



WHITE PAPER

Turn Compliance Pain into Performance Gain

TABLE OF CONTENTS

INTRODUCTION	3
The Compliance Wave.....	4
USA: The Sarbanes-Oxley Act (SOX).....	5
Canada: Ontario Bill 198	5
European Union	6
COMMON COMPLIANCE NEEDS	6
Stakeholders	6
Core Compliance Business Needs	7
BPM	8
Compliance Pain	9
The Cost of Compliance.....	9
Technology and Tools.....	10
Captaris Compliance Offering	11
REFERENCES	11
FOR MORE INFORMATION	11

Introduction

The Sarbanes-Oxley Act (SOX) is just the tip of the compliance iceberg in a sea of governance regulations. The purpose of this white paper is to put SOX in perspective with the broader compliance environment and discuss how executives can leverage their SOX compliance efforts (pain) into opportunities to improve corporate operational performance (gain). These gains can be achieved, for example, through business process management (BPM) that can improve financial performance by gains in effectiveness and efficiencies of the underlying operations processes that drive the financial results. This paper will also identify some common compliance requirements and describe some examples of how the efforts invested in achieving compliance can pay ongoing dividends through applying some of the compliance deliverables to business operations.

THE COMPLIANCE WAVE

Compliance is here to stay, and is "raising the bar" concerning the expectations that not only shareholders have of organizations for reliable financial reporting, but also reflects the growing trend of regulatory bodies demanding transparent, ethical operational management.

Executives are feeling increasing pressure from investors for higher standards of corporate ethical behavior. There are a number of regulatory acts that have been in place for several years but until now perhaps not rigorously enforced. In addition, several acts are just now being activated and are in the process of being implemented worldwide. Table 1 lists some of the key acts and regulations and their country of origin that make up the current and growing regulatory environment.

The following sections will examine key regulatory acts related to financial reporting:

USA - The Sarbanes-Oxley Act (SOX)

Canada - Ontario Bill 198 (Amendments to The Securities Act)

European Union - Proposed auditing rules for European Union corporations

Table 1: Key Compliance Acts

COUNTRY	ACT	DESCRIPTION
USA	Sarbanes-Oxley Act (July 2002)	Financial reporting accountability
USA	SEC Rules 17a-3 & 17a-4	All records related to securities transactions to be maintained for 3 years
USA	Gramm-Leach-Bliley Act	Privacy of financial information
USA	DoD 5015.2	Federal standards of records management
USA	US Patriot Act	Customer documentation requirements
USA	NASD 3010, 3110	Written policies and procedures for review of correspondence with the public
USA	Health Insurance Portability & Accountability Act (HIPAA)	Right to carry insurance between jobs; privacy of patient information
USA	Freedom of Information Act	Access to digital information in government files
USA	FDA CFR21 Part 11	Electronic records for clinical trials
Canada	Bill 198 (Amendments to The Securities Act and Ontario Securities Commission- OSC) (October 1, 2003)	Ontario Securities Commission (OSC) regulations similar to SOX
UK, Australia	PRO	Standards of Records Management
UK, Australia	MoReq/ISO 15489	Standards for electronic records management
Global	Basel II (Basel Committee on Banking Supervision) (By 2006 for most G10 countries) (http://www.bis.org/publ/bcbsca.htm)	Requires increased transparency and governance over capital decisions and management
Global	European Union Audit Rules - Proposed (March 16, 2004) (need to be passed by the European Parliament)	Set up internal audit committee that reports directly to the external auditor.

USA: THE SARBANES-OXLEY ACT (SOX)

The details of the compliance requirements in some cases are still in the process of being fully defined. The main requirements of SOX include the following sections:

Section 404: Annually

- Assessment of internal controls over financial reporting
- Management statement of responsibility for controls
- Management assertion that controls are effective for year-end reporting
- Confirm external auditor has "attested" to the assessment

Section 302: Quarterly

- Management certifications of controls effectiveness
- Disclose control deficiencies and acts of fraud to audit committee and auditors
- Disclose material changes in internal controls

Other

- 401: Disclosure in periodic reports
- 406: Reporting on Code of Ethics for Senior Financial Officers
- 409: Real time reporting of "material events"
- 806: Anonymous "whistle blower" process (internal & external)
- 906: Corporate responsibility for financial reports

Due to the imminent deadlines, and the scope of its impact, SOX is garnering the most current media and corporate attention. Although it has become law in the United States, it will impact organizations around the world. Publicly traded U.S.-based firms will have to comply, but also foreign-based companies with U.S. subsidiaries and foreign companies who are listed on an American stock exchange, or who raise financing in the U.S. will be caught in the SOX net.

