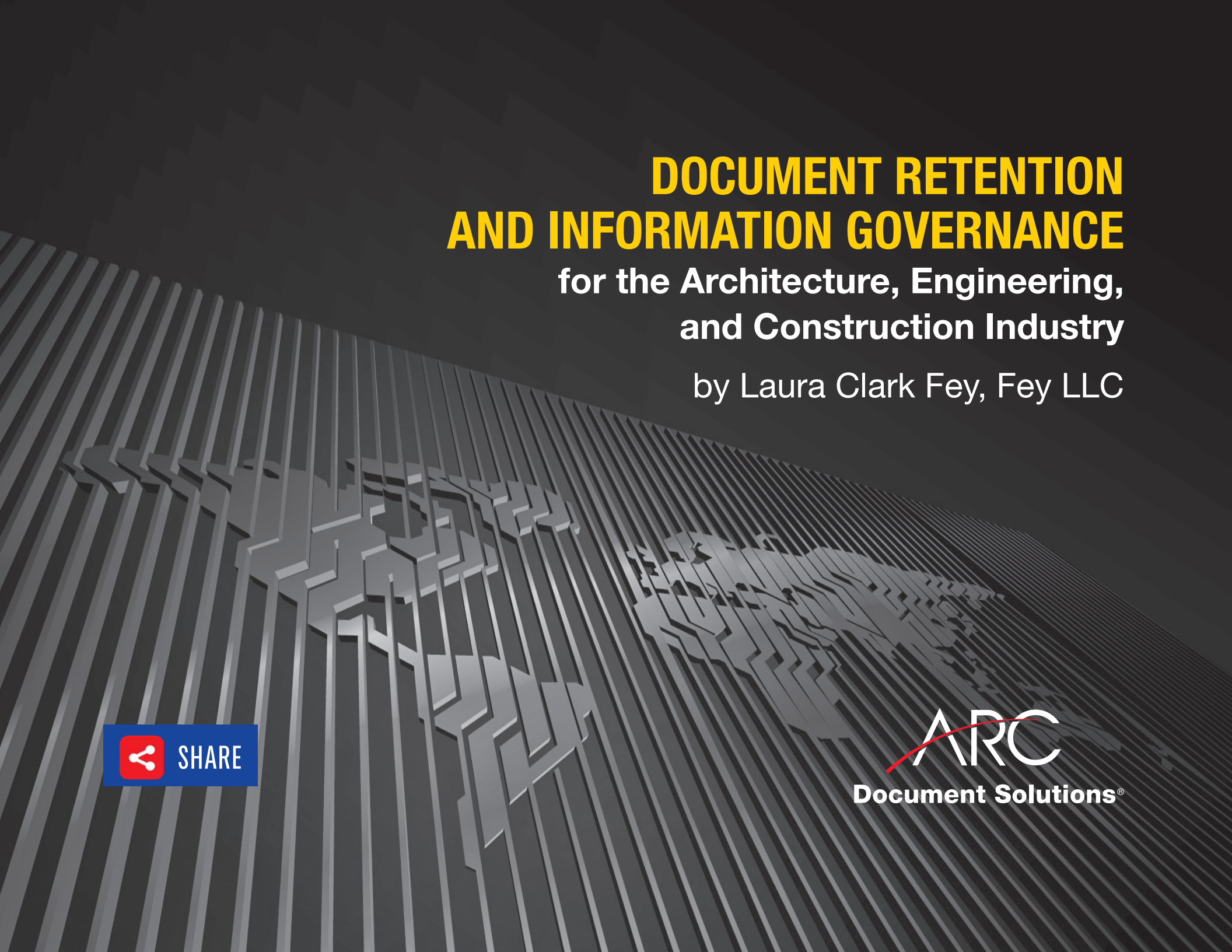


DOCUMENT RETENTION AND INFORMATION GOVERNANCE

for the Architecture, Engineering, and Construction Industry

by Laura Clark Fey, Fey LLC

SHARE

ARC Document Solutions®

SHARE

DOCUMENT RETENTION AND INFORMATION GOVERNANCE

for the Architecture, Engineering, and Construction Industry

Introduction

Most, if not all, companies today wrestle with issues of document retention and information governance. How long should you keep your documents? Do you have to keep paper copies? Are digital scans legally admissible? What's better, paper or digital?

In light of the strategic importance of information to companies, the flood of information created and received by companies on a daily basis, and the increasing focus by regulators, judges, and investigators on information governance practices, these and other questions relating to how companies should create, receive, store, protect, transfer, and dispose of documents, are vital questions for companies in all industries, including the Architecture, Engineering, and Construction (AEC) industry. That's why ARC Document Solutions asked us to create this ebook — as a high-level overview of significant document retention and information governance challenges for companies in the AEC industry, and solutions to those challenges.

Introduction - *continued*

Our team of attorneys and an information analyst at Fey LLC has decades of experience helping companies take control of their records and information in a way that makes sense for them given their business needs and legal requirements. We utilize our deep information governance, litigation, and technology expertise to assist corporate clients in developing and implementing practical, cost-effective, and legally compliant information governance solutions designed to meet their particular needs. We work with clients in a wide variety of industries, including the AEC industry.

