GALAXYCONSULTING
Information Management Solutions

Information – Governance, Risk, Compliance

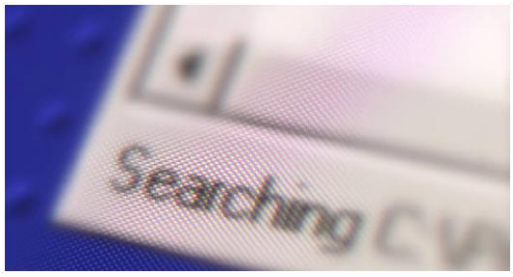
White Paper
By Galaxy Consulting

April

A

At Your Service…Today…Tomorrow
We Appreciate The Privilege Of Serving You!

May 2014



Abstract

Information is the lifeblood of any modern-day business. Companies succeed or falter based on the reliability, availability and security of their data. Strategically created enterprise-wide frameworks that define how information is controlled, accessed and used are the most critical elements in a successful information management program. This framework is information governance.

This white paper gives an insight on why information governance is important, where to begin with the information governance and what needs to be considered in information governance polices. Information governance policies as they relate to crisis management and e-discovery as well as general information governance control points are also described.

What is Information Governance?

Governance is about securing the information and also about using information for greater value. People don't talk much about value of information but information is strategic asset of a company.

What makes a company great among other things is the ability to take information and use it as an asset. Information is what drives an organization, whether it is through development of new drugs, new products, looking into new geographic regions to expand to, etc.

Governance is like an insurance policy that you feel like you are paying for nothing, until you need it. You don't know when and if an "accident" will happen and you don't know how big it will be, but when it does happen, you are very happy that you have that insurance policy. Until then you resent having to pay for it. Governance which is controls is your insurance policy.

Knowledge management can be costly in terms of fines, brand reputation, legal fees. In case of a legal discovery, the lack of documents means a disaster. Absence of document control in place will result in violating regulatory compliance.

To an increasing extent, organizations are focusing on risk management as a central issue in GRC equation. Enterprise Risk Management (ERM) is now a bigger driver for GRC than Sarbanes-Oxley or other compliance requirements. Organizations want a top-down viewpoint on risk whether it is resulting from non-compliance or operational issues and want to know what is being done to mitigate it. ERM is increasingly considered as a strategic tool to support governance and improve business performance.

Governance and compliance are essential business functions. Risks need to be understood and managed. Risk management does not mean that every risk can be anticipated but it can plan for the risk and have alternatives ready.

Information governance – effective content controls, allowing all information to be securely and properly shared across departments, geographic locations, and systems.

Organizations need a closed loop environment for assessing business risks, documenting compliance and automating control monitors to sift through their business systems.

For example, SharePoint is widely adopted system for knowledge management. According to a recent AIIM report, more than 60% of organizations have yet to bring their SharePoint deployment into existing compliance, retention, and long-term archive policies.

To prevent potential exposure of sensitive or classified information, it is imperative for organizations to bring their SharePoint in line with existing compliance policies.

Benefits of information governance: helps company management to enforce focus on business mission, employees have information that is accurate, current and is in suitable format for their use; employees are more efficient and productive; removing duplicate and unnecessary content reduces the time needed to find information, derive higher profits; operational cost is lowered; retention management optimizes cost-effectiveness of storage platforms; legal fees are reduced in case of a litigation.

Where to begin?

To start information governance initiative, create steering committee – CIO, legal officer, compliance officer, other main stakeholders. Outline the scope, the timeline, and the budget. It should be rolled out from the top. This way everybody will be on the same page.

Have a strategy. Strategy should drive what is measured and monitored for compliance and performance. Information governance strategy must account for the value of information and how it is classified and accessed.

Information governance policies should support all of the organization's governance controls – retention, disposition, legal hold, data privacy, and security. Policies need to be scalable, enforceable, and measurable. It is better not to have a policy than to have a policy which can't be enforced.

Policies should change depending on new business requirements, regulatory demands, rising costs, litigation. Companies must have a process to update, validate, deploy, and enforce these policies. They should be deployed without negatively impacting users and operations.

Rank the value of information depending on its type and where it is coming from. For example, information created by VP of sales should be ranked higher that information created by a marketing intern.

What needs to be considered in information governance polices?

Government mandates - If you are in a regulated industry, you need to consider first and foremost government mandates such as GMP/GxP, ISO 9001. You need to make sure that your documents management and IT are compliant with these requirements.

Proliferation of content - There has been explosive growth in the creation and collection of content by organization and individuals. Content is stored in CMS, data warehouses, physical warehouses, desktop computers, file shares, back-up archives, mobile devices, cloud services, employees personal computers and other devices such as tablets, smart phones, etc. To complicate matters this information is also geographically disbursed.

In SharePoint, for example, you get a small department that has a site, other departments take notice and start their own sites. Suddenly you have small SharePoint instances pervading everywhere. What organization should do instead is take those separate silos of SharePoint and combine them into one centrally managed environment. It is the matter of having a plan in place first, then applying the technology to achieve those business goals.

