Change Management and Compliance: An Approach to Demonstrating Value and Accountability

A White Paper Prepared for Active Reasoning
July 2005

ENTERPRISE MANAGEMENT ASSOCIATES ™

Change Management and Compliance: An Approach to Demonstrating Value and Accountability

Table of Contents

Shifting Dynamics for Change Management

Change management is not new—corporations have been dealing with change for as long as IT has existed and before. Some may even say that change management has already been addressed. It is true that enterprises have taken steps to develop, refine, and mature processes and procedures to address change management. Yet, the focus on change management today is much different. IT leaders must now concern themselves with continuing internal change management issues, but also take into consideration the multitude of external pressures that have developed in the areas of service management, compliance, and regulatory demands.

Managing IT from a services perspective has been steadily gaining traction in the industry for the past several years. IT executives are making specific service commitments of IT and business services and then measuring performance against those commitments. Since most IT organizations are accustomed to managing by technologies (or silos), this is major change in the management approach of IT professionals. Change management is a key concern since a failure to manage change well will result in a failure to meet service commitments.

Costs and Impacts of Not Managing Change:

- *Inability to rollback failed changes*
- *Dissatisfied customers*
- *Incomplete tracking of costs*
- *Inordinate amount of IT time*
- *Impact on financial filings*

Perhaps the most important drivers for change management today are compliance and IT governance. For those that may be unfamiliar, compliance refers to establishing policies and measures for IT and then adhering to those policies. This is often expressed in the context of security policies. However, compliance can address any type of policy including those that deal with adherence to regulatory requirements. IT governance, on the other hand, is essentially running IT as a business and includes risk management, portfolio management, productivity, and financial results for IT investments. Change management plays a role in compliance and governance from an audit perspective as well as operationally to ensure that all changes meet established policies and the regulations that are being supported by those policies.

Finally, the adoption of process models is also a big factor in change management evolution. Process models are gaining attention as a means to an end for service management, IT governance, and compliance. Process models help IT to define "how it will manage itself as a business" and they can serve as guidance to IT shops that are apprehensive when it comes to unfamiliar pressures. The predominant process model across the globe is the IT Infrastructure Library (ITIL). ITIL originated in the U.K.—defined by the government organization known as the Central Computer and Telecommunications Agency (CCTA). It is a best practices guideline aimed at managing IT from a services standpoint. ITIL consists of many different IT disciplines including service delivery, service support, security, and applications management. ITIL also introduces the notion of a configuration management database (CMDB)—a datastore that is used to track all IT assets, their configurations, and changes.

In the end, there are innumerable reasons for change management to be taking center stage in the market today. Managing change is a critical factor in managing services effectively and ensuring that the IT infrastructure is running smoothly. The dynamics of the regulatory environment and overall need to comply with various corporate policies add to the need for streamlining change management. EMA sees these forces working together to create a dynamic where change management has become critical, if not central, to ensuring that IT priorities and visibility remain stable. This paper will address the compliance side of the change management equation and offer recommendations for steps that can be taken by any organization to achieve effective change management.

Change Management

Change is a constant in any enterprise—application needs evolve, new technology enters the fray, upgrades to existing technology are needed, and users come and go. No enterprise can avoid the ongoing need to address change. Ongoing change has always existed, long before there even was such a thing as technology. Managing change is nothing more than ensuring that the operations of the business are not negatively impacted when the change is made, that the change is made as change was intended and within a reasonable timeframe, and that the change supports the company's business needs and priorities.

The nature of change varies substantially. IT staff may be dealing with a major implementation of an on-line transaction system, or something as simple as adding a component to a business user's PC. Change may also be physical or non-physical. An example of a non-physical change might be an update to a user's access privileges. Regardless of the type of change, the key to managing it successfully can be broken down into a process that consists of the basic elements of documenting the change request and tracking it, assessing its technical and business impact risks, gaining appropriate approval, scheduling the workflow for the change, and reviewing the change tasks. An additional requirement, not often covered by enterprises today, is the need for an audit trail for the change—making sure that you know what the state was prior to the change, details and timing of the change, and then the state following the change.