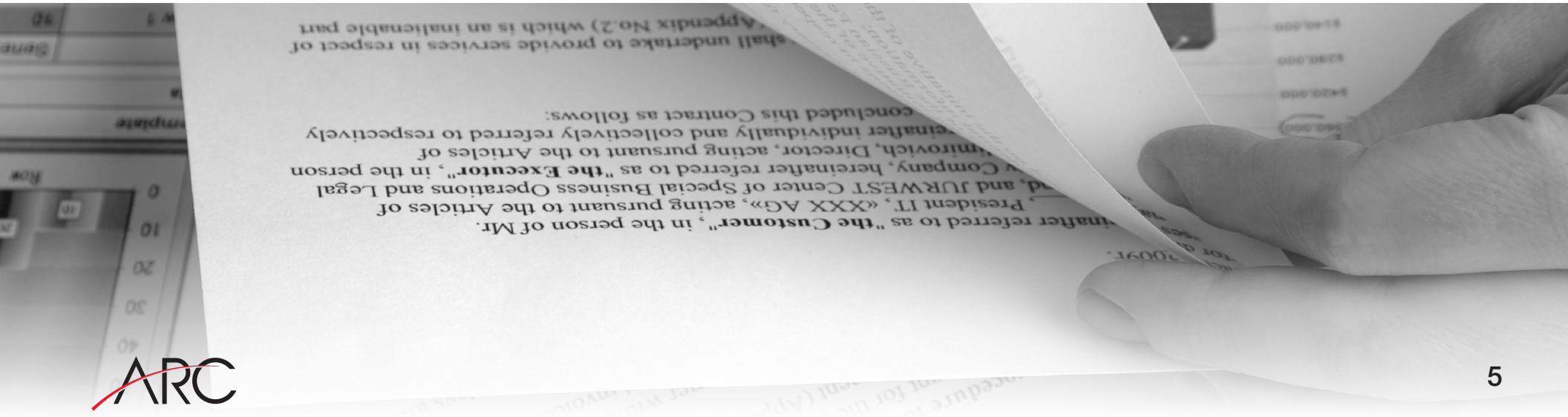
In this ebook, you will learn about a variety of information governance topics of importance for companies in the AEC industry, including, at a high level, how to prepare a records retention schedule; what should be covered in an information governance policy; and whether companies retaining documents in a digital archive also must retain their paper documents. You also will learn about significant information governance risks and steps companies can take to better control their information, which for many companies, is now doubling in quantity every 18-24 months.

Chapter 1: Getting Started with Information Governance

Why is it important to take control of your records and information?

Companies are rapidly moving away from traditional records management approaches. They no longer work. As technologies in use and information continues to expand at an exponential rate, it is critical for companies to take steps to better control their information. If companies don't take control of their information, they risk:

1. Losing their competitive edge because they cannot find critical business information in a timely manner.
2. Failing to meet their regulatory, legal hold, discovery, data privacy, and security obligations.
3. Facing ever-increasing costs and risks associated with retaining unneeded information.
4. Having to search through vast quantities of information for information needed for business or legal reasons.



Chapter 1: Getting Started with Information Governance

How can we get started?

Our work with clients typically begins with an analysis of the types of records and information they create, receive, and maintain; how they create or receive, transfer, and otherwise manage information throughout its lifecycle; the technology they use to manage their data; their corporate culture; their industry and litigation profile; their regulatory/legal obligations; and their specific information governance challenges and goals. We then utilize our experience, our legal and technical expertise, and our understanding of information governance best practices to help our clients develop a tailored information governance program designed to meet their business needs, as well as their information governance goals, which typically include, among others:

1. Complying with regulatory obligations to retain and protect specified categories of information.
2. Meeting legal obligations to preserve records and information relating to the subject matter of pending and reasonably anticipated litigation and regulatory actions.
3. Promptly disposing of records and information no longer needed in a reasonable, legally defensible manner.

We work with our clients to develop phased recommendations for information governance initiatives. Typically, we target early, relatively quick information governance "wins," which assist our clients in demonstrating the value of information governance to company executives and in obtaining buy-in for future information governance projects of greater proportion.

Chapter 2: Information Governance 101: Information Governance Basics

What is a record, anyway?

A record is generally defined as recorded information, regardless of medium or characteristics, made or received and retained by a company in pursuance of meeting its legal obligations or in the transaction of business.

What is the difference between records and information?

The term "records" is a much narrower term than "information." "Information" is typically defined to include all recorded information, regardless of medium or characteristics, made or received by a business; whereas "records" are limited to information that a company must retain in order to meet business needs and legal obligations. Most companies have a plethora of information, but only a small percentage of that information meets the definition of a record.

What are records retention schedules?

