Elements of Compliance

The Critical Role of Enterprise Content Management in Effective Regulatory Compliance
Governmental regulation is an ever-increasing fact of life in corporate boardrooms, financial institutions, HR departments, healthcare organizations, law enforcement agencies and even other government offices.

Driven by corporate scandals, natural disasters, financial collapse, global unrest, environmental concerns and public demand for information privacy (or in some cases, disclosure), the regulatory pressure on today’s businesses continues to increase.

According to the Economist, the 2009-2010 time period saw the U.S. federal government issuing 132 “economically significant” rules, “40% more than the annual rate” from 1999 to 2008. The publication notes that “Many rules associated with the newly passed health-care and financial-reform laws are still to come” and “Existing rules are also being enforced more keenly.” (“Red Tape Rising,” The Economist, January 20, 2011 print edition)

Forbes magazine notes that the cost per employee to comply with federal regulations (for businesses with fewer than 20 employees) grew at an average annual rate of 6.1% from 2001 to 2008, while inflation averaged only 2.8%. As a result, the per-employee federal compliance cost went from $6,975 to $10,585 per employee. (“Heavy Burden,” Forbes, July 18, 2011 print edition).

To a business community already facing HIPAA, Sarbanes-Oxley and other legislative acts, the reality of ever-increasing government mandates has made the search for cost-effective ways to comply with growing regulatory requirements more urgent than ever.

Elements of Compliance

Regulatory compliance can be viewed as a burden for business, but the use of process and content management technology aids in compliance while offering the potential of increased organizational efficiency and profitability.
Elements of Compliance

When wading through the deep waters of compliance details, it is important to note their common theme: the mandating of effective information management. In fact, all regulations have three key elements, or requirements, in common:

**Data Integrity**
Information must be complete, accurate, and stored with administrative, physical and technical safeguards to ensure it is not inappropriately altered, damaged or deleted.

**Data Confidentiality/Security**
Information must be accessible only to authorized users, protected from inappropriate use or disclosure.

**Data Accessibility**
Information must be accessible to authorized users so they can provide it for any legal purpose, including litigation and audits.

While the various regulations may be aimed at different industries or have different beneficiaries, they all essentially require companies to preserve the integrity and confidentiality of their records and to be able to produce records in an appropriate and timely manner.

What is Records Management?

The phrase Records Management is often interchanged with the term Information Management, but the latter represents a more general and all-encompassing view of managing enterprise information.

Records management, in comparison, is a discipline that focuses on managing business records, often referred to as information assets, for the information’s lifetime. RIM focuses on the value of information that is considered an organizational asset. Such information typically declines in value over time and eventually needs to be retained permanently or discarded. This concept is called Information Lifecycle Management (ILM).

In real-world terms, Records Management is the practice of maintaining the records of an organization from creation to disposition. A record is recorded information — physical or electronic, created or received by an organization — that is useful in the operation of the organization. Such information is managed for the purpose of supporting business initiatives, decision making, reducing operating costs, and risk management. The practice of records management may involve:

- Providing accurate, timely and complete information
- Creating and enforcing records management policies
- Identifying, classifying and storing records
- Managing the information lifecycle: creation or receipt, use and disposition of records
- Creating and executing a records retention and disposition policy and program
- Protecting information, in the event of disaster, for business continuity

These fundamental concepts of records management apply to both physical and electronic information.

Information that is declared as a record is the original or official copy of a record that is retained for legal and regulatory, fiscal, operational or historical purposes. An official copy that will satisfy an organization’s retention requirements for information that exists in multiple copies is also referred to as the record copy.

However, not all organizational information is declared a record or a record copy. Terms such as document or file are often used to identify general business information that does not meet these criteria. A document is recorded information in any format while a file is a group of documents that are related by subject, activity or transaction.

Declared records typically represent only about five to ten percent of an organization’s overall information. However, other types of organizational information that have traditionally been considered temporary or insignificant are increasingly subject to legal scrutiny, as well, and should be managed along with declared records.

In summary, the purpose of a records management program is to manage and protect an organization’s information assets for legal and regulatory, fiscal, operational and historical purposes — whether those assets are official records or more transitory forms of information.
Perceptive Software understands the compliance issues organizations face and offers solutions that they can leverage as part of their overall compliance strategy.

Why Comply?