The deadlines for initial compliance under section 404 of SOX have recently been extended. Companies with capitalization over \$75M now must report for their fiscal year ending after November 15, 2004; the deadline was extended from June 15, 2004. Foreign and smaller capitalization companies have until July 15, 2005—an extension from April 1, 2005. These changes will be helpful to firms whose year-end occurs within these extension periods; however, firms with a December 31, 2004 year-end did not receive a deadline extension.

Because SOX compliance will be viewed as a standard of financial governance and operational transparency, it will become a pre-requisite for business relations and "financial transparency" could become a competitive differentiator for conducting business in the same way that ISO (International Organization for Standardization) standards represents a level of operational quality. Consider an example where two foreign firms are bidding on a supply contract to a U.S. company. One is fully compliant under SOX. The second has some "SOX qualifications" attached to its financial reporting. The question of "unqualified SOX compliancy" could well become a deciding factor. SOX compliancy could become one of the pre-qualification criteria for business-to-business contracts.

CANADA: ONTARIO BILL 198

The compliance environment in Canada is somewhat different than in the United States, but will be no less stringent. One of the key differences is that Canada does not have a federal regulator analogous to the SEC, although there have been calls for such a national body⁽¹⁾. Instead securities regulation is currently a provincial jurisdiction, which at present introduces some inconsistencies in "regulatory rigor" across the country. British Columbia, Alberta, Saskatchewan, Manitoba, Quebec and Nova Scotia have securities legislation that provides for administrative fines—Ontario has introduced legislation granting this power to the Ontario Securities Commission (OSC). All Provinces except British Columbia are supporting the new compliance legislation being introduced by the Ontario government in the form of Bill 198, which will make amendments to The Securities Act in Ontario, to empower the OSC with some new mandates and enforcement measures.

The Canadian compliance requirements will be largely defined by Ontario's Bill 198 to amend The Securities Act, which strengthens the power and the enforcement options of the Ontario Securities Commission, which oversees the Toronto Stock Exchange (TSX). Bill 198 introduced the following excerpted provisions which were put into force as of April 2004:

- 200(1) "Defining auditing standards for attesting to and reporting on a reporting issuer's internal controls..."
- 200(3) "Requiring reporting issuers to appoint audit committees and prescribing requirements relating to the functioning of audit committees..."
- "Requiring reporting issuers to devise and maintain a system of internal controls related to the effectiveness and efficiency of the operations, including financial reporting and asset control..."
- "Requiring reporting issuers to devise and maintain disclosure controls and procedures sufficient to provide reasonable assurances that..."
- "Requiring chief executive officers and chief financial officers of reporting issuers, or persons performing similar functions, to provide certification that addresses the reporting issuer's internal controls, including a certification that addresses,
 - i. the establishment and maintenance of the internal controls
 - ii. the design of internal controls
 - iii. the evaluation of the effectiveness of the internal controls"

The new draft rules prepared by the Toronto Stock Exchange (TSX) support the requirement that financial statements be audited by a firm that is in good standing with the CPAB (Canadian Public Accountability Board). The Canadian federal government is considering changes to the Canada Business Corporations Act (CBCA) that will mandate the composition and roles of Boards of Directors and Audit Committees, and require management certification of financial reports. To allay corporate concerns of adding duplicative regulation, the Canadian government has indicated their intention to recognize compliance with the new OSC rules as deemed compliance with the CBCA provisions.

EUROPEAN UNION

The European Union has proposed some new audit rules designed to address issues similar to SOX as summarized in a recent Gartner Group First Take⁽²⁾:

"On 16 March 2004, the European Commission published a proposed directive on auditing rules for corporations within the European Union (EU). The proposal, which must be approved by the European Parliament and the Council of Ministers, is aimed at ensuring that shareholders can rely on the accuracy of audited corporate accounts. It is part of a larger plan for reforming corporate governance and contains some provisions similar to those of the U.S. Sarbanes-Oxley Act, which regulates financial reporting and external audits of U.S. corporations' accounts."

