



Compliance = ROI

Transforming
regulatory mandates
into business drivers

Executive Summary

From the European Union Directive on Data Protection to Sarbanes-Oxley, technology and business executives are struggling to ensure their IT operations and business processes comply with complex governance mandates.

In fact, 65% of chief information officers (CIOs) expect corporate governance initiatives to be a significant business distraction over the next two years, according to CIO Insight magazine.

In recent years, many companies errantly attempted to address the mandates one by one. But that approach often led to expensive, redundant initiatives that required constant retooling. A far better approach, savvy CIOs have discovered, requires executives to embrace a holistic view of corporate compliance.

Rather than viewing each mandate as a separate, discrete challenge, progressive CIOs are now designing compliance initiatives in an umbrella fashion, essentially using standardised business processes to simultaneously provide blanket coverage that can address multiple mandates.

Such is the case at Computer Associates International Inc., (CA). The Islandia, N.Y.-based company maintains a holistic view of compliance both internally (for its own business operations) and externally (for customers seeking compliance-related solutions that enhance overall business performance, identity management, security, and information storage/retrieval).

The successful holistic strategy has six core requirements:

1. Unwavering executive management commitment
2. Proper business controls
3. Regular audits
4. Extensive training and regular communication
5. Feedback mechanisms that empower employees
6. Effective disciplinary and corrective action plans to resolve compliance shortcomings

While compliance strategies will differ from company to company, successful initiatives share several key themes. First, compliance requires proper financial investment. Fully 51% of U.S. and European multi-national companies will increase compliance spending by an average of 23% during the next 12 to 24 months, according to PricewaterhouseCoopers.

Minding Your Business

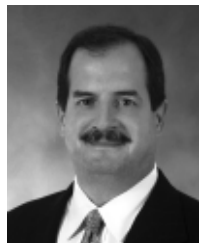
Savvy businesses have hired seasoned executives who are familiar with global compliance regulations. Here's a sampling of the compliance experts at CA.



Name: Robert W. Davis

Title: Executive Vice President, Chief Financial Officer

Background: Formerly vice president of corporate finance and chief accounting officer at Dell Inc. Named CA's chief accounting officer in 2002. Launched his career at Price Waterhouse, starting as a staff accountant and quickly earned senior manager position in the firm's SEC Services Department. Works closely with CEO John Swainson and the executive team to ensure CA's business and IT operations are properly aligned for compliance.



Name: Kevin Kern

Title: Senior Vice President and CIO

Background: Brings international business expertise to the table — a critical requirement for global compliance. Formerly CIO for Compaq Computer EMEA (Europe, Middle East and Africa). Responsible for global IT strategy, development and deployment encompassing data centres, systems and applications, systems security and networking.



Name: Patrick J. Gnazzo

Title: Senior Vice President, Business Practices and Chief Compliance Officer

Background: Works closely with Kenneth V. Handal, executive vice president and general counsel, and to the Compliance Committee of CA's Board of Directors. Responsible for developing and implementing CA's comprehensive compliance and ethics program. Oversees government regulatory compliance and the establishment of a records and information management program. Formerly a member of the board of directors of the Ethics Officers Association and he is a frequent lecturer on ethics and compliance.

Second, compliance affects all types of companies—public, private, large, midsize and small. Privately held start-up companies, for instance, must adhere to generally accepted accounting principles (GAAP) in order to ease possible initial public offerings (IPOs) or to more easily attract potential suitors. Moreover, privately held and non-U.S. companies must often demonstrate compliance in order to do business with large, publicly held companies that want to ensure all of their partners have reliable business operations. Third, compliance requires effective collaboration between an organisation's CEO, CFO, CIO, legal counsel and chief compliance officer, among other executives.

Such communication is critical because the compliance landscape continues to shift. Moreover, executives often receive conflicting advice and direction from one auditor to the next. International mandates involving data retention and business policies often contradict one another. And imminent compliance deadlines tempt organisations to seek shortcuts (such as documenting an antiquated business process) rather than more effective long-term solutions (such as automating such processes).