The reality is that change management is critical to the enterprise and to compliance. Failure to effectively manage change can have far-reaching affects on business stability, customer perceptions, and now, compliance with a company's policies and government regulations. Changes can go wrong and a wise organization will take the time to periodically assess its change management processes and ensure that they meet the demands of the organization.

Regulatory Pressures and Compliance

Compliance and adherence to policies have always existed within the IT organization. With the advent of new federal legislation over the past few years, compliance has taken on a sense of urgency. There are several regulations that impinge on IT, some of which will be discussed in the following paragraphs. All of them have implications for documentation, control measures, policies, and change management.

Sarbanes-Oxley

The Sarbanes-Oxley Act of 2002 (SOX) is on the minds of most IT executives along with the business leaders that are truly being held accountable. This legislation was designed to make the executives of publicly traded companies more responsible for oversight of their companies. At the heart of Sarbanes-Oxley, the goal of policy-makers was to drive the importance of overall stockholder value and its stewardship by the Board of Directors and management team. The SOX mandate was put into place to force public companies to develop better corporate governance controls. It is focused on a system of checks and balances regarding finance and accounting. There are a number of key requirements of SOX that are worthy of note:

- Auditing service restrictions that limit the cross-over business that can be performed by the auditing firm.
- Quicker understanding and reporting of material events as they occur, as opposed to "after-the-fact."
- Certification and auditor attestation on IT controls.
- Provisions for enforcement and criminal penalties.

A Perspective: Key Provisions of Sarbanes-Oxley

- *Financial reports—to be certified by corporate executives.*
- *No personal loans—to executives or Board members.*
- *Public compensation reporting— for the CEO and CFO.*
- *Insider trading controls—earlier reporting and blackout periods that apply to pension funds.*
- *Audit requirements—overing auditor independence, the addition of an internal audit function, and limitations on value-add services that can be provided by the audit firm.*
- *Penalties and consequences—criminal and civil penalties for securities violations including longer jail sentences and larger fines for corporate executives who intentionally misstate financial information.*
- *Annual audit reports—covering the existence and reliability of internal controls as they relate to financial reporting. IT is specifically required to participate in this reporting.*

SOX regulations are extensive. For IT professionals, the pertinent section is 404 – Internal Controls. Section 404 forces corporations to establish and maintain adequate internal controls over financial reporting. On the one-hand, this section is very specific. IT must implement an acceptable framework of documented processes, subject these controls to internal testing and external auditing, and report any material weaknesses in an annual IT status report. On the other hand, the legislation is vague in that guidance is not offered as to what these controls should be or how they should be implemented. IT professionals are generally nervous and at a loss about this, since they have not had to deal with this type of legislation in the past.

Other Regulatory Concerns

Many regulations exist that have implications for IT over and above SOX. These regulations are largely vertical-specific and address the dynamics of the given market. Healthcare and financial institutions may be called out as two that have more regulations than most. Still, virtually all types of industries have their own legal and operational dynamics that impact upon IT compliance.

Healthcare organizations have been dealing with implementation of the Health Insurance Portability and Accountability Act (HIPAA) —legislation that has touched nearly all Americans. The intent of HIPAA is to ensure the privacy of healthcare patients in an electronic age. Compliance with this law touches on electronic healthcare transactions, privacy of individual health information, and security.

The Gramm-Leach-Bliley Act of 1999 was primarily aimed at the handling of financial transactions. It impacts how some financial data is treated for both on-line and traditional transactions. This law specifically limits the disclosure of personal information by financial institutions to third parties. As with HIPAA, privacy policies must be communicated to customers.

Outside of the United States, regulations play a similar role in IT's concerns about compliance. The BASEL II regulations in Europe are equivalent to financial regulations in the U.S. BASEL II addresses disclosure as well as the need for financial institutions to better assess risk in general.

In the end, regulations will continue to evolve and change. They put pressure on IT shops today to operate more like a business, putting policies and procedures in place that enable IT to become more accountable. Doing so will help IT to be prepared for the changing nuances in these regulations.

