Making Sense of IG, IS and EDD: Three Typical Projects

Every IG, IS and EDD project should start by defining the objectives and assembling the right team of people for the tasks ahead. The second stage is to conduct a complete and accurate inventory of the data sources implicated by the project scope, reports **QDiscovery on its website**. Indiana attorney Helen Geib wrote the article.

The article continues:

Taken together, stages one and two lay the groundwork for the final stage of accomplishing the objectives.

Making it happen – and doing it right – is undoubtedly the most challenging and complex part of any project, and the point at which most stalled or unsuccessful efforts founder. However, it can be made more manageable by breaking it down into a series of mini-stages, each building on the one before:

1. Make a plan.
2. Evaluate technology options.
3. Implement new systems and policies.
4. Educate and train employees.
5. Audit compliance on an ongoing basis.

To flesh out what these steps look like in practice, the balance of this post outlines a typical project in each area.

A) eDiscovery

Objective: Produce responsive ESI from an inventory management database in a readable format.

Team: Outside litigation counsel, records custodian

Project Steps:

1. Make use of the built-in searching and reporting capabilities of the database to identify, collect and produce the relevant data.
2. Schedule an online demo of the database with a records custodian (an employee who regularly works in the database). Look at the forms to identify potentially relevant fields, ask about search capabilities and go over options for standard and custom reports. Select the best format after reviewing sample reports to assess readability.
3. Direct the client to generate a report, in the selected format, that includes the field entries that are responsive to the requests for production subject to appropriate limitations, such as a date cut-off.
4. Not applicable (but note that employee education is important in eDiscovery in the context of litigation holds).
5. Repeat step three as needed to comply with continuing obligations to supplement discovery.

B) Information Governance

Objective: Improve overall company compliance with records retention requirements, while also making it easier for employees to find useful documents and collaborate on creating and reviewing documents on a day-to-day basis.

Team: Legal department, IT and department managers

Project Steps:

1. Develop and implement a comprehensive records management policy for unstructured data (e.g., MS Office files, PDFs).
2. Research the capabilities, system requirements and costs of document management systems such as Sharepoint and Office 360. Select the best solution in light of employees' access needs, typical file types, data volume, the relative complexity of regulatory retention requirements, IT infrastructure and staffing, and of course, the budget.
3. Write or revise as needed a records retention schedule for

the different categories of company information within the scope of the project. Develop practical guidelines for organizing and saving documents. Finally, roll out the new DMS.
4. First, educate employees in the legal and business reasons for adopting the new system and the costs to the company from not complying with retention policies. Second, provide technical training in using the software.
5. Set and follow an appropriate schedule for making regular and/or spot audits of employee compliance with the retention schedules specifically and the new document management guidelines more generally.

C) Information Security

Objective: Protect the company against garden variety cyber-attacks.

Team: IT

Project Steps:

1. Install and/or upgrade cybersecurity software for secure email use and web browsing.
2. Conduct due diligence on firewall, anti-virus and encryption solutions and select the best software tools.
3. Install the selected software on the server and individual workstations.
4. Hold mandatory employee training sessions on safe web browsing, spotting phishing emails, promptly reporting suspected viruses to IT staff and similar topics.
5. Actively manage software updates, install software on all new computers and continue to hold employee training sessions on an occasional but ongoing basis. Constantly monitor for cyber threats and troubleshoot issues as the need arises.