By embracing a holistic view of compliance, organisations can overcome these challenges and more effectively meet new mandates as they arise.

Getting Started: The CIO Perspective

Time is a precious commodity for John Halamka. As chief information officer for Harvard Medical School, Halamka works overtime to address a range of compliance issues—from ensuring student privacy to safeguarding medical records.

“Focusing on compliance takes more and more of my time,” laments Halamka. “People have to recognise that the answer to compliance isn't a single magical product. It requires a series of processes and solutions, and demands continuous vigilance.”

Plenty of CIOs share Halamka's perspective. Fully 87% of corporate IT departments are formally involved in the process of ongoing regulatory compliance, and 46% of CIOs expect to increase their compliance-oriented IT spending in 2005, according to CIO Insight magazine.

Across the globe, senior IT executives are striving to fulfill dozens of compliance mandates from local, central and international governments. Generally speaking, the mandates strive to ensure customer privacy, data security and information integrity,

Six Steps to Compliance

1. **Lead By example:** Compliance starts at the top. Management must be serious and accountable for compliance
2. **Implement proper Controls:** Embrace proper processes and procedures to safeguard business operations from accidental or premeditated harm.
3. **Audit regularly:** Revisit your controls on a regular basis, and strengthen weak controls as soon as possible.
4. **Train and Communicate regularly:** Tell all employees what's expected of them in regular written and electronic communications, and follow-up with verbal discussions.
5. **Listen to Critics:** Have a process in place that allows employees to raise concerns without fear of retribution. This can include an anonymous tip hotline.
6. **Act Fast and Appropriately:** When compliance issues or problems arise, perform an audit and take disciplinary or corrective action wherever warranted.

while enhancing financial controls and overall business processes.

The road to compliance isn't easy. Many organisations reinvent the wheel as they move from one compliance initiative (for instance, EU Directive on Data Protection) to the next (for instance, Sarbanes-Oxley). Rather than tackling each mandate in a vacuum, savvy organisations take a holistic approach to compliance, embracing a set of processes, software and IT services that are largely applicable to all of today's major mandates (see list of regulations). Many of these progressive organisations are taking six key steps to achieve and maintain regulatory compliance (see chart).

Step 1: Start at the Top

The first step focuses entirely on executive leadership. Without a serious, ongoing commitment from a company's top leadership, compliance initiatives will stumble or fail completely. “Because of executive buy-in, businesses are starting to look at compliance more as a set of ‘best practices’ rather than just ‘legislation’ that they have to comply with,” says Sanjay Anand, author of “The Sarbanes-Oxley Guide for Finance and Information Technology Professionals.” “In other words, we are now embracing compliance as a necessary part of doing business

and keeping the honest person honest. The fear, anger and disregard for compliance-related legislation and initiatives is starting to give way to cooperation, opportunity and respect instead."

Such is the case within CA. "We've got to have buy-in from the board of directors on down," says Robert Davis, Chief Financial Officer of CA in Islandia, N.Y. Adds Patrick Gnazzo, Senior Vice President, Business

Practices and Chief Compliance Officer at CA, "Management has to be serious and accountable about compliance."

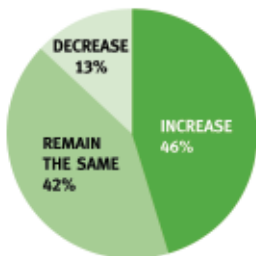
At CA, the company's board includes a Compliance Committee that meets formally at least eight times per year. Since the advent of Sarbanes-Oxley, that committee has been even more active, communicating regularly with CA President and CEO John Swainson; CFO Davis; CCO Gnazzo; Senior Vice President and CIO Kevin Kern; and other stakeholders in the compliance process.

Is your company's IT department formally involved in the process of ongoing regulatory compliance?



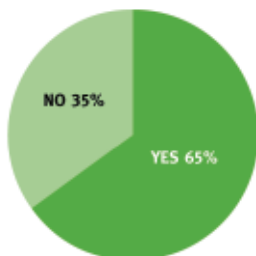
The board also plays a central role in recruiting compliance-savvy executives to CA, and ensuring CA's product portfolio includes compliance-oriented solutions. Prominent recruits include Gnazzo, who joined CA in January 2005 to develop and implement a comprehensive compliance and ethics program. He also oversees government regulatory compliance, and has established a records and information management program at CA.