Common Compliance Needs

STAKEHOLDERS

Compliance with these myriad of acts will require major changes to policies, organizational roles and responsibilities, business processes, information management and IT systems. The business needs emanate from a broad range of stakeholders in the compliance process; for example, SOX compliance involves the following group of players and roles:

- **Board of directors** oversight role for compliance and corporate governance
- **External auditors** audit the internal controls assessment and attest to the CEO and CFO assertions that effective controls for financial reporting are in place and functioning
- **External consultants** assist in defining risks and controls and their effectiveness
- **Internal audit committee** review the compliance program and deliverables
- **CEO and CFO** assert that internal controls are in place; certify financial statements
- **CIO** provide IT systems to support the compliance work
- **COO** minimize the impact of the compliance effort on day-to-day operations
- **Compliance project manager** manage the scope/schedule/budget aspects of the SOX compliance life cycle, not only with an annual assessment but ongoing quarterly evaluations

- **Financial account/Process owners** define accounts/business processes and risks
- **Knowledge workers/Control testers** front-line workers that test internal controls
- **Control evaluators** evaluate the effectiveness of internal controls

CORE COMPLIANCE BUSINESS NEEDS

Although each regulatory act will have its own specific requirements, there are some core high level business needs that will be common to effectively responding to the compliance requirements as shown in Figure 1.

Figure 1: Core Compliance Business Needs



Communication and Collaboration (C&C) Most organizations rely on email as their primary means of written communication and collaboration, supplemented by meetings, and the telephone. Email has become "part-of-the-problem" rather than the solution to effectively communicate across the organization. For example, a document is typically "pushed out" to multiple parties as an attachment to an email with a request to review and comment by a certain date. The result can be a "round robin" of revisions with no one knowing if they have the latest version or with any easy way to view the consolidated comments of all reviewers. This approach is ineffective, frustrating and does not produce reliable, quality responses to achieve compliance.

These C&C issues can be partially addressed by using existing email technology more effectively to help manage automated workflows.

Document Management technology as described below provides the collaboration functionality. However, automating the document creation/review/approval cycle and integrating it with a document management system enables more efficient communication by monitoring when documents are filed and then sending alerts to reviewers. This "system-generated" communication expedites the process and eliminates lag time between tasks. Working with only one document and using the functionality inherent in word processing applications, such as Track Changes, can help achieve effective collaboration.

Document Management Collaborative workspaces established in a document management system can address the issues related to document preparation involving multiple parties. These workspaces have access security, version control and "history" features that focus the communication on one copy of the document with the "check-out" and "check-in" functionality to ensure the latest version is filed in a single location. Establishing a central repository for documentation, structured in a manner that reflects the compliance "deliverables" eliminates the "email push"—users only receive emails with links to information and pull, (check-out) documents from a central repository as they need to in order to provide input and then "check-in" the revised version. Version history functionality provides an audit trail of who made changes to the document.

Records Management The records management requirements for compliance stem from the need for auditors and/or reviewers to be assured that documentation generated during the compliance process is secure, has not been altered and can easily be searched and reviewed as part of their attestation process. This requires that security can be assigned at the document level, not the folder level, and that document and information repositories contain an "audit trail" of how the documentation was developed. This documentation also needs to be searched effectively, and the results of the search presented to the user in a useful manner, preferably through an interface that the user is comfortable using. Regulations also require that documents, emails, and other forms of information be securely stored and retained for several years, and that proper authorizations are obtained before documents are destroyed.

BPM

The above needs can each be met using selected information technology and applications. However, in many cases the applications that address each of these needs may not communicate with each other and the organization is faced with not only an application deployment effort, but also an application integration project. The tight timelines for compliance make any major IT project an unwelcome component of a compliance solution as companies focus on achieving compliance. BPM has been identified as a central component to achieving compliance as evidenced by some of the following quotations from industry analyst groups:

"Compliance will drive key infrastructure decisions as companies strive to enable better decisions by improving business processes and strengthening internal controls."—Gartner Research

"Sarbanes-Oxley compliance calls for BPM."—AMR Research

"Business process management (BPM) and other real-time solutions are the best way to ensure compliance."—SEC attorney Michael T. Cronin

"Without identified and transparent processes, complying with the mandates is impossible..."—AMR Research.

