Choosing the Right In-House Electronic Discovery Solution for Your Organization

Buyer's Guide for IT Professionals

Guidance® SOFTWARE

I. Overview

Once an organization makes the decision to move forward with bringing their e-discovery process in-house with an onsite solution, careful review should be done to ensure the right vendor solution is selected. This buyer's guide is designed to help IT professionals navigate both the technical requirements and the legal electronic discovery requirements to make the right selection when purchasing and implementing an in-house e-discovery solution.

E-discovery is a process that involves many different stages and collaboration with internal and external resources; including: inside legal counsel, IT, and outside counsel who must work together for success. It can be difficult to decide on the right solution in terms of the best technology, people, and processes. Additionally, because of the varied vendors positioning their products as in-house e-discovery offerings, it has become increasingly difficult for corporate IT and legal teams to make the right decision.

One, key selection consideration is ensuring full-fledged legal hold capabilities are part-and-parcel of any comprehensive in-house e-discovery solution; including, hold notices, auto-reminders and auto-escalations, online custodian surveys, and automated tracking and reporting. Given the critical nature of legal holds in fulfilling preservation duties, offerings that do not include these capabilities should be removed from the evaluation list.

There are other critical in-house e-discovery solution features. Any offering must provide the in-house team with the means, broadly speaking, to collect data, process it, and view it. However, when looking at the specifics of available solutions, it is clear that a full-featured offering should have the following capabilities:

- First, an in-house e-discovery solution should be able to handle all types of cases and should not rely on the operating system to view and collect data. For example, there are a set of cases – such as IP theft, FCPA, fraud, or employee disputes– in which hidden data may be critically important. E-discovery solutions that rely on the computer operating system can only "see" what the operating system presents to them, so critical evidence can be missed entirely. Because of this, solutions that rely entirely on the operating system simply cannot be used.

- Second, an in-house solution should fit easily within the organization's existing infrastructure without additional resource burden on the IT department and should not disrupt custodian (employee or executive) use of their computer during collection.

- Third, an in-house solution should offer the ability to enhance your position before litigation strikes by cleaning up irrelevant, outdated, useless data that you don't need for your business.

- Fourth, an in-house solution should not miss potential evidence. It is important that it supports compound searches (i.e. "dog" or "cat" with five instances of "house" or tree" or yard"), and that it unpacks and searches embedded files, several layers deep (i.e. a Zip file with a Word document that has an embedded Excel spreadsheet that has an embedded PowerPoint presentation).

- Fifth, the solution should automatically preserve all file and email metadata. With this you avoid disputes over which metadata fields are relevant, and, more importantly, avoid the problems that have befallen litigants who failed to properly preserve metadata.

- Finally, an in-house solution should not limit capacity or number of cases. The main goal of bringing the e-discovery process in house is to reduce risk and lower cost, so ensuring there are no data capacity limits or charges by volume of data is a valuable consideration.

To help you navigate the above requirements, this guide provides a simple, ten-step process along with an evaluation checklist template to enable complete evaluation analysis:

- **Vendor Pedigree** provides focus areas for reviewing the vendor's background and experience
- **Total Cost of Ownership** helps assess the solution's effectiveness in enabling cost savings
- **Existing Infrastructure Integration** ensures the solution suits the existing systems, network, and security architecture and integrates with the organization's electronic data repositories
- **E-Discovery Team Collaboration** focuses on optimal collaboration between IT and legal and overall ease of use
- **Legal Hold** reviews the automation, completeness, and integration of the legal hold notification process to ensure duty to preserve obligations are met
- **Collection and Preservation** explores the solution's ability to collect all data across the network and ability to preserve in the file's native format
- **Processing** provides analysis of the solution's ability to cull ESI to the most relevant data set
- **First Pass Review** focuses on the ability to understand and assess document content for the purposes of developing a defensible, strategic plan
- **Export ESI – Load File Creation** ensures the ability to prepare and produce ESI in an agreed upon and usable format
- **Professional Services** helps understand the vendor's ability to further support customer's goals through training, certification, and onsite services
- **Product Evaluation Checklist** provides a template for multi-vendor evaluation analysis

II. Vendor Pedigree

Adopting an in-house e-discovery solution should begin with an objective review of the vendor's experience, stability, and independent references. The evaluation should place an emphasis in this area due to the long term nature of the relationship between an organization and their in-house e-discovery vendor.