What will happen to your regulatory compliance spending in 2005?



As a seasoned compliance executive, Gnazzo previously held a similar position at United Technologies Corp., the \$36.7 billion maker of building systems and aerospace products. He also was a member of the board of directors of the Ethics Officers Association (www.eoa.org), a leading organization for a world's foremost compliance experts.

Will the effort to comply with regulations be a significant business distraction of the next two years?



While many companies have taken compliance seriously for the past two or three years, Gnazzo has focused on compliance-oriented issues for more than two decades. In 1986, United Technologies was one of 32 defense contractors that embraced the Defense Industry Initiative on Business Ethics and Conduct (known as DII, www.dii.org). Members embraced and implemented a set of principles of business ethics, in an effort to eliminate alleged business misconduct by some defense contractors.

Gnazzo's experience with DII and United Technologies—which required compliance programs for more than 200,000 employees in 180 countries—bodes well for CA. "Pat is one of the best minds in the industry on compliance," asserts CA CIO Kern.

Think Globally

Rather than tackling compliance on a region-by-region basis, businesses must take a global view of compliance. This endeavor is only possible if the senior executive team has international experience, and is familiar with local customs and regulations around the world.

“Our CEO [Swainson] and I were just in Japan, where they’ve passed some restrictive privacy regulations for consumer information,” says CA CFO Davis. “You’ve got to be aware of these regulations as they cut across various industries and geographies.”

“Human nature doesn’t change much from country to country,” adds CA’s CCO Gnazzo. “The differences from region to region are cultural. To run a compliance program that’s international, you have to recognise culture. In some countries, a \$250 gift for a business partner may be proper and reasonable. In others, it might be against policy.”

Gnazzo also depends on lieutenants around the world to craft localised record retention programs. “We can’t manage corporate records from a U.S.-centric position. We have to ask our people around the world to determine which records are their primary records, and what the laws are for retention.”

CA’s international expertise blankets the company’s business and IT operations. CIO Kern, for instance, was previously CIO for Compaq Computer EMEA (Europe, Middle East, Africa). At the time, Compaq was a \$15 billion entity with complex operations,

recalls Kern. “I had to deal with local applications, data privacy regulations and other international laws that were often more stringent than some U.S. compliance regulations,” he says.

Adds CFO Davis: “In those cases, you’ve got to find the most restrictive regulations and address them, then throttle back from there to address all of the other regulations that apply to your business.”

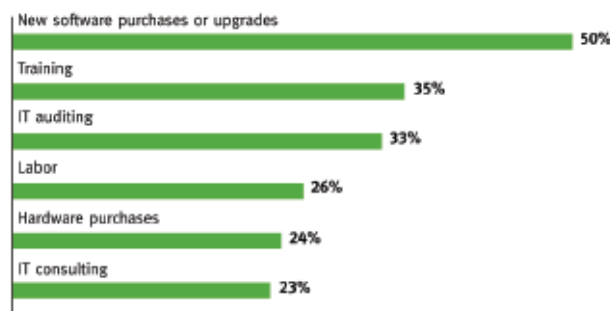
Step 2: Implement Proper Controls

Once a seasoned compliance team is in place, it’s time to document and evaluate all business procedures. During this step, many organisations discover that they have antiquated or manual procedures that don’t comply with modern regulations. For instance, some organisations lack a segregation of duties between sales staffs, financial executives and other departments in the business.

CA leverages its own software as well as SAP AG’s enterprise software platform to ensure proper business controls are in place. Indeed, the company’s Global Computing Controls (GCC) initiative uses BrightStor® solutions for data management, protection and recovery; eTrust™ for access control, auditing and administration; and eTrust™CA-TopSecret® Security to secure its enterprise operating systems and databases.

