

Litigation and Compliance:
Bridging the Gap between Legal and IT



ZyLAB White Paper

Chris Dale,
the e-Disclosure
Information Project



Contents

Introduction	3
Summary	4
The Relationship between Information Management and eDiscovery	5
Who are the Players?	8
IT departments	8
Security and HR departments	8
Legal departments	8
Understanding the gap	9
A human as well as a budgeting matter	11
Matching the solutions to the problems	12
The risks to be considered	14
Anticipating the problems	16
How to Bridge the Gap	17
About ZyLAB	19



Introduction

This paper is written by former commercial litigation solicitor Chris Dale of the UK-based eDisclosure Information Project in association with ZyLAB. The eDisclosure Information Project brings objective and informed comment to lawyers, judges, suppliers and clients aimed at encouraging the better use of technology in electronic disclosure for litigation.

This paper is sponsored by ZyLAB, a provider of eDisclosure and information management software for enterprise information management, for regulatory and other investigations, for compliance and litigation readiness and for electronic discovery. Its product range extends right across the Electronic Discovery Reference Model (EDRM) from e-mail archiving and SharePoint through to the preservation, collection and production of documents to a court or regulator. That very wide range of products and services brings ZyLAB into contact with many of the people responsible for specifying, purchasing, implementing and using information management software, and gives it a special perspective on their often differing interests.

Summary

This paper is called 'Bridging the Gap' because it quickly becomes clear to companies like ZyLAB that there are divisions – of pressures, of requirements, of objectives and of attitudes – between the various groups within a large company who have some interest in information management. A “gap” exists in the secondary sense that many of those who could benefit from modern information management software are not aware of its capabilities, or how it can be used for a wide range of purposes. This paper identifies the different interest groups and suggests that there is more commonality than one might think between them. The conclusion is that it takes board-level involvement and leadership to identify company interests which override sectional interests and to ensure that appropriate budgets are set for software acquisition, for training and for staffing.

Gartner says “...most organizations are ill-prepared for litigation because their records management policies and e-discovery processes are misaligned. IT professionals need to prepare for the special demands created by e-discovery.”¹

It is not just litigation which brings demands for the preservation, collection, analysis and review of all or part of a company's information. Furthermore, legal departments are not the only originators of the demands for such exercises. One of the matters considered in this paper is the range of possible use cases for eDiscovery software and the role which a provider can play in helping a product champion to develop the business case for technology investment. The people who perceive the value are not necessarily those who would most benefit from it; those who have the need are not necessarily the ones who are aware of the possible solutions.

¹ Gartner Report “E-Discovery for IT Professionals: An exceptional Process that Requires Unique Competencies”

The Relationship between Information Management and eDiscovery

Before we look at the players within an organisation, it is worth saying a little about eDiscovery as an end use of – and therefore an investment justification for – wider information management tools. The stages of eDiscovery are conventionally explained by reference to the Electronic Discovery Reference Model or EDRM.