Penalties of Noncompliance
Some of the common legislative acts that many businesses are currently addressing include: directors can go to prison or be banned, financial institutions can be dropped from stock exchanges, companies can be forced to cease business operations, and steep fines can be levied. For example, HIPAA penalties are up to $250,000 and ten years in prison, while Sarbanes-Oxley penalties can cost up to $5 million or 20 years in prison.

Business Efficiencies through Compliance
Even if your business is not required by law to comply with a specific act, competitors who voluntarily pursue compliance may speed past you as they streamline their operations and reap inherent efficiency benefits. This is because the fully documented processes and transaction audit trails required by compliance efforts can lead to better information management.

Companies who recognize this leverage their compliance efforts to gain efficiencies: to more quickly place critical information in the hands of decision makers, to settle claims faster out of court, to reduce manual paper processing and routing, to eliminate storage issues, to provide users with faster access to key documents (which can lead to better customer service) and so on.

Technology and Compliance
The expense of regulatory compliance is a daunting prospect. According to the Wall Street Journal, Sarbanes-Oxley compliance alone had “cost U.S. industry more than $200 billion by some estimates” by the end of 2008 (http://online.wsj.com/article/SB122990472028925207.html)

Regulatory compliance certainly requires more than just technology. It calls for commitment from management, effective internal communication, ongoing training, the coordinated efforts of individuals throughout an organization and, in some cases, outside consultants and legal counsel.

Yet technology can be a powerful asset in your compliance toolbox. And company policy makers are finding that effectively applied technology can help their organizations both avoid legal penalties and leverage compliance dollars to achieve business efficiencies that will yield a long-term return on investment.

Perceptive Software and Regulatory Compliance
With customers across multiple industries in more than 30 countries worldwide — finance, insurance, healthcare, public sector, higher education and others — Perceptive Software understands the compliance issues organizations face and offers solutions that they can leverage as part of their overall compliance strategy.
Compliance Legislation: An Overview

Some legislative acts that could affect your compliance policies and IT priorities include:

**Electronic Signature in Global and National Commerce Act (ESIGN)**
*Purpose: To facilitate the use of electronic records and signatures in interstate and foreign commerce*
Congress enacted ESIGN to establish the legal validity of electronic records and signatures, thus ensuring the validity and legal effect of contracts entered into electronically. It governs in the absence of a state law or where states have made modifications to UETA that are inconsistent with ESIGN.

**Family Educational Rights and Privacy Act (FERPA)**
*Purpose: To ensure student privacy*
FERPA protects the privacy of student education records, such as grades and behavior, and applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

**FDA 21 CFR Part 11**
*Purpose: To ensure the legitimacy of electronic records and signatures*
Title 21 CFR Part 11 of the Code of Federal Regulations deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures in the United States. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.

**Freedom of Information Act (FOIA)**
*Purpose: To keep citizens informed*
FOIA describes an individual’s rights to access previously unreleased information held by a U.S. Government agency, as well as the agency’s legal authority to refuse access to such information. The Act defines agency records subject to disclosure, outlines mandatory disclosure procedures and grants nine exemptions to the statute.

**Gramm-Leach-Bliley Act (GLBA)**
*Purpose: To ensure financial privacy*
The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. It also requires companies to track and honor consumers’ opt-out requests.

**Health Insurance Portability and Accountability Act (HIPAA)**
*Purpose: To ensure medical privacy*
HIPAA requires standardization of transactions between healthcare providers and payers. It also requires organizations that handle Personal Health Information (PHI) to protect the security and confidentiality of such information. The American Recovery and Reinvestment Act of 2009, sometimes referred to as the “Stimulus Package,” expanded HIPAA compliance to all organizations that work with the healthcare industry as well as increasing fines and punishments for those that do not comply.

**Health Information Technology for Economic and Clinical Health (HITECH) Act**
*Purpose: To improve health care quality, safety, and efficiency*
HITECH provides the U.S. Department of Health and Human Services with the authority to establish programs to improve health care quality, safety and efficiency through the promotion of health information technology (HIT), including electronic health records and private and secure electronic health information exchange.