At first, implementing proper controls can appear to be an overwhelming task. But senior executives can leverage several key standards to get started and simplify the process. For instance, organisations can embrace COBIT (Control Objectives for Information and related Technology), a popular standard from the Information Systems Audit and Control Association and the IT Governance Institute, released in 1996 and updated regularly. According to the institute, COBIT represents a set of generally accepted control objectives for enterprise-wide information systems, including personal computers, minicomputers, mainframes and distributed environments. It is based on the philosophy that IT resources need to be managed by a set of naturally grouped processes in order to provide the pertinent and reliable information an organisation needs to achieve its objectives, according to the institute. Companies in more than 100 countries have implemented COBIT. While COBIT focuses on effective IT governance, the IT Infrastructure Library (ITIL) is a service and process

Which two of the following categories received the most additional compliance-related funding in your 2005 budget?



SOURCE: CIO INSIGHT

management framework, and it is more pragmatic in its approach to IT management than COBIT, is and operates at a level below traditional governance frameworks, according to Forrester Research of Cambridge, Mass.

ITIL consists of a series of books giving guidance on the provision of quality IT services, and on the accommodation and environmental facilities needed to support IT according to the Office of Government Commerce in Norwich, Great Britain.

Another valuable standard for controls is ISO (International Organisation for Standardization) 17799. While COBIT and ITIL reference and expound the need for IT security, they do not give detailed guidance into the practical structure of IT security and controls, according to Forrester. Neither ITIL nor COBIT is specific enough on information security to meet an organisation's needs at this level. This is where

Which of the following software or systems has your company purchased or plan to for regulatory compliance?



SOURCE: CIO INSIGHT, TOP TEN RESPONSES

ISO17799 (BS7799) has seen the broadest adoption. Indeed, it provides a framework around which to build an information security architecture. As with other frameworks, ISO 17799 provides a structure for you to build and map the particular controls in your environment, although it does not automatically “fill in the blanks” during the documentation process, Forrester reports.

In addition to implementing control-oriented standards, corporations continue to invest heavily in

compliance-oriented software and IT services. In fact, 45% of organisations plan to purchase business continuity software this year, followed by e-mail tracking (38%), content management (32%) and financial reporting (29%) software, according to CIO Insight magazine.

CA has also acquired software companies that enhance corporate compliance initiatives. Netegrity Inc., purchased in November 2004, provides CA and its customers with robust identity and access management software. Now part of the eTrust™ Identity and Access Management Suite, Netegrity's software ensures that users can access only the business systems for which they are approved. Another recent acquisition, Niku, develops IT lifecycle management software that gives executives real-time views into their organisations' portfolio of IT investments, enabling them to run IT like a business. CA is integrating Niku's IT management and governance solutions into the CA Business Service Optimisation (BSO) unit. BSO solutions enable organisations to align their IT investments with business objectives, control IT costs, deliver IT as a service, and meet heightened compliance requirements.

Mergers and Compliance

Without proper execution, acquisitions can actually undermine compliance efforts. In fact, several high-profile mergers and acquisitions have collapsed because one—or both—of the companies involved hadn't properly addressed compliance.

When mulling a possible business combination, executives would be wise to follow CA's approach to mergers and acquisitions. CA CIO Kern is “deeply involved” in the early merger discussions. Working closely with Michael J. Christenson, CA's executive vice president of strategy and business development, Kern sizes up the target company, mapping people, processes and technologies to each other. “I certainly have input into whether a merger makes sense from a strategic perspective, and I can also identify any IT-oriented compliance issues we'll need to explore or address.”

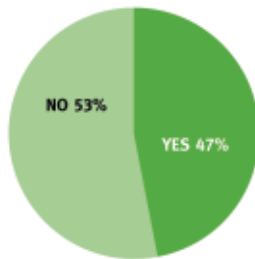
Kern also works closely with CA's development teams to ensure existing and new products meet customers' compliance needs. “Our role goes far beyond providing feedback to the development team,” says Kern. “We have a formal role that includes final signoff on all products and software going out the door. We give feedback on the software's quality, anticipated return on investment and total cost of ownership.”