It is expected that an organization's overall e-discovery needs will change over time; therefore, their selected vendor should have the support and adaptability to meet the customer's changing requirements.

Analysis of the vendor's pedigree should include review of the following:

- Obtain information on the vendor's financial health, years in the business, and number of clients. An organization should have extensive background and experience in e-discovery.
- Look for the "trusted vendor" factor by reviewing independent industry endorsements – awards, certifications, and customer references.
- Conduct online research or ask the vendor for judicial court references that sight their offering as a judicially accepted solution.
- Determine the vendor's ability to execute with a review of their future directionand roadmap plans.
- Ensure the vendor's ability to adapt to your changing needs with a wide array of service offerings – training, certifications, pre and post deployment services, as well as casework and staff augmentation services.
- Look for the vendor to have an internal team of e-discovery experts to continually innovate and drive the industry standard to meet customer's needs.
- Understand the vendor's support model; including, technical expertise, staff accessibility, hours of operation, and escalation process.

III. Total Cost of Ownership

Core to the decision of bringing e-discovery in-house is the desire to save on costs previously experienced through outsourcing expenses. For that reason, it is important to take extra time and consideration when evaluating a solution's ability to reduce costs.

Most significant cost savings are realized through saved time; that is, saved time managing and analyzing data as well as saved time in managing the solution, itself.

For maximized resource allocation to drive cost savings, the solution's ability in the following is essential:

- Does not limit your capacity or number of cases – confirm that there are no data capacity limits or charges by volume of data are valuable considerations.
- Handles all types of cases, not just civil, which are classic e-discovery cases; including, IP theft, FCPA, fraud, or employee disputes involving allegations of discrimination or harassment, in which hidden data may be critically important. Solutions that rely on the computer operating system can "see" only what the operating system presents to them, so critical evidence can be missed entirely. Because of this, for an entire set of sensitive cases, solutions that rely entirely on the operating system simply cannot be used.

- Supports information management with ongoing cleanup of irrelevant, outdated, and useless data, thereby reducing data volume and risk in advance of litigation. The ability to proactively manage data in this manner aids in reducing the overall e-discovery cost burden.

- Able to cull down the data to the greatest extent – should enable greatly reduce data volumes within a case to save significant time and expense when it comes to downstream attorney review.

- A single, integrated solution is critical to enable a more efficient business process in managing the e-discovery phases compared to patching together the phases with different tools or solutions.

- True early case assessment functionality to enable legal to asses case merits and risk to set case strategy as soon as possible, aiding in significantly minimizing costs.

IV. Existing Infrastructure Integration

As with all technology purchases, an in-house e-discovery product offering must integrate within the organization's existing infrastructure without creating critical choke points or adversely impacting the operations of other business critical applications.

Given that its core function is to access the corporate data repositories across the organization, an e-discovery solution must be able to manage this through a single interface and must support collection from all of the data stores; including, email, instant messenger, electronic files like word processing and spreadsheets, intranet sites, and any other electronic information that may be stored on desktops, laptops, file servers, mainframes, or on a variety of other platforms.

The best approach to analyze a solution's ability in the area of system integration is:

- Review the technical specifications to ensure the solution can be installed and managed from a central location.

- Verify that the solution can access the disparate data repositories across the organization and departments from this location.

- Understand the solution's throughput and scalability and ability to process terabytes of data; it is important that an enterprise quality solution is able to quickly process large data volumes.

- Conduct an inventory of the organization's data repository solutions (email servers, archival systems, content management systems, etc) and confirm that these are supported by the e-discovery product.

- Review the solution's ability to collect active content – email, servers, desktops, laptops and offsite employee systems without interruption, from a centralized location.

V. E-Discovery Team Collaboration

IT and legal are ultimately responsible for the e-discovery process; they are the key individuals on the e-discovery team. To ensure a fluid process with no unexpected interruptions or communication delays, a solution must maximize the efficiency and collaboration between both groups.