**Sarbanes-Oxley Act (SOX)**
*Purpose: To protect shareholders and the general public*
In response to corporate financial scandals, the Sarbanes-Oxley Act of 2002 (SOX) mandates corporate responsibility and controls over a company’s information, records and financial reporting. Basic provisions include signed verification of the completeness and accuracy of financial reports, effective internal controls over reporting and information, and “rapid and current” reproduction of information illustrative of material changes in financial condition.

**Section 508 of the Rehabilitation Act**
*Purpose: To improve information technology access to disabled people*
This addition to the Rehabilitation Act requires Federal agencies to give disabled employees and members of the public access to information that is comparable to the access available to others. The law was intended to eliminate barriers in information technology, make available new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals.

**Uniform Electronic Transactions Act (UETA)**
*Purpose: To provide a legal framework for the use of electronic signatures and records*
The Uniform Electronic Transactions Act (UETA) was developed by the National Conference of Commissioners on Uniform State Laws to provide a legal framework for the use of electronic signatures and records in government or business transactions. UETA makes electronic records and signatures as legal as paper and manually signed signatures.
Perceptive Software: Making Compliance Easier Through Enterprise Content Management (ECM)

An essential part of any compliance effort is effective enterprise content management. Without a centralized repository to store the vast amounts of unstructured data generated across an organization, meeting regulatory requirements is virtually impossible.

But compliance laws tend to be technology-neutral, meaning they do not specify how ongoing training data needs to be protected. This places the responsibility on businesses to identify technologies that can support an appropriate compliance solution.

Review the following summary of the common compliance requirements, as listed earlier in this document, along with the suggested capabilities of ECM technologies that can fulfill them.

### 1. Data Integrity

*Information must be complete, accurate, and stored with administrative, physical and technical safeguards to ensure it is not inappropriately altered, damaged or deleted.*

Storing all of an organization’s unstructured information using indexing and tracking features ensures data accuracy. Sophisticated system architecture provides secure storage and supports long-term retention. Version control, retention policy management, physical records tracking, annotation and redaction, and digital signatures all protect the integrity of enterprise content to help fulfill your legal and managerial obligations over long periods.

### 2. Data Confidentiality/Security

*Information must be accessible only to authorized users, protected from inappropriate use or disclosure.*

Authentication and encryption features ensure that authorized persons access only those documents to which they have been given permission. Secure redaction and communications encryption protect sensitive data, while logging and auditing features track critical activities. Records and information management features protect data from improper tampering or destruction when facing audits or legal actions.

### 3. Data Accessibility

*Information must be accessible to authorized users so they can provide it for any legal purpose, including litigation and audits.*

A comprehensive array of search, display, and output capabilities ensures authorized users can access data via a wide range of methods and platforms. An advanced content storage model allows rapid retrieval and easy repository expansion. And retention can be conveniently managed to prevent data destruction, while workflow provides structured accessibility.

Fulfilling the complete scope of these requirements is where Perceptive Software’s process and content management solutions offer value.

Without a centralized repository to store the vast amounts of unstructured data generated across an organization, meeting regulatory requirements is virtually impossible.
Data Integrity

Information must be complete, accurate, and stored with administrative, physical and technical safeguards to ensure it is not inappropriately altered, damaged or deleted.

Completeness: Storage of All Unstructured Data Types
Whether received via scan, fax, e-mail, or import, Perceptive captures and stores virtually any binary file, providing organizations with complete centralization of their unstructured data.

Data Accuracy

- **Accuracy of Indexing**: Perceptive Software’s patented LearnMode integration technology, which can automatically “link” newly capture documents directly to records in your business applications, eliminates the inherent data entry errors caused by manual indexing. Other available indexing methods drive accuracy through options like predefined capture-time variables, OCR and document-based ASCII data extraction, all of which can take advantage of both automated and manual validation processes to help assure index value integrity.

- **Accuracy of Tracking**: The Perceptive system tracks every document it stores, keeping information about capture, the queues the object has been in, user interactions and additional relevant data — all of which can be reported against for auditing purposes.

Secure Storage and Long-Term Retention
Content is stored in Perceptive via Object Storage Manager (OSM) technology, which physically separates the storage of document data from document metadata and allows configuration to accommodate customer-specific needs. In addition to supporting options such as RAID, Server Attached Storage, Storage Area Network (SAN), Network Attached Storage (NAS), optical jukebox, WORM drives and hierarchical storage management (HSM), Perceptive allows the movement of inactive or semi-active files to separate, secure or long-term storage media. Such actions can be taken manually by administrative personnel, or in conjunction with automated records and information management policies per your specific retention requirements.