Still, many IT managers are overwhelmed. Even though many, if not most, large enterprises have already dealt with the initial impact of compliance with these regulations, few companies have developed a sustainable compliance program. The initial phases were so foreign that much has been learned along the way. IT executives are now in a position where they are more interested in refining and filling in details that were missed in the initial projects. Several groups, methodologies, and best practices are available to provide insight despite the fact that they do not specifically address the needs of the regulations. Still, they can serve as a basis for ensuring better processes and thus better compliance.

COSO

The Treadway Commission's Committee of Sponsoring Organizations (COSO), formerly known as the National Commission of Fraudulent Financial Reporting, dates back long before Sarbanes-Oxley. It was established in the 1980s to assess the reasons for fraudulent financial reporting by public corporations—a concern that was beginning to surface nearly two decades ago. COSO is an independent, non-governmental initiative supported by five professional associations focused on accounting and finance. The Commission has been made up of representatives from public accounting, investment firms, and the New York Stock Exchange.

COSO offers guidelines called the "Internal Control – Integrated Framework," which is a standardized description of business controls. The controls address the following objectives: effective and efficient management of operations, accurate financial reporting, and compliance with all applicable laws and regulations. COSO is a very detailed approach for assessing a corporation's control mechanisms. Within each objective, there are breakdowns that evaluate the company's control environment, control activities, risk assessment, monitoring, and communication approaches. COSO can be used as an approach for evaluating weaknesses that must be addressed to comply with SOX directives.

COBIT

While COSO is useful to corporations, it has a financial orientation. Control Objectives for Information Technology (COBIT) is geared specifically towards information technology controls. It was developed by the IT Governance Institute. The COBIT control framework can be used in a way similar to the COSO framework. It was designed in the early 1990s and is now in its third revision. COBIT can be used by executive management as a way to evaluate IT's shortcomings with respect to control mechanisms.

COBIT was written from a business management perspective, which is compatible with today's IT move towards managing IT services according to business needs. The recommendations for controls identified in COBIT are not tied to any particular technology, but rather are general enough to address all IT environments. The recommendations themselves are made up of 34 high-level objectives that are detailed in many more sub-objectives. Both COSO and COBIT offer an approach to understanding current control strengths for any organization willing to invest in evaluating their business and IT practices.

Practical Considerations for IT Compliance and Change Management

Most professionals highly respect the experiences of their peers. There is clearly still apprehension around compliance. To gain access to "real-world" insight, EMA interviewed a number of IT organizations. The purpose of the interviews was to understand where companies are in the process of implementing change management as part of overall compliance and IT governance. After discussing the topic with those individuals, EMA developed the following commentary and guidance.

Control Points for Change Management

Irrespective of the structure in which change management is placed, there are core aspects that need to be defined and considered with respect to change management and related control points that can and should be put in place. This is not to say that all the following control points are necessary in all environments to achieve regulatory compliance, but certainly a large portion of them will exist regardless of company size or vertical market segment or regulations.

- **Requirements for process definition, controls, and documented deficiencies**
  This is the core requirement for any controls. Enterprises must have a basic process for change management defined and documented. It is also helpful to document deficiencies that exist and need to be addressed. During our interviews, EMA found that most users have had a change management process in place to one extent or another. However, this process may not be working for them as well as they would like, may not deal with all types of changes in the organization, or may not have the checks and balances necessary for ongoing SOX compliance.
- **Roles and decision-making processes**
  Is there a clear understanding of the relationships between roles in the management structure? If not, this needs to be documented and communicated across the enterprise. This is fundamental for change management because approvals for varying levels of change are handled according to this structure. In some case, supervisors within business units can be the approving authority. Other times, a cross-section of staff in multiple departments must be consulted to ensure the change is made correctly and implemented without a hitch.
- **Separation of IT from user department functions**
  The separation of decision-making between departments and IT is a control point or check-and-balance system. IT management needs to be clearly separated from business or user departmental functions so that IT does not influence or become influenced by the business function. IT should be a separate service organization providing supporting capabilities to the lines-of-business.
- **Protection of tangible and intangible assets**
  Protection of assets is key in any organization. These assets are not only the tangible capital property of the company, but also the intangible intellectual property or information. Protecting intangible assets is a critical component when it comes to compliance and also the competitive integrity of the business. These issues overlap,

since tangible assets house this sensitive information. This is important for change management in that inappropriately handled changes can place assets and information at risk. When a change is mishandled, access to information and assets may not be available and can present an integrity and competitive challenge for the business.