For streamlined collaboration look for the following requirements:

- A common repository for joint IT and legal access to case custodians and data
- Ability to share searches and create jobs for each to execute within the application
- Automated and real-time status tracking of job assignments – especially during the legal hold, preservation, and collection phases

VI. Legal Hold

When an organization is served with a lawsuit – or when litigation can be reasonably anticipated – there is a legal duty to preserve potentially relevant data. The most critical aspect of that duty for an in-house e-discovery solution is ensuring potential custodians are notified not to destroy any potentially relevant information, which is managed by a solution's legal hold capabilities.

For the legal hold process to be efficiently managed it must have full-fledged capabilities: hold notices, auto-reminders and auto-escalations, online custodian surveys, and automated tracking and reporting. It also must support real-time status updates and provide centralized management by both IT and legal to enable a streamlined process and fluid communication between both teams.

Just having legal hold notification capabilities isn't enough. Organizations can no longer justify simply sending an email legal hold request with no follow through. Instead, they need integrated legal hold capabilities that automate and enforce legal holds with full audit capabilities, and reporting so IT and legal teams can work together and ensure defensibility.

To ensure optimal legal hold, the solution must:

- Provide automation and complete management of the legal hold process to issue, monitor, and enforce litigation holds; including, hold notices, auto-reminders and auto-escalations, online custodian surveys, and automated tracking and reporting.
- Provide real-time, full audit trails and reporting to ensure legal obligations are being met. This should include details on who has acknowledged the hold and who has not, as well as how the questions have been answered.
- Inform collection and preservation by identifying custodians and provide the ability to adjust collection search terms based on responses.
- Integrate with ActiveDirectory to easily select potential custodians (or groups of potential custodians) and issue a standard legal hold notice with vendor provided templates.

- Custodian (employee) response to legal hold notices should be user friendly and self-explanatory to ensure the IT helpdesk is not flooded with calls. Ideally, the legal hold notice should be sent via email with a direct link to the page where the custodian can quickly acknowledge the hold and answer the questions.

- Entire process, from legal hold through to review, should be supported with automated tracking and reporting to best support the organization's defensibility.

VII. Collection & Preservation

Following the legal hold notice, the greatest risk – and the majority of case sanctions – occurs with collection and preservation of data. Organizations should keep in mind that 80% of the risk in the e-discovery process is in the duty to preserve (also sometimes referred to as "executing a legal hold").

Judicial decisions like *Pension Committee of the University of Montreal v. Banc of America Securities, LLC*, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010) and *Qualcomm Incorporated v. Broadcom Corporation*, 2010 WL 1336937 (S.D.Cal. April 2, 2010) illustrate that careless and indifferent collection efforts lead to sanctions. Once the identified custodians are sent legal hold notices, their information should also be available in the solution's database to easily target them for collection and preservation.

An in-house solution must also include pre-collection analytics capabilities that enable search criteria to be tested before electronically stored information (ESI) is collected. This should include the ability to refine search parameters for keywords, file types, and timeframes as well as identify relevant data sources, get metrics on total data versus potentially relevant data, and understand how much data could be eliminated.

When you use an in-house e-discovery solution, you shouldn't have to worry about metadata – the offering should automatically preserve *all* file and email metadata, so that you can avoid disputes over which metadata fields are relevant, and, more importantly, avoid the problems that have befallen litigants who failed to properly preserve metadata.

The solution should be able to reach out across the network to desktops, laptops, and servers collecting the specific files and email you need, automatically preserving metadata and doing it on a case-by-case basis. Automating the collection of ESI not only reduces cost, it also reduces legal risk.

Look for the following collection and preservation capabilities in an in-house solution:

- The process does not interrupt employee or business operations by relying on the operating system to find relevant data or by requiring imaging of hard drives. Solutions that rely on the operating system to find and collect potentially relevant data not only cannot find hidden data but cannot even collect files that are currently in use by the custodians; for instance, every custodian would be required to exit from Outlook before a search and collection of their PSTs can be conducted. Instead, the solution should have an automated process that is conducted seamlessly - without interruption to employee activity - across unstructured and semi-structured data stores.

