Building a GARP®-Compliant Solution

How the ability to understand meaning helps organizations govern information in compliance with ARMA International's GARP® Principles

Autonomy White Paper

Autonomy®
an HP company

Index

Introduction

Today's organizations run on information that is used to power nearly every effort including strategic decisions, product development, marketing campaigns, sales, as well as finance and legal processes. Information, when managed well, enables organizations to generate revenue and remain competitive. Not surprisingly, an organization's inability to govern information can, and has, lead to corporate collapses resulting from ill-timed paper shredding, inadvertent deletion of electronic records, and failure to identify and find content related to an investigation or litigation. As a result, these events have renewed interest in corporate records compliance, retention period requirements, litigation preparedness, and related issues. The US Sarbanes-Oxley Act, the Freedom of Information Act, the US and UK Rules of Civil Procedure, as well as other laws and regulations have created new concerns among C-level leaders. These concerns are driving greater standardization in information governance and records management practices across corporate America and the rest of the world.

Setting forth clear guidelines for records management best practices, ARMA International's Generally Accepted Recordkeeping Principles® (GARP®) have been published with two key goals in mind: to foster a general awareness of recordkeeping standards and principles, and to assist organizations in developing consistent records systems that comply with them. The GARP® Preamble goes on to state that, "These principles are comprehensive in scope, but general in nature. They are not addressed to a specific situation, industry, country, or organization, nor are they intended to set forth a legal rule for compliance that must be strictly adhered to by every organization in every circumstance. They are intended to set forth the characteristics of an effective recordkeeping program, while allowing flexibility based upon the unique circumstances of an organization's size, sophistication, legal environment, or resources. The objectivity of the principles, combined with a reasonable approach to applying them, will yield sound results for any organization: a responsive, effective, and legally compliant recordkeeping system."

As noted, closely tied to the ability to adhere to GARP® is the existence within an organization of its information governance program. Defined by Gartner, Information Governance ("IG") is "an accountability framework that includes the processes, roles, standards, and metrics that ensure the effective use of information in enabling an organization to achieve its goals." As organizations consider changes to ensure GARP® compliance, at the level that is appropriate for the organization, choosing solutions that can map capabilities to GARP® is critical.

Autonomy's full suite of Meaning Based Governance solutions, powered by its Intelligent Data Operating Layer (IDOL), provides a unique approach that understands the content and context of information to help organizations support GARP® compliance. With Autonomy, organizations can create and maintain a responsive, effective, and legally compliant information governance program that operates in accordance with the Principles.

Organizations can use the GARP® Maturity Model to conduct a preliminary evaluation of information governance practices to determine the level of capabilities, from one to five, as follows:

- ***Level 1 (Sub-standard)*** *– The organization's governance concerns are either not addressed at all, or are addressed in a very ad hoc manner. Organizations that identify primarily with these descriptions should be concerned that their programs will not meet legal or regulatory scrutiny.*
- ***Level 2 (In Development)*** *– The organization recognizes the impact of information governance and that it may benefit from a more defined IG program. Its current approach may be leaving the organization vulnerable to legal or regulatory scrutiny since practices are ill-defined and still largely ad hoc.*
- ***Level 3 (Essential)*** *– The organization addresses the essential or minimum requirements to meet legal and regulatory requirements. There are defined policies and procedures, and more specific decisions taken to improve the way information is managed.*
- ***Level 4 (Proactive)*** *– The organization is initiating IG improvements throughout its operations. IG issues and considerations are integrated into business decisions on a routine basis, enabling the organization to easily meet legal and regulatory requirements.*
- ***Level 5 (Transformational)*** *– The organization has integrated IG into its overall corporate infrastructure and business processes to such an extent that compliance with program requirements is routine.*

As the name suggests, the GARP® Maturity Model provides a framework for assessing an information governance program's maturity and to assist organizations in determining their level of compliance to uncover gaps. As GARP® experts know, technology alone cannot help an organization reach its desired level in the Maturity Model. The combination of people and processes with technology is required to deliver true results. It is important to note, achieving a Level 5 is not always a necessary goal for an organization. Determining the right level to target depends on a range of factors including an organization's, regulatory profile and business structure. For example, whether it operates across country or state lines or is publically traded. Business drivers also play a role, as well as desired risk/reward ratios.

GARP® can also be used to "cut through debates about what should happen to records," and is also useful in helping organizations "select systems that will meet the criteria laid out by GARP® to ensure effective and efficient management of vital business records in both local and global business environments."[1]

This white paper reviews the provisions of GARP®, outlines some of the challenges faced by organizations in meeting each principle, and offers guidance on how an organization, using Autonomy solutions, can build new systems and adopt practices to meet the requirements.

Creating Value through GARP® Compliance

With the explosion of ESI and the size of data sets reaching historical highs, relying on individuals to manually classify information is no longer feasible. It is also extremely difficult to monitor the multiple information channels that exist today given the expanded use of mobile devices, cloud computing, and social media. To keep pace, organizations must streamline and automate information governance processes according to defined policies and rules to enable compliance with GARP®.

Understanding and identifying the information that flows through an organization is the first order of business. Without the ability to understand what information exists, organizations cannot effectively manage nor leverage the value of information. With Autonomy IDOL (Intelligent Data Operating Layer), organizations can automate the process of understanding the content and context of data at a level that enables information to be used to increase revenues, innovate, and compete. GARP® provides a set of guidelines that can help companies leverage the opportunities that exist within information assets.

GARP® Principle #1 – Accountability

Accountability	**Level 1 (Sub-Standard)**	**Level 2 (In-Development)**	**Level 3 (Essential)**	**Level 4 (Proactive)**	**Level 5 (Transformational)**
A senior executive (or person of comparable authority) oversees the recordkeeping program and delegates program responsibility to appropriate individuals. The organization adopts policies and procedures to guide personnel, and ensure the program can be audited.	No senior executive (or person ofcomparable authority) is responsible for the records management program. The records manager role is largely non-existent or is an administrative and/or clerical role distributed among general staff.	No senior executive (or person of comparable authority) is involved in or responsible for the records management program. The records manager role is recognized, although he/she is responsible for tactical operation of the existing program. In many cases, the existing program covers paper records only. The information technology function or department is the de facto lead for storing electronic information, but this is not done in a systematic fashion. The records manager is not involved in discussions of electronic systems.	The records manager is an officer of the organization and is responsible for the tactical operation of the ongoing program on an organization-wide basis. The records manager is actively engaged in strategic information and record management initiatives with other officers of the organization. Senior management is aware of the program. The organization has defined specific goals related to accountability.	The records manager is a senior officer responsible for all tactical and strategic aspects of the program. A stakeholder committee representing all functional areas and chaired by the records manager meets on a periodic basis to review disposition policy and other records management-related issues. Records management activities are fully sponsored by a senior executive.	The organization's senior management and its governing board place great emphasis on the importance of the program. The records management program is directly responsible to an individual in the senior level of management, (e.g., chief risk officer, chief compliance officer, chief information officer) OR, A chief records officer (or similar title) is directly responsible for the records management program and is a member of senior management for the organization. The organization's stated goals related to accountability have been met.

