

WHITE PAPER

Global Records Compliance: What You Need to Know

Sponsored by: HP

Vivian Tero

June 2010

IDC OPINION

After the global economic and geopolitical turmoil of the past two and a half years, increased regulatory oversight is expected to become the norm. Organizations therefore need to be cognizant of their obligations and execute plans to manage information consistent with the records management, data retention, and data protection requirements across the countries in which they operate. Corporate written policies should address local requirements, keeping in mind that data protection implies obligations to (1) enforce the smart deletion of data and convenience copies as well as (2) prevent the destruction of critical business records due to legal and regulatory mandates. Written policies should also anticipate and plan for potential cross-border data transfer issues that may arise from these data protection and data retention (legal and regulatory) obligations.

Organizations should also have technical protocols in place to enforce these written policies. Operational service-level and cost objectives also demand that organizations seek ways to realize leverage and to have the ability to enforce policies consistently across multiple media and application types.

Adopting a global records management, data retention, and data protection framework and employing technology to enforce these policies into technical protocols will provide cost efficiencies and risk mitigation benefits.

IN THIS WHITE PAPER

This IDC White Paper discusses the impact of the critical records management, data retention, and data protection regulations across key geographies (namely, the United States, the United Kingdom, France, Germany, and Australia). It concludes with recommendations for developing global information governance best practices. Readers should note that providing legal and regulatory information is not legal advice. IDC does not provide legal advice. Readers should consult with their legal counsel experts accordingly.

SITUATION OVERVIEW

Digital information continues to grow aggressively. IDC sized the digital universe at close to 800,000 petabytes in 2009 and forecasts that the volume of digital data (created, captured, stored, and managed) will total 1.2 million petabytes (or 1.2 zettabytes) by the end of 2010 and 35 zettabytes by 2020. Volume growth will be fueled by the proliferation of new applications (such as social media and Web 2.0 applications), new infrastructure technologies (such as biometrics, virtualization, cloud computing, and intelligent grids), enhanced text analytics and data mining algorithms, and location-aware and nontraditional mobile devices (such as ebooks, tablet computers, and smartphones). The introduction of new technologies into the corporate network creates more digital information. Organizations need to assess and manage this new and growing digital information to comply with their regulatory, legal, and business obligations. In 2008, IDC concluded that between 22% and 33% of the digital universe is considered high-value information. Historical and business operations, legal obligations, and legal requirements demand that data be managed for its security, compliance, and preservation profile. IDC also concludes that valuable information will rise to 35% to 45% of the digital universe by the end of 2012.

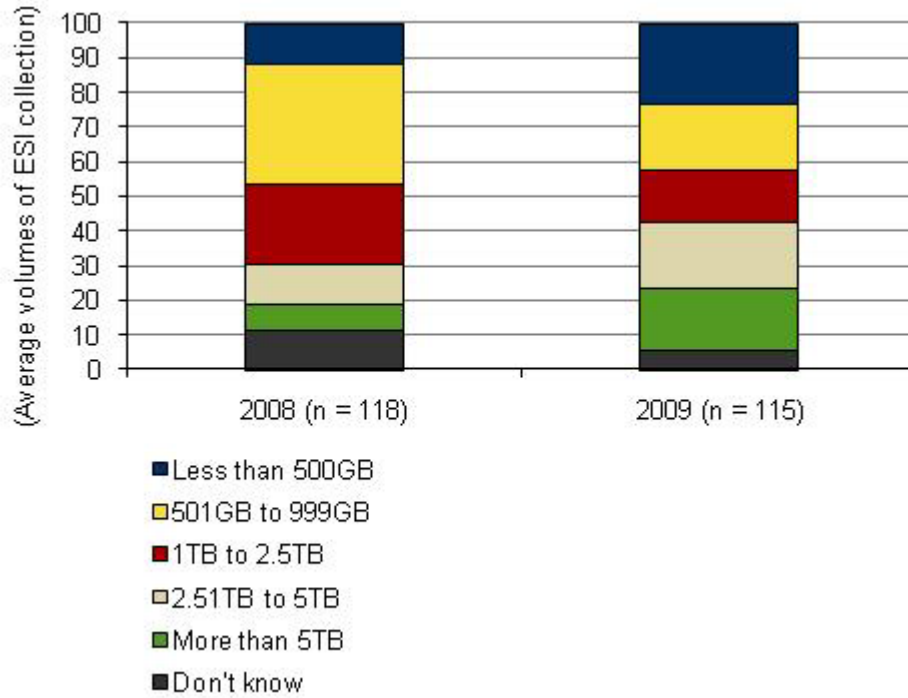
The Global Regulatory Landscape

The global economic and geopolitical turmoil of the past two and a half years, in combination with the rising recognition among consumers, businesses, and governments of the increasingly intrusive capabilities of location-aware, data mining, and predictive modeling technologies, also portends the rise of new regulations. Increased regulatory oversight is expected to become the norm worldwide. Organizations therefore need to be cognizant of their security, preservation, and compliance obligations and execute plans to manage information accordingly.

Business organizations also continue to face budget and IT operational constraints. IDC research concludes that although digital data will grow at a compound annual growth rate of more than 50% from 2008 to 2020, worldwide IT spending growth will be one-fifth of that rate. A separate IDC study also shows that while data volumes (see Figure 1) and the number of litigation events will continue to rise (see Figure 2), IT budgets for eDiscovery will remain constrained (see Figure 3).

FIGURE 1

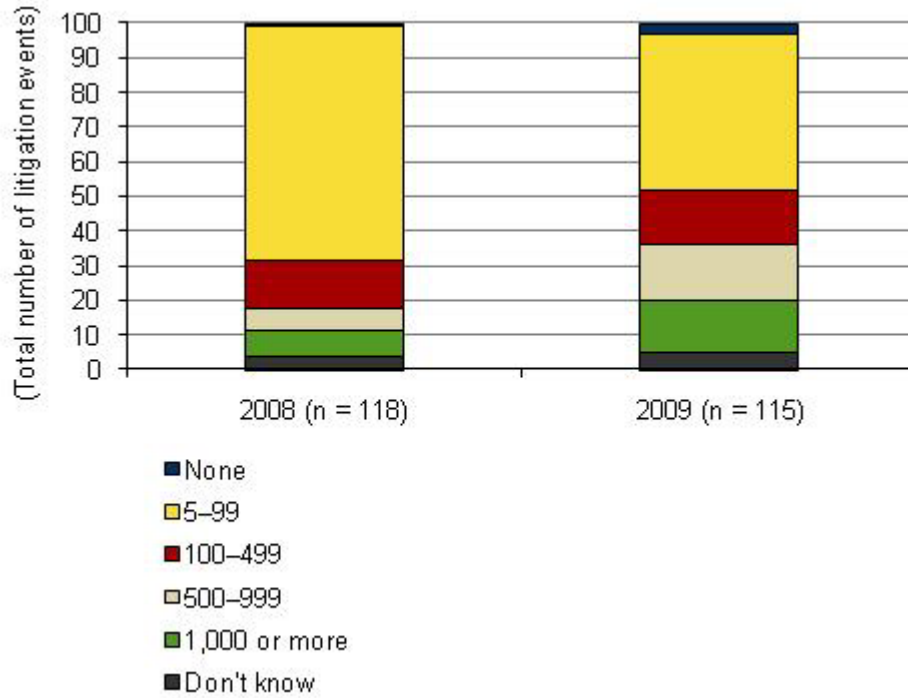
Comparison of Average Volumes of ESI Collected per Matter, 2008 Versus 2009



