# Updata Market Note: Compliance Shapes Future of IT

**July 2005**

UPDATA CAPITAL

## Inside This Issue



**Updata Capital:**

**Infrastructure Software**

**M&A Leader**

**Selected Updata Deals**



Updata Capital, Inc.

*www.updata.com*

***New Jersey Office:***

125 Half Mile Road
Suite 201
Red Bank, NJ 07701
(732) 945-1000

*********

***Virginia Office:***

11955 Freedom Drive
Suite 7000
Reston, VA 20190
(703) 736-0020

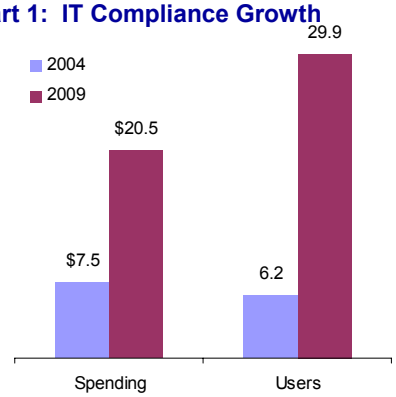

## IT is a Business Matter

Sarbanes-Oxley, "the most sweeping regulatory reform of publicly traded markets since the Exchange Act" (Gartner) aims to curb financial fraud. HIPAA, "the most significant healthcare law since Medicare" (Health & Human Services Dep't) protects patient privacy. These and other information safeguarding mandates (see ***Table I***) have, for the first time, made organizations broadly accountable for IT practices that undermine business operations. This responsibility is forcing major changes in how organizations manage their IT infrastructure, and will hasten evolution and consolidation of enterprise software by dissolving functional silos to support better management.

Beginning last year, compliance has led to readjustment of IT spending priorities. Almost half of businesses recently bought software or upgraded technology associated with compliance (IDC). Over 80% of larger hospitals and 60% of small/mid-sized hospitals are increasing IT security spending in 2005 to comply with HIPAA (Info-Tech Research). Overall, U.S. firms will spend $16 billion on compliance-related activities this year; "Sarbox" alone represents $6 billion (AMR Research). In five years, global IT compliance spending will reach $21 billion, impacting 299 million workers (see ***Chart 1***).

Despite the intense focus on compliance, organizations are only beginning to address the challenge. Only 18% of hospitals/ health systems are compliant with HIPAA security regulations (American Health Information Management Association), and Sarbox audit deficiencies attributable to IT systems are expected to double between 2005 and 2008 (Gartner). This compliance goals-reality gap will take years to close.

### Chart 1: IT Compliance Growth




Source: IDC March 2005; Radicati April 2005.
Spending is in $ billions. Users are in 10's of millions.

## Like Y2K but without an End?

Although hype surrounding compliance has led to comparisons with the Y2K bug, compliance is not a one-time tactical fix but an ongoing management improvement process that enterprises ideally should pursue even without legislative mandates. While expensive, most compliance "fixes" revolve around similar core best practices. Efforts pay off in terms of better IT performance and alignment with business.

### Table I: Major Compliance Legislation Overview

| Sarbanes-Oxley Act of 2002 | Health Insurance Portability and Accountability Act of 1996 | Other Compliance Mandates |
|---|---|---|
| • "Sarbox" makes senior officers of public companies in the U.S. accountable for financial report accuracy and underlying internal controls.<br>• Lack of control over IT processes affects integrity of financial reports. By extension, Sarbox mandates mechanisms to assure data integrity and secure records retention.<br>• The SEC granted firms with a market capitalization <$75 million, and foreign companies, a one-year compliance certification delay, to July 2006. | • HIPAA requires healthcare organizations to take reasonable steps to limit disclosure of personal health information.<br>• Someone must oversee an organization's privacy initiatives, and manage secure access to electronic patient records.<br>• Organizations must show a consistent, widespread set of internal processes to protect data.<br>• The privacy deadline for HIPAA was April 2003; the security deadline is April 2005. | • BASEL II: international banking<br>• FISMA: federal government<br>• Graham Leach Bliley: U.S. banking<br>• Many states and other countries have adopted or are considering privacy and data security-related statues.<br>• Financial and other industries are also in various stages of developing information handling standards. |