- **Skill inventories, assessments, training, and regular performance reviews**
  Documentation of the human resources includes an ongoing means for evaluating skills and updating those skills as required to support the business. This, of course, includes periodic performance reviews for individuals within IT. Training must address technology areas, business areas, and approaches to managing processes in support of the business. Staying on top of personnel issues and training ensures that your organization has the expertise required to execute changes in all aspects of its infrastructure.
- **System Documentation**
  Documentation is key for auditing purposes and for reference in planning for important changes. System documentation provides a resource for each technology that is in place and each process that has been implemented. This documentation includes, but is not limited to, manuals, online help files, system flowcharts, and operations manuals.
- **Help desk, effective incident management, and problem resolution**
  For many enterprises, change management processes start with the help desk. Requests for change often begin as trouble tickets in the help desk software. The help desk can request, document, and track the change through its natural workflow. If a help desk is not used, there must still be a system in place to address incidents and problem resolutions when changes are not implemented smoothly.
- **Documented infrastructure requirements including network, storage, systems**
  Requirements and specifications should be documented for all silos of technology. This documentation should detail the use of all components throughout the infrastructure and be easily accessible should the components need to be replaced in the course of any given change.
- **Service quality and service level agreements (SLAs)**
  Service quality and SLAs are a way of committing to a particular level of quality. In the context of change management, service quality becomes important and often a challenge in order to ensure consistency during the course of making and implementing the change.
- **Internet, privacy, and email usage policies and auditable controls**
  Security and usage policies are what many, if not most, people think of when they think about compliance. These policies define all of the sensitive aspects of infrastructure usage ranging from which users can access what systems to what extent sensitive personal information is protected in order to comply with regulations such as HIPAA.
- **Planning and budgetary controls**
  These controls are largely common sense—develop a budget in planning for IT needs and adhere to that budget. This can be tricky when it comes to unexpected changes, but can and should be done thoroughly for known changes.
- **Programming standards, documentation of program steps, and reusability**
  Programming standards and documentation, while often seen as a waste of time or unnecessary restriction, provide greater accuracy and maintainability. Reusable software and searchable software libraries are another way to control change by increasing the reliability of software modules through repeated testing and use.
- **Program change requests and change logs**
  The change control process should include data on change requests and an auditable change log. This step seems to be lacking in many organizations today. Adequate documentation of the before and after states, and the timing and frequency of change means the process is fully auditable, and also provides valuable feedback on the control process.

Common Issues in Change Management

Challenges with change management were consistent across all of the enterprises interviewed by EMA—irrespective of vertical focus. The themes around these challenges were generally related to difficulty handling emergency changes to material systems, unauthorized changes, and problems dealing with security and unauthorized access. We also know that auditors tend to focus on particular areas and are trying to answer the questions; did the work get completed as planned; why was the approved request not completed; and why was there no request for a particular change? The key to meeting many of these challenges is tight control on the change management process. There may be loopholes in approval procedures or in the change management guidelines. Reporting and tracking can also be a limitation due to insufficient automation in change management solutions and a lack of capabilities for tracking change history. Some specific areas to address in managing the change process are:

- **Request management**
  Determine who will initiate the change and how the workflow for the change will be managed. Many companies effectively use their help desk for initiating and tracking changes and this can work well. If not the help desk, then another means for tracing the change through its workflow steps will be needed.

