

E-discovery Mitigating risk through better communication



Survey methodology

In order to understand the e-discovery challenge facing corporate America, the Deloitte Forensic Center commissioned the Economist Intelligence Unit (EIU) to conduct a survey in September and October 2009 of 337 respondents in the information technology (IT), legal, risk, and compliance functions. Of the 167 respondents in IT, 43% were at the director level or above, and another 37% were at the manager level or above. Of the 170 respondents in legal, risk, and compliance, 22% carried a C-level title and another 44% were at the manager level or above. All survey takers were U.S. based. They represented a wide variety of industries.

For purposes of the survey conducted, e-discovery was defined as any procedure that involves records management and where electronically stored information (ESI) is identified, preserved, collected, searched, or otherwise processed with the intent of using it as evidence in a civil, criminal, or regulatory matter.

About one-third of respondents did not know the answer to several questions. While a general profile of them did not emerge, some groups were more knowledgeable about e-discovery than others, as identified in the report. Because of the large number of “don’t know” responses, the report also points out cases where the survey data only refers to those who had an answer.¹

¹ Certain calculations in this white paper do not include “Don’t Know” responses so that a more detailed comparison can be presented

Survey analysis

To assess the state of e-discovery readiness at U.S. companies, the Deloitte Forensic Center commissioned the EIU to conduct a survey in September and October 2009 of 337 respondents in the legal, risk, compliance, and IT functions. Of notable concern, the survey finds that almost half (49%) of respondents said their company is only somewhat effective or not at all effective in dealing with the challenges of e-discovery today. As the volume of ESI rises rapidly, improving the understanding among the C-suite, legal and IT functions is key to controlling costs and better managing e-discovery risks. The Deloitte Forensic Center's analysis of the survey results identified three interrelated challenges that are discussed in more detail in the sections that follow. They are:

- Communication
- Awareness
- Readiness

Communication hurdles

At the heart of e-discovery are two corporate functions that historically have had little in common and tend to speak their own technical languages: legal and IT. Neither can be truly effective in the e-discovery process without a clear understanding of the other, yet communication and coordination between these two departments appears to be unclear to many survey participants: More than one-third of respondents (36%) don't know the answer to how their legal and IT departments communicate. And of those with an opinion about how the two departments work together on e-discovery, 40% say they communicate poorly, and 35% say their companies have not created a "Discovery Response Team" or similar structure that includes representation from IT, legal, Human Resources (HR), and other relevant departments.

In its 2007 paper, "Electronic Discovery Best Practices," LexisNexis encouraged companies to "Establish an ongoing working relationship between in-house legal and IT personnel." Yet, even today, according to the survey respondents, the IT and legal departments are still remarkably disjointed when it comes to e-discovery: only 13% (Chart 1) of IT respondents say they understand their company's legal requirements for e-discovery very well and an equal number say the legal department works very well with IT to find solutions that meet the company's needs in this area. Of those in the IT department with an opinion about working with legal, 30% (Chart 1) say the two do not work well together at all. In the same subset of respondents, 37% (Chart 2) also say that their company's legal department does not understand well at all the limits of what IT can do in support of e-discovery.

Chart 1

IT Department Responses: How well does the legal department work with your department to find solutions that meet your company's e-discovery needs?

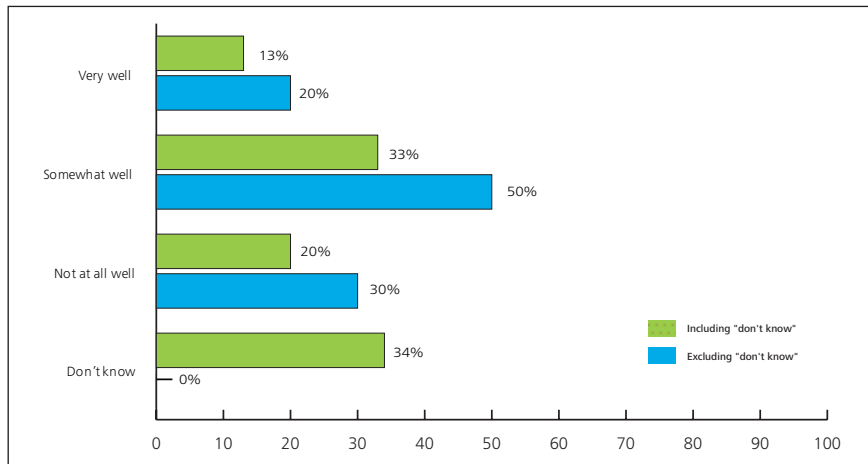


Chart 2

IT Department Responses: In your opinion, how well does your company's legal department understand the limits of what IT can do in support of e-discovery?

