



## Is Your Enterprise ‘Information Risky’ or ‘Information Ready’?

The size and complexity of enterprise data stores have increased to the point that information now poses more of a challenge than an advantage to most enterprises. The processes of categorizing, preserving, collecting and searching data have always been complex and costly to manage and maintain. This challenge is exacerbated by the fact that enterprises are creating exponentially more data every year, with increases of 50-100% annually – a growth rate that doubles to 100-200% when focusing on the skyrocketing amount of unstructured enterprise data (e.g., email, Web pages, instant messages, etc). And, when combined with increasingly stringent regulatory oversight and the threat of litigation constantly looming, enterprise data management has quickly evolved from a challenge to a full-scale threat.

In today’s data-driven world, enterprise competitiveness is often dictated by how quickly, accurately and thoroughly knowledge workers can locate the information they need. It was recently estimated that the inability of knowledge workers to efficiently search burgeoning data stores costs US businesses \$900B in lost productivity (source: Basex).

In most cases, enterprises are still relying on manual processes or one-size-fits-all solutions. Both of these methods dramatically raise the costs associated with finding and collecting information and create exponentially more work and risk for IT departments. While the recent financial crisis has certainly put these challenges under the microscope, enterprises always need to be thinking strategically and proactively about how to minimize exposure from information risk.

While it’s impossible to completely eliminate such threats, there are a series of steps that enterprises can and should take to mitigate exposure and convert data stores from a liability into a competitive advantage. What follows is an eight-step checklist that will help determine how prepared an enterprise is to deal with information risk. The elements are ranked by importance, each with an assigned point value (with more points equaling less risk). Check the elements that you feel accurately describe your enterprise then tally your score to see where your company stands.



## 10 points – Email: Managed, Maintained and Understood

### **Overview:**

The enterprise has clear email retention policies, automatically categorizes email in storage repositories and can quickly and cost-effectively handle email as part of eDiscovery.

### **Why it's important:**

Over the last decade, email has not only evolved into the primary form of business communication, but also now represents the most commonly occurring business record and source of electronically stored information (ESI). It has been estimated that email constitutes 80% of all ESI in a typical lawsuit or regulatory investigation. Government and other industry regulators routinely request massive quantities of email as part of their inquiries, while 2006 revisions to the Federal Rules of Civil Procedure (FRCP) require that email be produced in a timely manner as part of a discovery request in litigation. Having clear email policies and a comprehensive, automated categorization and legal hold system not only reduces risk but also improves overall employee productivity – while lowering IT costs.

### **Potential risk:**

In a word: massive. It has been estimated that the average eDiscovery event can cost enterprises upwards of \$20,000 per GB of data, resulting in millions of dollars in potential eDiscovery costs for any given proceeding. Given the role that email plays in eDiscovery and the sheer amount of email-based information being created, this problem has escalated into a significant threat.

## 10 points – eDiscovery Responsiveness

### **Overview:**

The enterprise can quickly, consistently and comprehensively respond to eDiscovery or regulatory inquiries (e.g., verify data map, preserve data, identify, preserve and collect data, etc.).

### **Why it's important:**

The ability to quickly and accurately identify appropriate custodians and access the right ESI is critical to limiting compliance, investigatory and eDiscovery risks and costs. Civil procedure rules typically allow only a brief window in which to identify, preserve, and begin collecting relevant data before the risk of spoliation (i.e., destruction or alteration of evidence) ensues. With one GB of ESI equaling 10,000-75,000 hard-copy pages, a single lawsuit can result in the production of more than one TB of material – the equivalent of 75 million pages.



**Potential risk:**

There is a wide assortment of risks ranging from the quantitative (e.g., fines, unfavorable judgments and increased operating costs) to the qualitative (e.g., reputational/brand diminution or loss of intellectual property). Alternatively, producing too much ESI may result in releasing privileged information with serious consequences on future strategies or product plans.

**10 points – Communication and Collaboration**

**Overview:**

The enterprise has tight integration with and open communication between the IT and legal departments.

**Why it's important:**

In order to effectively meet information management, eDiscovery and regulatory challenges, the departments need to have a clear understanding of their respective roles and open communication about individual and confluent needs. Legal and IT must communicate openly and regularly to ensure that legal counsel is not making technology decisions and, more importantly, IT is not making legal decisions. Furthermore, open communication between the two departments helps legal counsel understand the limitations and parameters of an enterprise's ability to identify, locate, preserve, collect and produce electronic data, without which inside counsel cannot effectively defend and protect the enterprise.

**Potential risk / cost:**

The most notorious instance of this may be the Zubulake series of cases, all of which stemmed from a discrimination and retaliation suit starting in April 2005. During the trial it was revealed that UBS had not preserved relevant email after the legal hold had (ostensibly) been implemented, leading the judge to give the jury an "adverse inference" instruction and eventually resulting in an almost \$30 million dollar settlement in favor of the plaintiff. An enterprise's inability to implement an effective legal hold process – and all of the requisite damage flowing from such an event – is just one example of the consequences of lack of communication between IT and legal departments.

**9 points – Bringing eDiscovery In-house**

**Overview:**

The enterprise uses automated tools to search for, assess, sample, collect, process and cull relevant ESI – all in-house (i.e., within the organization and not via 3<sup>rd</sup> party service providers).



**Why it's important:**

Any enterprise involved in regulatory inquiries, internal investigations or litigation knows that legal holds represent a critical step in the process of responding to a subpoena or summons – probably the single most important step. Organizations must invest in a toolset that can find, preserve and collect relevant ESI while simultaneously obviating the need for expensive, time-consuming 3<sup>rd</sup> party processing and culling providers. In today's challenging economic environment, every area of the business is being closely scrutinized in the search for cost savings - including legal and its ever-increasing eDiscovery expenses.