- **Change Approval**
  Change approval is perhaps one of the most difficult aspects of change management. It is important to take the necessary precautions in approving any change, involving the right people, and evaluating implications to the best of your ability. At the same time, you do not want to create too cumbersome a process, too many gates, and involve too many people so that it becomes inefficient and staff is looking for ways to avoid the change process itself.

  Many organizations, including those interviewed for this paper, have established a Change Advisory Board (CAB). The CAB is a cross-section of individuals that meet on a periodic basis, usually weekly, to plan and approve changes that will be needed over the coming week. This works well for important changes. However, in the field, the companies we spoke with suggested multiple gates for change approval. This essentially means that lower thresholds should be established for more routine changes—this would allow, for example, department supervisors to approve smaller changes. The number of gates needed depends upon the nature of the business.

- **Security and Direct Access**
  Security-related issues are the other big problem areas for change management. Unauthorized system and database access are a concern, as well as maintaining the confidentiality of super-user passwords. It is true that employees and their respective roles change frequently, and controlling that appropriate access to all types of systems is difficult. However, the challenges here boil down to diligence on the part of administration.

Common Gaps in SOX Audits

- *Incomplete change control processes*
- *Security administration*
  - *Inadequate controls to delete or change access when an individual leaves or changes job responsibilities (especially contractors)*
  - *Inadequate approval of access changes*
  - *Access levels not regularly reviewed and approved by management*
  - *Lack of appropriate level of security for infrastructure components*
- *Inadequate access privileges*
  - *Privileged access to operating system, database, and application environment where access is unnecessary*
  - *Inadequate segregation of duties and roles*
  - *Production-level access for non-production personnel*
- *IT controls not integrated into key business processes (e.g. SDLC, change control, compliance, testing and data conversion procedures)*
- *Lack of a regular process to assess effectiveness of controls*
- *No long term strategy to evaluate and address risks*

- **Unauthorized and emergency changes**
  Perhaps the stickiest part of change management is determining how you will deal with unauthorized and emergency changes. The problem is two-fold: it is difficult to document a change that has already taken place, and in many organizations staff members are resistant to the change management process itself. One company interviewed by EMA dealt with this challenge in a very heavy-handed way—something it felt was necessary to ensure that all staff members took its policies seriously. This company gives an official warning the first time a change policy is breached and lets the employee go the second time.

  There will always be emergency cases that will require staff to work outside of the formal process to address a problem situation. Similarly, some staff members will decide that the change management process does not apply to them. Considerations here are "how will you document unplanned changes" and "how will you discipline staff for failing to comply with the process?" Most companies that were interviewed felt that the penalty for failing to operate according to the process needs to be relatively severe. Successful solutions involved impacts to the financial reward system for the employee such as bonuses for staff that do comply and/or negative impacts to pay increases and incentives for those who do not.

  Regardless of the consequence, it is important for the change management process to have a continuous evaluation of unauthorized changes and to work towards identification and reduction of these changes. Some companies attempt to handle these changes just prior to an audit. However, it is generally obvious to an auditor that this was the case and that these types of changes are not being managed. A post-mortem report can take the place of a formal approval process for emergency changes.

Final Recommendations for Improving Change Management

The previous sections have outlined several specific ways to implement or improve change management processes for any organization. However, in conclusion a few general comments are also necessary. While most companies have a process for change, they have not evaluated it in the context of today's business and regulatory requirements. As organizations evolve and regulations change, IT must be more proactive in evaluating its existing methodologies, to address accountability for corporate executives and meet the increasing legal provisions.