Source: IDC, 2008 and 2009

FIGURE 2

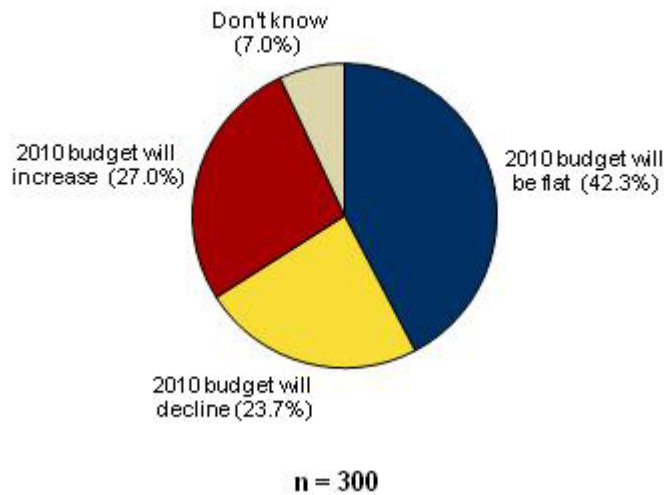
Comparison of Total Number of Litigation Events, 2008 Versus 2009



Source: IDC, 2008 and 2009

FIGURE 3

2010 eDiscovery Budgets Are Flat or Declining



Source: IDC, 2010

Business organizations therefore have a strong incentive to find opportunities for leverage as they operationalize protocols to meet their global records management, data retention, and data protection obligations. In addition to rationalizing duplicate compliance and risk management efforts, businesses also have a need to ensure that they are able to address conflicts in requirements between their headquarters and local statutes in the countries where they have business operations. These potential data protection conflicts will influence how digital information will be captured, stored, accessed, and archived.

Records Management and Information Retention

Information Isn't Always Considered a Record

ISO 15489 defines records as "information which is created, received, and maintained as evidence by an organization in the transaction of business, or in the pursuance of legal obligations, regardless of media." A record is commonly considered to be any form of content pertaining to the operations or transactions of an agency or a business. A record can be either a physical document or an electronic document in any file format. Laws, regulations, and corporate operational requirements dictate the life cycle of a record. Factors that are considered include how long the records should be kept, what becomes of a record once it reaches the end of the retention schedule, and when and which records are archived or destroyed.

Information includes the content, its associated metadata, and event logs that are produced in the normal course of business operations. It includes multiple versions of working documents or drafts, convenience copies of records, and associated metadata and event logs. Information can be declared a record at any point in its life cycle, but once declared a record, it cannot be changed or edited by the end user. The record is then signed and stamped with a date and time, classified either automatically or manually against a formal file plan, and assigned the appropriate retention schedule. Only a records administrator is able to modify or delete a record according to the retention schedule.

From a storage operations perspective, information that has been declared a "business record" is considered fixed content.

Making the Distinction Between Records Management and Retention Management

The ISO 15489:2001 standard defines records management as the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. ISO 15489 provides guidance on the (1) definition of organizational responsibilities for records and records policies, procedures, systems, and processes; (2) creation of a quality process framework that complies with ISO 9001 and ISO 14001; and (3) design and implementation of a records system.

According to ISO 15489:2001, records management programs should include the following components: (1) policies and standards definition; (2) assignment of responsibilities and authorities; (3) establishment and promulgation of procedures and guidelines; (4) provision of services related to the management and use of records; (5) design, implementation, and administration of specialized records management systems; and (6) integration of records management into business systems and processes. Records management would include policies and protocols for the retention management of said "business records."

Given the volume of information (created, captured, stored, secured, and managed) by organizations, records management protocols typically apply to a subset of the total volume. IDC's *Digital Universe Study* concludes that in 2008, 22% to 33% of the total volume of information had to be evaluated and managed for its compliance, preservation, and security profile. IDC estimates that 20% to 40% of the "high value" information is "business records." High-value information is expected to account for 35% to 45% of the digital universe by the end of 2012.

The practice of retention management focuses on the disposition of the rest of the information that is not deemed "business records." The advent of the 2006 amendments to the Federal Rules of Civil Procedure for Electronic Discovery underscored the criticality of adopting retention management for nonrecords. Specifically, Rule 34 defined electronically stored information as "discoverable" and removed the "hearsay" test. Given the potential volume that might be deemed as "discoverable" electronically stored information (ESI) in a litigation or regulatory investigation, the persistent nature of electronic data, and the unique challenges in maintaining chain of custody, it became even more important for organizations to adopt formalized retention protocols for "nonrecords" (i.e., documents that are not part of the business process and those not governed by security, compliance, or preservation obligations). Retention management is typically practiced in concert with a corporation's records management protocols, and it ensures that information is destroyed consistently. Retention management is done to address the following objectives:

- Mitigate future discovery liabilities that may arise from keeping the information
- Support plans to optimize the organization's datacenter storage operations
- Demonstrate compliance with data protection regulations. (Data protection regulations not only mandate the capture, storage, and destruction of specific data types — such as personal identification information [PII] and personal health information [PHI] — and records but also impose an obligation on the organization to prevent the inadvertent destruction of these data types.)

Global Records Management, Data Retention, and Data Protection Regulations and Standards

This section highlights the critical regulations and records management standards in the United States, the United Kingdom, Germany, France, and Australia. This document highlights these five countries because most global organizations have business operations in these locales. In addition, the regulatory and legal infrastructures in these countries tend to have the most stringent requirements. The records management and retention protocols in these countries are often used by multinational corporations as the model for developing an international global records retention program.

Australia

- ☒ **Archives Act of 1983.** This act established the National Archives of Australia, the organization mandated with providing records management standards and advice for government agencies. Each of the states in the Commonwealth has records management regulations that define how records should be managed. Records administration is the responsibility of each of the states.
- ☒ **Freedom of Information Act of 1982.** The regulation gives members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies, including ministers, departments, and public authorities of the Commonwealth. Each of the states and territories has similar legislation. The Freedom of Information Amendment (Reform Bill 2010) seeks to establish a statutory framework for an information publication scheme for Commonwealth agencies. The amendment also mandates that documents held by specific service providers are subject to the act. It also limits access to specific intelligence agency information and documents of the Department of Defense (DoD).
- ☒ **Corporate Law Economic Reform Program (CLERP 9)/Corporations Act.** This act amends the Corporations Act 2001 (Commonwealth), which governs corporate law in Australia. It was enacted in July 2004.
- ☒ **Part VA of the Trade Practices Act 1974.** The Trade Practices Act 1974 of the Parliament of Australia provides for protection of consumers and prevents some restrictive trade practices of companies. Part V deals with consumer protection.
- ☒ **Anti-Money Laundering and Counter-Terrorism Financing Act 2006.** The AML/CTF Act covers the financial sector, gambling sector, bullion dealers, and other professionals or businesses ("reporting entities") that provide particular "designated services." The regulation is intended to enable authorities to prevent and detect money laundering and terrorism financing.
- ☒ **Income Tax Assessment Act of 1997 (amended from Income Tax Assessment Act of 1936).** This is one of the main statutes by which income tax is calculated.

For more information on Australia's regulatory and legal landscape, see Table 1 in the Appendix section of this document.