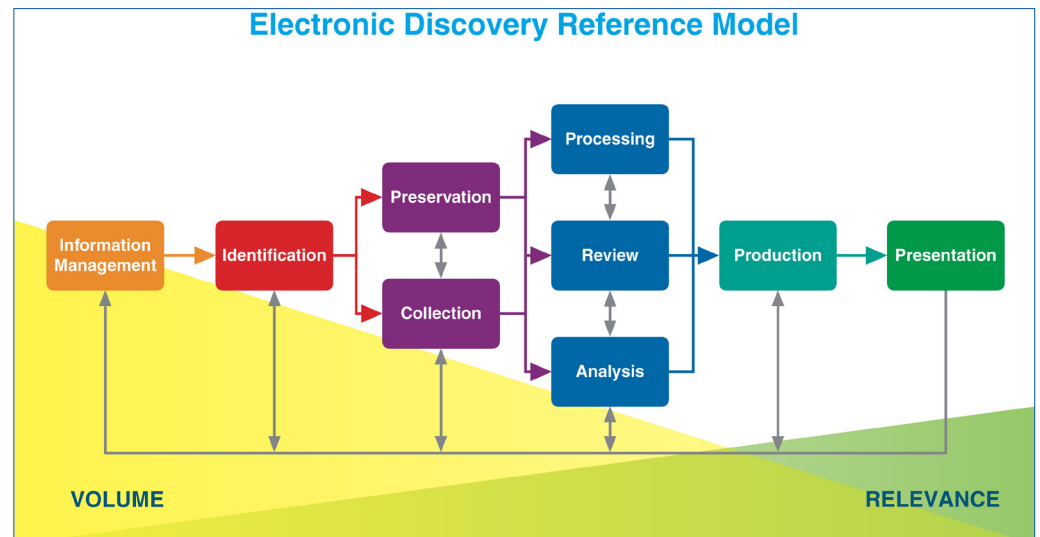


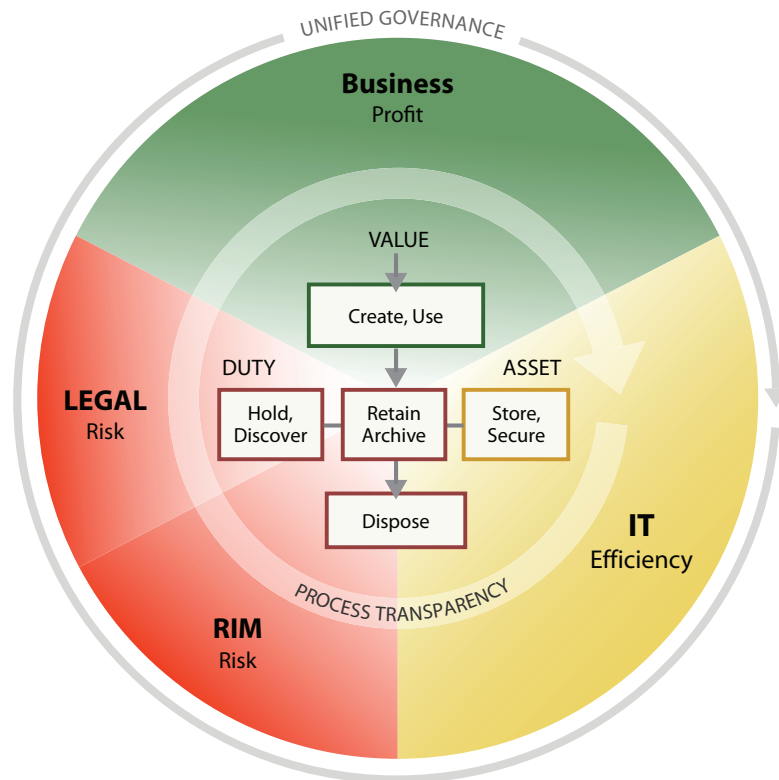
Figure 1: The Electronic Discovery Reference Model (EDRM)

Apart from its first component, Information Management, the EDRM is concerned with post-trigger stages – those things which must be done once proceedings become likely or an investigation is launched.

A new model is being developed as a counterpart to the EDRM. Called the Information Governance Reference Model or IGRM, it does more than merely expand on the Information Management part of the EDRM.

Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management



Duty: Legal Obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

Figure 2: The Information Governance Reference Model (IGRM)

It identifies four major interests – Business, Legal, Risk and IT - and three sub-elements – Value, Duty and Asset – which between them make up the business purposes of information, the legal obligations which arise in relation to it and the containers in which it sits. This diagram stresses the inter-relationship between these components and between the people who are responsible for them. The reality, in many organisations, is that the lines are inadequately drawn between the needs, purposes and budgets represented by the various elements.

ZyLAB has its own diagram which focuses on the asset element of the IGRM and its relationship with the eDiscovery components identified in the EDRM.