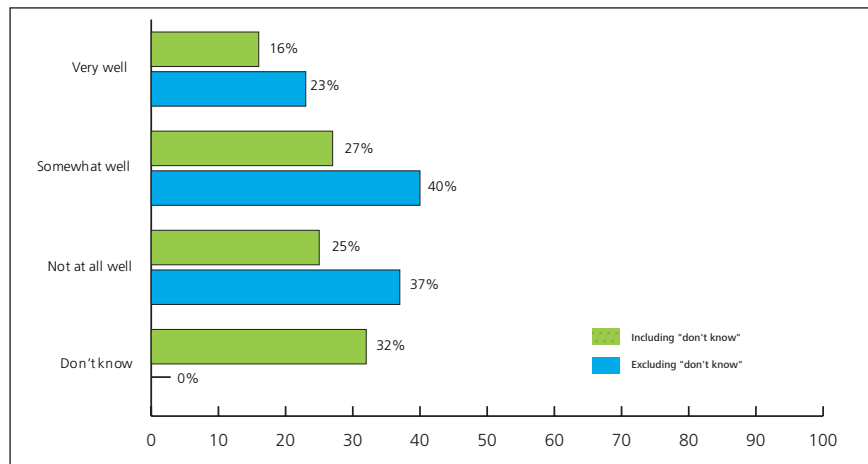
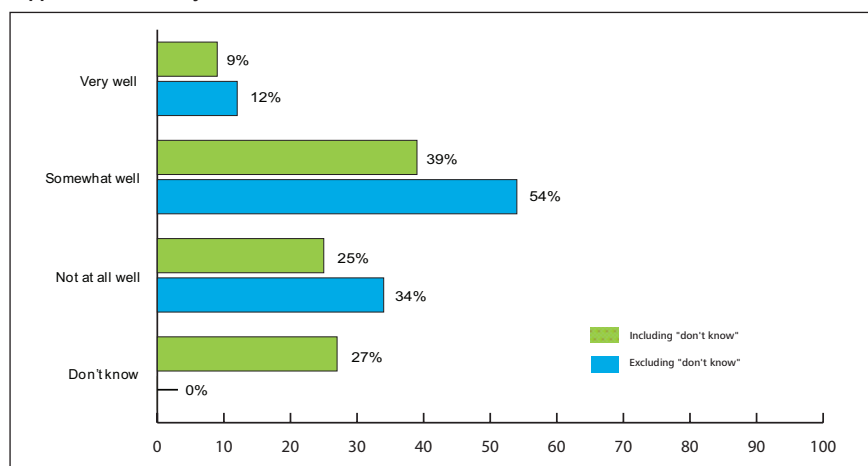


Chart 3

Responses Excluding the IT Function: How well do you understand the limits of what IT can do in support of e-discovery?



For those who work in compliance, risk assessment or the legal department, the current situation is similarly disturbing: More than one-third (Chart 3) of those with an opinion say they do not understand well at all the limits of what IT can do in support of e-discovery. And in that same subset of respondents, many feel poorly understood by their colleagues in IT: 30% say their company's IT department does not understand the company's legal requirements for e-discovery very well at all and 23% say the IT department does not work very well with legal to find solutions that meet the company's e-discovery needs.

Weaknesses in internal communication can lead to serious consequences. In a 2008 defamation case against a Canadian pharmaceutical firm, for example, the company's legal department's verbal instructions to preserve all relevant information were not followed until