France

- ☒ **NF Z42-013 (updated in 2009).** This standard provides specifications for the design and operation of computer systems to address preservation, management, storage, continuity, security, and integrity of records stored in computer systems. The guidelines reference MoReq, ISO 15489, and ISO 14721.
- ☒ **French Data Protection Mandates.** French data protection regulations require data controllers to provide information on their data processing activities to their data subjects in a clear, specific, and easily accessible manner. The data subjects would be able to exercise their right of access more easily, including by email.
- ☒ **Financial Security Law of France (LSF or Loi de Sécurité Financière).** Enacted in July 2003, this regulation strengthened the legal provisions relating to corporate governance. The French law on financial security (Loi de Sécurité Financière) was adopted by the French parliament on July 17, 2003, to enforce the enterprise governance principles. This law is applied to companies that call on the public savings.
- ☒ **Délibération n° 2009-474.** Issued on August 9, 2009, by the French Data Protection Authority (CNIL), the statute details the legal requirements for French/U.S. data transfers in discovery activities related to litigation or for U.S. investigations.
- ☒ **Ordinance 2004-178 (National Patrimony).** According to French records and archival laws, records are the whole of documents — regardless of date, form, and physical support — created or received by any physical or juridical person and by every public or private agency or organization in the course of their activities.
- ☒ **Law No. 80-538 of July 16, 1980, Journal Officiel de la République Française, July 17, 1980, p. 1799.** Blocking statutes are intended to restrict the export of important business records.
- ☒ **Freedom of Information Act (Loi n° 78-753).** The Directorate of the Archives of France is mandated with providing useful standards for electronic records, including long-term preservation.

For more information on France's regulatory and legal landscape, see Table 2 in the Appendix section of this document.

Germany

- ☒ **Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).** German data protection regulations stipulate that personal data — defined as data referring to an individual (natural person) — may only be stored or processed if either the person agrees in writing or the law allows the storage/processing.
- ☒ **Tax Mandates § 62(2) Implementing Regulation of the Turnover Tax Law (UstDV).** Germany's complex tax laws have document production and retention requirements and are governed by Federal Tax Court, Tax Procedure Act, and the Commercial Code.
- ☒ **German Corporate Governance Code.** The German Corporate Governance Code presents essential statutory regulations for the management and supervision of German listed companies and contains internationally and nationally recognized standards for good and responsible governance.

- ☒ **DOMEA.** This initiative of Germany's Department of Interior defines records management policies for government electronic records.
- ☒ **Telecommunications Data Retention Law.** On March 2, 2010, the German High Court rejected an EU mandate to retain telephone calls and email traffic for six months for law enforcement purposes.

For more information on Germany's regulatory and legal landscape, see Table 3 in the Appendix section of this document.

United Kingdom

- ☒ **U.K. Public Records Act of 1958 (and The National Archives 2002).** The Public Records Act of 1958 is an act of the Parliament of the United Kingdom forming the main legislation governing public records in the United Kingdom. The National Archives 2002 (TNA 2002) defines functional requirements for electronic document and records management.
- ☒ **Freedom of Information Act.** This act does not impose any obligations on public authorities or their agents to retain documents for a certain period. However, it does make it a criminal offense to destroy documents after a request for information (a "subject access request") has been made, if the destruction was with the intention of preventing disclosure.
- ☒ **eDisclosure (U.K. eDiscovery), Legal Records, and BSI PD 008.** There are no specific retention periods for legal records, but there are statutory limitation periods that define the length of time documents will be required to bring or defend proceedings, typically six years. The British Standards Institution (BSI) PD 008 provides the standards for addressing the authenticity, records management, and storage of electronic documents and records, including their admissibility for use in the court of law and their legal status.
- ☒ **Financial Services Authority (FSA): Companies Act and Tax Legislation.** FSA regulations and mandates cover a broad range of financial products. However, the records retention requirements covered by the FSA expand beyond the financial services industry and work in concert with the Information Office.
- ☒ **Electronic Communications Act 2000.** Regulations apply to communications data that is generated or processed in the United Kingdom by public communications providers in the process of supplying the communications services concerned.
- ☒ **U.K. Data Protection Act.** The act regulates the use of "personal data" and applies to most personnel records (paper, microform, or computerized format). Computerized systems are covered by law, as are certain manual systems: To be covered, manual systems must be organized into a "relevant filing system."

For more information on the United Kingdom's regulatory and legal landscape, see Table 4 in the Appendix section of this document.

United States

- ☒ **U.S. National Archives Act of 1934 (revised 1949, 1984).** This act established a new agency to care for the records of the federal government and ensure that they endured for future generations. The National Archives had a mandate to identify, preserve, and provide access to significant government documents and records.

- ☒ **US DoD 5015.2 V3 (United States Department of Defense Standard for Records Management).** This standard sets mandatory baseline functional requirements and requirements for classified marking, access control, and other processes and identifies nonmandatory features deemed desirable for records management application (RMA) software. The latest revisions of the standard include (1) requirements for compliance with the Freedom of Information Act and Privacy Act, (2) baseline requirements for RMA-to-RMA interoperability and archival transfer to the National Archives and Records Administration (NARA), and (3) requirements for adherence to DoD net-centric information-sharing principles including certification testing by the Joint Interoperability Test Command (JITC).
- ☒ **Health Insurance Portability and Accountability Act (HIPAA) and the HITECH Provisions of the American Recovery and Reinvestment Act (ARRA) 2009.** Title II (Privacy and Security Rules) of HIPAA covers health plans, healthcare clearinghouses, and healthcare providers that conduct certain financial and administrative transactions electronically.
- ☒ **State Medical Records Retention Requirements and ARRA 2009.** HIPAA does not include record retention periods for individual health information, but it allows individuals to request an accounting or report of who has accessed their records. This covers the six years prior to the date of request for the accounting. Under ARRA 2009, states have mandates covering the retention of various forms of medical records. Retention varies from state to state and across medical records type.
- ☒ **SEC/FINRA.** Rules 17a-3 and 17a-4 of the Securities Exchange Act of 1934 require broker-dealers to preserve certain electronic records. FINRA Rules 2110 (standards of commercial honor and principles of trade), 2210 (communications with the public), 2310 (recommendations to customers [suitability]), 3010 (supervision), and 3110 (books and records) as well as numerous interpretive releases speak about the retention and supervision of electronic communications (including email, IM, and even social networking applications).
- ☒ **Federal Rules of Civil Procedure for Electronic Discovery (eDiscovery).** The following sections impact an organization's records management and information retention practices: Rule 26(a) adds ESI as its own category. Rule 26(f) requires litigants to meet and confer before discovery begins to agree on some form of protocol. Rule 34(d) requires litigants to discuss and establish protocols on how documents will be produced for the requesting party. Rule 37(f) provides "safe harbor" when electronic evidence is lost and unrecoverable as a matter of regular business processes.
- ☒ **Sarbanes-Oxley Act of 2002.** SOX covers all publicly traded U.S. companies as well as foreign companies that are listed on the U.S. stock exchanges (NYSE, NASDAQ). SOX continues to influence financial reporting processes among public companies.

For more information on the United States' regulatory and legal landscape, see Table 5 in the Appendix section of this document.

Model Requirements for the Management of Electronic Records 2010

MoReq — Model Requirements for the Management of Electronic Records — was first published in 2001 as European guidance on electronic records management systems (ERMS). MoReq2 updated the standards in 2008, and the upcoming MoReq2010 is intended to enable a more modular and simpler framework. MoReq is an evolving set of base specifications to help government, financial, environmental, manufacturing, and commercial organizations acquire the most complete and tested ERMS quickly and safely. MoReq is intended to enable users, vendors, regulators, IT managers, and records managers across Europe to develop a framework that would help them translate requirements for information compliance in government, financial, environmental, manufacturing and commercial organizations into technical protocols. MoReq does not specify a particular electronic records management system but outlines the essential elements such a system should have to ensure records are properly managed and can be accessed at all times as well as ensure that records are retained in compliance with their retention schedules and are properly disposed of upon expiration. Records management standards in several European countries (including the United Kingdom, Germany, and France) are evolving to align with the MoReq framework.