An organization shall assign a senior executive who will oversee a recordkeeping program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.
Source: ARMA International at http://www.arma.org/garp/index.cfm

The lack of a unified method for managing and controlling information across departments, such as IT and Legal, can hinder an organization's ability to maintain accountability. At the same time, simply appointing an individual to enforce IG objectives is an inadequate approach by itself. The same holds true that technology alone cannot fulfill every responsibility. Establishing accountability for an information governance program requires leadership combined with the right technology to support reporting capabilities and accountability.

[1] Gartner, ARMA International's Generally Accepted Record-Keeping Principles: An IT Viewpoint Published: 7 June 2010, Analyst: Debra Logan

Accountability can be achieved when comprehensive information access and control is reliable, and supported by technology that offers a view into the organization. Systems that provide a dashboard of accountability make it easier to monitor and act on developments in real time. Relying on manual processes to govern information consistently is neither feasible, practical, or in most cases possible.

Employing technology to automate and streamline business and recordkeeping processes make it possible for organizations to reach their desired GARP® level. Available as an on-premise or cloud-based deployment, Autonomy Compliance Solutions enable corporate, government, and enterprise organizations to achieve effective control and visibility over any and all content by automating policy management.

Autonomy Compliance Solutions enable organizations to maintain accountability using a range of capabilities including:

Policy Enforcement for Distributed Content – As information grows and regulations tighten, it becomes more important to have visibility into and control over enterprise information. For instance, understanding how much information is on hold or expired is key to meeting compliance and storage goals. Autonomy Policy Authority enables policies to be enforced and monitored on distributed content, including content residing in ECM repositories like SharePoint.

Autonomy ControlPoint allows organization to automate policy application across all aspects of the information lifecycle, including application of meaning-based policies at the point of creation, storage management, and ultimately, disposition management. Automatic alerts for document custodians can be sent if deletion of important information is attempted. Among numerous other features, ControlPoint offers de-duplication capabilities to minimize storage costs and reduce discovery times.

Business Process Management – To support business process management (BPM) Autonomy Liquid Office supports document-centric BPM by accelerating cycles, ensuring compliance, and connecting people with information and processes, regardless of location. LiquidOffice is the first and only BPM solution that enables real-time access to, and use of, time-sensitive content throughout the process lifecycle.

Controlled Content Retention and Disposition – Autonomy Records Management solutions help organizations to proactively achieve information governance through its ability to manage, control and discover physical, electronic and email records located across the enterprise.

Intelligent Process Automation – Workflow Manager a full featured intelligent process automation engine with easy to use visual tools, rule-based routing, intelligent electronic forms, real-time business activity monitoring, secure connectivity and rich capabilities for modeling business processes.

GARP® Principle #2 – Integrity

Integrity	Level 1 (Sub-Standard)	Level 2 (In-Development)	Level 3 (Essential)	Level 4 (Proactive)	Level 5 (Transformational)
A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.	There are no systematic audits or defined processes for showing the origin and authenticity of a record. Various organizational functions use ad hoc methods to demonstrate authenticity and chain of custody, as appropriate, but their trustworthiness cannot easily be guaranteed.	Some organizational records are stored with their respective metadata that demonstrate authenticity; however, no formal process is defined for metadata storage and chain of custody. Metadata storage and chain of custody methods are acknowledged to be important, but are left to the different departments to handle as they determine is appropriate.	The organization has a formal process to ensure that the required level of authenticity and chain of custody can be applied to its systems and processes. Appropriate data elements to demonstrate compliance with the policy are captured. The organization has defined specific goals related to integrity.	There is a clear definition of metadata requirements for all systems, business applications, and paper records that are needed to ensure the authenticity of records. Metadata requirements include security and signature requirements and chain of custody as needed to demonstrate authenticity. The metadata definition process is an integral part of the records management practice in the organization.	There is a formal, defined process for introducing new record-generating systems and the capture of their metadata and other authenticity requirements, including chain of custody. This level is easily and regularly audited. The organization's stated goals related to integrity have been met. The organization can consistently and confidently demonstrate the accuracy and authenticity of its records.

A recordkeeping program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.
Source: ARMA International at http://www.arma.org/garp/index.cfm

Integrity violations have caused companies to fully collapse or suffer large sanctions or fines due to an inability to show that data produced in a given litigation or investigation is authentic and has maintained an auditable chain-of-custody throughout its lifecycle. Chain of custody refers to the chronological documentation that reflects the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. The ability to audit and report all of these steps can be challenging, only made more difficult by the fact that the nature of information itself has become more complex. Beyond structured data that fits neatly into the columns and rows of relational databases, information is increasingly less organized or "unstructured." As much as 85 percent of data is now unstructured and exists in the form of documents, email, text messages, audio, video, and social media interactions.

Compounding the issues of complex data is the fact that official records make up only 7 to 9 percent of all content in an organization, leaving the majority of information outside the formal records management scheme. This remaining 91 to 93 percent is usually managed on an inconsistent and ad hoc basis, which adds risk, and creates inconsistencies that must be addressed to ensure solid governance. To ensure integrity across all information, organizations must be able to manage all types of content, including paper and digital, structured and unstructured.

Organizations can ensure the integrity of information using technology that comprehends the meaning of the full content of any type of information—including its metadata. As the acknowledged leader in the rapidly growing area of Meaning Based Computing (MBC), Autonomy solutions use MBC to form an understanding of all information—whether structured or unstructured—and recognize relationships that exist within it. MBC enables computers to ingest and understand the full set of information contained within documents, video files, audio recordings, and social media interactions, while preserving associated metadata for auditable chain of custody. Through sophisticated functionality and analytics, Autonomy Meaning Based Governance (MBG) solutions enable organizations to automate manual operations in real time to proactively manage data while preserving metadata, with the highest levels of security, auditability, and integrity.

Additionally, when customers or employees know that an organization is managing itself with integrity, it allows those customers and/or employees to make better decisions regarding whether to do business with the organization or join its staff.

Policy Authority – Transforming information governance from an inefficient and error-prone process to an automated and defensible operation is critical to an organization's success. Autonomy provides a centralized meaning-based policy engine to provide a consistent set of rules to subscribing applications, thus automating all the steps in the policy control procedure, and elevating the corporate-wide policy above any one application. By providing central and consistent policies, data integrity is maintained for both structured and unstructured data.