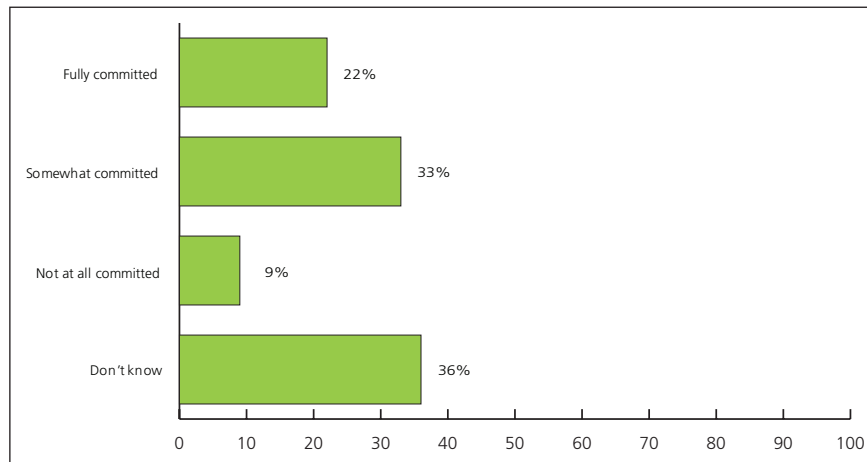
six months later, when it received written instructions to preserve all information that could be relevant to the claims and defenses of the plaintiff. The court criticized the company for failing to institute a full preservation program; specifically, the company did not back up its servers until seven months after it should have been aware of its obligation to begin preserving data.

Other examples include a 2009 case where the court ruled that sanctions may be appropriate against a computer manufacturer, a defendant in a suit brought by a larger competitor, for having no "coherent document retention policy." In another 2009 case about oil-lease royalties (*Spieker v. Quest Cherokee*), the court admonished the defendant for claiming not to have the ability to generate the requested ESI in-house.

Awareness issues

Deficient communication and a lack of coordination between departments can lead to an organizational lack of awareness about e-discovery. According to the survey, more than one-third of respondents, including C-suite, (36%) don't know how committed their company's C-suite is to finding a solution for e-discovery issues (Chart 4). In addition, one-quarter (25%) don't know if their company's C-suite is aware of e-discovery issues — 16% of respondents are sure that they are not!

Chart 4
In your opinion, how committed is your company's C-suite to finding solutions for e-discovery issues?



A lack of awareness about e-discovery and its challenges can naturally lead to a low priority being given to preparing for litigation: Only 20% of respondents think legal resources are appropriately allocated to e-discovery and only 18% say the same about financial resources. As ESI volumes increase and new sources of ESI emerge, those challenges are likely to become more difficult.

As one might expect, lack of awareness is already an obvious issue: overall about one-third of respondents did not know the answer to several questions in the survey and respondents from the risk and compliance functions actually had a higher tendency of reportedly not knowing the answer than survey takers from the IT and legal functions. On average, the risk and compliance groups answered "don't know" 48% and 53% of the time, respectively, while both IT and legal respondents answered "don't know" 37% of the time.

Survey participants with greater seniority appear to have more knowledge about e-discovery. On average, C-level respondents answered "don't know" only 25% of the time, while non-C-level respondents said "don't know" 47% of the time.

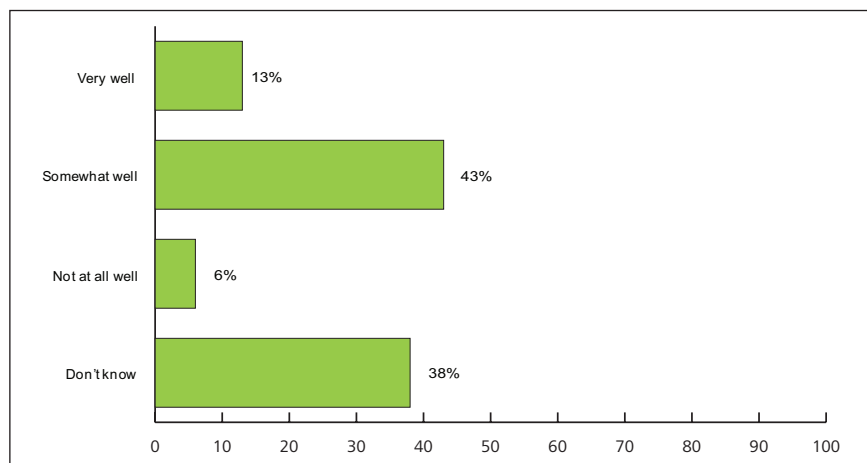
Not surprisingly, legal officers have more knowledge about e-discovery than other groups (note: there are 24 legal officers represented in the survey). On average, chief legal officers and legal counsel answered "don't know" only 15% of the time compared with 42% for all other groups.