International Council on Archives' Principles and Functional Requirements for Records in Electronic Office Environments

The Principles and Functional Requirements for Records in Electronic Office Environments was sponsored by the International Council on Archives. The aim of the project is to develop globally harmonized principles and functional requirements for software products used to create and manage electronic records in office environments. These functional requirements will be consistent with ISO 15489.

The suite of guidelines and functional requirements is organised into three modules:

Module 1: Overview and Statement of Principles: background information, organisation, fundamental principles and additional context;

Module 2: Guidelines and Functional Requirements for Records in Electronic Offices: a global high-level statement of core and optional requirements, including application guidelines and a compliance checklist; and

Module 3: Guidelines and Functional Requirements for Records in Business Systems: guidelines and generic core and optional functional requirements for records in business systems.

(Source: *Principles and Functional Requirements for Records in Electronic Office Environments*, <http://adri.gov.au/products/ICA-M1-overview-principles.pdf>)

FUTURE OUTLOOK

Best Practices for Architecting Global Information Governance Programs

IDC research identified the following high-level best practices for corporations seeking to navigate their global data retention and data protection obligations:

- ☒ Adopt a consistently enforced global information retention and disposition program. Retention schedules should be defined in accordance with business, regulatory, and legal obligations. Policies should address both physical (or hardcopy) and digital versions of the records. These policies should also reflect the business and legal requirements in the geographic boundaries in which the business operates. Given the data volume growth and the speed with which global regulations continue to evolve, chasing compliance by managing discrete records retention programs across each country is not an economically sustainable model. Country-specific programs also make it difficult for organizations to identify and plan for potential conflicts in policies across national jurisdictions. Corporations should consider adopting a master records retention schedule and allow for management by exceptions by country or region. In countries where data retention and data protection laws are nonexistent and where data is critical (such as financial records), several global corporations default to the retention and data protection protocols that govern corporate headquarters. Given the volume of data and the number of records classes involved, corporations are also advised to focus their efforts on adopting protocols to discover, identify, define, and enforce retention, disposition, and privacy policies for the corporation's strategic information assets in high-risk content stores.

- ☒ Ensure that a global organizational structure exists to support the program. IDC research notes that the more successful programs tend to come from organizations where the global records retention governance body remained independent from a discrete functional unit (such as IT or legal), had discrete budgets, and reported directly to the corporate board. Within each country or region, corporations should identify and assign the records owners and system custodians. These functions have the responsibility to ensure that local data retention and protection protocols harmonize with the global master data retention and protection programs and that the IT storage and security operations support these technical protocols. In addition, corporations should consider implementing training and periodic classes in corporate records management and data privacy for all employees. These policies are further reinforced through the employee performance review. To reinforce the records compliance and privacy-aware culture, corporations should conduct regular audits and systematically monitor system compliance with formal retention and data protection policies. These audit reports also include remediation plans for the failed checks, data leakage, and noncompliant postures in the most critical information assets.

- ☒ Developments in the eDiscovery and eDisclosure mandates in countries with stringent regimes in combination with pending changes to data sharing and data transfer agreements across national boundaries should compel global organizations to plan for international legal holds and collections. In countries with prescriptive and strict legal discovery requirements (such as the United States and the United Kingdom), corporations should consider adopting protocols to suspend and override scheduled destruction schedules in the event of a litigation event, arbitration, and requests for information.
- ☒ Global organizations should examine the data protection and data retention requirements in the most stringent and prescriptive nations and look for the commonalities (in records categories, data and application types/content stores, mandated retention and data protection obligations, and statutes of limitations). These common elements will make up the foundation of the global master records retention schedule and data protection protocol. This mapping exercise also points to areas of potential cross-boundary conflicts and points to areas that the organization should plan for proactively.
- ☒ Given the complex nature of a global organization's business, legal, and IT operations, technology — especially records management; data management technologies such as ETL, database archiving, and databases; archiving; search; data analytics; content/text analytics; content security and data loss prevention technologies; and storage — plays a critical function in ensuring that policies are harmonized and enforced consistently in accordance with the local data retention and protection requirements. When corporations adopt a global master retention schedule, they also have an opportunity to employ common technology solutions to enforce these common, baseline policies as well as handle exceptions. Leveraging these common technologies provides opportunities to simplify the organization's IT infrastructure and lower its IT operating and maintenance costs. The drive to utilize a global technology architecture should be tempered by local data protection requirements. As such, it is important for corporations to ensure that legal/compliance and the IT functions are made aware of these considerations.

Assess the Impact of Cloud Computing on Records Management, Information Retention, and Data Protection Protocols

Records management, information retention, and data protection policies should take into account corporate IT plans to deploy cloud (public or private) and software as a service (SaaS) services. Corporations should consider evaluating the following attributes prior to consuming cloud- and SaaS-based solutions:

- ☒ Assess the risk, security, preservation, and compliance profile of the data. Identify and determine the information that might potentially move into the cloud. This should include data and content that could be used in testing and development environments, in addition to production data. More often, corporations pay close attention to the security and privacy profile of the data but conduct less stringent assessments in determining the data's retention, archiving, and legal preservation profile. The evaluation should also include determining who would have access to the data, the conditions in which (physical and logical environments) the authorized users can access the data, and the activities they are allowed to perform when interfacing with the application.

- ☒ In the event that the organization moves security-, preservation-, and compliance-intensive data into the cloud, corporate protocols should ensure that information and records are managed consistently for their security, retention, and records management profile, regardless of the physical and logical location of the systems managing the data.
- ☒ Conduct proper due diligence on the capabilities of the cloud/SaaS service provider to address (1) data security; (2) application performance/service-level requirements; (3) content migration; (4) government and third-party litigation access; (5) protocols for handling confidential information, nonpublic information, and trade secrets; and (6) support for records management and retention management policies (including litigation hold requirements).
- ☒ Work very closely with the corporate legal team to carefully evaluate the cloud service agreements (CSAs), paying particular attention to any language that contains exclusionary clauses. Examples of such clauses include statements that contain a disclaimer of liability relating to service quality and availability; disclaimer of liability for any third-party action; and unilateral rights to limit, suspend, or terminate the service.

The HP Information Governance Portfolio

HP Software and HP Services provide a broad range of solutions to facilitate a corporation's information governance program.

HP Information Governance Services Portfolio

HP services include information governance and strategy planning; content management; and data management design, deployment, and implementation.

- ☒ HP Software Professional Services for Information Governance Strategy and Planning include the following:
 - ☐ Information Management Transformation Experience Workshop is an interactive, slide-free workshop for line-of-business (LOB) and IT executives to learn how information management can help drive business transformation.
 - ☐ Information Strategy and Planning Service is an assessment service that helps IT define its information strategy to meet business strategy, with specialized examples for records management, Microsoft SharePoint, and others.
 - ☐ Information Optimization Service is a custom assessment service to prioritize and purge relevant information to optimize cost and mitigate risk.
 - ☐ Microsoft SharePoint Governance helps develop the right strategy and plan to optimize and manage Microsoft SharePoint across the organization.

- ❑ File Planning Service enables organizations to create department and company file plans. The result is better records management implementation and improved information management maturity.
- ❑ Master Planning Service analyzes the client's business requirements from an information perspective and develops an iterative, cost-effective plan to capture, manage, retain, secure, and deliver all types of information.
- ☒ HP's Content Management services deliver solutions for document automation, records management, and document management.
- ☒ HP Data Management services include software product deployment and integration in support of HP Data Protector software, HP Database Archiving, HP Integrated Archive Platform, and HP Medical Archive solution. HP also offers design and implementation services for data migration across information management systems (storage, email, document management, and archiving platforms).