"Deficiencies in ad-hoc process management are causing enterprises to invest heavily in controlling this critical activity."—Gartner Group

"Business process management (BPM) systems can address several issues that will make it easier for organizations to respond effectively to the new compliance requirements and they should be evaluated as one of the critical components of a comprehensive response to the new law."—Microsoft Executive Circle

Terms such as workflow, business process automation (BPA), and BPM are sometimes used interchangeably. Table 2 presents a summary of suggested distinctions between these terms and shows how they connect to form a continuum starting with business process mapping and evolving up to BPM. Two of the major attributes that differentiate these terms are the scope and the metrics that are tracked and reported at each level. In the example shown in Table 2, the "loan application" business process could be mapped down to the task level, then automated using workflow to execute the tasks. If the "approval" and "renewal" workflows are linked together, then the entire business process can be fully automated, thus achieving BPA. If detailed metrics are tracked and reported, such as cycle time and Key Performance Indicators (KPIs), then the benefits of BPM such as business process improvement and optimization can be realized.

Table 2: The BPM Continuum

	SCOPE	METRICS/ CHARACTERISTICS	EXAMPLE
BPM (Business Process Management)	Enterprise-wide business processes	KPIs Operational metrics	Lifecycle management of loans (Application > Renewal > Payoff) Client retention metrics Resources consumed
BPA (Business Process Automation)	Interdepartmental processes Sub-processes Linked workflows	Cycle time	Loan application Loan approval Renewal
Workflow Automation	Apply IT to deploy workflow "Point solution"	BAM (Business Activity Monitoring): monitoring the number of tasks in progress Track scheduling of tasks	Business rules and routing applied to workflow tasks
Task Workflows	Define processes to the task level	Number of tasks Interdependencies	Level three or four process: Loan application
Business Process Maps	Value chain (LOB Line of Business processes) Support processes (IT, HR, Legal, etc.)		Level one Business Process: Manage mortgage loans

COMPLIANCE PAIN

The basic compliance business needs defined above can be translated into more specific "pain" points that many organizations currently feel. These include not only the incremental out-of-pocket costs for compliance consultants and additional auditor fees, but also the indirect costs of diverting key, "value-adding" resources from day-to-day business operations to necessary, but "non-value-adding" activities, associated with compliance. The key corporate compliance pains include:

- Achieving "unqualified" compliance within tight deadlines
- Diverting key value-adding resources to compliance efforts
- Managing internal controls documentation
- Implementing an effective IT infrastructure to support the compliance work
- Maintaining compliance during changes: business and organizational (e.g. acquisitions, divestitures)
- Change management - implementing new controls to address control deficiencies

Table 3 below summarizes the key issues that will be of interest to senior, or C-level, management (CEO, CFO, etc.)

Table 3: C-Level Compliance Pain

PAIN	CEO	CFO	CIO	COO
Multiple/overlapping regulatory requirements (SOX, Bill 198, privacy, Basel II)	X	X		
Achieve "unqualified" compliance, and confidence in "signing off" statements (e.g. SOX)	X	X		
Align compliance work with governance and transparency strategy	X	X		
Minimize diversion of key resources, and overall cost to comply	X	X	X	X
Meet new standards for records and information management and IT system controls			X	
Maximize ROI on existing IT investments, with additions needed to support compliance		X	X	
Minimize deployment and training time of IT system to support compliance work			X	X
Implement new processes and procedures to address deficiencies and be compliant		X	X	X
Leverage compliance efforts into ongoing performance gains	X	X	X	X

THE COST OF COMPLIANCE

Complying with new rules and regulations is a significant additional cost to do business. Even private companies that are, for example, outsourced service providers to public companies, will be required by their clients to demonstrate SOX compliance since these outsourced services are an integral part of the publicly-traded operations. There is a common recognition that the effort to achieve SOX compliance has been significantly underestimated. Surveys by various IT consulting groups have produced estimates of the compliance costs. Perhaps ironically these "net new" operating expenses, may well in-and-of-themselves be a "material event" as defined by Section 409, and may have an effect on the financial performance of most firms. For example:

"Large and midsize enterprises will spend \$2 M through 2005 to become compliant with Sarbanes-Oxley legislation."⁽³⁾

Estimates of the cost of compliance vary depending on the size of the organization. Large companies with revenues in the order of \$5B may spend 0.1 percent of revenue⁽⁴⁾ while the impact on small to medium-sized firms may be proportionately larger, in the range of 0.5-2.0 percent of revenues⁽⁵⁾.