Records retention schedules identify the different categories of records companies need to keep and the length of time records falling under each of the different categories must be retained to meet the companies' business and regulatory retention needs in the jurisdictions in which they operate. Records retention schedules often identify the records custodian and the location in which records are to be retained. They also may highlight records requiring enhanced security controls. Although many categories of records retained by companies in the same industry are likely to be similar, even companies in the same industry may have variances in the information they determine rises to the level of a "record," and in their desired business retention periods. This is one reason why it is important for companies to develop records retention schedules designed to meet their specific business needs and legal obligations.

Chapter 2: Information Governance 101: Information Governance Basics

Does the law require companies to have records retention schedules?

No. However, although records retention schedules are not specifically required by law, records retention is. Numerous federal, state, and local laws in the U.S., and in other countries, require companies to retain certain types of records for specified periods of time. A records retention schedule is an important tool for companies to use in helping to ensure they are meeting their regulatory retention obligations in all locations in which they operate. Additionally, having and following an up-to-date, legally compliant records retention schedule and information governance policy and procedures can assist companies in defending, if necessary, their decisions to dispose of records and information.

How is a records retention schedule developed?

A records retention schedule typically is developed by:

1. Obtaining input from employees in all business units concerning their records, records retention practices, and business retention needs.
2. Analyzing pertinent regulatory retention requirements and other legal requirements (e.g., data protection), as well as industry best practices relating to retention and management of specific categories of information in locations in which the company operates.
3. Working with information governance leaders at the company to develop a “user-friendly” chart identifying the categories of records the company needs to retain; the length of time those records should be retained; who is responsible for retaining each category of records; and other information governing management of records (e.g., security controls).

Chapter 2: Information Governance 101: Information Governance Basics

What do companies need besides a records retention schedule?

Today, more and more companies are recognizing the importance of developing an overall information governance program, consisting broadly of people, processes, and technology.

What is information governance?

Information governance is the discipline of managing information according to its business value and legal obligations. Among other benefits, the discipline of information governance enables defensible disposition and lowers costs of legal compliance.

What are the key elements of a strong information governance program?

A strong information governance program is:

1. Led by a well-respected executive.
2. Supported by management throughout the company.
3. Developed by a cross-section of stakeholders (including the legal department, IT, records management, and key business units).
4. Designed to reflect corporate realities and to meet the company's business needs and regulatory/legal requirements.
5. Approached as a shared responsibility by the legal department, IT, and records management.
6. Implemented to address the entire information lifecycle — from creation or receipt through disposition.

Chapter 2: Information Governance 101: Information Governance Basics

In developing their information governance programs, companies should consider not only their legal obligations, but also their culture and the potential impact of information governance initiatives on existing business processes.

What topics should be covered in an information governance policy and procedures document?

At the core of a strong information governance program is a fulsome information governance policy and procedures setting forth company mandates for managing information throughout its lifecycle—from creation or receipt to final disposition. A company's information governance program should be tailored to its specific business needs and legal obligations. An information governance policy should address the following topics:

1. Ownership of records and information.
2. Creation of records and information.
3. Preservation of records and information subject to legal hold.
4. Retention of company records.
5. Storage of records and information (including security controls for protecting confidential information).
6. Transfer of records and information (including security controls for transferring confidential information).
7. Disposal of records and information (including security controls for disposing of confidential information).
8. Protection of vital records/disaster recovery.

Information governance procedures should support the policy by providing detailed guidance on how to comply with the policy mandates.

Chapter 2: Information Governance 101: Information Governance Basics

What goals should be considered when drafting an information governance policy and procedures document?

The policy and procedures should be:

1. Easy to read and understand.
2. Tailored to the company's business needs and regulatory/legal obligations.
3. Drafted to reflect the company's reality.

It is a dangerous practice to simply copy and implement a policy and procedures drafted for another company without considering whether your company can, in fact, comply with the policy and procedures and whether your policy and procedures are in line with your legal obligations.

How can I help ensure our employees understand and will comply with the policy mandates?