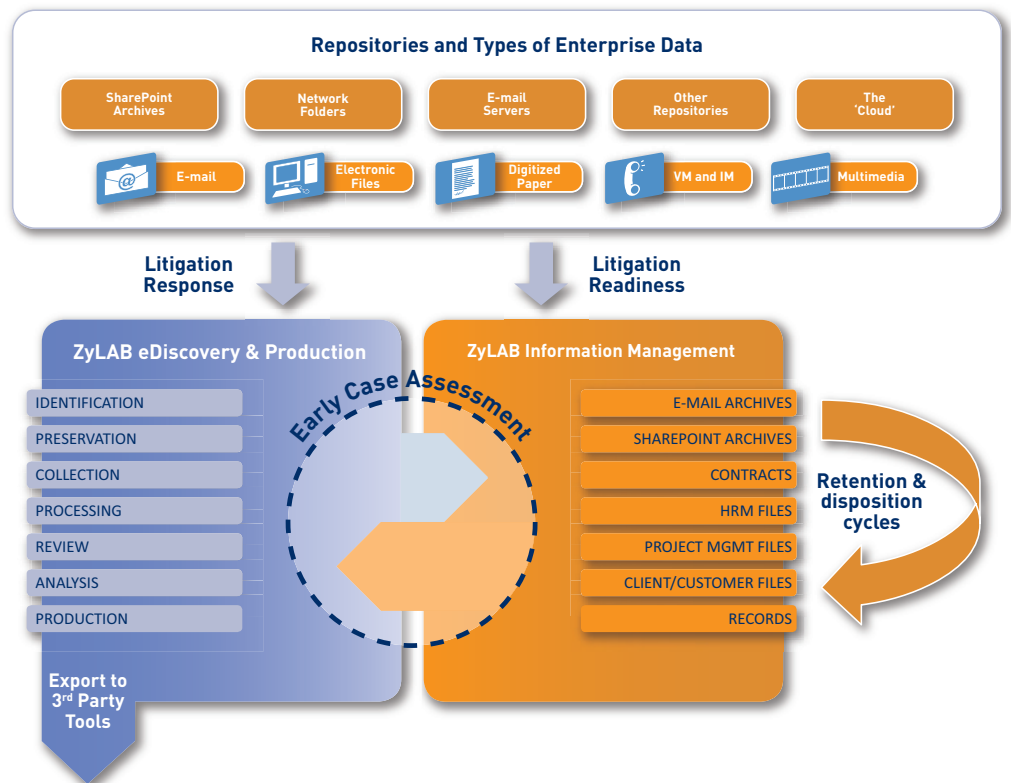


Figure 3: EDRM vs. IGRM

The three diagrams together illustrate the problem addressed in this paper: business units, legal and compliance departments and IT departments all have different interests in this information. Those who create and use the information and those responsible for maintaining and, in due course, disposing of it, are not necessarily alert to the responsibilities of those who may have to produce it to others, such as opponents in litigation or a regulator. The latter's instinct to keep everything which might be needed conflicts with the interests of those who own the data and of those responsible for looking after it.

What is needed is a comprehensive solution which deals with the whole life-cycle of the data in a way which reconciles these competing interests. This requires as a first step that the various players understand the imperatives of the others

Who are the Players?

Large companies will generally have separate teams responsible for IT, compliance, security, audit, finance, procurement, HR and legal amongst others with, perhaps, sub-groups responsible for discrete functions. Most of these departments have, at one extreme, long-term strategic functions and, at the other extreme, responsibility to react quickly to day-to-day problems. Budgets are set to cover strategic acquisitions and staffing and to make provision for reasonably foreseeable risks and contingencies.

IT departments

IT departments generally have fixed annual costs invested in infrastructure, licenses, maintenance and staff, and replacements and upgrades can generally be anticipated and provided for. If a case is made for some new functionality or a new application, quotations are obtained as part of a formal procurement exercise, and the budget is either made available or it is not.

Whether the resulting project runs to time and budget is a different matter, turning on the adequacy of the specification, the quality of the project management and the selection of the external providers; how the company handles system failures and other fire-fighting exercises depends on the quality of its support and maintenance arrangements. In general, however, it is possible for IT departments to look a year ahead and determine what is needed.

Security and HR departments

The same is true, for the most part, for departments like security and HR who may face fire-fighting requirements over a year but who can generally cover these by predetermined contingency plans and budgets.

eDiscovery can be the disruptive force which upsets this relatively even state of affairs, when demands placed on other players are passed to IT.