Addressing the U.S. SOX and Canadian compliance requirements will generally be regarded as non-value-adding activities that will consume key resources. However if management adopts a proactive attitude and looks for opportunities to springboard this compliance effort into some short and/or long term improvements in operational efficiency, compliance pains can be turned into performance gains. Some of the management consulting firms are suggesting that their clients use the compliance requirements to drive organizational change and improvement. The opportunity is to leverage, over the long term, the very significant investment in compliance activities such as documenting business processes, identifying and mitigating operational and financial risk areas, and implementing new procedures to ensure controls are consistently effective.

For example, BPM, which noted earlier is considered crucial to achieving compliance, is an emerging approach to improving corporate performance. In the course of assessing internal controls, organizations may need to document or map their key business processes down to the task level in order to identify the risks that may impact their financial statements. Internal controls to mitigate these risks will need to be identified, tested and reported upon. If the business process workflows are mapped using a software tool which enables these workflows to be automated subsequent to the compliance project, then organizations can leverage the compliance work into the first step toward BPM; that is automated workflow.

By mapping, for example, the monthly financial closing process, this may highlight opportunities to automate and shorten the cycle, combine steps and ultimately lead to costs savings. Similar opportunities include applying "value-based management" techniques to identify the "value-drivers" of the business which become the focus of performance improvement efforts. A "value driver" is a key decision point in a business process that has a major influence on the operating results. The decision to grant or reject a loan application based on the applicant's credit assessment impacts the performance of the loan portfolio as reflected in KPIs, such as the Percentage of Loans with Repayment Defaults. Moving then to business process automation and monitoring the metrics for KPIs that are fed into enterprise management will uncover opportunities for operational improvements that ultimately impact financial performance. The following specific areas illustrate opportunities for performance gains:

- **Better financial controls** since this is the basic purpose of The Sarbanes-Oxley Act there will be cases where better control procedures will be identified and implemented.
- **Improved risk management** during the process of mapping business processes there will be situations that highlight operational risk areas that impact financial performance; addressing these can improve the risk/reward profile of a business unit's operations.
- **Productivity improvements** by documenting business processes and procedures (a pre-requisite to identify risk areas), an organization can first benchmark their operations against best practices and implement process improvements, and thereafter implement standard processes and procedures that will yield savings in training, team and inter-unit coordination which should ultimately translate into improved operational and financial performance.
- **Staged implementation of BPM** mapping business processes in increasing layers of granularity to the workflow level (e.g., process/sub-process/activity/workflow) enables an organization to automate these workflows. If these processes are mapped in the same software tool that enables workflow automation, such as Captaris Teemplate for .NET, this is the first step toward linking these workflow models together to achieve BPM.

TECHNOLOGY AND TOOLS

It is unlikely that there will be a single "compliance software product" that will meet all compliance business needs of even one of the regulatory acts, not to mention several simultaneously. Vendors are adapting and enhancing their products to address a portion of the compliance requirements. For example, Records Management and Integrated Document Management vendors are promoting their functionality to address the information and records management needs of compliance. Enterprise Resource Planning suppliers are focusing on the transactional aspects of compliance and building more robust control functionality into their products.

Major vendors such as Microsoft are encouraging current clients to apply the latest releases of their products to address the compliance requirements. For example Microsoft has released the Microsoft Office Solution Accelerator for Sarbanes-Oxley, which uses the latest functionality of Office System 2003, SharePoint and InfoPath to offer a structured platform that can be rapidly deployed and adopted by the organization since it uses familiar interfaces and provides an excellent framework for managing the documentation required to achieve compliance. (See Reference 6 for the link to the Microsoft SOX site).