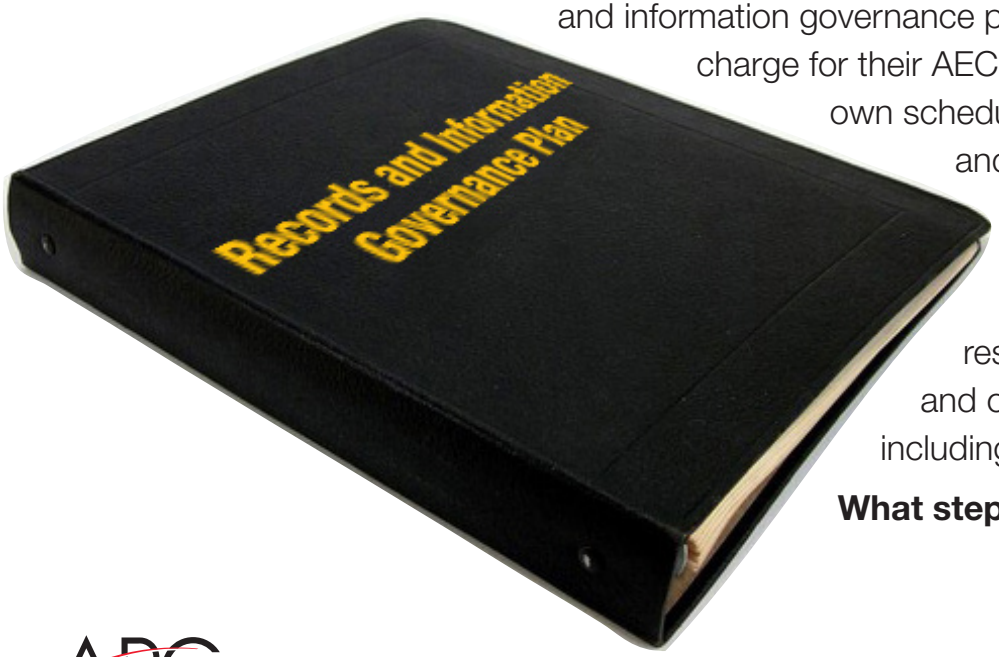
Companies should provide information governance training to employees, and should monitor compliance with the policy. As needed, companies should modify the policy, procedures, and/or training based upon input received through the compliance monitoring process. In training employees, it is important to address not only what employees should do to manage and protect company information, but also why information governance matters. Training should emphasize how the company's information governance program will benefit employees individually, as well as the company. Good information governance practices will reduce legal risks for the company and help employees do their jobs better. For example, promptly disposing of information the company no longer needs for business or legal reasons makes it easier for employees to find what they need when they need it. And that will reduce employee frustration, and also help the the company stay competitive.

Chapter 3: Records Retention Schedule and Information Governance Policy and Procedures for Companies in the AEC Industry

Does a standardized records retention schedule or information governance policy and procedures for the AEC industry exist?

No. Although websites of professional organizations, such as the AIA or the National Society of Professional Engineers, may post information governance resources from time-to-time, fulsome, "industry-blessed," up-to-date records retention schedule or information governance policy and procedures exists for companies in the AEC Industry to use as a template in creating their own records retention schedule or information governance policy and procedures.

That is why ARC Document Solutions asked Fey LLC to prepare a template records retention schedule and information governance policy and procedures that could be provided at no charge for their AEC customers to use as a starting point in developing their own schedule, policy, procedures, with input from their employees and legal counsel. We prepared these materials utilizing our information governance expertise; our knowledge of information governance best practices generally and AEC information governance specifically; our updated research and analysis of applicable laws and regulations; and our review and analysis of AEC-specific resources, including information provided by ARC Document Solutions.



What steps should companies in the AEC industry take

Chapter 3: Records Retention Schedule and Information Governance Policy and Procedures for Companies in the AEC Industry

in developing their own records retention schedule and information governance policy and procedures?

Companies in the AEC Industry may use the template records retention schedule and information governance policy and procedures as a starting point in creating their own records retention schedule and information governance policy and procedures. But companies should revise and finalize these templates based upon their corporate realities, including but not limited to their specific business needs and legal obligations. Companies should retain legal counsel to guide them through this process, or, at a minimum, to review, revise (as necessary), and ultimately approve of the records retention schedule and information governance policy and procedures.

How often should companies review their records retention schedule and information governance policy and procedures?

In light of the rapid changes in law and technology that companies confront these days, companies should review their records retention schedule and information governance policy and procedures annually, and more often if significant changes in the law or changes in technology used by the company merits an earlier review. As part of the updating process, companies should incorporate any necessary modifications identified through their compliance monitoring processes. With respect to the records retention schedule, companies should ask employees to provide input into new records categories and other necessary records retention schedule revisions as soon as such information is identified, and should update their records retention schedule accordingly.

Chapter 4: The Three Most Important Information Governance Actions Companies Can Take: Preserve, Protect, and Promptly Dispose

From an information governance perspective, what are the three most important actions companies should take?

If only three actions could be selected, my top three would be: Preserve, protect, and promptly dispose.

Preserve

First, in order to meet regulatory/legal obligations, it's critical for companies to implement policies, procedures, and processes to preserve both:

1. Records needed to meet company business needs and regulatory obligations.
2. All records and information relating to the subject matter of pending or reasonably anticipated litigation or regulatory matters in the U.S., which must be preserved as part of a company's legal hold obligations.

Protect

Second, companies need to implement policies, procedures, and processes to protect confidential information, including both confidential corporate information (e.g., trade secrets and attorney-client privileged information) and personally identifiable information, in particular, sensitive personally identifiable information (e.g., credit card data, Social Security or other identification numbers) that companies would not want to get into the wrong hands. In developing these policies, procedures, and processes, companies should consider not only technical safeguards for protecting confidential electronic information (at rest and in transit), but also physical safeguards for protecting confidential information in both electronic and paper formats.

Chapter 4: The Three Most Important Information Governance Actions Companies Can Take: Preserve, Protect, and Promptly Dispose

Promptly Dispose

Third, in order to help stem the tide of data overload that most, if not all, companies confront today, it is very important for companies to implement policies, procedures, and processes to assist them in promptly disposing of records and information no longer needed in a reasonable, legally defensible manner. In the 2010 Compliance, Governance and Oversight Council (CGOC) Information Governance Benchmark Report in Global 1000 Companies, 72% of companies cited disposal of information as the greatest benefit of an information governance program.