Information governance policies should cover desktops and shared drives, CMSs, databases and data warehouses, email systems, cloud based apps, social media platforms, physical warehouses. Content may be stored with the 3rd party, this also needs to be considered.

Employees send email with documents attachments. This email and attachments have significant value to the business whether they contain contract terms, meeting notes or even employees opinions on a given topic. Email requires governance and so it needs to be included in your information governance policies.

Big data – Are you prepared? What measures your IT has taken to help with this issue?

Cloud computing – If you use cloud computing, you need to create governance policy for it.

Mobile Devices - Employees use mobile devices to do their job. Many companies don't have policies that cover things like tablets and handhelds. They are starting to, but it is just a beginning. You need to create polices for mobile devices and a mechanism to enforce those policies. And in the regulated environment, you would need to prove that you are enforcing those policies.

Social media - Effectively leveraging social media while protecting the organization from non-compliance.

Create comprehensive social media governance plan. It should include compliance, supervision to interactive social content; perform conceptual search and policy-based monitoring of all info, inside and outside the firewall; establish social media usage policies and procedures and then train staff on them; preserve and collect relevant social media content for compliance and litigation purposes.

Consider all content and access methods involved as users connect via smartphones and tablets. Employ solutions that capture additional approval on a site-by-site basis to verify assent for capturing and monitoring. Wherever possible create separate business identities for social media to minimize capture of personal or private information.

Govern employees' interactions. Most regulated organizations are taking a measured approach to social media, starting with small number of employees and approved social media sites. Monitor and capture inside-based interactions within corporate networks. Moderate inside-based interactions. Be mindful of legal and regulatory guidelines.

BYOD phenomena – "Bring Your Own Device". People bring their iPads, iPhones, etc. to conferences, work, taking notes, making presentations, responding to email, updating pipeline, etc. All this content belongs to the organization but the device is not. What happens when this employee leaves the company? Or that employee loses the tablet? What happens to information?

There was the case where a doctor had all his patients' medical records unencrypted on his laptop. The laptop was stolen.

It could also be that there are multiple versions of documents floating around, gets passed from one person to another person, and maybe tweaked a little along the way. And they each are legally discoverable.

Be sure that the official version of the document is stored in your CMS and managed by your governance program.

It is imperative to have a policy to protect this information and to enforce that policy across all those devices.

Security – sensitive information must be protected – encrypted. LinkedIn got hacked and all passwords got stolen. What are you going to do that this does not happen to your organization?

Intellectual property - What about a pharmaceutical company developing a new drug, not yet under patent protection and an employee takes that information to a competitor?

Of special importance is information related to future revenue. For example, a pharmaceutical company should place a high priority on protecting information related to future products which are not covered by patents.

It is vital for companies to have a system in place to protect sensitive content such as for example product roadmaps, manufacturing plans, vendor supply lists, marketing and promotional strategies.

Information Governance for Crisis Management

Crisis management is set of procedures for unplanned situation that would prevent you from doing critical functions on your job.

Such situations can be:

- Availability – illness, weather, turnover, fire, flood, severe weather, facility issues
- Technology – phone cut-off, system outage, applications is down, network problems
- Volume/Capacity – huge number of calls (in the example of call center)
- Special situations – pandemic, loss of facility, tornado, etc.

An approaching storm or disaster does not provide much leeway to assess your disaster recovery preparations.

For example, if your CMS is down, what happens to those departments who need to use critical documents?

Solutions

What you need to do is to develop a plan for each crisis situation. It should be designed to implement disaster recovery. Planning is very important.

Prioritize requirements – short, medium, long-term. Assess business needs. For example, how do you want to handle spike of calls (if you are in the call center)? Short term plan could be such as – re-route calls for live answer where there are people. Medium to long term could be such as plan for alternative site, work from home.

Make your plan flexible. Have incident coordinator. Create communication plan which should include who is responsible for coordinating the recovery process. Create crisis team which could include IT, QA, management, business partners. Outline responsibilities and procedure in the document.

Test this procedure at least once a year. Do post-analysis – timing, access gaps, communications of results, recommend changes and training plan for next testing, maybe next quarter, not next year. Evaluate your systems when you have no crisis.

Other points:

- Address disaster recovery in addressing planned and unplanned downtime.
- Virtualize your data center.
- Ensure swift restoration of content items following corruption or accidental deletion.
- Maintain all metadata during and after recovery events.
- Ensure seamless transition to a warm stand-by system should the main system fail.
- Plan what to do if outage happens.
- Maximize platform up-time and swift restoration of platform following a disaster event.
- Users need to feel confident that the system will protect content and will be available regardless of any disaster, otherwise user adoption will fail – users will go back to their old habits essentially halting KM effort in its tracks.