Next Generation Archiving – Maintaining the proper chain of custody requires archiving solutions that provide the flexibility, scalability, and security needed to meet the demands of growing data stores. Chain of custody must be maintained across structured and unstructured data, rich media, and multichannel communications. As owner of the largest private cloud in existence, with over 31 petabytes under management, Autonomy records are hosted in the world's most state-of-the-art high security data centers. Data and eDiscovery processing centers are Safe Harbor-certified, span the globe, and are audited to Statement of Accounting Standard number 70 (SAS 70 Type II). The data centers are under 24/7 surveillance and protected by biometrically controlled doors, exterior and interior CCTV cameras, glass break and motion detectors, alarm panels, audible alarms, lights, and silent alarms.

Businesses can also choose a hybrid deployment that uses a combination of cloud and on-premise solutions, allocating data to each environment based on policies and company strategy. This greatly benefits organizations that wish to move to the cloud in stages. For example, managing email over six months old in the cloud and keeping new types of application data, such as SharePoint, on premise.

Rapid First Review and Analysis – Maintaining the integrity of data comes into play in an organization's ability to preserve potentially relevant data. Since the threat of litigation is an unavoidable reality for organizations worldwide, the duty to preserve is a requirement that begins when litigation or an investigation is reasonably anticipated. Complying with the duty can minimize the inherent risks of litigation, including the potential for damage to an organization's reputation and finances. Potentially relevant information must also be preserved until a given legal matter or investigation reaches its ultimate resolution. Compounding this challenge, the explosion of electronic data, and amendments to the US Federal Rules of Civil Procedure (FRCP), has introduced aggressive timeframes into the electronic discovery process.

Adding complexity to the ability to preserve information is the intricacy of customer and client communications. These communications have expanded to include new channels such as social networking sites, websites, blogs, email, chat, phone, CRM applications, and collaboration tools, which has amplified the risk of insider theft, fraud, and data loss. The lines between internal and external data are blurring, as more organizations use information from outside the firewall—and outside the enterprise corporate compliance and governance strategies.

Autonomy eDiscovery is specifically designed to assess and analyze data in place, to help organizations determine the probability of litigation. Autonomy eDiscovery provides a rapid first-pass analysis prior to a formal review and production—all while maintaining a defensible audit trail. Rather than the weeks or months required with legacy technology, Autonomy eDiscovery can assess a case within hours of anticipated litigation or investigation, rapidly retrieving and analyzing relevant data to answer the initial question, "Is there a case?"

Controlled Content Retention and Disposition – The ability to manage, control, and discover physical, electronic, and email information assets supports proactive information governance—a requirement in today's ever-changing array of regulatory, legislative, and business requirements. By automating record keeping processes and policy enforcement across all content, organizations can save time and money, while maintaining information integrity and empowering users with faster access to the right information at the right time.

Autonomy Records Management solutions ensure business information is effectively controlled through retention and disposition management policies. Autonomy allows organizations to manage paper and digital records with built-in audit trail capabilities for greater control and visibility into the information lifecycle.

These capabilities enable organizations to ensure the integrity of information by:

- *Guaranteeing chain of custody throughout the complete lifecycle from creation and retention to destruction*
- *Capturing metadata along the chain of custody to provide an audit trail and support verification of authenticity*
- *Automatically classifying information against the records management file plan*
- *Tightly integrating with consolidated archives both on site and hosted*
- *Securely accessing records, while respecting and protecting organizational access rights across all content sources*
- *Ensuring global certification with standards such as US DoD 5015.02 (ch. 2, 3, and 4), UK TNA2002, Australia's VERS*

Intelligent Process Automation – In today's fast-paced business environment, the right set of solutions can make a significant difference by streamlining overall processes, accelerating new business development, and increasing client satisfaction. Autonomy delivers a full featured intelligent process automation engine with rich capabilities for modeling and simulating business processes. Easy to use visual tools, rule-based routing, intelligent electronic forms, real-time business activity monitoring, secure connectivity into other business systems and digital signatures are available across a wide variety of interfaces including the Web, Outlook and Mobile devices.

Unlike other approaches, Autonomy embraces the unstructured and human elements of business processes and turns the variability of information and human behavior into tangible business advantages. Autonomy's fundamentally different approach can use Meaning Based Computing (MBC) to look across all real time business process related data, as well as any other data sources and automatically form an understanding of that information.

For organizations that must adhere to FOIA, Autonomy provides a Workflow Interface that automates the processing of FOIA and Privacy Act requests, including extensive workflows, notifications, tracking, reporting, accounting, and redaction functionality.

GARP® Principle #3 – Protection

Protection	**Level 1 (Sub-Standard)**	**Level 2 (In-Development)**	**Level 3 (Essential)**	**Level 4 (Proactive)**	**Level 5 (Transformational)**
A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.	No consideration is given to record privacy. Records are stored haphazardly, with protection taken by various groups and departments with no centralized access controls. Access controls, if any, are assigned by the author.	Some protection of records is exercised. There is a written policy for records that require a level of protection (e.g., personnel records). However, the policy does not give clear and definitive guidelines for all records in all media types. Guidance for employees is not universal or uniform. Employee training is not formalized. The policy does not address how to exchange these records between employees. Access controls are still implemented by individual record owners.	The organization has a formal written policy for protecting records and centralized access controls. Confidentiality and privacy are well defined. The importance of chain of custody is defined, when appropriate. Training for employees is available. Records and information audits are only conducted in regulated areas of the business. Audits in other areas may be conducted, but are left to the discretion of each function area. The organization has defined specific goals related to record protection.	The organization has implemented systems that provide for the protection of the information. Employee training is formalized and well documented. Auditing of compliance and protection is conducted on a regular basis.	Executives and/or senior management and the board place great value in the protection of information. Audit information is regularly examined and continuous improvement is undertaken. The organization's stated goals related to record protection have been met. Inappropriate or inadvertent information disclosure or loss incidents are rare.

A recordkeeping program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.
Source: ARMA International at http://www.arma.org/garp/index.cfm

The Principle of Protection provides a framework for ensuring that access to certain information is granted only when appropriate, determined by who needs access and under what circumstances. To support these policies, employees are trained regarding the rules that ensure information is protected, and how to remain in compliance with them. To this end, an information governance program must include appropriate protection controls that:

- *Prevent unauthorized access to protect against inadvertent, malicious alteration*
- *Apply protection controls to information from the moment it is created to the moment it undergoes final disposition*
- *Ensure steps are taken to keep the information in a readable format*
- *Apply policy across all enterprise information regardless of location or communication channel to ensure organizations keep all information private and confidential, in line with applicable laws and regulations*

Traditional approaches to policy management often rely on multiple applications that combine unique sets of capabilities to enforce policies; however, coordinating these to create a consistent, corporate-wide policy requires a manual, time-consuming process. This scenario is more difficult as organizations struggle to manage growing data volumes consisting of a wide range of structured and unstructured data.