Most companies retain significantly more information than they need for business or legal reasons. In fact, according to a 2012 CGOC Summit Survey:

1. Only 1% of information being retained by the companies surveyed was subject to legal hold requirements (i.e., required to be preserved because it related to the subject matter of actual or reasonably anticipated litigation or regulatory proceeding).
2. Only 5% was subject to regulatory retention requirements.
3. Only 25% had temporary business value.

The remaining 69% of information being retained by the companies was, in effect, “data debris,” information having no current business or legal value.

Most companies recognize the high costs of retaining large quantities of information unnecessarily. Yet, companies are properly concerned about risks associated with improper disposal of information. In fact, in the same CGOC Benchmark Report, 75% of companies cited inability to defensibly dispose of data as their greatest challenge. It is important that companies retain legal counsel to assist them in developing and implementing reasonable and legally defensible disposition processes.

Chapter 5: Issues of Legal Admissibility

Do U.S. courts admit electronic documents into evidence?

Yes, electronic documents are routinely admitted into evidence by courts in the U.S., and they will continue to play an important role in trials and hearings. The majority of the evidence in many cases, and virtually all of the evidence in some cases, is created or used in electronic form.

However, it should be noted that courts' decisions on the admissibility of electronic documents and other evidence are fact-driven and made on a case-by-case basis. Courts' decisions vary depending on a variety of factors, including the specific facts at issue, the judge presiding over the case, and the applicable rules of evidence. Companies should retain legal counsel for advice concerning specific evidentiary questions.

If electronic copies of documents are retained, may the original paper documents be disposed of?

The Uniform Photographic Copies of Business and Public Records as Evidence Act — also sometimes referred to as the "Business Records Act" — is a law adopted federally and in most states. Under that law, if an accurate reproduction of an original business record is made in the regular course of business, then the original paper record may be destroyed unless its preservation is required by law.

Chapter 5: Issues of Legal Admissibility

Are there different rules or standards that apply in court to electronic documents versus paper originals of documents?

Federal and state courts do not apply different rules of evidence to electronic documents versus paper originals of documents. The Uniform Rules of Evidence support the admissibility of electronic documents that are accurate reproductions of original documents, and those Rules have been adopted in federal courts and in the rules of evidence of most states.

What rules of evidence are most important when it comes to the admission of documents in court?

Courts may consider multiple evidentiary rules when analyzing the admissibility of both electronic and paper documents. But the rules that most often determine whether courts admit electronic documents into evidence are:

1. Whether the documents are authentic.
2. Whether documents offered "to prove the truth of the matter asserted" are admissible under an exception to the hearsay rule.

What does it mean for an electronic document to be "authentic" such that it can be admitted by a court?

If there's not an agreement between the parties as to admissibility, a party seeking to admit electronic documents is required to produce evidence sufficient to support a finding that the document is what the party seeking to admit the document purports it to be. This is referred to as "authentication," and courts have described it as "not a particularly high barrier to overcome." Key factors in the authenticity analysis are the accuracy, trustworthiness, and reliability of the electronic document.

Chapter 5: Issues of Legal Admissibility

How may electronic documents be "authenticated"?

Courts recognize that electronic documents can be authenticated in a number of different ways. Those ways include, among others: Party agreement; testimony from a witness with knowledge that the electronic document is what it's claimed to be; evidence showing the process or system produces an accurate result; and self-authentication through a business records custodian's affidavit certifying the electronic documents are true and accurate copies of business records of regularly conducted business activities. The "self-authentication" approach is often used for electronic business records.

How can a document get past the "hearsay" rule in order to be admitted in court?

Under the "hearsay" rule, when a party is offering a paper or electronic document for the purpose of proving the truth of the matter asserted in the document, the document is generally inadmissible unless it falls within an exception to the hearsay rule. The hearsay exception courts most often analyze when ruling on admissibility is the business records exception. It has three requirements:

1. A foundation is established by someone demonstrating sufficient knowledge of the record keeping system.
2. The records must be "kept in the course of a regularly conducted business activity."
3. The source of the information and the method of preparation must be trustworthy.

For electronic documents, some courts may also require a party to demonstrate that the system creating or storing the electronic documents retained and retrieved the documents in an accurate, trustworthy, and reliable manner. When these requirements are demonstrated, courts routinely admit paper and electronic documents into evidence over hearsay objections.

Chapter 6: Risk and Risk Management

What are the five greatest risks of poor information governance practices?

1. Failing to preserve records and information relating to the subject matter of pending or reasonably anticipated litigation or regulatory matters resulting in spoliation of evidence or even obstruction of justice claims.