Version Control and Library Services
Through intuitive version control and library services functionality, Perceptive users can perform a wide range of document tasks that not only streamline collaborative processes, but ensure content integrity throughout editing and approval processes.

- Check in a document to create an original version or update a revised document.
- Check out a document to control the integrity of the document while it’s being edited.
- Promote a previously saved version to the current version, essentially undoing in-between changes while preserving every version.
- Review historical versions and make copies for merging or creating new documents.
- View a read-only version of a checked-out document and mark documents as private.

Records and Information Management (RIM)
Perceptive’s RIM component, Retention Policy Manager (see p. 12), protects data integrity by preserving enterprise content indefinitely or for a specific period of time according to defined retention policies. With appropriate policy design and an activated legal hold in place, no documents can be destroyed, and no document data changed or removed, without deliberate actions by authorized individuals in coordination with overall retention policies, if applicable.

Retention Policy Manager even enables tracking and management, including policies and holds, for physical records.

Annotation and Redaction
Perceptive lets you create custom templates to define user access rules for annotation and redaction actions. By controlling changes that can alter the readability of original documents, this capability continually protects their integrity.
Data Confidentiality / Security

Information must be accessible only to authorized users, protected from inappropriate use or disclosure.

User and Document Privileges

Perceptive was designed with a security model that combines both rigorous authentication and comprehensive user authorization.

First, instead of storing passwords for users, Perceptive relies on external sources within a variety of customer security infrastructures to authenticate user identity. This lets you choose from multiple industry-standard alternatives for authentication, including LDAP integration.

After a user is authenticated, he or she is subject to another critical stage of identity examination: authorization. Authorization determines if the user that passed the authentication process is a registered Perceptive user — someone with a user name identical to that supplied in the authentication process. With authorization, every logged-in user’s assigned privileges are checked, during every session, to comprehensively control user actions and access.

You can assign function and access privileges with detailed control over individual and group rights for each distinct system function, including those that might compromise confidentiality, such as viewing, printing or saving a document. You can even restrict user access to documents and document types based on that user’s role.

So there’s no way around the privileges a user has been assigned. And conflicting privileges based on individual identity and multiple group membership are reconciled according to a hierarchy that allows administrators to review and limit every action a user can take and every document he or she can access.

Comprehensive user and document control ensures that only those who should access specific documents actually can access them. And that translates into the complete document confidentiality that regulatory compliance requires.
Redaction
Perceptive has a comprehensive redaction feature to provide permanent and tamperproof masking of sensitive, confidential or legally significant information — without altering the state of the underlying document.

The real strength of redaction is giving users with appropriate privileges the ability to perform irreversible replacement of readable image information at the image’s smallest meaningful unit — the pixel — with solid areas that cannot be moved, altered or hidden. Visually discernible data simply no longer exists as part of the file structure in redacted areas (except for those with sufficient privileges to access the original), so you can e-mail or export the redacted version without fear of anyone discovering sensitive information. This provides an extraordinary degree of information security and is a significant advance over using annotation tools that create solid masks.

To maximize document security, Perceptive offers flexible classification schemes that grant specific users access to the original document or only redacted copies. Although an individual index value may be changed to identify redacted documents, other index values are preserved, ensuring that application integration based on those values remains unaffected.

Perceptive Workflow leverages the power of redaction by allowing the configuration of workflow queues in which only authorized personnel (such as a security, privacy or information officer) can appropriately redact specific documents before allowing others to access them.

Communications Encryption
Protecting the confidentiality of data in support of regulatory compliance requires more than just securing user privileges and protecting document access — it’s essential to safeguard the links between individual system components, such as a server and connected clients, to keep digital content out of the wrong hands.

Whether adding a scanned item to storage on the server or streaming a requested image to a client, Perceptive offers encrypted communications utilizing the Advanced Encryption Standard (AES-128), the encryption standard approved by the National Security Administration for the transport of “secret” classified information.

AES encryption, provided with FIPS 140-2-compliant cryptographic modules, is also available between Perceptive Server and remote services such as e-mail and fax management running on separate computers, and between Perceptive Server and WebNow application server.