Step 3: Audit Regularly

Nearly 60% of companies have processes in place to continually monitor the effectiveness of their compliance initiatives, according to CIO Insight, with an additional 30% planning to develop such processes over the next year.

Many CIOs compare today's compliance deadlines to the Year 2000 panic in 1999. Back then, companies were racing to audit billions of lines of code, and

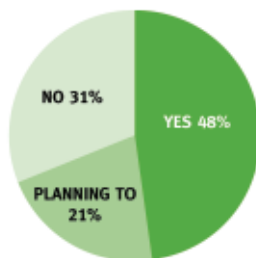
Will your company require its CIO to certify financial results?



Has your company created a process for continually monitoring compliance effectiveness?



Has your company appointed a chief compliance officer or equivalent to oversee compliance activity?



upgrading applications wherever necessary to support four-digit dates (i.e., "2000") rather than two-digit dates (i.e., "00").

Unlike Y2K, today's compliance initiatives require ongoing enforcement and repeated audits. "Most companies are waiting to see how the auditors' opinions stack up and how the market reacts to less-than-clean internal control opinions," says Larry White, chairman of the board of the Institute of Management Accountants (www.imanet.org), which has more than 70,000 members. "Companies are starting to realise [compliance] isn't a major one-time event followed by a dramatic drop off in work. It has a high premium to be paid when trying to sustain compliance. Companies will have to start looking for a way to make the ongoing work more efficient."

Just ask Harvard's Halamka. "Six months ago, we thought we had all the necessary controls in place for our security policies," recalls Halamka. "But the new attacks and latest malware have forced us to modify our policies and build metrics to see if people are using peer-to-peer software and other applications that violate our policies."

Unlike Harvard Medical School's proactive approach to compliance, many organisations tackle compliance issues as they arise. "There is a tendency to respond to the fire and not build efficient sustainable processes," laments White. "Particularly with Sarbanes-Oxley, organisations tend to apply audit logic to controls. But they don't draw on continuous process control techniques established in manufacturing processes to control quality."

Undocumented code changes to legacy applications can also undermine compliance efforts. "In the IT world, you'll find that many of the better programmers and staff members use shortcuts to get their work done on legacy systems," notes Chellappa Kumar, CIO of the New York College of Osteopathic Medicine (NYCOM), the nation's second-largest medical school, located in Old Westbury, N.Y. "These workers would never purposely leak data, but the shortcuts can cause such leaks to happen inadvertently."

Step 4: Spread the Word

Of course, compliance-oriented business controls are worthless without proper communication and user training. "Communicating the vision and adequate training are the two areas where companies are struggling the most with compliance," says compliance expert and best-selling author Anand.

“Despite the appropriate tone from the top and sufficient investments in systems and technology, training employees in the importance of compliance and how to use the tools appropriately is the area where companies lack the most.”

“Training and cultural reorientation are two of the most important keys to successful compliance,” adds NYCOM’s Kumar, who spends roughly 20% of his time focused on compliance-oriented issues. “You’ve got to make sure your staff takes compliance seriously. I often see organisations seeking only a technical solution; they frequently forget that they have to sell employees on the importance of compliance.”

Know Your Options

A sampling of CA’s compliance-oriented IT solutions.

Security Management. CA’s eTrust Compliance Platform is an integrated set of solutions that enables enterprises to significantly simplify and automate their internal IT controls, a major component of a successful regulatory compliance program.

Business Service Optimisation. CA’s Business Service Optimisation solutions support compliance initiatives with the ability to support both Application Controls and IT General Controls. The BSO solutions can enable the automation of IT processes and controls with by the broadest support for ITIL processes (incident, problem, change, configuration and release management).

Enterprise Systems Management. CA’s enterprise management tools can help organisations develop cost-effective, best practice approaches to maximize network and systems availability, ensure business continuity and provide consolidated financial reporting systems that bring together information from multiple sources and systems throughout an organisation.

Storage Management. CA Storage Management solutions enable organisations to maximise the value of their storage investments and accommodate the additional storage requirements to meet government regulations and corporate policies. CA provides integrated storage management and data availability solutions to manage information assets from laptop to mainframe.