One of the largest risks arising from poor information governance practices is the failure to promptly and properly preserve records and information relating to the subject matter of pending and reasonably anticipated litigation and regulatory matters. When companies fail to comply with such "legal hold" obligations, they put themselves at risk of being hit with sanctions for spoliation of evidence, and even, under certain circumstances, as Pacific Gas & Electric Company (PG&E) recently experienced after failing to retain records relating to pipeline testing in connection with the San Bruno pipeline explosion investigation, charges of criminal obstruction of justice. The criminal indictment against PG&E included twelve separate charges of failing to maintain important pipeline records. Monetary sanctions for failure to preserve records and information can rise into the millions of dollars. Sanctions also can include the loss of claims and defenses, witness preclusion, and adverse inference instructions.

2. Violating data privacy regulations by failing to protect sensitive personally identifiable information.

Another significant risk is the risk of violating data privacy regulations by failing to protect sensitive personally identifiable information, such as financial information and protected health information. If companies fail to take proper administrative, technical, and physical precautions to protect sensitive personally identifiable

Chapter 6: Risk and Risk Management

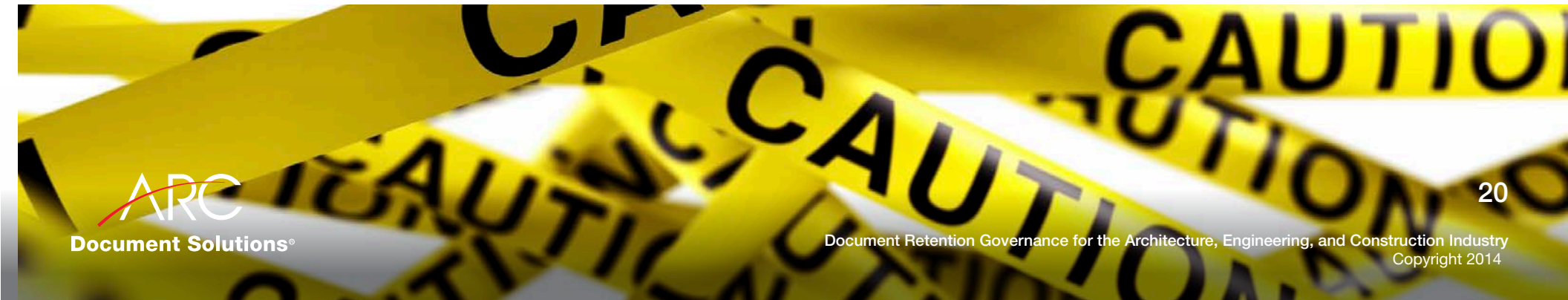
information, they may end up as targets in regulatory investigations and civil litigation — forced to spend millions of dollars providing notice of the breach and defending against lawsuits and regulatory actions, and then potentially impacted by the much more costly, long-term reputational consequences.

3. Allowing highly confidential corporate information to get into the hands of a hacker or competitor because of failure to protect such information.

Similarly, when companies fail to protect their confidential corporate information (e.g., intellectual property and trade secrets), they risk allowing that information to get into the hands of a competitor or others who may want to sell the information. If good policies, processes, and technology are not in place to protect confidential information, there is significant risk that that such information may "walk out the door."

4. Violating regulatory retention requirements by failing to retain records for the necessary retention period.

Another important risk of poor information governance practices is the risk of violating regulatory retention requirements because of failure to retain records for the necessary retention period. Like legal hold violations, regulatory retention violations can result in multi-million dollar fines.



Chapter 6: Risk and Risk Management

5. Losing business because of failure to locate necessary information in a timely manner.

The last of the top-five risks is the simple, but costly risk of losing business because of an inability to locate needed information in a timely manner, if at all. When an employee has to "reinvent the wheel" because critical business information cannot be found, it negatively impacts the productivity and overall competitiveness of the business.

When should companies address information governance risks?

The best time to address information governance risks is now. This is particularly true in light of the data deluge that most companies are experiencing and will continue to experience. It has been estimated that volume of enterprise-wide data grew at the rate of 40-60% in 2013, with a predicted annual increase of 4,300% by 2020.

There will not be an easier time to start than now, because the different types of technology in use by companies, the amount of information created and stored by companies, and the laws regulating companies' information governance practices will only increase with time. Things will not get less complex.

At Fey LLC, we spend around 80% of our time assisting companies in proactively addressing their information governance risks. The other 20% of our time is spent assisting companies in reacting to information governance failures (e.g., investigating and responding to data breach allegations). As we have seen over and over again, and as PG&E can certainly attest, it is much more costly to address information governance failures than to proactively identify and address information governance risks.

Chapter 7: Information Governance and the Advantages of a Digital Archive

What have been the primary drivers for digitally archiving information?

Information has often been referred to as the "life blood" of a company. It is a critically important corporate asset. Today, most companies store information in a variety of different information storage containers, from personal devices to flash drives to CAD files.

Beginning in the 1980's, companies began converting their paper documents to digital documents in order to process and access needed documents more quickly. Today, digital documents are widely used in business. The primary drivers for the movement to digital archiving include the desire to reduce storage costs and the need for more efficient search and retrieval capabilities.

What are the advantages of digitally archiving information?