HP Information Governance Software Portfolio

The HP software portfolio for information governance consists of the following products:

- ☒ HP TRIM is a scalable enterprise records management system that enables organizations to easily capture, secure, and manage all business records regardless of source and meet governance and regulatory compliance obligations while improving business process efficiency and staff productivity. The HP TRIM for SharePoint module extends HP TRIM enterprise records management to provide transparent records management and seamless site archiving for all SharePoint content and supports Microsoft SharePoint 2010 and SharePoint 2007.
- ☒ HP Integrated Archive Platform consolidates long-term retention of email and files into a single, scalable content archive. The platform offers connectors to facilitate the retention and legal hold of content for Microsoft Exchange, Lotus Domino, and Windows-based file, Web, and application data, including medical records and application databases.

Market Challenges

The biggest impediment to any company seeking to adopt a global retention and data protection program is organizational apathy. Successful execution of such programs hinges on close collaboration among key stakeholders — IT, compliance, legal, and LOB functions. Before embarking on these programs, corporations and their vendor partners should plan on getting these key stakeholders engaged and invested in the data retention and data protection program very early on. The organizational design should take into account organizational reporting structure, budgets, and degree and frequency of formal interaction. The plan should also include incentives and training to encourage these stakeholders to own the program and evangelize it to the rest of the organization.

CONCLUSION

Business organizations that operate across multiple national boundaries are advised to adopt a global records retention and disposition program. Such a program should have the following attributes:

- ☒ A consistently enforced global information retention and disposition program that takes into account regulatory retention, legal hold, data protection and business objectives. Policies should address both physical (or hardcopy) and digital versions of the records. Corporations should also have a master records retention schedule and allow for management by exceptions by country or region.
- ☒ Protocols to discover, identify, define, and enforce retention, disposition, and privacy policies for the corporation's strategic information assets in high-risk content stores. Local data retention policies should also take into account the local data protection requirements.
- ☒ The global organizational structure is designed to support successful execution of the global retention program. The makeup and design of the retention program's governance organization impact the degree to which retention and data protection are aligned with IT storage and IT security operations practices.
- ☒ Global organizations should examine the data protection and data retention requirements in the most stringent and prescriptive nations and look for the commonalities (in records categories, data and application types/content stores, mandated retention and data protection obligations, and statutes of limitations). These common elements will make up the foundation of the global master records retention schedule and data protection protocol. This mapping exercise also points to areas of potential cross-boundary conflicts and points to areas that the organization should plan for proactively.
- ☒ Use technology to map information assets and records classes to policies, logical and physical location, and control statements. Technology also facilitates the ability to identify leverage when designing the global master retention schedule and to consistently enforce compliance.
- ☒ Conduct periodic audits to verify compliance with the records retention and legal hold policies.

APPENDIX

Key Global Records Management Standards and Information Retention and Data Protection Regulations

Australia

TABLE 1

Australia Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
Archives Act of 1983	<p>This act established the National Archives of Australia. The National Archives is mandated with providing records management standards and advice for government agencies, as well as ensuring that the national archival collection is controlled and described and that it remains stable and accessible over time. The National Archives also maintains the administrative history of the Australian government so that records can be related to their original context.</p> <p>Each of the states in the Commonwealth has records management regulations that define how records should be managed. Records administration is the responsibility of each of the states:</p> <ul style="list-style-type: none"> • New South Wales: State Records Act 1998 • Queensland: Public Records Act of 2002 • Victoria: Victorian Electronic Records Strategy (VERS Standard)/PROV Standard Management of Electronic Records (PROS 99/007) • Western Australia: State Records Act of 2000 • Tasmania: The Archives Act 1983 and amendments and the Archives Regulations 2004 	<p>Records retention and disposal schedules are the primary formal instruments through which the relevant state archivists define the length of time for which records must be retained. Schedules cover both electronic and nonelectronic forms of the documents and records.</p> <p>Normal administrative practice (NAP) allows agencies to destroy certain types of records in the normal course of business. Agencies do not require the permission of the National Archives to dispose of records (in the normal course of business) that fit within the scope of NAP. This includes (1) facilitative, transitory, or short-term items, including appointment diaries, calendars, "with compliments" slips, personal emails, listserv messages and emails in personal or shared drives, and emails that have been captured in a corporate records management system; (2) rough working papers and/or calculations; (3) drafts not intended for further use or reference; (4) copies of material retained for reference purposes only; and (5) published material not included as part of an agency's records.</p>

TABLE 1**Australia Records Compliance Environment**

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
Freedom of Information Act of 1982/Freedom of Information Amendment (Reform) Bill 2010	The regulation gives members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies.	The act provides for access to official documents of government ministers, departments, and public authorities of the Commonwealth. Each of the states and territories has similar legislation. The proposed 2010 amendments to the act seek to establish a statutory framework for an information publication scheme for Commonwealth agencies. The amendment also mandates that documents held by specific service providers are subject to the act. It also limits access to specific intelligence agency information and documents of the Department of Defense. The amendments are having an impact on how records are made available for FOI requests.
Corporate Law Economic Reform Program (CLERP 9)/ Corporations Act	This act amends the Corporations Act 2001 (Commonwealth), which governs corporate law in Australia. It was enacted in July 2004.	<p>The act mandates the retention of financial records.</p> <ul style="list-style-type: none"> • s 1306: The company must take all reasonable precautions for guarding against damage to, or destruction or falsification of or in, any book or part of a record required to be kept or prepared by the company. • s 286: The company must keep financial records that correctly record and explain its transactions and financial performance for seven years. Financial records include invoices, receipts, and documents of prime entry. • s 288: Electronic storage is allowed provided that records are available and can be converted into hardcopy within a reasonable time.
Part VA of the Trade Practices Act 1974 (Cth)	<p>This act details the obligations of a corporation during health and product liability issues.</p> <p>The Trade Practices Act 1974 of the Parliament of Australia provides for protection of consumers and prevents</p>	Manufacturers should keep records or products manufactured and/or sold for 11 years in case a situation arises where a consumer suffers injury, loss, or damage from a product defect.

TABLE 1**Australia Records Compliance Environment**

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
	some restrictive trade practices of companies. Part V deals with consumer protection, including unfair practices, product safety and information, conditions and warranties in consumer transactions, actions against manufacturers and importers of goods, and product liability.	
Income Tax Assessment Act of 1936 (amended 1997)	This act focuses on tax documentation and transfer pricing.	<p>This act mandates the retention of supporting documentation:</p> <ul style="list-style-type: none"> • s 262A(1)-(2): An entity is required to keep records that record and explain all transactions and other acts engaged in by the person that are relevant for the purposes of the relevant Act. • s 262A(4): Generally records must be kept for five years.
Anti-Money Laundering and Counter-Terrorism Financing Act 2006	This act specifies compliance and regulatory obligations in the financial services industry to address money laundering and tax evasion.	The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act) imposes significant compliance and regulatory obligations on the financial services industry. These provisions relate not only to existing money laundering offenses such as dealing in the proceeds of crime but also to tax evasion.