- Enables culling the dataset at the point of collection – provided by targeting and collecting only potentially relevant ESI based on keywords, date ranges or any file system metadata property.

- Provide highly efficient, targeted collection technology that delivers fast results. The solution's search should be performed on the original data sources, as they exist in the environment, without requiring pre-indexing. This saves time and reduces the impact on the target computers. Additionally, there should not be any requirements to migrate data to another platform before searching.

- Automatically preserve all metadata in a read-only container to maintain chain of custody and ensure ESI is genuine and provide timelines to understand 'who knew what when.' Preservation of the data and metadata also needs to be verifiable to ensure a defensible process that reduces legal risk.

- Includes complete and automated tracking of the collection & preservation process to enhance defensibility. For example, if there is an allegation of spoliation, the organization should be able to show how and why they conducted the search the way they did.

VIII. Processing

Along with targeted data collection capabilities, a solution should also have comprehensive processing capabilities to further cull the data before it is reviewed. A significant ESI volume reduction during processing is important for providing significant cost savings.

The in-house product should filter data based on any keywords, hash values, and file system metadata property: including, date ranges, file types, custodian, and path. In addition, data should be able to be de-duplicated, with the option to do so across all custodians in the case or only within each custodian's data.

Additional processing features should include:

- Complete tracking of selected culling criteria

- Evidence should be stored in a separate database during processing to ensure data integrity

- Processing support should include double-byte character and unicode foreign language support

- Preservation of all electronic data and metadata throughout the process

IX. First Pass Review

To best support your legal team, their key in-house solution requirement is the ability to conduct case assessment – to *see* the relevant data as quickly as possible in order to analyze the case merits and develop a strategy. The early case assessment should provide analysis and first-pass review at any point in the e-discovery process.

It is equally important that an in-house e-discovery solution should be able to process your data without missing potential evidence. This includes the ability to conduct a compound search (i.e. "dog" or "cat" with five instances of "house" or tree" or yard"), and the ability to unpack and search embedded files, several layers deep (i.e. a Zip file with a Word document that has an embedded Excel spreadsheet that has an embedded PowerPoint presentation). Disregard e-discovery solutions that are unable to search the PowerPoint presentation in this scenario or are limited to unpacking and searching embedded documents up to three layers deep.

For analysis and first-pass review, the solution should provide:

- Analysis and first-pass review throughout the process – during collection and processing. It should support analysis at any point during the e-discovery process; such as, analysis of one collected custodian while the others are still in process.
- A web-based, user-friendly interface, for easy access by the legal teams that provides the ability to browse through and view documents and emails prior to indexing.
- Ability to search, analyze, and review ESI content to understand case merits, identify responsive documents, and further cull down the dataset prior to outside attorney review.
- Support for compound searches (i.e. "dog" or "cat" with five instances of "house" or tree" or yard"), and the ability to unpack and search embedded files, several layers deep (i.e. a Zip file with a Word document that has an embedded Excel spreadsheet that has an embedded PowerPoint presentation).
- Advanced search term analysis should identify ESI that is distinctively responsive to a search term or keyword and should also provide a relevance ranking for the search results.
- Linear review with hit highlighting, email thread and conversation viewing to identify responsive ESI, tagging with comments to classify, categorize, manage, and reduce content.
- Ability to immediately distribute responsive ESI that is determined critical to the case.
- History, full audit trail, and detailed access controls to support the organization's defensibility.
- Support for search in all languages relevant to your business operations.

X. Export ESI – Load File Creation

The selected vendor should provide all the capabilities that an organization wants to perform in-house, and for some matters, that may mean sending the relevant ESI to outside counsel or a service provider for more complete review and production. To support this effort, an in-house solution should support load file creation for sending evidence files to legal teams for production and review in desired formats and platforms; including:

- EDRM XML
- Concordance
- Summation
- kCura Relativity
- Native files

XI. Professional Services

Bringing the e-discovery process in-house requires commitment from internal teams to not only manage the solution but also to learn how to execute and optimize the e-discovery process, itself. To achieve this, most organizations will need to invest in staff education and training.