Obstacles to readiness

Almost half of respondents said their companies are only somewhat effective (43%) or not at all effective (6%) in dealing with the challenges of e-discovery today (Chart 5). And compliance with e-discovery requests poses a challenge for more than one-third of companies, according to those surveyed.

Chart 5

How effective is your company in dealing with the challenges of e-discovery today?



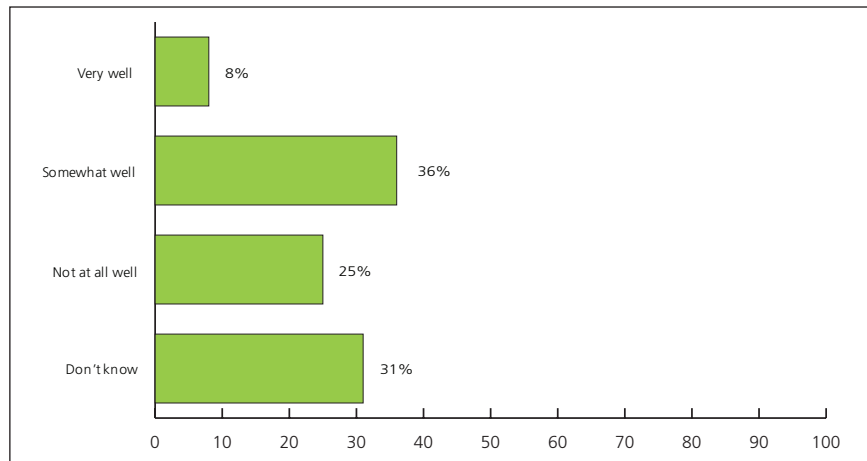
Many companies also lack the resources and sophistication to manage e-discovery effectively. For respondents that say their firms are challenged by e-discovery, the most common complaints are: a lack of funds to address e-discovery requirements (25%), the volume of data subject to e-discovery (23%), and the complexity of data privacy and security requirements (19%).

The challenge associated with data volumes is not just an internal issue. Consider the following product-liability case. A drug maker produced more than 2 million documents for discovery in that litigation. And in a recent antitrust litigation against a large global microprocessor manufacturer, reports indicate the company produced 150 million pages of documents in response to discovery. Larger amounts of data take up time and resources and many expect the problem of being unprepared for e-discovery to get worse, especially since each new trend in computing — be it mobile phones, netbooks, cloud computing, or social networking — makes e-discovery more complex.

Of those respondents with an opinion, 62% say their company is concerned about e-discovery challenges posed by social media web sites and blogs.

Of those respondents with an opinion, 62% say their company is concerned about e-discovery challenges posed by social media web sites and blogs. Indeed, only 8% of respondents said their company was well prepared and more than half of respondents' companies are either unprepared (25%) or only somewhat prepared (36%) to handle e-discovery requests relating to social media (Chart 6). Given the extensive use today of social media, such as Facebook and Twitter during employees' work and personal time, companies may need to update their procedures to address this growing area of risk.

Chart 6
How prepared is your company to address e-discovery requests as it relates to business-related communications via social media web technologies (i.e., social media sites, blogs)?



Meanwhile, 53% of those with an opinion say their firm is concerned about e-discovery requests that relate to data held by third-party service providers, such as Salesforce.com or Google Mail. Only 9% of respondents say their companies are well prepared to capture ESI on third-party platforms, such as those accessed through cloud computing.

Such challenges are not hypothetical: 13% of public companies in the United States produced ESI from a social media site as part of discovery over the past year, according to Fulbright & Jaworski's 2009 Litigation Trends Survey.

The future of e-discovery

The demands of e-discovery are growing

None of these challenges appear likely to diminish in the foreseeable future. Forty-four percent of respondents expect e-discovery challenges to increase over the coming three years and 39% expect to devote more resources to e-discovery over the same period. And nearly half of respondents (49%) expect their company's IT department to work on e-discovery efforts more over the next three years.

Of respondents with an opinion, 61% percent expect their companies to be only somewhat effective or not effective at all in dealing with e-discovery's challenges three years from now.

In terms of timing, 16% say conflicts between e-discovery and European privacy laws will reach a crisis point within the next 12 months. Twenty-nine percent of respondents think that, within three years, courts will demand certain relevancy algorithms to be used for e-discovery and 36% expect that federal rules governing e-discovery will be further amended in that time.