There are multiple advantages to digitally archiving information. Here are a few of them. First, digital archives provide employees with the ability to efficiently search for and retrieve information. Second, the security controls of a strong digital solution help companies protect their confidential information, including personally identifiable information and confidential corporate information. Digital documents are significantly more secure than paper documents stored in boxes or in areas where employees can access, revise, or take and not return them. Third, a strong digital solution can automate the retention of records and prohibit deletion of records subject to legal holds. Fourth, a strong digital solution assists companies in protecting the integrity of their information. This can be a particular challenge with respect to AEC paper documents, which can be significantly impacted by environmental factors such as temperature, humidity, and pollution. Fifth, digital archives reduce overall storage costs.

Chapter 8: What to Consider When Starting Document Conversion

There are a number of factors companies should consider in converting their paper documents to digital documents. First and foremost, companies should select a digital archiving solution that is trusted, reliable and sustainable, and capable of managing the complete range of the companies' materials. Companies should take steps to confirm the selected digital archiving solution is capable of converting, retaining, preserving, retrieving, and reproducing complete and accurate documents (without smudging or other distortion) throughout the retention life of the documents stored in the system. In connection with this, companies should review any and all applicable industry standards before selecting and implementing a digital archiving solution. For example, companies should confirm the archiving solution can store CAD files in conformance with the National CAD Standard (NCS). This will help ensure the accessibility, usability, uniformity, and readability of archived files for the entire retention life of the records and information.

Second, companies should implement quality control procedures to help ensure capture of complete and accurate digital copies.

Third, companies should confirm the archiving solution has reasonable controls in place to ensure the integrity, accuracy, reliability, and security of the system throughout the time the system will be used.

Fourth, companies should implement reasonable controls to detect and prevent the unauthorized creation of, addition to, alteration of, deletion of, or deterioration of electronic documents.

Fifth, companies should maintain documents in a usable format, and retain information on how to access them, for the entire required retention period. Companies should index digital documents in a way that facilitates access, retrieval, and management of information, and should migrate and convert data, if necessary.

Chapter 8: What to Consider When Starting Document Conversion

Sixth, companies should retain documentation concerning the system and how the system works.

Seventh, companies should develop and implement written procedures governing how documents will be completely and accurately captured, retained, indexed, preserved, retrieved, and reproduced; train users on procedures; document and retain documentation of compliance with those procedures; and monitor compliance with those procedures.

Eighth, companies should conduct regular risk assessments of the system to ensure the system is performing appropriately.

Ninth, companies should maintain backups of the data on the system in an offsite location.

And tenth, companies should develop and implement sound records retention and information governance policies, procedures, and processes tailored to the business and its industry to help preserve, protect, and dispose of digital documents.

In making decisions concerning whether to keep information both electronically and in paper format, companies should consider all applicable laws and regulations, as well as industry best practices. Companies should obtain input from legal counsel concerning specific retention questions.

About the Author

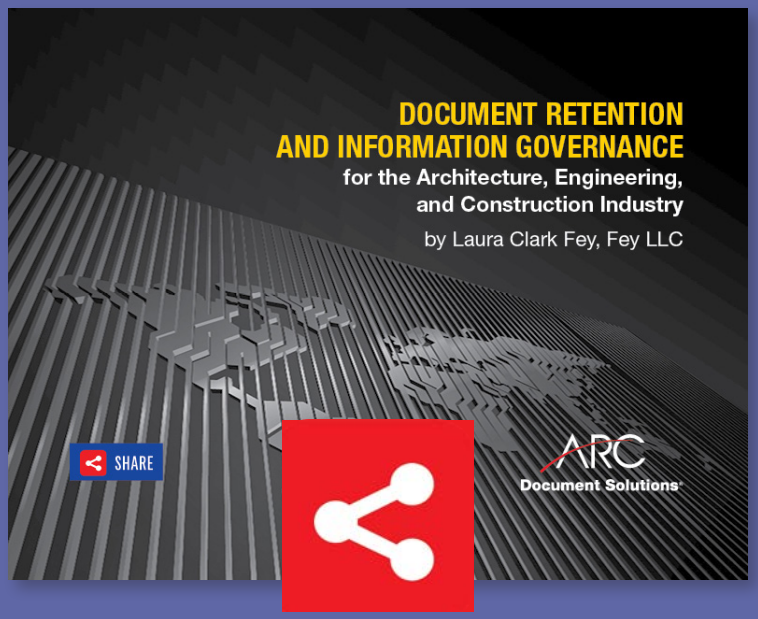
Laura Clark Fey, who has been practicing law for 23 years, is a Certified Information Privacy Professional for the U.S. and Europe (CIPP/US/E). Laura is the principal of Fey LLC, a law firm specializing in information governance solutions designed to assist companies in bolstering the strategic value of their information while minimizing risks and costs. Laura's team of attorneys and an information analyst assist corporate clients around the globe in developing and implementing practical, legally compliant solutions to their specific challenges at the crossroads of law and information technology. Fey LLC's specific practice areas include: Enterprise Content Management & Defensible Disposition; Regulatory Compliance; eDiscovery & Legal Holds; and Data Privacy & Cybersecurity.