Autonomy Compliance Solutions provide a range of products and capabilities to help organizations protect information by consistently enforcing policies, in real time, across the enterprise, including the following:

Centralized Policy Enforcement – Autonomy Policy Authority provides meaning-based policy control, enabling centralized information governance and compliance across the enterprise. Built upon Autonomy IDOL's unique ability to understand, analyze, and act on the meaning of information in any file format and language, Policy Authority is the only solution that automatically applies consistent policy for all applications, such as records management and legal hold, as well as content repositories for both structured and unstructured data. With a central meaning-based policy engine, a consistent set of rules is provided to subscribing applications, which automates all steps in the policy control procedure, and elevates the corporate-wide policy above any one application. Autonomy Policy Authority transforms information governance from an inefficient, error-prone process into an automated, defensible operation.

Policy Authority can also ensure consistent, secure access to items, while properly recording all lifecycle events, regardless of whether the asset sits behind a fire wall, is protected by US DoD 5015.02, or is confined by an ethical wall, as is common in law firms.

Monitoring Interactions – The array of communication channels used in business today, if not properly monitored, can create gaps that leave organizations vulnerable to privacy or confidentiality violations. These channels amplify the risk of insider theft, fraud, and data loss by providing easier access to highly sensitive information and data generated outside corporate compliance and governance strategies. Organizations can mitigate this risk, however, using tools that monitor interactions. With Autonomy, organizations can manage supplemental markings, secure individual assets, and manage who accesses what information and when. In addition, Autonomy offers capabilities that facilitate operations that are in compliance with rigorous protection requirements, beyond traditional security measures, such as US DoD 5015.02, UK TNA2002, or Australia's VERS, ISO 15489 to ensure maximum protection of information assets.

Autonomy Interaction Control Element (ICE) simplifies compliance with industry regulations, data privacy laws, and litigation requirements by understanding the meaning of employee interactions with customers, websites, and desktop applications, enabling organizations to effectively monitor and control sensitive corporate and client data inside and outside the firewall. ICE can help enterprise, government, regulatory, and legal organizations ensure that they are operating ethically and responsibly.

ICE provides real-time information security and compliance, protecting sensitive information through data monitoring, masking, muting, triggers, and alerts. Organizations may monitor all channels including customer and client communications occurring via email, chat, phone, CRM applications, and collaboration tools.

Auditing Capabilities – Regular compliance audits of company information are key to information protection. An audit of company information requires adherence to its own policy and close supervision. Autonomy ICE allows organizations to conduct audits in a highly flexible manner either across the organization, by department, or by information repository. Straightforward reports can be produced for management to enable action to be taken quickly and efficiently.

GARP® Principle #4 – Compliance

Compliance	Level 1 (Sub-Standard)	Level 2 (In-Development)	Level 3 (Essential)	Level 4 (Proactive)	Level 5 (Transformational)
The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.	There is no clear definition of the records the organization is obligated to keep. Records and other business documentation are not systematically managed according to records management principles. Various groups of the organization define this to the best of their ability based on their interpretation of rules and regulations. There is no central oversight and no consistently defensible position. There is no defined or understood process for imposing "holds."	The organization has identified the rules and regulations that govern its business and introduced some compliance policies and recordkeeping practices around those policies. Policies are not complete and there is no apparent or well-defined accountability for compliance. There is a hold process, but it is not well-integrated with the organization's information management and discovery processes.	The organization has identified all relevant compliance laws and regulations. Record creation and capture are systematically carried out in accordance with records management principles. The organization has a strong code of business conduct which is integrated into its overall information governance structure and recordkeeping policies. Compliance and the records that demonstrate it are highly valued and measurable. The hold process is integrated into the organization's information management and discovery processes for the "most critical" systems. The organization has defined specific goals related to compliance.	The organization has implemented systems to capture and protect records. Records are linked with the metadata used to demonstrate and measure compliance. Employees are trained appropriately and audits are conducted regularly. Records of the audits and training are available for review. Lack of compliance is remedied through implementation of defined corrective actions. The hold process is well-managed with defined roles and a repeatable process that is integrated into the organization's information management and discovery processes.	The importance of compliance and the role of records and information in it are clearly recognized at the senior management and board levels. Auditing and continuous improvement processes are well-established and monitored by senior management. The roles and processes for information management and discovery are integrated. The organization's stated goals related to compliance have been met. The organization suffers few or no adverse consequences based on information governance and compliance failures.

The recordkeeping program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies. Source: ARMA International at http://www.arma.org/garp/index.cfm

Depending on the industry and/or structure of an organization, there may be any number of regulations and laws to adhere to, from a few dozen to a few thousand. Regulations and laws present incredibly diverse compliance requirements that can be based on numerous factors, including location (e.g. data segregation requirements), type of product or service (e.g. consumer products, wireless services), corporate structure (e.g. public, private, or non-profit), type of organization (e.g. corporate, legal, or government), and internal policies regarding client or patient information. Laws can also impact what employees can do or not do, or how a business conducts itself as it may relate to county, state, or federal requirements.

From a tactical perspective, regulations often impact organizations by directing how information is managed and how policies are enforced using various technology systems. For instance, Sarbanes-Oxley requires US organizations to accept the legal responsibility of creating and applying policies and controls across financial and transactional systems. Following suit, electronic communications and unstructured data are now viewed as traditional documents according to regulations like SEC 17a-4, cases like Zubulake v. UBS Warburg, and the Amended Federal Rules of Civil Procedure. The financial services arena has new requirements for accountability and transparency that come with the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act. In the UK, the Financial Services Authority's COBS 11.8 presents guidelines for the capture and management of recorded communications. Meanwhile, the Foreign Corrupt Practices Act (FCPA) creates compliance challenges for corporations and individuals, and has recently become one of the sharpest instruments in the government's toolbox, with FCPA prosecutions on the upswing. At the same time, information growth continues to explode, as does the diversity of unstructured content such as audio and video, social media interactions, web transactions and instant messages, making it more difficult to remain compliant.

Addressing these challenges, Autonomy's Compliance Solutions deliver the industry's first platform to automate critical management processes by forming a conceptual and contextual understanding of the entire corpus of enterprise information regardless of communication channel or data format—structured or unstructured. Autonomy's unique technology represents a major step forward in reducing the risks inherent in huge content stores and multichannel interactions.

Compliant Communications – Autonomy Supervisor, a core component of the Autonomy Compliance Solution, with the IDOL platform at its core, is able to set and enforce policies based on the meaning of the data, regardless of its format, and govern audio content (including chats, wikis and blogs), and social media interactions. Autonomy's communications and interaction monitoring and policy tools have become the de facto standard among regulated industries, including large Wall Street firms.