Source: IDC, 2010

France

TABLE 2

France Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
NF Z42-013 (updated in 2009)	The standard is intended for organizations or businesses wishing to implement electronic records management systems, publishers of electronic archiving systems, and electronic document and records management application vendors and services providers. RFPs for records management software applications increasingly require certification to this standard.	NF Z42-013 from the French Association for Standardization (AFNOR) — a member of the International Organization for Standards (ISO) — provides specifications for the design and operation of computer systems to address preservation, management, storage, continuity, security, and integrity of records stored in computer systems. The guidelines reference MoReq, ISO 15489, and ISO 14721.
French Data Protection Mandates	Law requires that data controllers provide information on their data processing activities to their data subjects in a clear, specific, and easily accessible manner. The data subjects would be able to exercise their right of access more easily, including by email.	Retention requirements must comply with core principles mandating that "personal data not be kept for longer than is necessary, data is processed in line with individual rights, and data not be transferred to other countries without adequate protection." These requirements have implications on data capture, storage, and archiving protocols.
Financial Security Law of France (LSF or Loi de Sécurité Financière)	Enacted in July 2003, this regulation strengthened the legal provisions relating to corporate governance. The French law on financial security (Loi de Sécurité Financière) was adopted by the French parliament on July 17, 2003, to enforce the enterprise governance principles. This law is applied to companies that call on the public savings.	Like the Sarbanes-Oxley Act, this law relies mainly on three topics : <ul style="list-style-type: none"> • Increased accountability by top management • Enhancement of internal control • A reduction of conflicts of interest
Délibération n° 2009-474	Issued on August 9, 2009, by the French Data Protection Authority (CNIL), this statute details the legal requirements for French/U.S. data transfers in discovery activities related to litigation or for U.S. investigations.	The statute reiterates that all data that flows out of France for litigation purposes must be in line with the French Data Protection Law of 1978 (as amended): <ul style="list-style-type: none"> • Data storage: Data sent to the United States may be stored only for the "duration of the proceedings." • Informing the individuals: Pursuant to French data protection laws, the individuals to whom the personal data in France refers must be

TABLE 2

France Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
		informed about the data transfer (exceptions may apply if such disclosure "endangers the proceeding"). These individuals must have the right to know what is sent and to "rectify" false or incomplete information about them. (source: Bingham.com)
Ordinance 2004-178 (National Patrimony)	This legislation provides for official definition of records and archives as governed by French records management, data protection, and archival laws.	<p>According to French records and archival laws, records are the whole of documents — regardless of date, form, and physical support — created or received by any physical or juridical person and by every public or private agency or organization in the course of their activities.</p> <p>Archives is defined as a "collection of documents, because of their age, their form, and their material support, made or received by a physical or moral person, whether private or public, in the course of their normal activities." (L.211-1)</p>
Law No. 80-538 of July 16, 1980, Journal Officiel de la République Française, July 17, 1980, p. 1799.	Blocking statutes are intended to restrict the export of important business records.	<p>This law forbids French nationals from disclosing to foreign governments (such as courts) documents that are important to the sovereignty, security, or fundamental economic interests of France.</p> <p>Corporations with operations in France have to ensure cross-border controls exists in their information management and storage infrastructure systems.</p> <p>Controls typically focus on managing efforts to retrieve large quantities of records (for eDiscovery and regulatory requests for information) rather than just a few records at a time (ordinary course of business). Controls would typically address written policies to forbid violation of national data protection law; technical blocks to prevent unauthorized people or departments from accessing particular records while granting access to those who have been authorized; and alerts and audit trails to enable after-the-fact review of who accessed which records and when.</p>

TABLE 2

France Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
Freedom of Information Act (Loi n° 78-753)	The Directorate of the Archives of France is mandated with providing useful standards for electronic records, including long-term preservation. Title I addresses freedom of access to administrative documents and the reuse of public information. The act defines the right of everyone to information as defined and guaranteed by the provisions of Chapters I, III, and IV of this title regarding freedom of access to government documents, including records, reports, studies, statistics, directives, instructions, circulars, notes and ministerial responses, correspondence, opinions, forecasts, and decisions.	<p>Public records covered by Loi n° 78-753 have an automatic expiration of 25 years from the date of the document or the most recent document included in the file, with the exception of documents produced under a contract of services performed on behalf of one or more specific persons when those documents come in.</p> <p>Retention periods for the deceased individuals (Loi n° 78-17) are set 25 years from the date of death of the person for documents whose disclosure violates patient confidentiality. If the date of death is unknown, the time is 120 years from the date of birth of the person concerned. For defense and security (Décret n° 79-1035), the retention period is set at 50 years after the date of the document or the most recent document included in the file for documents whose disclosure violates the secrecy of national defense and the fundamental interests of the state in the conduct of monetary policy. The same deadline applies to documents that have an assessment or value judgments about an individual, named or readily identifiable, or that reveal the behavior of a person under circumstances likely to cause damage.</p> <p>The same deadline applies to documents relating to the construction, equipment, and operation of structures, buildings, or parts of buildings used for detention of persons detained. This period is counted from the end of the allocation to these uses of works, buildings, or parts of buildings in question.</p> <p>4.) 65 years from the date of the document or the most recent document included in the file, or a period of 25 years from the date of death of a person where the latter period is shorter:</p>

TABLE 2

France Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
		<p>a) For documents whose disclosure violates the secrecy of statistics where relevant data is collected through questionnaires relating to facts and behavior of a private nature;</p> <p>b) For documents relating to investigations conducted by judicial police services;</p> <p>c) For documents relating to cases before the courts, subject to special provisions relating to judgments, and enforcement of judgments;</p> <p>d) The minutes and registers of public officers or officers;</p> <p>e) For records of birth and marriage vital statistics, after their completion;</p> <p>5.) 100 years from the date of the document or the most recent document included in the file, or a period of 25 years from the date of death of a person where the latter period is shorter for the papers referred to in section 4, relating to a minor.</p> <p>The same limits apply to documents that covered or were covered by the national defense secrets whose disclosure is likely to endanger the safety of persons named or readily identifiable. It is the same for documents relating to investigations conducted by police services judicial matters brought before the courts, subject to special provisions relating to judgments, and execution of court decisions that affect communication regarding intimate sexual details of individuals.</p> <p>II. Documents that can be found on the public record whose disclosure would lead to the dissemination of information to design, manufacture, use, or location of nuclear, biological, chemical, or other weapons that have direct or indirect destruction of a similar level.</p>

Source: IDC, 2010

Germany

TABLE 3

Germany Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)	Personal data (that is, data referring to an individual [natural person]) may only be stored or processed if either the person agrees in writing or the law allows the storage/processing.	<p>Section 10 establishes rules for automated data retrieval procedures. Organizations are required to adopt measures to ensure that the admissibility of the retrieval procedure can be monitored. For such purpose, they shall specify in writing: (1) the reason for and purpose of the retrieval procedure, (2) the data recipient, (3) the type of data to be communicated.</p> <p>Section 14 indicates that the "storage, modification, or use of personal data shall be admissible where it is necessary for the performance of the duties of the controller of the data file and if it serves the purposes for which the data was collected. If there has been no preceding collection, the data may be modified or used only for the purposes for which it was stored.</p> <p>Sections 19, 20, and 21 define the rights of the data subject.</p>
Tax Mandates § 62(2) Implementing Regulation of the Turnover Tax Law (UstDV)	Complex tax laws have document production and retention requirements and are governed by Federal Tax Court, Tax Procedure Act, and the Commercial Code.	<p>Tax and commercial documents must be kept for 10 years. This includes commercial books, inventories, accounting records, opening balance sheets, annual accounts, directors' reports, and consolidated accounts.</p> <p>Other commercial documents, such as "transaction letters" (referring to transactions between traders for the purpose of preparing, pursuing, ceasing, or repudiating business transactions), must be retained for six years.</p> <p>Under some special tax laws, such as § 62(2) Implementing Regulation of the Turnover Tax Law, the destruction of an original document is not permitted during the retention period.</p>