In her specialized information governance practice, Laura draws upon many years of litigation and trial experience successfully defending large corporations in a variety of complex matters—including attorney general actions, multi-district litigation, and class actions—as well as her experience as a former Honor's Program attorney with the U.S. Department of Justice, where she was selected as an Outstanding Performance Award recipient. Laura is a widely sought-after speaker, author, and national television and radio commentator on a variety of information governance and corporate compliance issues.

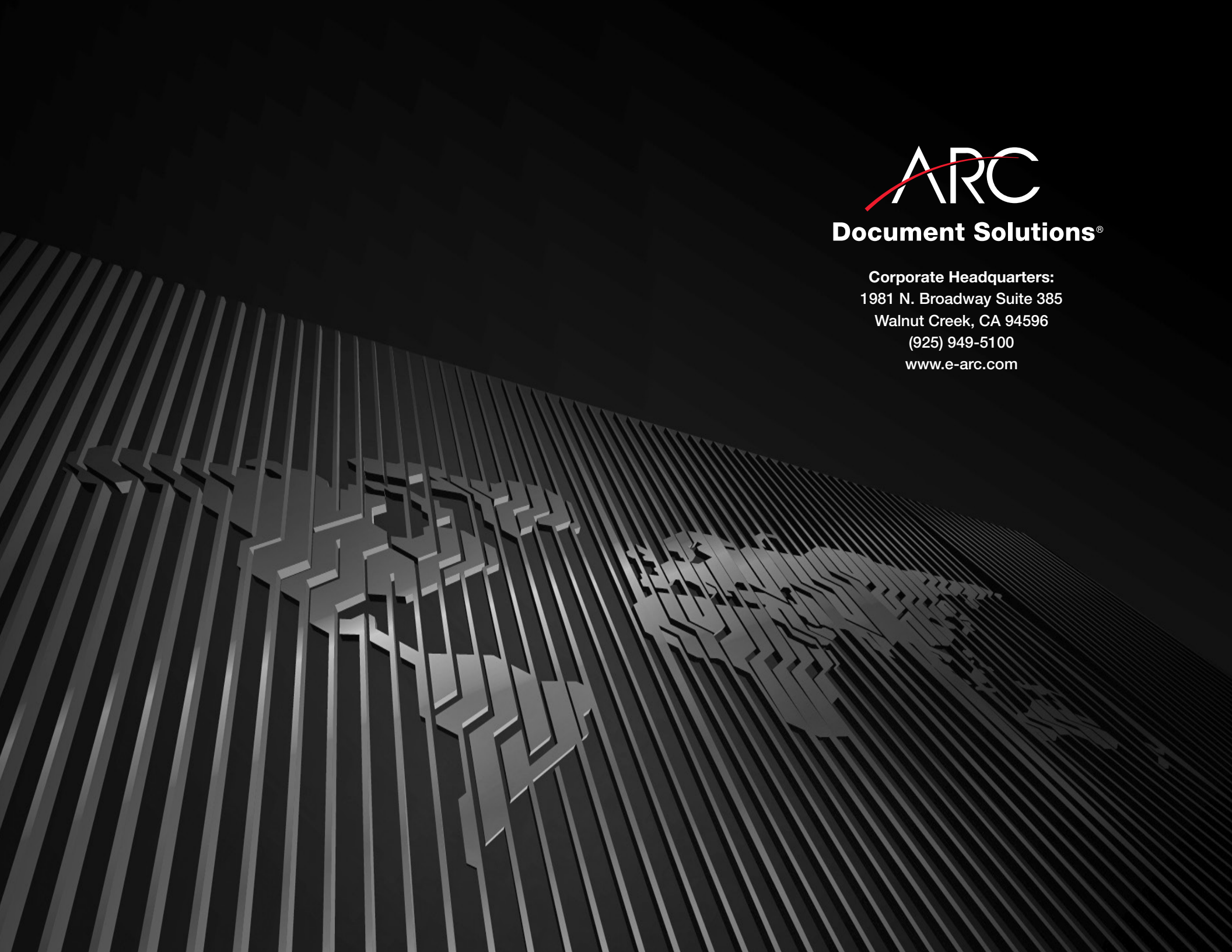
Disclaimer

This e-book does not constitute legal advice. Any entity seeking to implement a records retention schedule, information governance program, information governance policy and procedures, and/or digital archiving solution should analyze its records and information practices, as well as any internal records and information governance, data privacy, and information technology/information security policies, procedures, and guidelines, to help ensure that the schedule, program, policy, procedures, and/or solution implemented is consistent with the entity's current practices, policies, procedures, and guidelines. In addition, any entity seeking to implement a records retention schedule, information governance program, information governance policy and procedures, and/or digital archiving solution should seek legal counsel for advice concerning legal requirements specifically applicable to the entity and its records and information.

TABLE OF CONTENTS



Share this ebook



ARC
Document Solutions®

Corporate Headquarters:
1981 N. Broadway Suite 385
Walnut Creek, CA 94596
(925) 949-5100
www.e-arc.com