Confidence in future e-discovery performance is low: of those respondents with an opinion, 61% expect their companies to be only somewhat effective or not effective at all in dealing with e-discovery's challenges three years from now.

The consequences of deficient e-discovery processes can be severe

Failure to address e-discovery mandates can lead to serious repercussions. For example, mismanaged e-discovery can lead to the disclosure of privileged documents — those

meant to be kept private under attorney-client privilege — that can potentially damage one's case. As outlined in the new Federal Rule of Evidence 502, clawback arrangements — the retraction of privileged information following discovery — can help in such situations, but there is no clear method among the courts to handle inadvertent disclosure of privileged documents. For example, a federal judge in Baltimore ruled in an intellectual property case in 2008 that Creative Pipe, a Southern California-based outdoor furniture distributor, waived attorney-client privilege and other protections when it inadvertently turned over 165 electronic documents to opposing counsel in a suit brought by Maryland-based manufacturing company Victor Stanley (*Victor Stanley, Inc. v. Creative Pipe, Inc.*).

In a January 2010 ruling, Southern District of New York federal court Judge Shira A. Scheindlin strongly underscored the need for sufficient attention to preserving, collecting, and producing relevant electronic documents and to determine when those obligations take effect in a case. In *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*, her ruling (which she entitled "Zubulake Revisited: Six Years Later," in reference to her landmark e-discovery ruling in 2004), all 13 plaintiffs were found to be negligent in meeting their e-discovery obligations and monetary sanctions were imposed on all.

Six of the plaintiffs were also found to be grossly negligent, which subjected them to an "adverse inference instruction," under which the jury will be told to presume that the destroyed documents would have hurt the plaintiffs' case if had they been available. Such a ruling can be a fatal blow in a party's litigation.

While indicating that every case is a judgment call, Judge Scheindlin stated in the January 2010 ruling, "after a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence." One of the challenges with this is that contemporary standards keep changing, potentially making last year's adequate e-discovery process inadequate this year.

E-discovery failings that amount to gross negligence

In her January 2010 ruling, Judge Scheindlin identified the following e-discovery failures as sufficient to show gross negligence:

1. Failure "to issue a written litigation hold" when the duty to preserve documents first attached
2. Failure "to identify the key players and to ensure that their electronic and paper records are preserved"
3. Failure "to cease the deletion of e-mail or to preserve the records of former employees ... and to preserve backup tapes when they are the sole source of relevant information or relate to key players"
4. Failure "to sufficiently supervise or monitor their employees' document collection"

E-discovery trouble can extend beyond court sanctions. As the Sedona Conference (the legal industry's leading forum on e-discovery) points out, a lack of proper management of electronic information can lead to a host of corporate problems, including a loss of strategic opportunities when valuable information is not recognized or leveraged, increased costs of doing business when data is disparately organized or inaccessible, and a failure to comply with regulations concerning document retention and destruction or security breach notification. Conversely, a well-designed and implemented e-discovery program can help a company retain its strategic edge, keep costs down, and stay in compliance with federal and state regulations.

E-discovery tools and techniques

Understandably, putting together such a program can be daunting, given the technical and organizational complexity of e-discovery, not to mention the large number of vendors and the wide variety of products in the market. Among survey respondents, 56% have implemented e-mail management or archiving, while 32% are in the process of doing so. About half (49%) of survey takers say their firm is using or plans to use document or content management platforms. And while just 27% have implemented an electronic records management program, 29% are in the process of doing so.

Yet when asked if their firms use enterprise forensic collection technologies, nearly half (49%) of all respondents say they don't know the answer. Of the remainder who do, only 41% say it is under way or already implemented. Likewise, few are using web-based, software-as-a-service e-discovery products—26% are sure their firms are not using web-based tools; 47% don't know if they are or not.

One way companies may choose to improve their e-discovery approach is through the consolidation of e-discovery technology around a single or a reduced number of vendors. Such consolidation appears to be a potential opportunity for improvement, given that 48% of respondents don't know if their companies have consolidated around a single or reduced number of vendors and of those who do know, 41% are sure that they haven't consolidated.