In addition to AES encryption between Perceptive Server and WebNow application server, WebNow supports industry-standard 128-bit SSL/HTTPS for secure communications between the web application server and browser-based users. SSL is also supported for Perceptive Interact products and custom-developed applications connecting via Web services.

And the AES encryption of the authentication handshake between the client and server (full client or web client) can never be disabled. So passwords are never transmitted in clear text.

Common Criteria Certification
Perceptive achieved the Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) at Evaluation Assurance Level 2+ through the National Information Assurance Partnership (NIAP).

The United States and 22 other countries — including Australia, the Czech Republic, India, Japan and the United Kingdom — recognize the Common Criteria as the official third-party evaluation criteria for IT security procedures. NIAP is a U.S. Government initiative between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The CCEVS is a national program for the evaluation of information technology products for conformance to the International Common Criteria for Information Technology Security Evaluation. The program helps consumers select IT products that meet their security requirements and helps the manufacturers of those products gain acceptance in the global marketplace.

Perceptive was submitted to the Common Criteria Testing Laboratory run by the Science Applications International Corporation (SAIC), one of nine NIAP-approved independent testing facilities. SAIC evaluated Perceptive against Common Criteria Evaluation Assurance Level (EAL) Two augmented with Flaw Remediation and Examination of Guidance. Testing confirmed Perceptive met EAL2+ certification requirements including Flaw Remediation and Examination of Guidance.
Reasons to Audit
An effective regulatory compliance policy includes a systematic approach to auditing business processes, including the RIM program, compliance auditing and technology processes. Benefits of regular internal auditing include:

1. It ensures adherence to internal standards and practices.
2. It facilitates compliance with regulations and standards to ensure adherence to required oversight bodies.
3. It improves efficiency thorough the creation of clearly defined business policies and processes.
4. It shows your organization’s dexterity if an externally initiated audit occurs.

Records and Information Management (RIM)
The RIM component of Perceptive Software’s ECM solutions, Retention Policy Manager (see p. 12), supports data confidentiality and security with an integrated and easy-to-use litigation and audit hold capability that prevents the modification or deletion of designated information even if a specified retention period has been met. With a few clicks, relevant documents are instantly locked down for authorized users as audits or legal discovery proceeds.

Auditing
Auditing is an important part of information lifecycle management — and a key component of complying with regulations that require proof of protecting confidential information.

Perceptive’s user identity, document protection and server data security features form a digital shield to keep external threats at a distance. But sometimes user and automated system activities need monitoring, and Perceptive auditing and logging functions are ready to help.

The Perceptive Server Administration console has a GUI interface that allows administrators to configure multiple audit templates to log up to 500 different functions.

Audit log files record each action being tracked (such as viewing, deleting or re-indexing an object) along with a number of details such as the user ID, user name, time and date, duration, status, and audit type.

Client information saved in audit logs includes API versions, IP address, Windows user name, Windows domain, computer name and client type. The resulting reports can assist you in tracking the activities of specific individuals or groups of users and may be helpful for troubleshooting.

In addition, Perceptive supports multiple types of logging, controlled through a combination of client and server settings. Logging can be enabled to record client-side user activity, server-user interaction, server actions and user authentication.

The system can even audit all authentication attempts or only failed authentication attempts, based on settings controlled through the Perceptive Server.
Data Accessibility

Information must be accessible to authorized users so they can provide it for any legal purpose, including litigation and audits.

Search Capabilities
At its most basic level, data accessibility for compliance simply means that those authorized to view specific enterprise content can readily locate what they’re looking for.

Perceptive enables the instant retrieval of documents with a single click from your business applications, and allows manual searching via any combination of index values, custom properties, and words or phrases within a document. Saved queries and predefined “views” further extend the ease and convenience of document search for authorized users.

Display Capabilities
Perceptive lets authorized users view virtually any type of document via a range of clients including standalone applications, web-based clients and third-party applications. This makes documents accessible to authorized users from next door — or around the world.

Cross-Platform Accessibility
Perceptive Software’s Message Agent is a middle tier for the system architecture that uses XML messages to make selected functionality accessible to third-party applications via web services.

Message Agent provides the connecting link for this near-universal accessibility from other applications, as long as they are written in languages that support SOAP and WSDL standards.

Document Storage Model
The hybrid data storage model of Perceptive supports accessibility by maximizing input-output performance and enabling rapid retrieval even for highly scaled content repositories using a variety of storage technologies.