Organizations can take advantage of the following key features:

- *Hosted or on-site compliant archiving for regulated content*
- *Real-time policy-based monitoring*
- *Escalation and workflow management*
- *Conceptual search of all indexed content*
- *Advanced analytical options such as clustering and visualization tools*
- *Reporting and trend analysis*
- *Executive web-based dashboards*

Compliance and Risk Practices – Maintaining sound recordkeeping, information management, and legal hold processes requires that adherence to laws and regulations rank in priority alongside other business initiatives, risks, or compliance requirements. Beyond developing, implementing, and training on a records program, processes must be in place to ensure the organization is truly complying with the policies and requirements. This effort can require significant resources, particularly in organizations that try to handle these tasks manually. Autonomy's Meaning Based Governance and Compliance solutions offer unique capabilities to help organizations comply with records requirements by automating processes using technology that understands the meaning of data and interactions and can then act on that understanding. These capabilities distinguish Autonomy in the marketplace and are not available from any other vendor.

Policy Enforcement – Reaching the upper end of the GARP® scale for this principle takes far more than having a policy and retention schedule posted on an intranet. The real leap comes at the point where enterprises implement systems to automate the capture, retention, and disposition of all company information and records.

With Autonomy ControlPoint, records and content are indexed into IDOL, which makes all information visible, transparent, and available to be controlled and governed. This allows organizations to perform a comprehensive search across all information to find out what content sits outside the disposition spectrum and create a policy to manage the information according to regulatory, legal, or corporate mandates. These capabilities enable organizations to discover potentially sensitive information that is not properly governed, or that does not adhere to appropriate security and compliance procedures. With this knowledge, information that increases the risk of non-compliance can be moved to a secure repository or designated for legal hold, should it be subject to a legal matter.

Auditability – Part of the ability to comply with laws, regulations, and policies involve the capacity to audit systems and information across the enterprise. Readily auditable systems allow organizations to validate records program at any time for internal audit or at the request of external authorities or investigators. To greatly simplify the process, Autonomy Supervisor provides a series of customizable, built-in review and escalation workflows to address the best practice needs of a particular organization. A set of message-based tools enables one-step approval or escalation, depending on the appropriate action. All actions create an event that is recorded and fully auditable to demonstrate compliance and proof of supervisory controls. With Autonomy Supervisor and Autonomy ICE, organizations can monitor information for potential violations related to over-retention or inadvertent disposition.

GARP® Principle #5 – Availability

Availability	**Level 1 (Sub-Standard)**	**Level 2 (In-Development)**	**Level 3 (Essential)**	**Level 4 (Proactive)**	**Level 5 (Transformational)**
An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.	Records are not readily available when needed and/or it is unclear who to ask when records need to be produced. It takes time to find the correct version, the signed version, or the final version, if it can be found at all. The records lack finding aides: indices, metadata, and locators. Legal discovery is difficult because it is not clear where information resides or where the final copy of a record is located.	Record retrieval mechanisms have been implemented in certain areas of the organization. In those areas with retrieval mechanisms, it is possible to distinguish between official records, duplicates, and non-record materials. There are some policies on where and how to store official records, but a standard is not imposed across the organization. Legal discovery is complicated and costly due to the inconsistent treatment of information.	There is a standard for where and how official records and information are stored, protected, and made available. Record retrieval mechanisms are consistent and contribute to timely records retrieval. Most of the time, it is easy to determine where to find the authentic and final version of any record. Legal discovery is a welldefined and systematic business process. The organization has defined specific goals related to availability.	There are clearly defined policies regarding storage of records and information. There are clear guidelines and an inventory that identifies and defines the systems and their information assets. Records and information are consistently and readily available when needed. Appropriate systems and controls are in place for legal discovery. Automation is adopted to facilitate the implementation of the hold process.	The senior management and board levels provide support to continually upgrade the processes that affect record availability. There is an organized training and continuous improvement program. The organization's stated goals related to availability have been met. There is a measurable ROI to the business as a result of records availability.

An organization shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
Source: ARMA International at http://www.arma.org/garp/index.cfm

Information availability enables organizations to perform at optimal levels, whether the task involves responding to a FOIA request or conducting an eDiscovery investigation. Records and information must be available in the event of litigation, often within short periods of time. As courts become more technologically savvy, they are less lenient in extending the amount of time allowed to complete discovery. Company records must be readily available to ensure the organization does not incur fines or sanctions.

Consider, for instance, the repercussions that occur when information becomes unavailable: a server goes down, email suddenly goes offline, or information is received in a way that is not understandable by existing systems. Business can come to a grinding halt, contributing to lost opportunity and revenues. Information availability, however, constitutes more than just being able to search and find records. It requires the ability to know what information exists, understand its category and type, and then retrieve the right copy of the document or the right piece of data, in a timely manner regardless of format, location, or language.

Knowing What Exists – At the heart of Autonomy's technology is the Intelligent Data Operating Layer (IDOL). IDOL is the platform for all Autonomy Meaning Based Governance solutions. As the information processing layer, IDOL forms a conceptual and contextual understanding of all information in an enterprise, automatically analyzing any piece of information from over 1,000 different content formats and even people's interests, over 400 repositories, and more than 150 languages. Over 500 operations can be performed on digital content by IDOL, including hyperlinking, agents, summarization, taxonomy generation, clustering, eduction, profiling, alerting and retrieval. IDOL sits above an organization's data to perform keyword and conceptual search, speech analytics, audio and video search, and automated, intelligent categorization. Because Autonomy's unique technology can extract the meaning of all the information used throughout the enterprise and automate the processing and retrieval of it, many manual processes and tasks can be eliminated.

Autonomy's Meaning Based Governance solutions, which operate on the IDOL platform, help organizations know what they have to ensure information assets are easy to find and access when needed. Unlike other solutions that rely solely on metadata or keywords to find information, Autonomy forms an understanding of the full piece of information, which makes Autonomy's Meaning Based Governance solutions truly unique, allowing organizations to ensure information availability in the context of this GARP® Principle.

With Autonomy, organizations can oversee the management of business information to better:

- *Know what information they have*
- *Quickly respond to requests for information*
- *Organize information for efficient access*
- *Ensure that all content is properly secured*
- *Retain and dispose of content, based on defensible policy*
- *Identify unknown areas of potential interest, trends, users, and topics*
- *Control and manage all information, rich media, and interaction methods*

Search – Amassing large amounts of information can be a futile exercise if information assets are not locatable by the individuals that need it to meet business objectives. Built on Autonomy's market leading IDOL platform, Autonomy iManage Universal Search (IUS) delivers advanced enterprise search tailored specifically to meet the needs of knowledge workers. With Universal Search, organizations can efficiently locate relevant information, leverage past work product, understand activity occurring in a legal matter, provide timely and accurate responses to client inquiries, and enable eDiscovery processes. iManage Universal Search takes information availability to the next level by allowing workers to find relevant business concepts, entities, and experts contained in all types of human information, including documents, email, audio and video files, and social media content. Without relying on tags or keywords, Universal Search automatically identifies information and delivers alerts based on news, social media, or industry-specific data sources. Inside the enterprise, Universal Search can search intranets, wikis, SharePoint and applications for specific information and experts working on similar projects. Automatic links, categorization, analytics and visualization tools improve the usefulness of information.