Defining a change management process needs to be done in the context of regulatory and business process constructs in your enterprise and there really is no right or wrong way to do it. Corporations can look to published guidelines such as ITIL, but in the end, the specific steps involved will relate to a particular organization's needs. Perhaps the most important recommendation to make is that a "closed-loop" process be created with review on a periodic basis. That said, there are some considerations that present common challenges for IT in implementing or modifying the change management process:

- **Identification of all Regulatory Requirements**
  SOX requirements apply across the board to all public companies. Any corporation should start with SOX, but not end there. Depending on the nature of the business, there may be other laws in place that encumber the company to manage its infrastructure in a given way. Develop a strategy that addresses all regulations in a structured way.
- **Understand Key Business Processes**
  Business processes in any company are always in a state of evolution as business goals, staff, and organizational responsibilities change. Additionally, there will be some business processes that need to be modified to accommodate new regulations.
- **Maintain a Sustainable Compliance Framework**
  The compliance framework encompasses business processes, documentation, and audit information that proves your organization is meeting its regulatory obligations. The framework is important because it provides a structure for you to implement actions necessary depending upon your regulatory pressures. It should be evaluated in a continuous improvement mode such that your organization is positioned to comply with current and future regulatory requirements.

- **Evaluation of Change Success**
  Lastly, and often overlooked, is the need to assess the success of the change. This is related to the need for audit records. In order to evaluate the effectiveness of the change, IT must know about the change, when it occurred, and how it was implemented, how often changes occur, and their success or failure rate. The same applies to unauthorized changes. Companies should look to the post-mortem report to understand whether or not the unauthorized change could be avoided and if not, was it properly documented and assessed after-the-fact.
- **Compliance as a Catalyst for IT Operations**
  Compliance does not have to be a four-letter-word. For enterprises that use it effectively, compliance can serve multiple purposes. It can improve core IT competencies in operations overall as well as change management. The benefit here is to increase IT's credibility in the enterprise and improve the cost/benefit of IT investments.

In the future, compliance and change management issues are expected to grow in light of the industry movement toward the implementation of an ITIL-related CMDB. A stronger link must be forged between modeling IT as a service and the IT service model, and change management. IT will need to understand the impact of changes and potential changes as they relate to services. Risk assessment must determine just how any given change might impact critical business services. In addition, change management will need to be closer aligned with costing of IT services. Some companies are already comparing the estimated cost of a change against the cost of failed infrastructure. In the future, the precision and level of detail will increase in this area just as it is increasing for service management in general.

Active Reasoning Technology

Active Reasoning is addressing the issues of compliance and change management together. Active Reasoning's mission is to automate the process of validating and auditing change activities on material financial systems—its solutions are supportive of the control objectives necessary for SOX compliance. Specific solutions include the Compliance Inspector and Compliance Auditor as shown in Figure 1.

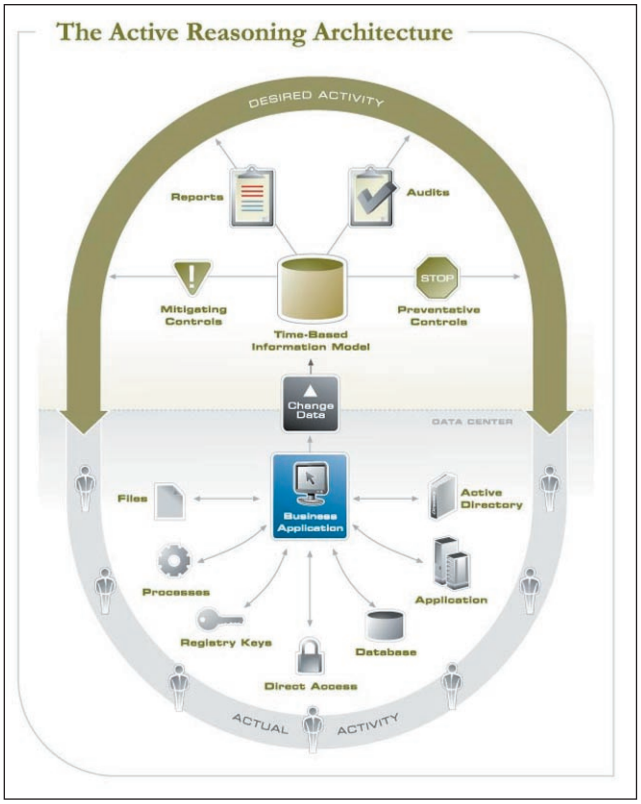

Figure 1: The Active Reasoning Architecture

Active Reasoning's Compliance Inspector solution validates individual activities within the IT infrastructure. Detected changes include file, process, direct access, Active Directory and databases. In most cases, the system can attribute the individual user associated with the change. Based upon reported change activity, users can create customized reports or IT control notifications to prevent inappropriate changes and to alert appropriate staff to take intervening action.