For that reason, the vendor selection criteria should extend beyond the technology to also include the vendor's ability to deliver services support from legal e-discovery expert personnel. A seasoned e-discovery software vendor should offer a broad set of services that enable the organization at all stages of the e-discovery lifecycle – from solution implementation through to supplemental casework management support during peak periods.

Verifying that your selected vendor has a wide array of service offerings available will ensure your organization has these resources at your disposal if and when they are required – an essential buying criterion as e-discovery casework demands can vary widely from year to year.

A complete set of services should include:

- Solution implementation services that help get the solution integrated into the existing infrastructure as well as aide with the solution optimization.
- Staff training and certification courses provided by legal e-discovery experts to help staff personnel become e-discovery experts – and learn the latest e-discovery best practices for organizations.
- Casework services that help provide staff augmentation to internal legal resources at various peak and high necessity periods.
- Business process and operations services that analyze, plan, and assess the organization's overall e-discovery management to help optimize and mitigate risk.
- The services delivery should be provided by e-discovery experts with years in the field.

- The vendor should employ a team of attorneys on staff who consult with the services and training teams and provide e-discovery best practices expertise.

XII. Conclusion

When looking for an e-discovery solution, organizations should start with mapping out their specific needs. Remember there will be a long relationship with the selected vendor, so careful consideration should be taken during the evaluation process.

In addition to reviewing the technology for completeness, organizations should confirm that the vendor has extensive industry experience and breadth of services to ensure they will be a strong e-discovery trusted advisor. The vendor should have a proven track record and independent endorsements and customer references.

Ultimately, organizations are seeking to reduce costs with their selection, compared to existing annual outsourced e-discovery expenses. Therefore, this end goal should be maintained at the center of focus during the technology review. Optimal cost savings can be achieved from an integrated solution with a comprehensive feature set that delivers fast access to the relevant ESI.

Finally, an in-house e-discovery solution should empower the organization to quickly manage an issue at hand by providing the ability to assess case merits and set strategy as early as possible. This is achieved with a solution's pre-collection analytics and early case assessment capabilities that should support first-pass review throughout the process – during collection and processing.

Selecting a vendor with strengths across these areas should provide your organization with the best fit now and years to come.

	Guidance Software	Vendor 2
Vendor Pedigree		
Years in the industry with extensive experience and technical expertise	Yes	
Independent endorsements – awards, customer references, and positive judicial court references that sight vendor's offering as a judicially accepted solution.	Yes	
Vendor stability – financial health, future direction, and roadmap plans	Yes	
Employs internal legal team of e-discovery experts	Yes	
Comprehensive support model	Yes	

Total Cost of Ownership		
Does not limit your capacity or number of cases (i.e. no data capacity limits or charges by volume of data)	Yes	
Information management data clean up	Yes	
Handles all types of cases and does not rely on the computer OS for data collection	Yes	
Automated workflow processes	Yes	
Single integrated solution	Yes	
Extensive data set culling features	Yes	
Early case assessment to obtain relevant data prior to review	Yes	
Infrastructure Integration		
Centralized management of distributed services	Yes	
Solution supports your email and content management data repositories	Yes	
Data repositories managed from central management console	Yes	
Throughput and scalability specs support large data volume processing	Yes	
Collects active content without employee or business disruption	Yes	
E-Discovery Team Collaboration		
Includes repository for joint IT and legal access to case custodians and data	Yes	
Share searches and create jobs for each team to execute within the application	Yes	
Automated and real-time status tracking of job assignments	Yes	
Legal Hold		
Automated and complete management – issue, monitor, and enforce litigation holds	Yes	
Hold notices, auto-reminders and auto-escalations, online custodian surveys, and automated tracking and reporting	Yes	
Real-time full audit trails, status updates, & reporting	Yes	
Ability to adjust collection search terms based on legal hold responses	Yes	
Active Directory integration	Yes	
Legal hold notification templates	Yes	
User-friendly interface for custodians (employees)	Yes	