Rich Media Availability – Rich media assets, or audio and video, are the most difficult information types to search and leverage because most systems only allow the metadata attached to the file to be searched. This shortcoming does not provide sufficient insight into the content of the video file. Autonomy Virage Video Search provides powerful next-generation search capabilities over video content (e.g. by channel, program, or time) in order to support reliable, consistent information availability. Users can reach right inside video streams, navigate vast quantities of rich media content, and search by a range of parameters including audio, scene, speaker, location, key frame, on-screen text, face, token, and concept. Autonomy Virage can recognize content at a level of granularity that has been unavailable until now. Viewers can skip to the precise sentence in a televised interview on a particular topic of interest, or select only those scenes within the video stream that are relevant and splice them together to create a new, personalized video. Users can also identify and select only those news stories in a regular bulletin or those scenes in a film that are of real interest, and splice them into a single program.

Audio content provides similar challenges to video, limiting search capability to only the metadata attached to the file. However, to analyze an audio file or audio track of a video, technology must be able to understand the meaning of the interaction, whether live or recorded. This process is affected by a variety of factors, such as the speaker's language, dialect or accent, as well as background noise or interference. Due to the variables in speech and language, legacy approaches like phoneme matching and word-spotting alone are not enough to determine what is truly being said. Autonomy Virage's SoftSound delivers sophisticated audio recognition and analysis technology that processes spoken interactions based on their conceptual content, not just the way they sound.

Autonomy delivers a streamlined, unified process for indexing, understanding, managing and retrieving rich media such as audio and video files to eliminate the need for multiple systems. This capability drastically streamlines content search, identification, preservation and review processes to deliver more complete and relevant results in a shorter amount of time.

Automating the Reduction of Content – Disposing of irrelevant content is vital to ensuring information availability because it controls the volume of content stored. With solid information management practices, organizations can control the growth of information through automatic classification and disposition, which systematically and defensibly removes ROT (Redundant, Outdated and Trivial content). Eliminating extraneous content beyond what the organization must legally keep for compliance purposes streamlines search results and brings back results to users that are more relevant and on point.

GARP® Principle #6 – Retention

Retention	Level 1 (Sub-Standard)	Level 2 (In-Development)	Level 3 (Essential)	Level 4 (Proactive)	Level 5 (Transformational)
An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical equirements.	There is no current documented records retention schedule. Rules and regulations that should define retention are not identified or centralized. Retention guidelines are haphazard at best. In the absence of retention schedules, employees either keep everything or dispose of records based on their own business needs, rather than organizational needs.	A retention schedule is available, but does not encompass all records, did not go through official review, and is not well known around the organization. The retention schedule is not regularly updated or maintained Education and training about the retention policies are not available.	A formal retention schedule that is tied to rules and regulations is consistently applied throughout the organization. The organization's employees are knowledgeable about the retention schedule and they understand their personal responsibilities for records retention. The organization has defined specific goals related to retention.	Employees understand how to classify records appropriately. Retention training is in place. Retention schedules are reviewed on a regular basis, and there is a process to adjust retention schedules as needed. Records retention is a major corporate concern.	Retention is an important item at the senior management and board levels. Retention is looked at holistically and is applied to all information in an organization, not just to official records. The organization's stated goals related to retention have been met. Information is consistently retained for appropriate periods of time.

An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.
Source: ARMA International at http://www.arma.org/garp/index.cfm

All organizations create records, which make up approximately 7 to 9 percent of all enterprise content, as they conduct daily operations. Simultaneously, a wide range of "non-records" exist within most organizations. Non-records, or the other 90+ percent, may include audio recordings captured from a corporate call center, interactions monitored and captured from social networks, most email messages, and data stored in relational databases. Most of this information is unstructured and whether it is a record or a non-record, it all requires consistent management—regardless of format or status.

Critical to a sound information governance program are processes that automate the retention of records and non-records, according to official retention periods. When choosing systems to automate records retention, it is important that the solution can manage information "in place," where it resides in its native repository and format. This eliminates the need for training and complicated hand offs between repositories.

The GARP® Principle of Retention indicates the need for all organizations to have a fully vetted records policy and retention schedule. These policies and schedules must encompass the needs of the business and must specifically reflect the organizational commitment to ensure records required by law or regulation are captured and retained accordingly. This includes an organization's ability to react and comply with litigation, audit, or investigation.

Autonomy provides a number of solutions designed to help organizations oversee the retention and disposition of all types of business information. A few areas include:

Records Management – Autonomy Records Management solutions allow organizations to retain and dispose of records using a single, unified enterprise platform that offers unique analytical capabilities to understand what is contained in the information with real-time policy management and process automation. Information can be managed in place, bypassing the need to copy or transfer data from existing locations. Autonomy also has the ability to access, manage, and process over 1,000 data types including audio and video through pre-packaged, intelligent connectors. Autonomy solutions integrate seamlessly with current systems to eliminate the need to replace existing infrastructure. Additional advantages include the following:

- *A consolidated, enterprise-wide index provides conceptual and keyword search*
- *Automatic classification and clustering creates and extends records management file plans and taxonomies*
- *Simple implementation and execution of retention and disposition schedules*
- *Integrated electronic and physical records management, including warehouse management, barcoding and RFID*
- *Secure lockdown that ensures data is not deleted during retention or while subject to legal hold*
- *Seamless connectivity with on-site and hosted email messaging and content archives*
- *Seamless integration with desktop applications, providing users with automated guidance for content categorization*
- *Military-grade security and certification to US DoD 5015.02 (ch. 2, 3, and 4), UK TNA2002, Australia's VERS, ISO 15489*

Managing Non-Records – When coupled with Autonomy Records Management solutions, Autonomy ControlPoint enables organizations to apply policy controls to non-records while leveraging a unique governance dashboard for complete control and visibility of all enterprise content. Autonomy ControlPoint with Autonomy Records Management solutions provides full document and records management functionality, automating the retention and disposition of information. The combination delivers both records management capabilities and massive scalability to traditional ECM portals and repositories. The functionality to declare records through native application interfaces, access to the Autonomy Records Management solutions file plan via web parts, and integrated searching across multiple repositories allows organizations to fully utilize enterprise-wide information while applying consistent policies regardless of the information source or records status.

Long-term Preservation – Information retained for the long term must have a place within the retention and disposition review cycle to determine if it is still accessible and readable. Critical to proper retention, organizations must establish plans for dealing with longevity, readability, and the aging of business records, regardless of format or difficulty in migration. Autonomy helps companies automate the process of executing review and migration strategies, and provides conversion options to formats such as TIFF or PDFA for long-term preservation.