## Automation: Key to the Realm

On its face, complying with myriad information safeguarding requirements seems almost impossible, given (1) constant interactions between people and sensitive data in most organizations, with the possibility that even one information-handling lapse may trigger a violation, and (2) the complexity and constant change of IT and business practices. Compliance is in fact only possible where processes are automated and holistic. Otherwise, organizations must restrict information flow or accept non-compliance – neither viable alternatives.

IT services currently represent the largest slice of compliance spending (see ***Chart 2***), and efforts have thus far focused on manual processes such as process documentation and policy development. However, the next wave of compliance investment will emphasize implementation of platform solutions that automate monitoring and auditing, as well as detection and remediation of compliance gaps. IDC predicts such platforms will become widespread as early as 2006. As such solutions require visibility and management of all IT assets across traditional silos like security and storage, they will accelerate pending dissolution of the enterprise stack.

Enterprise software vendors in pursuit of growth and differentiation have already begun offering cross-segment platforms under such banners as Business Technology Optimization (Mercury), Business Service Management (BMC), Enterprise IT Management (CA), Information Integrity (Symantec), and Information Lifecycle Management (EMC). Such vendors are well positioned to leverage their IT infrastructure management capabilities to serve evolving compliance needs.

## IT Sectors Benefiting from Compliance

While compliance expenditures are rising more than 20% annually, IT budgets are only expanding at single-digit rates. This means organizations are giving priority to compliance-related purchases, while all other projects are being back-burnered. This clearly benefits vendors with solutions most directly related to compliance, mostly in Security, Storage and Content management.

Security segments most directly relevant to compliance include:

(1) security event monitoring, which enables centralized IT event data collection and analysis, and real-time vulnerability and threat management;

(2) identity & access management, which audits resource accessing activity, and prevents unauthorized entry to IT resources;

(3) content filtering (Web, e-mail, IM, FTP, etc.), which detects and blocks unauthorized information use;

(4) database security through encryption and activity tracking;

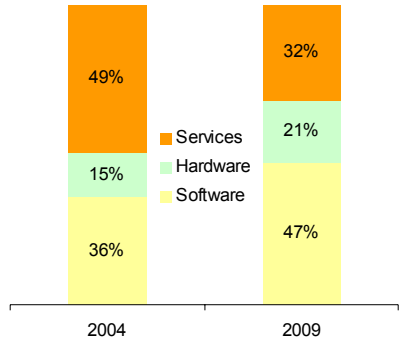
(5) configuration and change management, which although historically not viewed as security-related have become so as they enforce software controls critical to secure processes; and

(6) outsourced security management to simplify operations and offload risk associated with maintaining operations in-house.

In storage, regulation-related segments include electronic message and record archiving, disaster recovery, tiered-storage and, broadly, information life-cycle management.

Content management also stands to benefit, given growing prevalence of unstructured and web content, and the relevance of document tracking and retention.

### Chart 2: IT Compliance Spending by Type




Source: IDC March 2005.

## Placing Compliance in Perspective

Compliance represents one of the most significant trends shaping enterprise IT this decade. It is accelerating evolution toward a more orderly, efficient and secure IT infrastructure that is better aligned with business needs. Compliance – along with open source and outsourcing – is one of several game-changing forces that must be considered by every vendor in developing a growth strategy.

Despite its importance, compliance is not the sole priority of CIOs. Other areas of similar or greater importance in a recent survey (Saugatuck Technology) include cost containment, revenue growth and innovation. And even when met, IT compliance requirements do not address the most common sources of information integrity violations – non-Internet theft, fraud and mismanagement.