Active Reasoning's Compliance Auditor solution creates a closed loop system where changes of all types can be audited to determine which changes were not authorized by the change approval process. The audit is conducted through integration with change management systems such as Remedy or Peregrine. It picks up where many change management solutions leave off—when the change itself is approved.

For both solutions, Active Reasoning automates the data collection process and requires no changes to operational procedures. In addition, the solutions can enable and report on the policy enforcement required to demonstrate the organization's compliance with regulations, policies, and procedures.

EMA's Perspective

There is a lack of clarity in the technology market when it comes to terms and concepts such as compliance and IT governance. Some IT professionals equate the two terms and others do not. For many, compliance is "complying with whatever regulations are applicable to the business." Compliance is also heavily associated with security policies and there are those that view compliance in this strict sense. EMA, however, views compliance in the more general sense of complying with all legal requirements and security policies imposed upon the business. IT governance has a much broader meaning covering areas of risk management, IT portfolio management, project management, and for some, including compliance with business policies and goals.

Definitions aside, Sarbanes-Oxley and other important legislative efforts will continue to have implications for IT. This legal environment is intimidating for most IT professionals. IT leaders looking to move forward often feel like compliance and IT governance is an elephant and prefer to deal with it a little at a time. Change management represents an area where definite progress can be made towards support of the detailed requirements of SOX and other regulations.

Compliance with SOX requires the implementation of ongoing monitoring and evaluation of Control Objectives—something that Active Reasoning can help IT to achieve. Active Reasoning stands out from the crowd because it is addressing change and compliance management holistically, recognizing that there are existing solutions that deal with the core of change management and adding value by closing the loop and more specifically addressing compliance needs. The one caution for some buyers may be in dealing with an emerging company on an important issue. However, Active Reasoning is very customer-oriented and works to address customer-specific needs by helping to fill the gaps that occur in the change management process. It is by taking this approach that Active Reasoning has ascertained the real requirements for complying with SOX and has added auditing features, automation, and policies that one customer said "act as a gatekeeper for IT."

The real keys for managing change are to have a solid process and tools in place to track that process. It goes beyond the change request and approvals, to ensuring that the change was handled correctly and reporting on "the who" and "the how" of that change. Organizations can begin to document proof of compliance by clearly articulating control measures and then proving that those control measures have been properly followed.

About Active Reasoning

Active Reasoning develops IT compliance software that audits peoples' activities within the enterprise data center. By automating the process of monitoring, validating, and controlling changes to the IT infrastructure, Active Reasoning simplifies ongoing compliance requirements and strengthens IT operations. Fortune 1000 companies across a broad set of industries currently use Active Reasoning software to more effectively meet compliance demands. Active Reasoning is a privately held company, founded in 2002 and headquartered in Palo Alto, Calif. For more information, visit the company's website at www.activereasoning.com or call +1.650.404.9900.

About Enterprise Management Associates, Inc.

Enterprise Management Associates, Inc. is the fastest-growing analyst firm focused on the management software and services market. EMA brings strategic insights to both vendors and IT professionals seeking to leverage areas of growth across e-business, network, systems, and application management. Enterprise Management Associates' vision and insights draw from its ongoing research and the perspectives of an experienced team with diverse, real-world backgrounds in the IT, service provider, ISV, and publishing communities, and is frequently requested to share their observations at management forums worldwide.

Corporate Headquarters:
Enterprise Management Associates
2585 Central Avenue, Suite 100
Boulder, CO 80301, U.S.A.

™
ENTERPRISE MANAGEMENT
ASSOCIATES
Phone: 303.543.9500
Fax: 303.543.7687
info@enterprisemanagement.com
http://www.emausa.com
953.071905