Legal departments

Legal and compliance teams have many more wild cards and variables in their work. A single piece of unexpected litigation, a regulatory investigation, claims by a whistleblower or an internal investigation giving rise to a potential self-reporting obligation can arrive from nowhere. These do not have the luxury of deferral and cannot necessarily be scaled down to fit within a budget or the available resources. This breeds a different ap-

proach to acquiring a solution, the budgeting and planning, one which is not always straightforward for stakeholders, such as IT, upon whom the legal and compliance teams depend for access to information and to the tools needed to react appropriately to whatever has come up.

Understanding the gap

IT departments pick up these burdens by proxy. Already servicing (and therefore having to understand) the routine business needs of every business unit and support function within the organisation, IT departments face sudden demands for data and for system information which may come from or relate to any department – legal, compliance or HR will often be the originator of the demand, but it may relate to any part of the organisation’s activities. Furthermore, multiple demands may appear simultaneously, and may require an understanding of external requirements – of a court or regulator – with which IT are unfamiliar.


A yet further complication is that these demands for data may extend to unconventional data sources such as social media, instant messaging and BYOD (Bring Your Own Device) elements such as tablets. Even company-sponsored sources may be relatively uncontrolled – SharePoint for example. Lastly, the difficulties will be exacerbated if there has been little or no control over the classification of data and its deletion.

In some organisations, IT will have been involved in the decision-making which led to this proliferation. Ideally, the use of unconventional data sources (that is, anything beyond e-mail, Microsoft office files and structured data) will have been the subject of a policy taking account of all foreseeable eventualities including eDiscovery. Similarly, many companies have document retention policies which dictate what is kept and what is deleted, with provision for the interruption of deletions where necessary.

Even in this idealised situation, an eDiscovery demand can be disruptive. If any of these elements are not in place then the burden which falls on IT can be crippling or, at least, very demanding and expensive.

Many companies lack one or more of these elements, meaning that IT has urgent responsibility for things over which it has had no power.

This is part of the “gap” referred to in the title to this paper. The position may be that no-one in the organisation has the knowledge and experience to cover all the implications which arise on an eDiscovery demand. Those with the need will not be alert to the technical implications of, say, retrieving social media, whilst those with notional responsibility for the organisation’s technology are unlikely to be aware of the potential scope of a demand, whilst being expected to react to it urgently.



Those who, like ZyLAB, provide software and services across the full range of an organisation's activities, will have seen it all before and, perhaps uniquely, will be aware of both the "Duty" element in the Information Management Reference Model and the "Asset" component represented by the data and its supporting technology.

The need for such services will often (though not always) arise at the instigation of an IT department which has been made aware of the potential for disruption and seeks to head it off. Less ideally, it may need urgent advice on the occurrence of a trigger event. That, all too often, results in demands for a solution "yesterday". It will always conflict with an organisation's usual time-frames and procedures for specifying, identifying and budgeting for new technology and with the resources generally available for implementation and training.

A human as well as a budgeting matter

There is a story, unattributed but wholly credible, of an external consultant who was invited to talk about these things to a company. The opening to his speech, intended as an ice-breaker, was “you have the advantage of knowing each other whereas I know none of you”. He realised as he spoke that this was simply not true and that the IT and legal people present did not actually speak to each other.

This is often both a physical and a psychological issue. IT departments are often located remotely from those whom they serve; automated help-desk requests for existing installations reduce personal interaction, and there is reduced communication between users and internal providers, both in terms of user needs and when a new application or an upgrade is rolled out.

If this is true of routine business needs then it is obviously even harder for there to be communication about specific information management needs and solutions such as eDiscovery where, as identified above, IT knows little of the business requirements and users have little grasp of the technical problems or the potential solutions.

The real issue is one of communication and mutual education. Someone with IT knowledge should be given responsibility for liaison with users both on routine matters and on more esoteric needs and opportunities. Such a person might be more than merely a conduit for problem-solving and become the champion for the IT department itself, for users with identifiable needs (that is, business needs for which IT offers solutions), and for products and services which meet those needs. Having identified problems and potential solutions, this person would then help convert the requirement into a business case, pulling together the internal stakeholders and an appropriate external provider to navigate the internal budget and authorisation procedures, to set expectations, to calculate the return on investment and generally to make it happen.