According to Gartner's December 2009 report *MarketScope for e-Discovery Software Vendors*, "By the end of 2011... there will be 25% fewer vendors in the e-discovery market as a result of mergers and acquisitions and vendors exiting the market." This raises the specter of potential disruption to e-discovery operations as certain products and services are withdrawn, are no longer supported, or require a forced transition to a successor product on an inconvenient timeline. Proactive assessment of potential market changes and identification of alternative vendors could help companies to avert such disruption.

Another approach companies may take is reassessing what capabilities they need to respond promptly to discovery requests and evaluating how current technologies can support that. As Gartner's MarketScope report noted, "More companies are taking a proactive approach by investing in content and records technologies and processes to be able to respond quickly to discovery requests, as well as to provide in-house counsel with a tool that can be used to assess potential risk or early case assessment." Half of all survey respondents don't know if outsourcing e-discovery makes it more efficient and 40% say it makes e-discovery more expensive. Eleven percent think that outsourcing e-discovery is the best option for their company.

What many companies may be discovering is that the most effective e-discovery process may not be all in-house or all outsourced, but a collaboration between internal and external resources or “cosourcing.” The cosourcing balance may vary based on factors, such as the complexity of the company’s systems, the volume of ESI to be processed, the time frame available, the level of e-discovery knowledge and experience in-house, and the amount of risk or exposure in a particular matter.

Three years from now

E-discovery is anticipated to become harder: 44% of respondents expect e-discovery challenges, along with government rules and regulations, to increase over the coming three years. And of those respondents with an opinion, 61% expect to be only somewhat effective or not at all effective in dealing with e-discovery challenges three years from now. That could suggest a lot of risk for companies, unless improvements are implemented to avoid this expectation becoming reality.

Yet when asked if their firms use enterprise forensic collection technologies, nearly half (49%) of all respondents say they don’t know the answer.

Five areas of potential improvement

With ESI rising rapidly in volume, the challenges of communication, awareness, and readiness should be addressed if the risk of e-discovery missteps is to be mitigated. Mismanaged e-discovery has led to many tales of litigation woe, involving sanctions, lost cases, and fines. Improper ESI management, as the Sedona Conference points out, is simply bad business. Improving communications among the C-suite, legal and IT functions is crucial to controlling the costs and mitigating the risks of these e-discovery challenges.

Our survey results suggest five areas for companies to consider for potential improvement in e-discovery management:

1. **Training:** Due to a lack of knowledge and effectiveness in dealing with e-discovery issues, greater training in e-discovery awareness, procedures, data privacy, and security may be needed by employees who deal with legal, privacy, compliance, risk assessment or IT issues.
2. **Communication:** Because of the continuing communication challenge between legal and IT, cross-departmental e-discovery training sessions could help the IT department better understand what the legal department needs from them and help the legal department better understand what IT can and cannot accomplish.
3. **Social media:** New challenges for e-discovery. Given the extensive use today of social media, such as Facebook and Twitter during employees' work and personal time, companies may need to update their procedures to address this growing area of risk.
4. **Leadership commitment:** Senior executives may need to make their support and expectations for e-discovery plans and projects more explicit to strengthen employees' perceptions about how committed the C-suite is to finding solutions to e-discovery issues.
5. **Vendor consolidation:** The survey reveals little knowledge of technology vendor consolidation. This may be an opportunity for companies to take an inventory of their e-discovery technologies and vendors to see where greater efficiencies can be achieved through the use of fewer vendors.

This report is published as part of *ForThoughts*, the Deloitte Forensic Center's newsletter series, which is edited by Toby Bishop, director of the Deloitte Forensic Center. *ForThoughts* highlights the trends and issues in fraud, corruption, and other complex business issues. To subscribe to *ForThoughts*, visit www.deloitte.com/forensiccenter or send an e-mail to dfc@deloitte.com.

This publication contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this publication, rendering accounting, auditing, business, financial, investment, legal, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Deloitte Forensic Center

The Deloitte Forensic Center is a think tank aimed at exploring new approaches for mitigating the costs, risks and effects of fraud corruption, and other issues facing the global business community.

The Center aims to advance the state of thinking in areas such as fraud and corruption by exploring issues from the perspective of forensic accountants, corporate leaders, and other professionals involved in forensic matters. The Deloitte Forensic Center is sponsored by Deloitte Financial Advisory Services LLP. For more information, visit www.deloitte.com/forensiccenter.

About Deloitte

As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.