprehensively and update IG practices accordingly.

- E-mail policy. E-mail often presents a significant IG challenge for organizations because of employee reliance on e-mail for both important business communications and insignificant exchanges. Companies should develop an e-mail policy that designates:
  - how company e-mail can be used;
  - what retention restrictions apply to e-mail; and
  - how automatic archiving and traditional records categorization function with respect to e-mail.

- Records retention schedule policy. This policy includes important information about the type of records the organization should retain and for what length of time. However, individual employees routinely ignore these policies, to the detriment of organizational efficiency and information management obligations. Simplifying the organization’s records retention schedule and providing clear instructions on how to properly dispose of records can help increase compliance with company-mandated records retention periods. (For a sample records retention policy and schedule, with explanatory notes and drafting tips, search Document Retention Policy on Practical Law.)

DEFENSIBLY DISPOSING OF DATA

Organizations consistently struggle with how to dispose of information while complying with company policies and procedures on a proactive and an ongoing basis. For many organizations, this challenge is propelled by employees’ desire to keep all information regardless of its value. Many organizations are now facing the consequences of permitting this accumulation of data in the form of massive archives of legacy data.

There are three primary drivers that require organizations to retain certain information:

- Statutory and regulatory retention requirements. The US and foreign jurisdictions have laws and regulations requiring organizations in specific industries to retain certain records for mandated periods of time. These retention requirements vary within and across industries depending on company business practices.

- Litigation holds. When litigation occurs, or is reasonably likely to occur, parties to the litigation have a duty to preserve information that is relevant to the subject matter of the litigation. This duty to preserve extends to relevant information within the possession, custody or control of
Identifying the Stakeholders: The IGI RACI Matrix

One way to organize IG actors is to form an organizational IG steering committee based on a RACI matrix that outlines the individuals or departments in the organization who are:
- Responsible.
- Accountable (also known as the Approver).
- Consulted.
- Informed.

The IGI developed a RACI matrix summarizing input from IG practitioners on what this matrix looks like at their organizations, in order of popularity (see IGI 2014 Annual Report, at 29). There is no one RACI matrix that will work for every organization. Each organization should evaluate its structure and needs to determine which functions fit best within each role.

- **RESPONSIBLE (THE DOERS)**
  - RIM
  - Information Security and Protection
  - Legal
  - Compliance
  - Business Operations and Management
  - Risk Management
  - Data Storage and Archiving
  - Privacy

- **ACCOUNTABLE (THE BOSS)**
  - Senior Business Management
    - Such as CEO, SVP, VP
  - (The second most popular answer was: Senior Legal such as General Counsel, VP of Legal, Head of Litigation. The third most popular was: Senior IT such as CIO, VP of Technology, IT Lead.)

- **CONSULTED (THE ADVISORS)**
  - Legal
  - Information Security and Protection
  - RIM
  - Business Operations and Management
  - Compliance
  - Risk Management
  - Audit
  - Privacy

- **INFORMED (THE DEPENDENTS)**
  - Business Operations and Management
  - Legal
  - Information Security and Protection
  - RIM
  - Audit
  - Finance
  - Risk Management
  - Privacy

the party, regardless of the format or the location in which it is stored. Similarly, organizations may need to preserve information in response to a regulatory agency’s request or investigation.

- **Business value.** Some of the information created or obtained in the regular course of business has significant value to the organization regardless of the date of its creation. This information should be retained until it no longer serves a legitimate business need. For example, pharmaceutical
One of the value-driven benefits of IG is that it enables organizations to analyze data to identify trends, discern patterns and predict future states.

Companies often retain research laboratory notebooks for long periods of time because of the potential intellectual property value the information could have, even decades later.

Organizations often use a records retention schedule to communicate to employees the records that have business value or are subject to regulatory retention requirements. For the records retention schedule to serve both purposes, the retention periods specified for business records must satisfy minimum regulatory retention requirements that are applicable to the organization.

To satisfy litigation hold requirements, organizations must have a robust litigation response protocol in place. This protocol helps an organization recognize when its duty to preserve is triggered, properly determine the scope of the duty to preserve and react quickly to preserve relevant information. It should include, at a minimum, the suspension of automatic deletion procedures related to retention periods regardless of the information’s format.

Once the policies and procedures discussed above are in place and being followed by employees, an organization can support ongoing remediation of information by:

- **Training employees on company RIM procedures and policies.** Employees often struggle to manage information because they are unsure of whether it is acceptable to dispose of information or of the proper disposal procedure. A robust training program that clearly delineates company RIM policies and procedures can support ongoing disposition by employees in accordance with those policies and procedures. (For a sample presentation to train employees on company retention policies, search Document Retention: Presentation Materials on Practical Law.)

- **Having a company-directed information review and preservation day.** On a specified day, employees should be provided with a dedicated amount of time to review their records and information to ensure proper retention and disposal in accordance with company RIM policies.