Quite apart from the benefits to the organisation, there are career opportunities here for the individual who acquires the skills and the status to fulfill this role. Service departments like IT are increasingly under threat from outsourced providers and from automation. These may prove to be the answers to part at least of the eDiscovery problem when it arises, but that increases the need for a liaison and project management role within the company.

The next section looks more closely at the gap which presently exists in most organisations between those who have the business problems and those who can offer the solutions.

Matching the solutions to the problems

The conventional approach to procurement within large organisations is often institutionally unsuited to meeting the challenges of eDiscovery. The 2011 Gartner Magic Quadrant for eDiscovery Software summarised the position in this way:

Many purchases of software and technology services are decided by the IT department (with input from the finance department and perhaps the procurement department). With e-discovery software, however, at least three groups within the corporation and one outside the standard corporate or governmental hierarchy are potential buyers.

The IT department has the main say in buying archiving solutions, with a great deal of input from the legal department as to how the software handles retention, identification, preservation, collection and early case assessment ... if these capabilities are part of the vendor's offering.

The legal department typically decides on purchases of ECA, review, analysis and production software. In many cases, particularly when this functionality is purchased as SaaS [Software as a Service], the IT department is not consulted at all. Legal departments still rely on outside counsel to advise – or sometimes tell – them which SaaS providers to use. Even when outside counsel is not involved, legal departments still want to avoid involvement with enterprise IT departments or to form their own IT departments. In the past they were also able to avoid having to use corporate procurement functions when purchasing external legal services, though this situation has changed as a result of an intense focus on cost cutting during the recession of 2008 to 2009. The source of the friction here is twofold. Legal staff have never before had to involve IT staff in these decisions, and in some cases they view them as unresponsive or obstructive because of implementation cycle times. Procurement staff, for their part, are struggling to understand the pricing, service and support models historically used by legal service providers.

If this is right, then part of the move towards a SaaS solution may be precisely because it allows legal and compliance departments to by-pass the IT department. A SaaS solution, paid for transaction by transaction, may in fact be the right approach, but it is not right to go down that route simply to avoid having to deal with IT. One hears of examples going both ways – on the one hand of IT objecting to a solution whose concept and function they did not understand or a procurement timeline which took no account of the urgency of a typical legal department requirement and, on the other, of legal departments' unrealistic expectation that a new system can be specified, approved, installed and ready to run with trained users by yesterday.

Just as there is no standard “problem” in eDiscovery, so there is no solution which is right, ‘out of the box’, for all circumstances. The choice between an in-house solution and one which is entirely provided externally depends on an analysis of frequency, volumes, urgency and cost, as well as questions like the availability of internal resources, including suitably skilled (and available) staff.

Increasingly, companies are turning to a trusted third party provider who, like ZyLAB, is able to offer all relevant permutations of in-house and external resources, to help determine what is right for the organisation. As with most things, pre-emptive planning is better than ad hoc reaction to problems which must be dealt with immediately.

Decisions about things like this involve more than functionality and transactional cost. Someone needs to have an overview of what the company’s total outlay is in a year on external providers of software and related consultancy as well as on external lawyers and to compare that with the costs of taking some or all of that functionality in-house.

At a budgeting level, this is almost too obvious to recite – there are many other areas of a company’s business for which it is necessary to anticipate foreseeable external costs for a year and to set them against a one-off capital cost plus maintenance costs to see how many years it would take before the asset – software in this case - becomes effectively free to use. The pure mathematics of that may be qualified by the availability or otherwise of capital budget. The budgeting questions themselves may be confused by the departmental breakdown of the risks and responsibilities because it is hard for any one department to assess what contribution it should make to an acquisition relative to its share of the problems and its benefit from the spending.

However obvious the mathematics, the real challenge is getting an overall corporate view to override the departmental or sectional interests.

The risks to be considered

The preceding section implies that situations arise which are important for the company for various reasons which include but are not limited to cost, which involve or depend upon IT departments but are considered “not their problem”. Some of these problems are so serious and so urgent that, according to Gartner in the passage quoted above, legal departments “form their own IT departments”, viewing IT staff as “unresponsive or obstructive”. By implication as well as by anecdote, IT staff see these demands as a distraction from their own job of keeping the infrastructure up, the e-mail flowing and the hackers and viruses at bay.