GARP® Principle #7 – Disposition

Disposition	Level 1 (Sub-Standard)	Level 2 (In-Development)	Level 3 (Essential)	Level 4 (Proactive)	Level 5 (Transformational)
An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.	There is no documentation of the processes, if any, that are used to guide the transfer or disposition of records. The process for suspending disposition in the event of investigation or litigation is non-existent or is inconsistent across the organization.	Preliminary guidelines for disposition are established. There is a realization of the importance of suspending disposition in a consistent manner, repeatable by certain legal groupings. There may or may not be enforcement and auditing of disposition.	Official procedures for records disposition and transfer are developed. Official policy and procedures for suspending disposition have been developed. Although policies and procedures exist, they are not standardized across the organization. Individual departments have devised alternative procedures to suit their particular business needs. The organization has defined specific goals related to disposition.	Disposition procedures are understood by all and are consistently applied across the enterprise. The process for suspending disposition due to legal holds is defined, understood, and used consistently across the organization. Electronic information is expunged, not just deleted, in accordance with retention policies.	The disposition process covers all records and information in all media. Disposition is assisted by technology and is integrated into all applications, data warehouses, and repositories. Disposition processes are consistently applied and effective. Processes for disposition are regularly evaluated and improved. The organization's stated goals related to disposition have been met.

An organization shall provide secure and appropriate disposition for records that are no longer required to be maintained by applicable laws and the organization's policies.
Source: ARMA International at http://www.arma.org/garp/index.cfm

From the smoking gun memos of Enron to potentially risk-laden files kept beyond their destruction date, the secure, appropriate disposition of records and information is critical to comprehensive information governance. In addition to compliance reasons, disposition is important to reducing space requirements, improving operational efficiency, and saving money on equipment supply costs. For reasons like eDiscovery and knowledge management, it is no longer feasible either to keep all information or delete it without following appropriate disposition rules. The management of information must be carried out according to applicable laws and organizational policies that treat information as a valuable corporate asset.

Autonomy Records Management solutions, Autonomy ControlPoint, and Autonomy Consolidated Archive help organizations manage the disposition process based on policies and regulations. These solutions eliminate the inertia by automating these processes to ensure they do not go unaddressed or be viewed as too difficult to achieve. With Autonomy, information can be understood and quickly categorized by content and action taken against it for disposal purposes. Disposal can be scheduled to occur automatically, or records administrators can be prompted when a disposal is necessary. Rules can be applied by function, document type, repository, and a host of additional variables. ControlPoint provides a flexible set of capabilities for applying policy that can realize true savings in storage costs while mitigating the risk of disposing information that is no longer needed.

The same systems and processes used in records disposition are also leveraged in similar scenarios, such as transferring content to archives, moving records with an attorney who has left the firm, asset divestitures, or migrating information due to a merger or acquisition. These capabilities enable organizations to safely transfer records with metadata and file plan information to another custodian, such as NARA, as required by the DoD 5015.02 standard, but yet still guarantee that everything was transferred. Metadata should be maintained to provide provenance of custody, proof of transfer and an audit trial for compliance.

Autonomy Record Management solutions also allow organizations to automate the disposition processing workflow to meet the business process requirements of the organization through: codification of the organization's file plan, inheritance of retention rules upon record creation, and email notification to responsible parties of links to online reports detailing records due for disposition processing, among other capabilities.

Autonomy eDiscovery is the only processing solution to help organizations meet disposition obligations over all forms of content, including audio, video, and social media. Solutions that cannot understand the entire corpus of information in an enterprise is at a severe disadvantage when information must be reviewed quickly and comprehensively. With Autonomy eDiscovery, users are able to cull data sets to the most relevant files and discard those that are not relevant with unprecedented speed and accuracy using IDOL's ability to automatically group data with similar conceptual meaning.

GARP® Principle #8 – Transparency

Transparency	**Level 1 (Sub-Standard)**	**Level 2 (In-Development)**	**Level 3 (Essential)**	**Level 4 (Proactive)**	**Level 5 (Transformational)**
The processes and activities of an organization's recordkeeping program are documented in a manner that is open and verifiable and is available to all personnel and appropriate interested parties.	It is difficult to obtain information about the organization or its records in a timely fashion. No clear documentation is readily available. There is no emphasis on transparency. Public requests for information, discovery for litigation, regulatory responses, or other requests (e.g., from potential business partners, investors, or buyers) cannot be readily accommodated. The organization has not established controls to ensure the consistency of information disclosure. Business processes are not well defined.	The organization realizes that some degree of transparency is important in its recordkeeping for business or regulatory needs. Although a limited amount of transparency exists in areas where regulations demand transparency, there is no systematic or organizationwide drive to transparency.	Transparency in recordkeeping is taken seriously and information is readily and systematically available when needed. There is a written policy regarding transparency. Employees are educated on the importance of transparency and the specifics of the organization's commitment to transparency. The organization has defined specific goals related to transparency.	Transparency is an essential part of the corporate culture and is emphasized in training. The organization monitors compliance on a regular basis.	The organization's senior management considers transparency as a key component of information governance. The organization's stated goals related to transparency have been met. The organization has implemented a continuous improvement process to ensure transparency is maintained over time. Software tools that are in place assist in transparency. Requestors, courts, and other legitimately interested parties are consistently satisfied with the transparency of the processes and the response.

The processes and activities of an organization's recordkeeping program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.
Source: ARMA International at http://www.arma.org/garp/index.cfm

Creating a culture of transparency within an organization can help drive information governance best practices such as proactive compliance and appropriate information access. Similar to the principle of integrity, transparency implies that organizational policies are clearly documented and that users are aware of the rules and processes that must be followed, eliminating guesswork in the areas of compliance.

Centralized Policy Administration – Autonomy Policy Authority provides a wide array of tools to support this Principle by enabling a transparent look into the information policies of an organization. With Autonomy Policy Authority, organizations can automate the process of applying consistent policy across all applications, such as records management and legal hold, and content repositories for both structured and unstructured data. By creating a central meaning-based policy engine, many of the manual processes previously used to administer policy control are eliminated. The ability to automate all the steps in the policy control procedure elevates the corporate-wide policy above any one application.

Transparency across Paper Information Assets – To ensure that all information, including paper records, is managed alongside digital content, Autonomy LiquidOffice can be leveraged to increase access and streamline workflows, for example in support of a FOIA request. The ability to monitor workflow activity supports transparency by providing visibility into processes and, when necessary, notifying risk managers of non-compliance and automating corrective action and responses. Transparency is further supported by the organization's ability to rely on a secure audit trail that automatically tracks approvals, reviews, edits and business activity at every step of a process.

