



DEFENSIBLE DATA SOLUTIONS™

The E-Discovery Maturity Model

ADAM HURWITZ, CISSP
September 2010

E-Discovery has evolved and grown over the last ten years to become a necessary part of doing business. Companies have enormous quantities of electronically stored information that are clearly subject to discovery in legal and regulatory matters. Yet most companies struggle to incorporate e-discovery as a business process, mainly because of its vast scope and the evolving governing laws. Accurately accessing, searching and preparing the large volume of information that is stored on many different systems, created by numerous employees, working in different departments and diverse locations, in the short timeframe permitted, is a daunting task made more difficult by the stringent rules that govern how that process must occur to be legally defensible.

The process itself has been described at a high level in the well-known E-Discovery Reference Model (EDRM), which has come to be used by almost everyone seeking to understand and talk about e-discovery. But there has been no real guidance for companies to measure their maturity in implementing that process or to chart their development. Many companies want (and need) to improve their execution of e-discovery, but are not sure how to progress.

The E-Discovery Maturity Model remedies this lack of direction and common understanding. The Maturity Model has been created following eight years of observation and consulting to a diverse sample of companies, each grappling with e-discovery requirements. The Maturity Model documents the evolution of organizational e-discovery strategy used to respond to litigation or regulatory demands. As a maturity model, it has the standard 5 levels that range from “ad hoc and chaotic” at early stages to degrees of “optimizing” at more mature stages. Besides describing the different levels of process maturity, the movement through the levels of this model also represents the acceptance and incorporation of e-discovery as a necessary business process.

E-Discovery Maturity Model

Level	Focus	Strategy	Expertise	Costs
5 Integrated, Optimized	Automate and Integrate	Legal and IT Manage In-house with Strategic Vendor Use	Expert Team of Legal and IT	Shared Costs, Mainly with IT
4 Semi-Integrated	Reduce Costs	Legal Manages Blend of Vendor and In-house Resources	Single Expert in either Legal or IT	Targeted Reductions
3 Standardized	Standard, Repeatable Process	Vetted and Trusted Vendor(s)	Expert at Trusted Vendor	Controlled
2 Managed	Plan and Manage	Outside Counsel Manages Many Vendors	Expert at Outside Counsel	Overruns, Unexpected Costs
1 Ad Hoc, Chaotic	Just Get It Done	Individual Heroics	None	Surprising

© 2010, Business Intelligence Associates
www.biaprotect.com

Level 1 – Ad hoc, chaotic process. The company has little to no experience with e-discovery and the risks involved with evidence spoliation, chain of custody, legal hold, etc. The process is completely unstructured and frequently moves in fits and starts. Decisions are made by outside counsel, and integration with corporate resources is often strained due to overall corporate inexperience or lack of effective preparation for the process. IT makes collections, generally without knowledge of the requirements for a forensically-sound collection, and is not clearly directed or coordinated by anyone. Different data is collected from custodians at different times. A variety of tools and methods are used.

Level 2 – Managed process. The company is learning about e-discovery and has decided to trust outside counsel to manage the process from the beginning, generally because the company has become aware of and is appropriately worried about the risks involved. Outside counsel utilizes multiple service providers. The company relies on outside counsel to select vendors. IT and internal resources are coordinated by outside counsel. A set of tools is used throughout the project, but they are the favored tools of each vendor and may not work well together. Both the company and/or its outside counsel may not fully understand all of the technical issues involved, which can result in miscommunications with the vendor(s).

Level 3 – Standardized process. The company has picked a trusted service provider (partner) to manage the whole process in a repeatable fashion. This partner standardizes the process across matters and the implementation across the organization. The legal department generally has an e-discovery paralegal or staff attorney to manage the process internally. The company likes the idea of mitigating risk through vendor services and understands that someone may have to testify about the process. The company has probably selected one of the vendors that its outside counsel had used. IT and internal resources are coordinated by the vendor and produce efficiencies, especially as the vendor establishes relationships with individuals in the company. There are few technical problems across the whole process. And for the second e-discovery project, there are additional savings that appear from re-use of collected data and protocols.

Level 4 – Semi-integrated process. The company brings specialized knowledge and tools in-house for targeted parts of the process. The company uses a combination of internal resources and service providers. With an understanding of e-discovery nuances, the focus now is on reducing costs, but not through integration. The legal department is confident about its e-discovery knowledge and has a lawyer managing the process. Company-wide IT policy and systems are not fully engaged, but it is likely that Legal has begun developing and deploying policy management of information. The first area that is frequently addressed is email management and archiving. Collections are generally handled by IT security personnel who are familiar with forensic principles. The relationship with IT is a standard business unit relation with the typical frustrations, because IT does not understand the full range of legal needs nor does it have the resources to devote to the endeavor. But the IT department now realizes that it must acquire a more in-depth understanding of e-discovery.

Level 5 – Integrated and optimizing process. This company has brought the e-discovery process in-house and makes strategic use of vendors. The focus is on integration of IT systems, like ECM, Enterprise Search, Archiving, etc. The company has expert level e-discovery knowledge and may have an AGC focused on it. There is Legal – IT co-ownership of the process, and an e-discovery team involving the CIO and business unit representatives has likely been formed. This team has a strategic perspective on company e-discovery efforts and is not purely project-motivated. IT policies and procedures are reviewed and modified accordingly. For example, the company data retention policy may have been rewritten.

The general motivation in progressing through these levels starts out as risk in the lower levels and then shifts to cost in the higher levels. The risks in the e-discovery process are obviously highest at the bottom of the Maturity Model. Risk drops considerably at level 3, because having a standard, repeatable process controlled by a set of experts is essentially what is required of the process. At levels 4 and 5 there are further controls for risk, as the company will start incorporating e-discovery into IT policies and procedures, but they are relatively small steps from 3. These higher levels are focused on reducing costs and improving the internal management of the process; however, progressing from level 3 to 4 and onto

5 requires investment in products and personnel. Level 5, for instance, will usually involve a significant, one-time cost for a large integration project. So companies with a low volume of e-discovery matters will not see the benefit, nor have the resources, to mature beyond the middle levels. The higher levels are populated right now with companies that have a high volume of matters and the associated costs that go with them.

About BIA

For almost a decade, BIA has been developing and implementing defensible, technology driven solutions that reduce the costs and risks related to litigation, regulatory compliance and internal audits. BIA offers enterprise software solutions complemented by mature professional services in the areas of Litigation, Digital Investigations and Electronic Policy Consulting. BIA provides software and services to Fortune 1000, Global 2000 companies and Am Law 100 law firms. Headquartered in New York City, BIA also has offices in San Francisco, Seattle, Washington DC and in Southwest Michigan. The company maintains digital evidence response units throughout the United States, Europe, Asia, and the Middle East. BIA's unique and positive workplace culture promotes diversity and celebrates the professional skills of each individual.



About the Author

Adam Hurwitz, CISSP

BIA CIO

Adam Hurwitz has over twelve years of information technology experience. As CIO, he oversees the development of BIA's industry leading e-discovery software for collection and processing of electronically stored information (ESI). Adam directs and manages computing and information technology strategic plans, policies, programs and schedules for business and finance data processing, computer services, network communications, and information management services. He previously served as BIA's Senior Database Expert on matters involving the analysis of large enterprise databases and IT systems, including ERP, Oracle, and various proprietary and legacy systems. He is a Certified Information Systems Security Professional (CISSP) and has a BA from Vassar College in both Physics and Philosophy.

If you have questions or comments about this article, Adam Hurwitz can be reached at:

ahurwitz@biaprotect.com