TABLE 3**Germany Records Compliance Environment**

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
German Corporate Governance Code	The German Corporate Governance Code presents essential statutory regulations for the management and supervision of German listed companies and contains internationally and nationally recognized standards for good and responsible governance. (http://www.ecgi.org/codes/documents/cg_code_germany_june2009_en.pdf)	Complex and stringent data protection mandates mean that German companies normally do not have general document retention policies. Specialized individual departments of larger companies, such as legal, tax and accounting, or patent departments, will often have special and very sophisticated internal document retention guidelines.
DOMEA (German Ministry of Interior)	DOMEA stands for "Document Management and Electronic Archiving in Electronic Business" and is also known as the "Paperless Office Concept." This initiative of Germany's Department of Interior defines records management policies for government electronic records. DOMEA is intended to support the creation of a governmentwide IT system that supports records management, the creation of electronic records, and cooperative business processes. (http://www.verwaltung-innovativ.de/cIn_047/nn_684678/DE/Organisation/domea__konzept/domea__konzept__node.html?__nnn=true)	The DOMEA project recognizes that electronic records have to meet the requirements for recordkeeping in public administrations, which are prescribed in laws, standing orders, regulations, and instructions. They include salient points such as the completeness, integrity, and authenticity of official records; the records principle of public administration; and the accountability and lawfulness of administrative procedures. It includes a framework for the detailed procedure for the disposal and archiving of electronic records and created 440 criteria that defined the functional requirements of an electronic records management system.
Telecommunications Data Retention Law	On March 2, 2010, the German High Court rejected an EU mandate to retain telephone calls and email traffic for six months for law enforcement purposes.	This law overturns the 2008 directive requiring telecommunications service providers to retain mobile and fixed telephony and Internet service data for six months. The courts demanded that data stored so far be deleted immediately.

Source: IDC, 2010

United Kingdom

TABLE 4

United Kingdom Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
<p>U.K. Public Records Act of 1958 (and The National Archives 2002 [TNA 2002])</p>	<p>The Public Records Act of 1958 is an act of the Parliament of the United Kingdom forming the main legislation governing public records in the United Kingdom. It applies to the U.K. Central Government, including Executive Agencies and Non-Departmental Public Bodies.</p> <p>TNA 2002 defines functional requirements for electronic document and records management (and takes into account the obligations defined by the Freedom of Information Act, ISO 15489, MoReq, egovernment interoperability framework of the United Kingdom, and Data Protection Act of 1988).</p> <p>(http://www.nationalarchives.gov.uk/policy/act/default.htm)</p>	<p>The Public Records Act of 1958 requires that every person responsible for public records of any description shall make arrangements for the selection of records for permanent preservation and for their safekeeping. U.K. government agencies have an obligation to maintain inventories of their electronic and other records and subject the records to disposal schedules based on the administrative and permanent value of the information. Public records selected for permanent preservation must be transferred to the Public Record Office not later than 30 years after their creation (except with the approval by the Lord Chancellor in certain defined circumstances). In order to ensure that Web sites (or parts of Web sites) can be preserved as long as necessary for the conduct of public business, proper electronic records management procedures must be followed to safeguard copies of different versions against loss, interference, or electronic degradation. The Freedom of Information Act (which came into effect in January 2005) impacted archive provision by both public records and private collections held in public institutions and places of deposit. The Freedom of Information Act (FOIA) replaces the access provisions in the Public Records Act of 1958. Section 45 Code of FOIA sets out good practice in handling requests for information. It also includes a section on Freedom of Information and public sector contracts.</p>
<p>Freedom of Information Act</p>	<p>This act does not impose any obligations on public authorities or their agents to retain documents for a certain period. However, it does make it a criminal offense to destroy documents after a request for information (a "subject access request") has been made, if the destruction was with the intention of preventing disclosure.</p> <p>(http://www.nationalarchives.gov.uk/policy/foi/default.htm)</p>	<p>FSA Freedom on Information policy-related documents can be disposed of seven years after the creation or when policy has been superseded. Right-to-know requests should be retained three to seven years after a case is closed, depending on the record class subcategory. Certain documents should be kept as originals, such as documents under seal, stamped documents, and documents of title. There is an implicit requirement that retention practice should</p>

TABLE 4

United Kingdom Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
		be application and media agnostic. Both paper/physical-based records and electronic records need to be managed consistently.
eDisclosure (U.K. eDiscovery), Legal Records, and BSI PD 008	<p>Legal records include legal advice given and received, contracts and agreements under seal, title deeds and other property-related documents, major agreements, royalty agreements, and royalty payments. There are no specific retention periods, but there are statutory limitation periods that define the length of time documents will be required to bring or defend proceedings, typically six years.</p> <p>The British Standards Institution (BSI) PD 008 provides the standards for addressing the authenticity, records management, and storage of electronic documents and records, including their admissibility for use in the court of law and their legal status.</p>	<p>In any arbitration in which issues relating to eDisclosure are likely to arise, the parties should confer at the earliest opportunity regarding the preservation and disclosure of electronically stored documents and seek to agree on the scope and methods of production. The primary source of disclosure of electronic documents should be reasonably accessible data; namely, active data, nearline data, or offline data on disks. For more on this, see http://www.ciarb.org/information-and-resources/E-Disclosure%20in%20Arbitration.pdf.</p> <p>BSI PD 008 provides the framework and best practices for the implementation and operation of electronic records systems. It also includes practices addressing the protocols for ensuring the legal admissibility of documents and records as these are being transferred across computing systems and procedures for the use of digital certificates to ensure the authenticity of such documents and records.</p>
Financial Services Authority/Companies Act/Tax Legislation	FSA regulations and mandates cover a broad range of financial products. However, the records retention requirements covered by the FSA expand beyond the financial services industry and work in concert with the Information Office.	<p>Rule 5.3.1 (6) requires organizations to retain accounting records for a minimum of six years, where the first two years of records are stored in a manner that allows the organization to produce the document within 24 hours of request.</p> <p>Retention requirements cover a broad range of records categories. Retention periods vary depending on the records categories and subcategories from 30 days (for short-circuit TV footage) to permanent (for corporate records and legacy information on rule books).</p> <p>For more information on recommended best practices, see http://www.fsa.gov.uk/pubs/staff/retention.pdf.</p>

TABLE 4

United Kingdom Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
		There is an implicit requirement that retention practice should be application and media agnostic. Both paper/physical-based records and electronic records need to be managed consistently.
Electronic Communications Act 2000	Regulations apply to communications data that is generated or processed in the United Kingdom by public communications providers in the process of supplying the communications services concerned.	<p>The act covers the capture, retention, and storage of data in fixed telephony, mobile telephony, and Internet services. It also includes data relating to unsuccessful call attempts for telephony data that is stored in the United Kingdom and Internet data that is logged in the United Kingdom. Data retention requirements mandate that data be retained by the public communications provider for a period of 12 months from the date of the communication in question. The security rules also require the public communications provider to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access, or disclosure. The regulation also imposes an obligation to ensure lawful access and proper destruction of the data (ensure that data is inaccessible) at the end of the retention period.</p> <p>For more on this, see http://www.opsi.gov.uk/si/si2009/pdf/ukxi_20090859_en.pdf.</p>
U.K. Data Protection Act	The act regulates the use of "personal data" and applies to most personnel records (paper, microform, or computerized format). Computerized systems are covered by the law, as are certain manual systems: To be covered, manual systems must be organized into a "relevant filing system." For more on this, see http://www.ico.gov.uk/what_we_cover/data_protection.aspx .	Personal data should not be kept for longer than is necessary, data must be processed in line with individual rights, and data cannot be transferred to other countries without adequate protection. Retention periods cover a broad range and are dependent on the record subclass category. For more on this, see http://www.ico.gov.uk/what_we_cover/data_protection.aspx .