Increasing Transparency in eDiscovery – Autonomy eDiscovery supports transparency by turning an enterprise full of diverse data, in multiple silos and generated by a range of applications, into an open book. When faced with litigation, organizations typically embark upon costly and protracted data collection, processing and filtering before properly assessing the case. Hampered by non-scalable and slow technology, legal teams often have to wait weeks before assessing the data to determine the merits of a case and formulate a strategy, due to systems and processes that cannot "see" into the entire database because it is not transparent. Being able to quickly develop an informed initial case strategy is of critical importance in a world where eDiscovery costs routinely total millions of dollars well before cases even come to trial, making it extremely important to be able to analyze data early in the case so critical strategy decisions can be made. Autonomy solutions enable legal teams to search across all data to determine if there is a case. Autonomy IDOL serves as the platform underpinning all systems to enable complete transparency across all types of records and information regardless of format, source repository, or language.

Conclusion

While establishing compliant information practices can be a challenge, if reasonable expectations are established, the process can be accomplished. The first step begins with a thorough evaluation of current processes, systems, and goals. Based upon that evaluation, organizations can readily map current levels within GARP® to determine the desired performance level. Using the GARP® Maturity Model, organizations can understand what level in the Principle is best suited to meet their specific needs based on the type, size, and regulatory profile of the organization. These critical issues become more import as regulators, stakeholders, shareholders, and customers increase their concern about the business practices of organizations. Using Autonomy Governance and Compliance Solutions, which have the ability to understand the meaning of information for total control and visibility in real time, organizations can quickly optimize their approach to managing to their desired level of GARP®.

About Autonomy

Autonomy Corporation, an HP Company, is a global leader in software that processes human information, or unstructured data, including social media, email, video, audio, text, web pages, and more. Autonomy's technology manages and extracts meaning in real time from all forms of information, both unstructured and structured, enabling companies to leverage their data assets. Autonomy's product portfolio helps power companies through enterprise search analytics, business process management and OEM operations. Autonomy also offers information governance solutions in areas such as eDiscovery, content management and compliance, as well as marketing solutions that help companies grow revenue, such as web content management, online marketing optimization and rich media management.

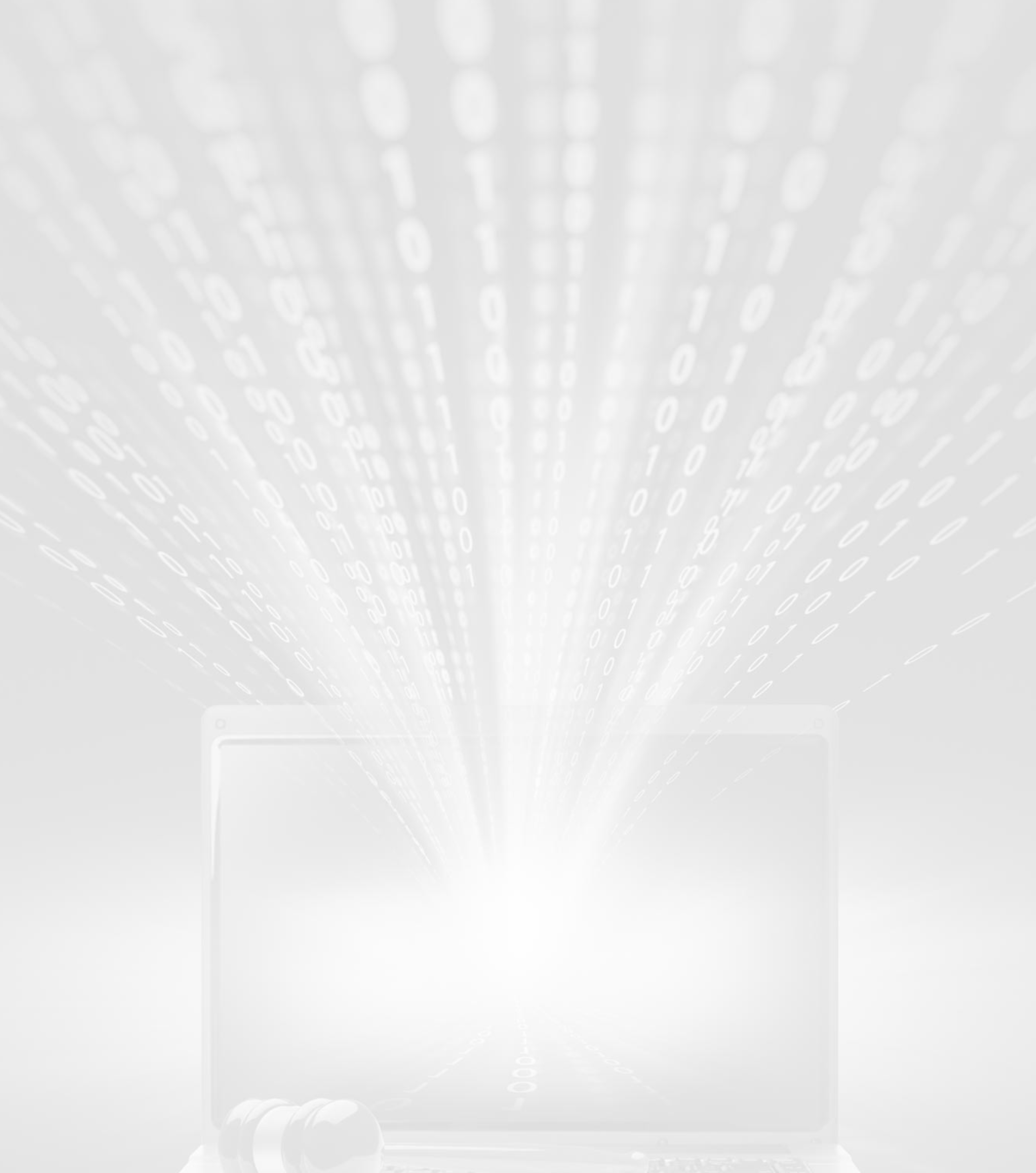
Autonomy's solutions are used by more than 25,000 customers including 87 of the Fortune 100, 10 of the top 10 financial services firms, 75 percent of the global 100 law firms, 9 of the top 10 pharmaceutical companies and many government agencies. Over 400 of the world's leading technology companies embed Autonomy's technology in their products. Autonomy also owns the largest private cloud of diverse data, with over 31 petabytes of information.

Please visit **www.autonomy.com** to find out more.

About ARMA International and the Generally Accepted Recordkeeping Principles®

ARMA International (www.arma.org) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes Information Management magazine, and the Generally Accepted Recordkeeping Principles® (GARP®).

More information about GARP® can be found at **www.arma.org/garp**.



The information contained herein is subject to change without notice. Autonomy shall not be liable for technical or editorial errors or omissions contained herein. All other product and company names may be trademarks or registered trademarks of their respective owners. This document is for informational purposes only. Autonomy is not making warranties, express or implied, in this document.

20120227_RL_WP_GARP_Solution

Autonomy®
an HP company