Collection and Preservation		
Automated process with no interruption to employee or business operations (i.e. no hard drive imaging required; no reliance on the OS to locate data)	Yes	
Includes pre-collection analytics capabilities that enables search criteria to be tested before ESI is collected	Yes	
Search performed on the original data sources, as they exist in the environment, without pre-indexing or data migration requirements	Yes	
Search based on keywords, date ranges, file types or any file system metadata property	Yes	
Does not miss potential evidence – supports compound searches and unpacks and searches embedded files, several layers deep	Yes	
Dataset culling at the point of collection – provided by targeting and collecting only potentially relevant ESI	Yes	
Automatically preserves data and metadata in a read-only container to maintain chain of custody and ensure ESI is genuine	Yes	
Solution reach across network to access email, servers, desktops, laptops and offsite employee systems	Yes	
The preservation of the data and metadata is automated and verifiable	Yes	
Includes complete and automated tracking of every step of the collection and preservation process	Yes	
Processing		
Powerful culling features - filter data based on any keywords, hash values, and file system metadata property: including, date ranges, file types, custodian, and path	Yes	
Criteria validation and workflow reports	Yes	
Automated workflow processes	Yes	
De-duplication: across all custodians and for selected custodian	Yes	
Tracking of selected culling criteria	Yes	
Evidence integrity with storage in separate database during processing	Yes	
Supports double-byte characters and Unicode foreign language	Yes	
Preservation of all electronic data and metadata	Yes	

First Pass Review		
Analysis and first-pass review at any point in the e-discovery process	Yes	
Web-based interface for easy access by legal teams	Yes	
Ability to browse through and view data prior to indexing	Yes	
Ability to search, analyze, and review ESI content to understand case merits, identify responsive documents, and further cull down the dataset prior outside attorney review	Yes	
Advanced search term analysis that identifies distinctively responsive ESI	Yes	
Does not miss potential evidence – supports compound searches and unpacks and searches embedded files, several layers deep	Yes	
Provides a relevance ranking for the search results	Yes	
Linear review with hit highlighting, email thread and conversation viewing to identify responsive ESI	Yes	
Provides tagging with comments to classify, categorize, and manage as well as further reduce content	Yes	
Ability to immediately distribute responsive ESI that is determined critical to the case	Yes	
History, full audit trail, and detailed access controls	Yes	
Export ESI – Load File Creation		
Solution supports load file creation for sending to outside legal counsel and/or service providers	Yes	
Supports organization’s desired formats and platforms	Yes	
Professional Services		
Offers overall breadth of services – training, certification, professional services	Yes	
Solution implementation and optimization services	Yes	
Staff certification and training courses	Yes	
Casework and staff augmentation services to support organization in high need periods	Yes	
Services provided by a team with technical e-discovery experience and expertise supported by vendor’s on staff attorneys	Yes	

Our Customers

Guidance Software's customers are corporations and government agencies in a wide variety of industries, such as financial and insurance services, technology, defense contracting, pharmaceutical, manufacturing and retail. Representative customers include Allstate, Chevron, FBI, Ford, General Electric, Honeywell, NATO, Northrop Grumman, Pfizer, SEC, UnitedHealth Group and Viacom.

About Guidance Software (NASDAQ: GUID)

Guidance Software is recognized worldwide as the industry leader in digital investigative solutions. Its EnCase® platform provides the foundation for government, corporate and law enforcement organizations to conduct thorough, network-enabled, and court-validated computer investigations of any kind, such as responding to eDiscovery requests, conducting internal investigations, responding to regulatory inquiries or performing data and compliance auditing - all while maintaining the integrity of the data. There are more than 30,000 licensed users of the EnCase technology worldwide, the EnCase® Enterprise platform is used by over half of the Fortune 100, and thousands attend Guidance Software's renowned training programs annually. Validated by numerous courts, corporate legal departments, government agencies and law enforcement organizations worldwide, EnCase has been honored with industry awards and recognition from Law Technology News, KMWorld, Government Security News, and Law Enforcement Technology.

Guidance® SOFTWARE
The World Leader in Digital Investigations™