**Potential risk / cost:**

Failure to conduct timely, comprehensive and accurate notification, preservation and collection of ESI can present large legal bills and even greater risk down the road. This is particularly important with enterprises becoming more global in nature, as the prospect of forensic imaging of tens or hundreds of custodians' laptops all over the US and world is not just unnecessary but downright risky.

**9 points – Have a Policy and Plan...and Revisit Both Regularly**

**Overview:**

The enterprise doesn't react or respond hastily to crises but has a regularly scrutinized policy and proactive plan for responding to events.

**Why it's important:**

By the time an enterprise receives an inquiry from the government, subpoena or summons, it is far too late to respond rationally, thoughtfully and cost-effectively. In contrast, identifying potential problem areas upfront and planning accordingly allows an enterprise to prepare/respond far more accurately, comprehensively, consistently and cost-effectively.

**Potential risk / cost:**

Without having had the benefit of a sound policy, enterprises are at the mercy of claims their internal policies and practices were unreasonable – which can create myriad sources of unnecessary risk from countless potential adverse parties – as well as high prices from 3<sup>rd</sup> party vendors brought in at the last minute. Without an effective response plan, enterprises find themselves constantly under the gun, with a response that is fraught with far more risk and cost than is necessary.



## 8 points – Users’ Ability to Find Things is Critical

### **Overview:**

The enterprise recognizes the critical role played by search throughout the enterprise. It doesn’t rely solely on a single, one-size-fits-all search technology or simple keyword search, but supplements search tools with more accurate and relevant search capabilities (e.g., conceptual search).

### **Why it’s important:**

Even with documented evidence of the inherent limitations of keyword-centric search methodologies, enterprises and the eDiscovery industry still largely rely on this outdated approach. These limitations have been on public display in countless research reports (e.g., IDC’s proclamation that enterprise search users find what they seek only 30-50% of the time) and in several high-profile cases such as *U.S. v. O’Keefe*, *Equity Analytics v. Lundin*, and *Victor Stanley, Inc. v. Creative Pipe, Inc.* This has spurred many leading enterprises to deploy far more sophisticated – and effective – search tools to allow their employees to access the information, expertise, relationships and projects they need instantly and securely, while enabling their legal and risk departments to concomitantly find the people and information they need – instantly.

### **Potential risk / cost:**

On a broad scale, homogeneous, one-size-fits-all search applications (e.g., Google or Autonomy) have failed miserably: a recent Information Week survey detailed broad user dissatisfaction with ‘Enterprise Search v2.0’ applications and their (in)ability to help users complete their daily tasks. This represents incalculable losses in productivity, revenue and information risk exposure.

## 7 points – Enterprise-wide Information Access is Highly Secure

### **Overview:**

The enterprise can manage access to information in a highly secure manner across multiple systems.

### **Why it’s important:**

User and content-based access to search results has wide-reaching benefits across the organization. Customizing the search process to match the needs and specific requirements of individual employees will greatly improve relevancy and reduce the time spent filtering through results. It also greatly simplifies management and provides more control and a better display for IT administrators and KM workers. In professional service firms, permission control will limit any breach of confidentiality by ensuring that specific teams are segmented within the firm.



**Potential risk / cost:**

Two primary risks: lost productivity and confidentiality / confidence. Enterprise search without access controls forces employees to search within search results, causing enormous productivity losses and limiting the overall efficacy of the application. For professional service firms, the inability to construct and maintain ethical walls between internal teams can lead to breach of client confidences and duty of loyalty owed to clients, not to mention potential regulatory violations in some jurisdictions. Not only does this have severe legal implications, but can also lead to even more damaging reputational loss.

**6 points – Ability to Find Experts Should Be Easy, Instant and Automated**

**Overview:**

The enterprise uses automated tools to allow employees to instantly locate expertise within the organization, securely and regardless of geography or language.

**Why it's important:**

While information is the lifeblood of today's businesses, the individual expertise of an enterprise's employees is still its most potent competitive advantage. With experts spread across the globe in myriad teams and business units, it can be increasingly difficult to identify exactly who knows what within an organization – a situation exacerbated by massive layoffs over the past few quarters. In addition to the ability to seamlessly access different data sets, employees in 'Information Ready' enterprises can immediately find and collaborate with colleagues who have unique expertise or specialized knowledge. Having one centralized, searchable directory of experts in the organization saves incalculable time and ensures that each employee is working with the most current resources available.

**Potential risk / cost:**

The threat of employees working with less than adequate resources and knowledge is significant. The ultimate goal of the 'Information Ready' effort is to convert enterprise data from a threat to a competitive advantage. Having real-time access to experts across the organization represents a crucial – and often overlooked – step towards achieving this goal.



## **Score Card**

### **60 points or higher: *Information Ready***

While it's impossible to completely eliminate information risk, your enterprise has significantly reduced its information risk exposure by having the technologies, people and policies in place to respond quickly and adapt to new threats and challenges. Your enterprise has an information-based competitive advantage over its peers.

### **50-59 points: *Almost Ready***

Your enterprise has made great strides towards controlling its information risk and information-related challenges, but there's still work to be done before it is 'Information Ready.'

### **40-49 points: *At Risk***

Your enterprise has made some level of information-preparedness investment but still has quite a bit of work to do in order to minimize information risk.

### **Less than 40 points: *Information Risky***

Your enterprise needs to make a significant investment in modernizing the information management infrastructure to lessen reliance on manual and/or outdated processes, in order to minimize the threat of information and enable your employees to be more effective overall. Your enterprise is likely at a competitive disadvantage to its peers.