



MANAGING RECORDS TO MINIMIZE RISK

BY STEVE MACKES

Because they contain information, often sensitive information, that can be lost, misplaced, misused or altered, records are a risky business. And with more and more records created, faster and faster, every moment of every day, that risk only grows in exponential ways. As records can be used to defend, to attack, to justify or call something into question, it's difficult to predict and quantify their potential impact. Even the lack of records, rather than freeing an organization from liability often has just the opposite effect. Records, by their very existence or lack of existence, by the content they contain or the way they are interpreted can be damaging. All of which puts those who manage records as well as the organizations that create, use and retain them in a particularly risky bind. The inescapable fact is this: Records Equal Risk.

But it is also a fact that the risk posed by records can be significantly reduced, largely mitigated when a comprehensive, knowledge-based information management program is set in motion. And that's not all. Because when records are managed effectively, end-to-end throughout their lifecycle, they become valuable resources, tools of opportunity, building blocks of present policies and future initiatives. This further reduces risk, providing an organization the means not only to grow, but also to build a strong, information-based defense of its operations and policies.

Another issue related to operations and policies is the increasing use of casual conversation in lieu of structured business language. This often leads to ambiguity and misinterpretation. What's called for is a return to fundamentals where an organization trains its employees on how to write memos, letters and other communications. And then these standards need to be enforced in audited procedures.

THE BIGGEST RISK: LACK OF CONTROL

The greatest risk for most organizations, both public and private, comes not from the information itself, but their inability to control it. Of course, the sheer volume of information contributes to this, making it harder, if not impossible to review and process everything and make accurate risk assessments in a timely, executable way.

Information assets can include email content and distribution, copies of documents in multiple formats and media, multiple data/paper storage repositories, data and documents retained by third parties, compliance regulations and much more. On top of that, there are numerous record-related issues

that must be addressed and that, in themselves, provide additional layers of information to review, process and manage. These issues can include: leaked information and its impact on the organization, government investigations and audits, legal claims, litigations and eDiscovery, court sanctions for information mishandling, government compliance regulations and executive liability. With all that on their plate, it's small wonder many organizations find it difficult to effectively manage their records and thereby, lower their risk.

Making a concerted effort in reducing information volume can go a long way toward solving this issue. Getting rid of duplicates, distributed copies and content that is no longer of retention value can improve workflow and make the processing of information more streamlined and manageable overall. It's also important to adopt meaningful terminology standards so that documents can be easily and clearly identified and distinguished from other similar records.

5 QUESTIONS IN NEED OF ANSWERS

Before records-related risk can be dealt with and brought under control, it must be identified throughout the entire record lifecycle and existing information management system. The objective is to provide an organization with the awareness, based on knowledge, of what types of risk it is up against. In completing this evaluation, there are 5 essential questions in need of answers. They are:

1. What are your organizational exposures and associated costs?
2. How is information a component of those exposures?
3. Where do the gaps lie in your organization's information lifecycle?
4. How is content managed in your organization?
5. What policies and procedures are in place to manage your organization's risk?

Honest, thorough answers to these questions are the foundation for developing and implementing an effective risk management program. As a customized, enterprise-wide solution, it would address all major issues and provide a roadmap for maintaining information control and mitigating risk over the long term.

PROGRAM DEVELOPMENT

A risk management program needs to be based on an accurate understanding of an organization's information universe. Getting there calls for the inventorying of all information assets—documents, files, various media and data—in both electronic and paper form. Mapping of the information infrastructure and the data and paper storage repositories is also essential, as is determining the utilization of software for Electronic Data Management. Also imperative are responsibility assessments, identifying who is driving/overseeing the program and which personnel and/or departments are in charge of which information areas.

Next, based on risk findings (both internal and external), business rules and standards need to be

established. While aimed at reducing risk, these rules and standards must be realistic and flexible enough not to inhibit the normal flow of operations and business conduct.

With government regulations increasingly widespread and potentially costly, compliance plays an important role in defining business rules and standards. Maintaining compliance clearly enables an organization to avoid or at least significantly minimize related fines and penalties. But that's not its only benefit. Used as a positive in marketing, compliance strengthens an organization's reputation and business position.

Impacting the final shape and scope of a risk management program is the dynamic of risk mitigation versus Change Management. Substantial benefits and costs are associated with each. Because risk management requires change (never easy), an organization must weigh its program not just in implementation costs, but also in terms of how much change the organization can withstand and is willing to assume. Change means the introduction of new training, rules and processes for every employee to learn. The goal is to find the optimal balance of risk and change that will ensure program success.

When all of this done, after the size and nature of the program have been determined and a long-term strategy has been devised, a communications effort begins that includes educating the workforce and training all relevant personnel.

PROGRAM IMPLEMENTATION

Implementation requires actively and accurately following the program strategy. Based on all the evaluations, assessments and structuring completed to this point, the strategy lays out the path to follow. It's a roadmap of sorts providing both direction and guidance for reaching risk mitigation objectives. Depending on the size of an organization and the complexity of its policies, products and services, implementation may need to be phased in, which can sometimes take a period of years.

Implementation covers a whole range of activities that include email and social media controls, the digital conversion of paper, planned reductions in the volume of information, strict adherence to retention and destruction schedules, and the combining of day forward and back file conversion efforts with annual audits. It also includes report generation and continuous program monitoring as to effectiveness and the possible need for adjustment.

THE SOLUTION IS IN SIGHT

In response to the growing need for a 'big picture' approach to information-related risk management, GRM has introduced the Solutions Group. This new division, offers a team of top experts serving in a full advisory capacity. Rather than addressing issues piecemeal, the Solutions Group takes a holistic approach, evaluating the entire information lifecycle and making custom recommendations to achieve a comprehensive risk management solution.

Throughout, from data collection and research to mapping, from establishing best practices to training and monitoring, the Solutions Group is there, at an organization's side, offering advice and knowledge-based guidance, overseeing all facets of the complete program and ensuring its ongoing success.

CONCLUSION

While risk is never to be entirely eliminated, it most certainly can be brought under manageable control. Still, this can be a complicated, formidable task, requiring the highest levels of information management expertise. Reason enough why any organization—swamped by information, grappling with its many associated risks and loathe to waste valuable time, energy and resources—shouldn't attempt to go it alone.

Fortunately, with GRM's Solutions Group, expert help is a no-risk, no-obligation phone call or email away. Contact the Solutions Group and find out how to cost-effectively bring the risk inherent in your organization's records, once and for all, under control.

MORE ABOUT GRM

GRM Document Management is a leading provider of lifecycle records and information management solutions. The company brings proprietary innovation, blended integration and new levels of cost efficiency to document storage, data protection, digital/electronic document management and certified destruction. With over 25 years of experience, GRM has earned the trust and continued business of more than 5,000 customers—large and small, domestic and multinational—representing a wide range of industries. Clients are served from state-of-the-art, climate-controlled facilities in major U.S. markets and internationally throughout China.