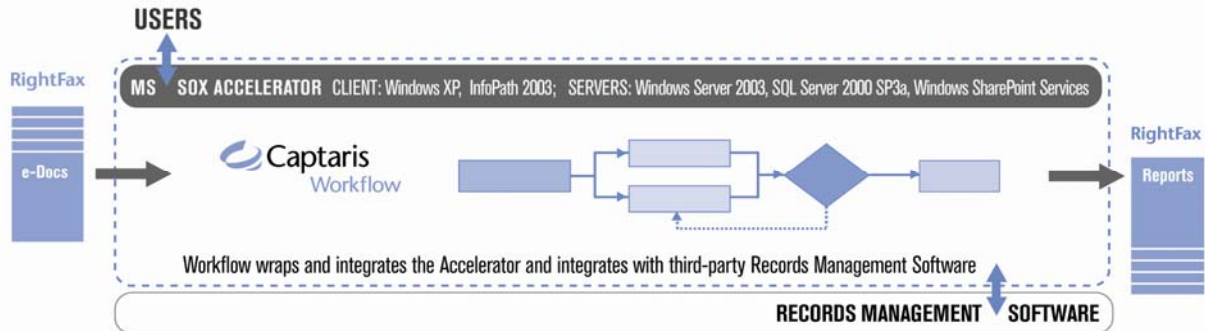
The challenge will be to leverage existing IT systems and augment them with components that can be combined into a system that responds to the specific compliance requirements. SOX requires rigorous documentation, identification of risks and controls, extensive testing, the ability to demonstrate that the internal controls are indeed effective, and to provide external auditors with the required level of detail so they are prepared to attest to the effectiveness of a firm's internal financial control system.

Enterprise Application Integration (EAI) technology and Business To Business (B2B) systems can connect IT business systems, but it is the people-centric business processes that need to be able to operate cross-functionally and utilize information and content from various IT applications. Mapping the business processes is the first step toward BPM and the selection of the mapping tool is important in creating "actionable" processes.

CAPTARIS COMPLIANCE OFFERING

Captaris has taken a more comprehensive approach to meeting compliance requirements. Complying with SOX requires an annual 404 as well as a quarterly 302 evaluation of the financial controls, and these financial controls must become part of the normal operational practices. Captaris has applied its Teemplate for .NET BPM workflow product and in future releases integrate its RightFax enterprise fax and e-document delivery product, to offer a compliance framework built upon the Microsoft Office Solution Accelerator for Sarbanes-Oxley.

Figure 2: Captaris Workflow SOX Accelerator



Captaris has augmented and extended the Microsoft Office Solution Accelerator for Sarbanes-Oxley by integrating proven Teemplate BPM workflows, with the ability to integrate with third party software, and with the RightFax enterprise fax and e-document delivery product to provide a more comprehensive framework that will enable organizations to manage the COSO compliance process more efficiently and effectively, to mitigate risk, and to "operationalize" compliance deliverables to improve ongoing operating performance.

The Captaris Teemplate SOX Accelerator has been designed to not only address the organizational, C-level, and functional business needs described above in this paper, but is also flexible enough to be adaptable to similar compliance requirements, such as Ontario's Bill 198. The solution is built upon Microsoft technology, and is based on the philosophy of looking for ways to leverage the results of the compliance work to improve ongoing operating performance with the theme "**Turn Compliance Pain into Performance Gain.**" The Captaris Teemplate SOX Accelerator can help organizations achieve the operational gains outlined above and realize ongoing value from their compliance efforts.

To learn more about how this solution can address the organizational and executive needs of SOX, and similar regulatory acts, please visit the Captaris Web site at www.captaris.com/SOX.

REFERENCES

1. New push for a single regulator; Globe and Mail, Report on Business, March 29, 2004, p. B1
2. Gartner FirstTake, March 17, 2004 Debra Logan FT-22-4793, "Get Ready For European 'Sarbanes-Oxley' Audit Rules"
3. "Understand how to go about building a strategic compliance platform to help you target spending to meet ever-increasing and shifting regulatory demands." (From Gartner Research, Sponsored by IBM)
4. The Globe and Mail, February 10, 2004
5. Various sources: Captaris, with revenues in the order of \$100M, has a SOX budget that falls in this range
6. <http://www.microsoft.com/office/solutions/accelerators/sarbanes/default.mspx>

FOR MORE INFORMATION

Captaris Business Information Delivery solutions help organizations of all sizes automate the information and document flow throughout the information lifecycle (capture, process, deliver, manage and archive). With a comprehensive suite of software and services, Captaris helps organizations to grow revenues and increase profits while meeting compliance goals. Through a global distribution network of leading enterprise technology partners, Captaris has installed more than 90,000 systems in 95 countries in companies of all sizes, including the entire Fortune 100. For more information, visit www.captaris.com or call 1.800.443.0806.

©2005 Captaris. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Captaris. Captaris products Alchemy, Interchange, RightFax and Captaris Workflow are trademarks of Captaris. All other company, brand and product names are the property and/or trademarks of their respective companies. MC0010122 RB0505