- **Implementing automatic e-mail deletion policies and procedures.** For certain organizations, automatic e-mail deletion policies and procedures may be an appropriate tool to prevent massive accumulations of data. To implement automatic deletion of e-mail of a certain age, for example, older than 12 months, an organization must have clear processes in place to ensure preservation of e-mail information that is subject to a regulatory retention requirement, a litigation hold obligation or serves a vital business need.

**Implementing systems to automatically classify information.** Some organizations have been able to implement systems that automatically classify information when it is created, though these processes remain new and have room for improvement. The easiest way to automatically classify information is to have as few retention periods as possible and create large “buckets” of information that are all retained similarly, without burdensome reliance on user involvement or tagging. However, some organizations operating in complex regulatory environments may find it challenging to take a simplified approach to retention times and classifications.

**Using RIM policy and procedure audits.** Auditing employee compliance with RIM policies and procedures can help identify areas for improvement and provide a basis for enforcement actions. At a macro level, the results of an audit can show an organization the areas of the business that need additional training and support to follow company policies and procedures. An organization may choose to include audit findings in performance reviews of employees to encourage greater compliance.

**CLEANING UP LEGACY DATA**

Similar to enacting a strategy for ongoing defensible disposition, to clean up legacy data, an organization must identify information that it is required to retain for legal purposes or wants to retain for business purposes. If the organization does not have disposal policies and procedures in place, it should implement them before engaging in legacy data clean-up activities.

Unlike ongoing disposition, a legacy data clean-up project looks backwards rather than forwards. Legacy data clean up may take place at either an individual level, where employees remediate their own legacy data, or at an enterprise level, impacting shared systems or repositories. In either case, an organization must have a records retention schedule that takes into account both regulatory obligations and applicable litigation holds.

An organization must be able to form a reasonable belief about the contents of a repository and understand whether there are retention obligations for those contents to make defensible disposition decisions. Where an organization knows and understands its retention obligations, it can determine how to treat a repository’s content while complying with applicable requirements.

At an individual level, determining applicable litigation holds is relatively straightforward. Individuals who have received...
litigation hold notices must take them into account as they remediate legacy data to comply with the organization’s records retention schedule. Any information subject to a litigation hold must be retained.

For non-custodial information stored in shared repositories, such as shared drives, an organization should evaluate whether the legacy data is subject to litigation holds on an enterprise-wide basis. One method for reviewing non-custodial information against all litigation holds is to create a litigation hold abstract. A litigation hold abstract summarizes information about each enterprise-wide litigation hold to allow for more efficient review and comprehensive understanding. Each row represents an individual litigation hold and each column represents an aspect of the litigation hold that helps identify its scope.

Examples of column headings in a litigation hold abstract include:

- Employees covered.
- Summary of subject matter.
- Materials and documents covered.
- Start and end dates.
- Systems targeted for remediation.
- Collections performed.

After creating the litigation hold abstract, an organization can make determinations on legacy data remediation by comparing the information gathered about the legacy data against the information in the organization’s records retention schedule and litigation hold abstract. To make this comparison, an organization must analyze its target repositories, including indexed summaries of repository contents, and as much metadata about the contents as is readily available. An organization may determine that it can use the metadata for the information it is considering for disposition to determine whether there are any legal or business reasons to retain the information, eliminating the utility of a linear document review that may not be feasible or necessary. To make disposition decisions on a particular repository’s contents, an organization must form a reasonable belief about the contents of the repository and understand whether a retention obligation covers those contents.

Vendors offer organizations several options for technical tools and procedures to identify and remediate the contents of electronic repositories. The options vary in their cost, user-friendliness, functionality and dependency on other IT processes. For paper records, most vendors are able to provide an index of the metadata available for each carton.

**USING BIG DATA ANALYTICS**

One of the value-driven benefits of IG is that it enables organizations to analyze data to identify trends, discern patterns and predict future states. An organization’s pursuit of analytics varies greatly depending on the type of industry, its big data budget and the focus of the organization’s analytical interest.

Big data analytics have the potential to improve company performance. For example, a company may want to conduct an analysis of its manufacturing operations to determine areas of optimization and potential improvement. The specific data related to the areas of optimization may inform adjustments that the organization can make to the areas that need improvement. Likewise, to improve its market share worldwide, an organization may want to evaluate its global sales data to determine where its promotional and marketing efforts are most effective.

Before performing these analyses, an organization should have its IG steering committee consider the proposed analytics to determine any areas of potential concern, such as privacy or information security requirements. For example, the committee should consider whether:

- The use qualifies as one of the legitimate interests allowed by the EU directive on data privacy, if the analytics involve EU data.
- The organization must obtain permissions or enact protections to ensure it meets US privacy requirements, if the analytics involve personally identifiable information and personal health information in particular.
- Information security procedures will be applied to the data and the output of the analyses and, if so, what types of procedures will be put in place.
- There are any contractual obligations the organization must adhere to when using the data.
- Access to the data will be restricted.
- The company has policies or procedures regarding the use of data analytics.

Having the IG steering committee consider these issues in advance helps ensure regulatory compliance and protects the organization, its employees and its customers from misuse or inadvertent disclosure of data.