Information Governance for E-Discovery

E-Discovery preparedness makes it imperative for organizations to develop an enterprise wide strategy to manage the volume of electronic information. The discovery process affects many individuals in an organization, not just lawyers and others involved in discovery, but also IT professionals and records managers, who have to be prepared to produce electronic content for discovery and litigation.

You need to have an ability to respond to legal request, to solve litigation issue, mitigate the risk of sanctions, and reduce impact and cost associated with future litigation.

For legal counsel, it means having a review process to determine what discovered content is relevant to the case. For an IT person, it means restoring backup tapes to show evidence on file shares, content management systems, e-mail systems, or other applications. But for records managers, this work will have begun long before any lawsuit with managing records for retention, placing legal holds, and finalizing disposition.

E-discovery could be costly because it requires organizations to retrieve content from servers, archives, backup tapes, and other media.

In some cases, an organization is unable to execute a discovery order because it is unable to locate all content in a timely manner, or it is unable to place holds on all content and some of it is deleted during the lawsuit. The inability to do this correctly also has a cost, and it can be considerable.

To address these costs, many organizations are looking at e-discovery solutions that will enable them to review the found content and take it through litigation.

But organizations can also lower costs for archiving and restoring, legal review, and sanctions by simply cutting down how much content it retains. Less stored content means less content on which to perform discovery.

Developing a strategy and a plan of action for handling e-discovery will help organizations mitigate their risk and save them a significant amount of money in the event of litigation. Organizations need to have a retention policy to determine which content can be destroyed and at what time and which content should be kept and for how long. The key is to have a retention program that is flexible enough to keep content for the right retention period.

By categorizing content, creating a catalog of the content, creating a retention plan, implementing a hold methodology, and having disposition procedures, an organization will benefit in many ways.

Solutions

Integrate e-discovery into information governance practice. Include key capabilities:

- Understand and secure – identify and categorize docs; docs are distributed globally; find and correctly identify them.
- Automate and enforce - extend policies to docs within unmanaged repositories such as file shares, SharePoint, etc. Automate processes in a transparent manner to manage and control docs. Retention and disposition policies that can be enforced within ECM.
- Protect and control – regulate how documents accessed and used; security controls over documents; control who can access protected documents.
- Discover and produce – ability to produce relevant docs upon demand is a mandatory requirement.

Develop retention programs. Create committees within your organizations and bring their expertise together with legal counsel and IT to prepare for e-discovery and litigation.

General Governance Controls

- Understand your data topology – holistically across the enterprise: how much, where, who owns it, and what value does it provide.
- Employ real-time indexing of content – to keep track of its changes.
- Store the intelligence about your content (metadata).
- Create an information intelligence service center and include data analysis, governance analysis.
- Employ change management to stay current of new forms of content and new business requirements.
- Become proactive in deploying policies for securing data, storing data, sharing data and enforcing compliance.
- Remove obsolete or unnecessary content.
- Define content life cycle and retention policies.
- Tier your access to enable relevant data to be closer to users and devices that are local.
- Educate the organization on the value of good governance; it is less about control and more about raising the intelligence and health of information.
- Categorize your information and determine its value and rank.
- Use content approval function in your CMS.
- As deployments grow, organizations must also find ways to efficiently store records in compliance with retention of records management policies.
- Create retention schedule, content controls, consistent disposition of content in accordance with records management policies for content preservation, remediation, and retention.

- Keep track of what info is created, stored, and accessed.
- Use auto-classification and semantic tools within the search engines.
- Move relevant documents from desktops and shared drives to your central docs repository.
- Create efficient document versioning and check-in/check-out management for information consistency.
- Create robust administration of users to ensure that each as access rights for only documents that they are authorized to have access to.

Conclusion

The future of information governance depends on continually evaluating policies and adapting them as business priorities and market conditions evolve. Just as an effective corporate governance strategy can yield competitive advantages, effective information governance can turn information into a more consistent generator of business value.

If you develop a plan, implement a governance architecture that supports that plan, assess the architecture on an ongoing basis, and react and revise as necessary, your organization will have the support and agility necessary to truly use all of the information it possesses to improve business processes, innovation, and competitiveness while lowering total costs.

About Galaxy Consulting

GALAXYCONSULTING
Information Management Solutions

Galaxy Consulting provides services in business analysis and usability, content and knowledge management, records management, information architecture, enterprise search, taxonomy development and management, document control, and information governance.

Galaxy Consulting was founded with the mission and vision of helping organizations to manage their valuable information assets. Many of our clients, both large and small, have dramatically improved efficiency and reduced unnecessary labor hours through efficient methods, processes, and solutions we created.

Galaxy Consulting believes in partnerships with our clients. We are committed to working with you and to helping you transform your business. We will increase efficiency and productivity, maintain regulatory and legal compliance, improve collaboration, enhance innovation, and reduce costs through effective information management!

Call us TODAY to schedule a free, no obligation consultation!

Contact Us

Office: 650-474-0955
Mobile: 650-716-3609
Info@galaxyconsulting.net
www.galaxyconsulting.net