By separating document metadata from the document itself, Perceptive allows each component of application data storage to do what it does best. The structured storage of a relational database is optimized for data, and can swiftly save, search and retrieve document metadata without having to deal with large binary document files that some systems put directly in SQL tables.

At the same time, putting the actual documents on file systems under the control of Perceptive Server means document storage can be expanded simply by adding storage volumes — no need to touch the database or its hardware.

With Perceptive, accessing the documents you need is fast and trouble free — no matter how big your system gets.

Records and Information Management (RIM)
Retention Policy Manager (see p. 12) protects document accessibility by preserving enterprise content indefinitely or for a specific period of time according to defined retention policies. With appropriate policy design and an activated legal hold in place, no documents can be destroyed, and no document data changed or removed, without deliberate actions by authorized individuals in coordination with overall retention policies, if applicable. That prevents the unauthorized or unintentional modification or deletion of information even if a specified retention period has expired.

Workflow Capabilities
Some documents can’t be shared without proper authorization, and Perceptive Workflow can easily be configured to route such documents through a streamlined review process governed by your corporate policies, regulatory requirements, and business rules. When it comes to document accessibility and accountability, workflow provides a way to balance speed of request fulfillment with the need for defined, auditable procedures.

Output Capabilities
Accessibility often means more than simply looking up documents on a computer — It means providing content in multiple forms to fit the needs of those requesting them. With Perceptive, authorized users can easily e-mail, print, or export exact copies of documents — a helpful tool in support of a customer request, audit, or litigation discovery procedure.
Records and Information Management (RIM)

Increasingly, keeping pace with regulatory compliance requires systematically managing, accessing, preserving and even destroying one of your most valuable assets — enterprise information and business content.

Perceptive Records and Information Management products provide an intuitive way to track, audit and access documents and content in the Perceptive system— from creation through final disposition. This enables your organization to automatically manage the complete lifecycle of all information while mitigating legal risks, strengthening compliance initiatives and reducing costs through efficient discovery.

The Retention Policy Manager (RPM) option supports retention-related compliance with features such as:

- Retention Policy Design: Quickly define time- and event-based retention policies that can have multiple phases, enabling you to automatically transfer, retain and destroy all document types according to business requirements and legal standards.
- Litigation and Audit Hold Management: Easily create holds that prevent the modification or deletion of information even if the specified retention period has expired. Simply search for relevant information and apply the hold, ensuring your information is locked down until the hold is lifted.
- Physical Document Tracking: Seamlessly track physical documents by creating a reference in the system, which can be managed with policies and holds. A physical reference is instantly accessible and displays the exact location of the box, folder or document.
- Disposition Approvals: Automatically require a user — or multiple users in a predefined order — to approve a transfer or destruction before it occurs.
- Auditing: Effortlessly generate a certificate of destruction and produce a chain of custody for all information. Detailed audits validate the accuracy of your information at any time.

Perceptive Software: Your Enterprise Compliance Partner

We can’t make regulations go away, but we can help you cope with them.

By centralizing all unstructured data, documents, and corporate records within a unified architecture that ensures data integrity, confidentiality/security, and accessibility, the Perceptive Software enterprise content management system serves as a critical component of overall compliance strategy for hundreds of organizations today.

Built around a secure, high-performance storage model, Perceptive captures and centralizes virtually every type of enterprise content, including e-mail and e-mail attachments, faxes, enterprise reports, scanned paper, imported files and more.

With version control, digital signatures, physical records tracking and the structured accessibility of workflow, Perceptive makes information readily available via a wide range of platforms. With a rigorous user authentication and authorization subsystem, it also keeps data out of the wrong hands, further fortifying the pursuit of full compliance.

Finally, Perceptive puts your content in a framework of retention management, supporting greater control over the access, control, auditing and disposition of corporate information over any time period.

Perceptive Software products make it possible for companies to not just meet regulatory requirements, but to transform compliance-related IT investments into tools for enhanced efficiency and profitability.

About Perceptive Software

Perceptive Software, a Lexmark company (NYSE: LXK), builds a complete family of intelligent capture, content and process management, enterprise search and integration products that connect enterprise applications to the processes and information outside those applications, providing the visibility and control needed to improve financial performance, reduce risk and ensure future flexibility.