Source: IDC, 2010

United States

TABLE 5

United States Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
U.S. National Archives Act of 1934 (revised 1949, 1984)	The National Archives Act, signed by President Franklin Roosevelt on June 19, 1934, established a new agency to care for the records of the federal government and ensure that they endured for future generations. The National Archives had a mandate to identify, preserve, and provide access to significant government documents and records. In 1949 the archives was incorporated into the General Services Administration and renamed the National Archives and Records Service. In 1984, Congress reestablished the National Archives as an independent agency, designated the National Archives and Records Administration (NARA). The archivist of the United States, appointed by the President and confirmed by the Senate for a 10-year term, oversees the agency.	NARA is responsible for the records management and retention of documents generated by the executive, legislative, and judicial branches of the federal government. NARA maintains the U.S. Presidential Libraries and works with the National Historical Publications and Records Commission to encourage and fund programs to preserve, publish, and use archival materials relating to U.S. history.
US DoD 5015.2 V3 (United States Department of Defense Standard for Records Management) This standard is the most frequently referenced certification by U.S. and global organizations in defense and federal government.	This standard sets mandatory baseline functional requirements and requirements for classified marking, access control, and other processes and identifies nonmandatory features deemed desirable for records management application (RMA) software. The latest revisions of the standard include (1) requirements for compliance with the Freedom of Information Act and Privacy Act, (2) baseline requirements for RMA-to-RMA interoperability and archival transfer to the NARA, and (3) requirements for adherence to DoD net-centric information-sharing principles including certification testing by the Joint Interoperability Test Command (JITC). The goal of the information-sharing principles is to make records visible through the development and registration of standardized metadata, accessible through Web services with usable standardized interfaces, and understandable through the availability and use of rich metadata describing the records and their context.	The standard expects records management applications to adhere to DoD net-centric information-sharing principles and is intended to provide guidance to vendors. It requires implementation protocols to include certification testing by JITC and compliance with DoD information-sharing principles, identifying the need to make data holdings visible, accessible, understandable, and trusted. The standards also demand that records management software applications include information access (IA) controls for availability, integrity, confidentiality, authentications, and nonrepudiation and comply with the National Telecommunications and Information Systems Security Policy. (http://jitic.fhu.disa.mil/recmgt/p50152stdapr07.pdf)

TABLE 5

United States Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
<p>Health Insurance Portability and Accountability Act (HIPAA) and the HITECH Provisions of the American Recovery and Reinvestment Act (ARRA) 2009</p>	<p>Title II (Privacy and Security Rules) of HIPAA covers health plans, healthcare clearinghouses, and healthcare providers that conduct certain financial and administrative transactions electronically.</p>	<p>The Privacy and Security Rules govern patients privacy rights. Covered entities also have an obligation to secure patient records containing individually identifiable health information so that they are not readily available to those who do not need them.</p> <p>Highlights of the HITECH provisions of ARRA 2009 include:</p> <ul style="list-style-type: none"> • Individuals must be notified of a data breach, including Web-based vendors that store medical data and HIPAA-covered entities. • Individuals have a right to restrict disclosure of health information. • Sale of protected health information is prohibited.
<p>State Medical Records Retention Requirements and ARRA 2009</p>	<p>HIPAA does not include record retention periods for individual health information, but it allows individuals to request an accounting or report of who has accessed their records. This covers the six years prior to the date of request for the accounting.</p> <p>Under ARRA 2009, states have mandates covering the retention of various forms of medical records. Retention varies from state to state and across medical records type. The American Health Information Management Association (AHIMA) maintains a database of best practices recommendations and state medical records retention requirements for various types of medical records. For more on this, see AHIMA.org.</p>	<p>Practices and protocols cover a broad range of physical and electronically maintained patient health information. Retention mandates range from five years (for diagnostic images) to permanent (for register of birth, register of deaths, and register of surgical procedures). For electronic health information, protocols and technical procedures should include creation, capture, authentication, correction, retrieval, archiving, and destruction of information (in accordance with record retention policies). It should also include protocols and technical procedures for producing a hardcopy output of the information as necessary for litigation and other warranted use as well as adhere to federal and state privacy and security requirements.</p>

TABLE 5

United States Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
SEC/FINRA	<p>Rules 17a-3 and 17a-4 of the Securities Exchange Act of 1934 require broker-dealers to preserve certain electronic records.</p> <p>FINRA Rules 2110 (standards of commercial honor and principles of trade), 2210 (communications with the public), 2310 (recommendations to customers [suitability]), 3010 (supervision), and 3110 (books and records) as well as numerous interpretive releases speak about the retention and supervision of electronic communications (including email, IM, and even social networking applications).</p>	<p>Documents filed with the Securities and Exchange Commission by public companies must be kept for five years. Banks must retain records relating to credit transactions for at least 25 months.</p> <p>Recordkeeping requirements exist in connection with purchase and sale documents, customer records, associated person records, customer complaint records, and certain other matters and range from three years (for customer complaints) to seven years (for transactions and sales). Electronic communications has been expanded to include not only email, digital voicemail, and instant messaging but also social networking sites such as Twitter, LinkedIn, and blogs.</p>
Federal Rules of Civil Procedure for Electronic Discovery (eDiscovery)	<p>Corporations need to be aware of and plan for the following sections:</p> <ul style="list-style-type: none"> • Rule 26(a) adds electronically stored information (ESI) as its own category. • Rule 26(f) requires litigants to meet and confer before discovery begins to agree on some form of protocol. • Rule 34(d) requires litigants to discuss and establish protocols on how documents will be produced for the requesting party. • Rule 37(f) provides "safe harbor" when electronic evidence is lost and unrecoverable as a matter of regular business processes. 	<p>Corporations would need to adopt and deploy an enterprisewide records management and retention program.</p> <p>Key attributes are:</p> <ul style="list-style-type: none"> • The records management and retention policies should be consistently enforced regardless of the format by which the content and data is created, captured, and stored. • The program should address both physical or paper-based records and electronic records. • The program should address search, retrieval, chain of custody, and production requirements.
Sarbanes-Oxley Act of 2002	SOX covers all publicly traded U.S. companies as well as foreign companies that are listed on the U.S. stock exchanges (NYSE, NASDAQ). SOX continues to influence financial reporting processes among public companies.	Section 401 requires that financial statements published by issuers be accurate and presented in a manner that does not contain incorrect statements or admit to state material information. These financial statements shall also include all material off-balance sheet liabilities, obligations, or transactions.

TABLE 5

United States Records Compliance Environment

Regulations/Legal Mandates/ Industry Standards	Description	Corporate Records Management, Data Protection, and Data Retention Implications
		Section 802 addresses fraud and defines penalties of fines and/or up to 20 years' imprisonment for altering, destroying, mutilating, concealing, or falsifying records, documents, or tangible objects with the intent to obstruct, impede, or influence a legal investigation. It imposes minimum retention periods for both audit records and financial records and communications pertaining to financial reporting. It specifically calls out accounting firms that audit publicly traded companies to keep related audit documents for no less than seven years after the completion of an audit.

Source: IDC, 2010

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2010 IDC. Reproduction without written permission is completely forbidden.