It is worth reciting briefly what these reasons might include and why they matter to the company. Taking them in no particular order:

Litigation – the company wants to bring or must defend civil proceedings and must give disclosure of documents under the rules. Before they can do that, the lawyers need to know what document sources the company has and to get some idea of the volume in order to begin to assess the scale of the problem, quite apart from what the documents say.

Regulation – a letter, or perhaps a large squad of investigators, from a regulator has appeared in reception. A large range of documents must be produced, and quickly. The problem is the same as for litigation save that the regulator will not wait for the relatively leisurely timescales allowed in litigation; besides, the company’s share price and its ability to continue trading turns on a swift and proper response.

The Bribery Act – as above, save that the visitor is a prosecutor not a regulator, has powers over all commercial organisations and not merely regulated ones, and has prison sentences amongst his possible remedies.

Investigations – the HR or audit department raise concerns about an employee which require immediate investigation, including analysis of e-mails and other documents, including the employee’s relationships with other people within or outside the company. The least of the issues is that the company might be losing money – there may be IP protection or other confidential information at stake, and every hour counts.

A whistle-blower – allegations are made about the company with a threat to take them to the appropriate authority. Prompt investigation may satisfy the whistle-blower that the allegations are unfounded; alternatively it may show that the allegations are correct which may trigger a range of implications including a self-reporting obligation.

This is not necessarily a complete list, but it is enough to show that legal, compliance, HR and other departments may have urgent need to involve IT in the preservation, identification and collection of an unspecified range of documents and data for reasons which may involve substantial risk and expense to the company, perhaps affecting its reputation and viability and not merely its bottom line.

As a budgetary matter, the costs of these exercises may be spread between departments, including the business department whose activities have given rise to the problem. It is quite possible that no one in the company will have an overview enabling the observation that these are all costs of broadly the same kind and should be considered together as a prerequisite for considering if there is a better approach. To the IT department, this may not be considered a cost at all, merely an unwanted call on time and resources.

Any of these may trigger a requirement to collate and analyse information not only about the data sources (the “Assets” in IMRM terms) but about the state of knowledge of particular people within the organisation. They may also require some urgent decision-making. It is for the legal and compliance departments to specify what is needed, but an IT department which has at least a broad understanding of the likely needs is better able both to provide them on demand and (more usefully) to consider how they can be pre-empted by policies and by the technology support for those policies.

The table below is far from comprehensive, but it gives some idea of the factors which arise, often without warning:

Trigger	Data demanded by a third party – opponent in civil litigation, regulator, prosecutor, internal investigator
Data	User files (e.g. Microsoft Office), email, IM, blogs/Twitter/Facebook, web sites, multiple in-house data-types
Sources	Mail boxes, file shares, structured databases, SharePoint, phones, tablets, memory sticks, home computers, cloud, social networks, paper
Classification	Relevant information qualified by considerations of confidentiality and privilege in addition to the culling of irrelevant information
Unknowns	Is there more? Who knew what when? How many stones must be turned over?
Consequences	Expense, penalties, sanctions, reputational damage, share price, non-executive directors’ concerns, consequential claims or investigations
Assessments	Risk, cost, how much do we really need?

Anticipating the problems

A glance at the table in the preceding section shows the sort of demands which IT departments may have to respond to urgently in relation to matters of which they have had no prior warning, still less any opportunity for pre-emptive input commensurate with the responsibility. It goes beyond the scope of this paper to define what policies and procedures ought to be in place to anticipate such eventualities, but it is clear that IT departments ought to have a role in defining them or in initiating them.

The introduction of new data types and sources (instant messaging (IM) and tablets for example) will often initiate questions about security – it becomes immediately obvious to an IT department that such sources have the potential to bypass existing security arrangements from the moment the first user introduces them and, generally, a mixture of policies, staff rules and technology defences are devised to repel or accommodate the threat.

eDiscovery demands warrant the same attention. Once an IT department is made aware of the possibility of the kinds of demands identified in the preceding section, it becomes obvious (or ought to become obvious) that anticipatory steps must be taken. Two broad questions arise: the primary one concerns the bare ability to comply with the demands, raising questions as to whether all the data types and sources can be preserved and collected; the second involves the need for a data retention policy which defines how much data must be kept (for business reasons or to meet the “Duty” obligations of the IMRM) and what can be safely deleted.