At NYCOM, Kumar holds monthly all-hands-on meetings for users. The meetings examine current process issues, and potential technical solutions to the issues at hand. Other organisations have added compliance-oriented materials to their HR handbooks, intranets and monthly e-newsletters to employees.

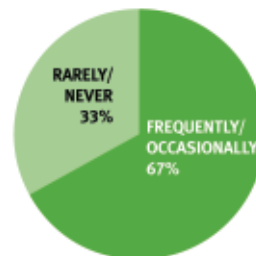
Step 5: Listen to Critics

If a company suffers a compliance setback, employees need communication channels that allow them to raise concerns without fear of retribution. This can include an anonymous tip hotline or anonymous e-mail accounts that empower employees to share their observations. “In addition to ensuring these communication channels are in place, you must also ensure that all of your employees are aware of the channels,” said Ed Golod, president of Revenue Accelerators, an executive strategy consulting firm in New York.

The University of Texas Health Science Center, for instance, has a toll-free number that allows employees to anonymously report suspected violations of federal or state law or university policy. Employees also can use the compliance hotline to ask questions if they are unsure of what to do in a particular situation.

All allegations are relayed to the University of Texas Health Science Center Office of Legal Affairs and Institutional Compliance for investigation. Calls are neither traced nor recorded, and the centre does not have caller ID capabilities. However, anonymous callers are given a case number. They may call the Compliance Hotline back with the case number to receive updates on their call. Employees who call the hotline are protected from retaliation or retribution by

Has often does your CIO meet with your company’s chief counsel to discuss regulatory compliance?



SOURCE: CIO INSIGHT

state and federal law and by university policy.

Similarly, CA has an Ethical Compliance hotline. During the company's Audit Committee meetings, Gnazzo reviews the status of all calls with committee members to ensure all calls have received proper investigation.

Step 6: Act Quickly and Appropriately

When compliance issues or problems arise, companies must perform an audit and take disciplinary or corrective action wherever warranted.

Companies should think about how they will conduct compliance investigations before they are faced with a specific charge or complaint, according to Faegre & Benson, a law firm headquartered in Minneapolis, Minn. A key consideration, the firm says, will be whether to do the investigation internally (and if so, who should do it) or use an outside investigator. The latter may enhance the independence and credibility of the investigation, better facilitate interaction with the company's auditors concerning the scope and findings of the investigation, and make it easier to manage issues relating to attorney-client privilege.

Another key consideration: Ensure that the investigator has prompt access to all relevant documents—which means businesses must have effective data storage and retention systems in place for today's regulations, and tomorrow's potential mandates.

"The number and severity of compliance-related legislations is only going to increase, not decrease," says Anand. "This has to do with the socio-economic evolution of business and society. We will also see the antagonism towards such legislation diminish exponentially in the years to come as we learn to adapt with the new realities of executive power and corporate responsibility. Compliance will continue to seek to keeping the honest person honest, serving the greatest good to the greatest number of constituents and stakeholders."

Concludes CA's CCO, Gnazzo, "Someone has to have umbrella responsibility to ensure there's coordination for existing and new compliance mandates."

At CA and other progressive companies, that umbrella responsibility begins with the board of directors, and encompasses the CEO, CFO, CIO and Chief Compliance Officer. Leveraging such brainpower and the proper IT tools, companies can effectively achieve and maintain compliance.

Worldwide information management for compliance spending by segment (in \$ millions).

	2004	2005	2006	2007	2008	2009	2004–2009 CAGR (%)
Software	2,741	3,839	5,292	6,764	8,219	9,650	28.6
Hardware	1,063	1,483	2,068	2,723	3,498	4,346	32.5
Services	3,719	4,191	4,702	5,269	5,850	6,484	11.8
Total	7,523	9,513	12,062	14,756	17,567	20,480	22.2

SOURCE: IDC, "WORLDWIDE INFORMATION MANAGEMENT FOR COMPLIANCE 2005-2009 FORECAST", IDC #33024, MARCH 2005

