

# SOA Meets Compliance: Compliance Oriented Architecture

---

Stephen O'Grady

**Compliance requirements are increasingly driving business agendas, to the point of dominating many information technology budgets. Businesses of many different shapes and sizes have compliance projects to manage, whether in conformance with specific vertical regulatory issues such as SEC 17a for broker/dealers, horizontal legislation such as Sarbanes Oxley or even internal process frameworks such as Six Sigma and ISO 9000. Leveraging IT to enhance business processes with transactional transparency is a necessary response to corporate governance scandals. Building the "real time enterprise" is fast becoming the preferred method for reducing fraud, and, in more and more cases, it is a mandated one.**

---

"Organizations should deploy a services-based architecture that can deliver compliance specific services as necessary, based on specific acts and regulations."

---

Given the breadth and depth of compliance requirements plus the fact that the regulatory landscape is highly dynamic, it's clear that businesses now require a flexible architecture to keep pace. Leading with siloed applications may be adequate for initial, tactical compliance, but that approach introduces significant complexity and limitations over the longer term. The sheer variety and scope of compliance challenges require that IT organizations address compliance issues at an architectural level, using a fluid, adaptive approach. Organizations should deploy a services-based architecture that can deliver compliance specific services as necessary, based on specific acts and regulations. RedMonk recommends they adopt a Compliance Oriented Architecture (COA.)



## Introduction (2)

---

- Regulatory requirements and standards are fluid and evolving, requiring an infrastructure that can adapt to changing needs
- Many compliance projects occur in isolation and fail to leverage existing resources and assets



## COA: An Architectural Approach (3)

---

- Compliance requirements can be expressed as a set of core services
- Compliance challenged organizations can realize tangible cost and productivity savings by embracing a services-based architecture



## COA In Action: Geisinger Health (10)

---

- Geisinger Health took a services-based approach to simplify the cost and challenge of organizational compliance with HIPAA and other state and federal regulations



## RedMonk Take (12)

---

- COAs apply the virtues of Service Oriented Architectures (SOAs) to the specific business challenge of compliance, and the result is a flexible architecture that can meet compliance challenges now and in the future

## Introduction:

### *Compliance, a Never Ending Story*

IT organizations are being tasked with establishing mechanisms for more effective, systematic control of fundamental business processes, even when compliance issues cut across national and continental boundaries. Thus, irrespective of business size or industry, compliance is becoming a primary concern for CIOs and CTOs at virtually every organization we work with. An increasing focus on transparency, reporting and risk mitigation indicates that the growing demand for compliance capabilities will not plateau in the near future. Indeed, just as the banking industry begins to grapple with the challenges of Basel II, along comes its counterpart in the insurance industry, Solvency II.

At the risk of reading like a cliché, compliance is a journey not a destination. Rarely is anything completed. Rather, compliance calls for constant attention, tweaking and vigilance combined with a balancing of cost, risk and transparency. Sarbanes Oxley, for example, is very much a living regulation. Upfront costs can be conceived of as similar to corporate year 2000 (Y2K) projects for some organizations, but unlike Y2K, Sarbanes requires ongoing improvements in process controls and reporting.

#### What is Compliance?

Simply put, compliance is the process of adhering to a set of established guidelines or rules established by external bodies such as government agencies or by internal corporate policies.

---

“Irrespective of business size or industry, compliance is becoming a primary concern for CIOs and CTOs at virtually every organization we work with.”

---

It's by design that many regulations are ongoing concerns. Regardless of regulation or risk management, many of those prone to commit fraud will continue to do so. As described by J.K. Loebbecke, M.M. Eining, and J.J. Willingham, Jr., the fundamental components of fraud are incentive, opportunity and attitude.<sup>i</sup> Compliance legislation can deter many types of fraud, but won't eliminate base motivations any more than laws prevent violence, theft or other crimes. Compliance can't compel ethics.

Compliance is not restricted to preventing negative corporate behaviors, however; there are quite often tangible business benefits to be received. Indeed, any compliance project should carefully consider and market internally the potential business benefits. Compliance with Software Engineering Institute's Capability Maturity Model Integration (CMMI), for example, is focused primarily on establishing and optimizing repeatable processes that improve software quality. Progressive CIOs are looking for similar gains in business quality from their Sarbanes Oxley efforts. Basel II compliance, meanwhile, frees up capital that would otherwise be reserved against financial risks, which is one reason the European standard is seeing such enthusiastic adoption by financial services companies outside the geography, particularly in the Asia Pacific region.

### *Compliance in a Vacuum*

Compliance projects face immense integration challenges. Despite the increasing attention on compliance as a pervasive business concern, technical efforts to address the various challenges posed by compliance requirements are being undermined by a myopic focus on tactical initiatives. The typical IT organization is addressing compliance reactively. Therefore, rather than thinking about how a

Sarbanes Oxley project and a Basel II project might be merged or cross-leveraged, the respective implementation teams often have little to no knowledge of each other's activities.