How is this to be achieved when IT departments do not fully understand the needs of the business units and of the legal and compliance departments, and when the users have no concept of the technical implications? How is the process to be initiated in anticipation of one of the triggering events referred to above, that is, before the pain of an actual eDiscovery exercise shows up the defects in the existing systems?

How to Bridge the Gap


The overarching answer to this question at the highest level is that companies ought to have a governance, risk management and compliance (GRC) structure with oversight of all the disciplines and functions within the company. It is well beyond the scope of this paper to cover that, and also usually beyond the power of the departments affected by the issues discussed here.

A GRC regime involves devising a strategy which rests on processes, people and technology. A process, in the context discussed here, is the answer to the question “What do we do if...?” and it is clear that the answers would not include those which Gartner identified as being common as between legal and IT departments. If a SaaS solution was in fact the right one, that should be because legal and IT had agreed on it after considering the options, not because legal felt it was the only way of solving the immediate problem. IT liaison should be by seconding someone from the company’s IT department to the legal department, not by the latter setting up its own IT department – avoiding duplication of effort and resources is one of the functions of a proper GRC regime.

In the absence of corporate overview, the burden falls on the department which has the problem to negotiate with others who share the problem or whose similar problems might be eased by a concerted approach. If, for one or more of the reasons identified above, legal, compliance, HR, audit and IT all make or receive demands for a rationalised and unified way of managing information, then they might join forces (and budgets) to share both the cost and benefits of the investment. The one most affected will presumably take the lead in identifying alternative software solutions and can then “sell” that idea to others. Very often, the department most affected is the IT department.

Three factors make it certain that eDiscovery problems are going to get bigger and more frequent: demands for data increase all the time with increasing regulation and as the courts insist that electronic data be disclosed electronically; the range of sources of disclosable data widens continually, particularly with the growth of social media; and pure volumes go up all the time, doubling year on year for some organisations. The need to know what is stored in the organisation’s “liability vault” cannot be ignored.

Leaving aside the less than ideal circumstance that some crisis prompts the reaction “never again”, the development of appropriate policies and procedures, and the investment in technology solutions to back them, is likely to happen only where a “champion” promotes a project which understands the business needs across the enterprise and develops a plan which addresses them.



eDiscovery is a “problem” but it is better to approach it as an end use of an enterprise-wide system which does more than merely solve problems. Solutions such as the ZyLAB Information Management and eDiscovery Platform are designed to maximise the value of the data and address daily information management needs rather than merely “solve” the eDiscovery problem.

This can best be done by involving a potential provider of software and services as a trusted adviser prior to specification to help develop the business case. Such an adviser brings more than merely the ability to sell its own solution. Part of the problem inherent in the “gap” which is the theme of this paper is that no one person or group within an organisation is aware of all the potential use cases for an enterprise-wide system such as ZyLAB’s, which embrace records management, compliance and litigation readiness, communications intelligence and archiving as well as the mechanics of preservation, collection and all the other components of the EDRM.

Each of these use cases currently has a cost, both internally and with outside providers of both legal and technology services. Part of the exercise is to identify what that cost is and to show how it can be reduced and/or better spent for both the conduct of routine business and for disruptive events like eDiscovery.

A trusted adviser like ZyLAB has seen it all before in a way which no one organisation can, as a result of working with similar organisations. They make good allies for an internal champion who may come from either side of the “gap” but who is unlikely to have feet in both.

About ZyLAB

ZyLAB's industry-leading, modular e-Discovery and enterprise information management solutions enable organizations to manage boundless amounts of enterprise data in any format and language, to mitigate risk, reduce costs, investigate matters and elicit business productivity and intelligence.

For nearly 30 years ZyLAB has been a dominant player in compliance and e-Discovery-related solutions, due in part to its' advanced capabilities for multi language support, searching, content analytics, document reviewing, and e-mail and records management (for both scanned and electronic documents).

While the ZyLAB eDiscovery & Production system is generally implemented to investigate a specific legal matter, it is a solid and robust foundation from which to pursue proactive, enterprise-wide objectives for information management. Those broader goals are achieved through the use of the ZyLAB Compliance & Litigation Readiness system.

The ZyLAB eDiscovery system is directly aligned with the Electronic Discovery Reference Model (EDRM) and features modules for forensic sound collection, culling, advanced e-mail conversion (Exchange and Lotus Notes) and legal review.

The company's products and services are used on an enterprise level by corporations, government agencies, courts, and law firms, as well as on specific projects for legal services, auditing, and accounting providers. ZyLAB systems are also available in a Software-as-a-Service (SaaS) model.

ZyLAB's products are extremely open and scalable, with installations managing some of the largest collections of mission-critical data in the world. The award-winning ZyLAB Information Management Platform bundles our core capabilities into a single solution that provides an optimal framework for six, specialized, all-in-one system deployments.

Currently the company has sold 1.7 million user licenses through more than 9,000 installations. All of our solutions include full installation, project management and integration services. Current customers include The White House, Amtrak and US Army OIGs, US Department of Treasury, The EPA, National Agriculture Library, and Royal Library of the Netherlands, FBI, Arkansas and Ohio state police forces, German customs police, and Danish national police, War Crimes Tribunals for Rwanda, Cambodia, and the former Yugoslavia, KPMG, PricewaterhouseCoopers, and Deloitte, Akzo Nobel, Sara Lee, Pacific Life, Siemens, Dow Automotive and Lloyds of London.

ZyLAB has received numerous industry accolades and is one of the few companies to be positioned as a Leader in Gartner's "Magic Quadrant for Information Access Technology" for 2007, 2008 and 2009. ZyLAB has received numerous industry accolades and is one of the few companies to be positioned as a Leader in Gartner's "Magic Quadrant for Information Access Technology" for 2007, 2008 and 2009. In addition, Gartner has given ZyLAB the highest rating ("Strong Positive") in its "MarketScope for E-Discovery and Litigation Support Vendors" for 2007, 2008 and 2009, as well as a "Visionary" rating in its 2011 "Magic Quadrant for E-Discovery".

ZyLAB is certified and registered as compliant with the International Standards Organization (ISO) 9001:2000. ZyLAB also lets Microsoft, Oracle and other infrastructure providers regularly certify critical components that work closely with their infrastructure. ZyLAB was certified under the US-DoD 5015.2 records management standard and ZyLAB is compliant with the European MoReq2 standard and various other regulations

Headquartered in Amsterdam, the Netherlands and McLean, Virginia, ZyLAB also serves local markets from regional offices in New York, Barcelona, Frankfurt, London, Paris, and Singapore. To learn more about ZyLAB visit www.zylab.com

Copyright:

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of ZyLAB Technologies B.V. The information contained in this document is subject to change without notice. ZyLAB Technologies B.V. assumes no responsibility for any errors that may appear. All computer software programs, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. ZyLAB Technologies B.V. either owns or has the right to license the computer software programs described in this document. ZyLAB Technologies B.V. retains all rights, title and interest in the computer software programs.

This White Paper is for informational purposes only. ZyLAB Technologies B.V. makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer software programs described herein. ZYLAB TECHNOLOGIES B.V. DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall ZyLAB Technologies B.V. be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.

Copyright © 2009-2011 ZyLAB Technologies B.V. All rights reserved.

ZyLAB, ZyIMAGE, ZyINDEX, ZyFIND, ZySCAN, ZyPUBLISH, and the flying Z are registered trademarks of ZyLAB Technologies BV. ZySEARCH, ZyALERT, ZyBUILD, ZyIMPORT, ZyOCR, ZyFIELD, ZyEXPORT, ZyARCHIVE, ZyTIMER, and MyZyLAB are trademarks of ZyLAB Technologies B.V. All other brand and product names are trademarks or registered trademarks of their respective companies.

www.zylab.com

ZyLAB[®]
eDiscovery & Information Management