Given regulatory deadlines and other external requirements this narrowness of scope may be necessary, but it also means organizations are creating substantial downstream headaches. Overlapping point applications will soon require integration with the organization's follow-on compliance applications. Addressing specific tactical challenges on a case-by-case basis almost inevitably yields a complicated, highly redundant infrastructure which replicates functionality while producing both higher initial implementation costs as well as additional ongoing systems management expenditures. Building a 'one-off' for Basel II compliance is all very well and good, but it may not be capable of scaling up, or otherwise encompassing the scope of the inevitable refinements to the Basel standard.

Another set of pitfalls are created by line-of-business executives, operating in divisional or departmental fiefdoms, who make the mistake of assuming they alone know what's best and that IT can't really help with compliance. According to the Economist Intelligence Unit (EIU) research, this is exactly what is happening. A recent EIU survey of C-level executives shows that only 27% of senior executives ask for input from their IT departments when planning major deployments.<sup>ii</sup>

---

"The typical IT organization is addressing compliance reactively."

---

We're likely to see enterprises experience significant integration pains associated with hurried, non-strategic Sarbanes Oxley compliance efforts over the next 12 months. Many will meet the November 2004 deadline, only to discover their victory is a pyrrhic one, as they are left with a mass of point applications that will not interoperate. The predictable furor is likely to be reminiscent of the aftermath of the dotcom purchasing and implementation frenzy. The need to digest some of those standalone decisions led to a subsequent spate of integration technology purchasing that persists to this day.

IT must assume some responsibility for not being included in compliance strategies, as CIOs shouldn't expect to be consulted until they're able to articulate exactly why and how technology is relevant to the broader set of compliance challenges. But compliance is without question a fundamental strength of most IT shops. After all, aren't virtually all software and support systems built to comply with externally set codes and business objectives? What's needed is a framework that makes the linkages between IT and business controls management more explicit. RedMonk believes the concept of a Compliance Oriented Architecture (COA) can provide the appropriate context for conducting such discussions with business executives.<sup>iii</sup>

### **COA: An Architectural Approach**

#### ***What is Old is New Again***

Crucial to COA is a seminal computing concept that has been reborn with the development of new integration and messaging technologies. That concept, Services Oriented Architectures (SOA), while it currently enjoys the spotlight, is difficult to define in simple terms because it has many different connotations and definitions. The underlying philosophy behind SOA is straightforward: the

dynamic delivery and consumption of a set of rationalized and documented core services, by a variety of applications.

Decomposing an online store like Amazon.com, for example, into its fundamental piece parts yields a set of services - among them: a presentation service to deliver the HTML, a search service to find appropriate items, a shopping cart service and a credit card verification/payment service to check out and purchase items. While many speak of SOA purely in terms of Web services, it's RedMonk's view that Web services are not a prerequisite for delivering a SOA. Web services greatly ease the task of exposing services, but a SOA should seek to exploit available services, resources and applications wherever possible. Indeed, many firms have run *de facto* SOAs using decades old mainframe applications without any assistance from Web technologies. An SOA should seek to exploit available services, resources and applications wherever possible.

---

"While useful in and of itself, however, a SOA is simply a tool for addressing technical problems."

---

What is meant by the term "services" though? Data warehouses, for example, are not traditionally considered to be service-oriented. If we take a broad view, however, data warehouses are indeed a constituency of services. Data is extracted, transformed and loaded into them, whereupon storage, indexing, and querying services are performed. Ideally, a data warehouse would just be another storage/retention/archiving resource - or service - to draw on as necessary, rather than a massive, non-decomposable freestanding entity.

#### What is a Service Oriented Architecture (SOA)?

A decomposable architecture, and associated set of development and IT management disciplines, composed of loosely coupled services communicating via pre-established protocols. These services can be assembled ad-hoc to form customized applications that address a wide variety of business requirements.

While useful in and of itself, however, a SOA is simply a tool for addressing technical problems. It yields value only through imbuing the architecture with specific business requirements, manifested as services. While RedMonk expects many specific flavors of SOAs to emerge - in other words, SOAs that include a specialized set of services aimed at a particular business challenge - we believe that COA is currently the most pressing for IT departments.

#### **Business Requirements Distilled**

A COA then is a specialized instance of SOA, designed to support a broad array of compliance requirements. Though detailed requirements may vary, many generic services are common from institution to institution, compliance standard to compliance standard. Rather than a product or packaged application, a COA is a set of core, compliance-oriented services that can be assembled and deployed to solve a specific need or set of needs.

The COA concept is reliant on a radical—even heretical—notion. Its underlying assumption is that there are services common amongst the volumes of disparate regulatory acts. COA thinking is predicated on the notion that Sarbanes Oxley and the Health Insurance Portability And Accountability Act (HIPAA), for example, have much in common, that automotive industry TREAD reporting regulations are not so different from those demanded of manufacturing companies by the Environmental Protection Agency. Anyone familiar with the

regulatory requirements of a particular vertical industry can attest to the fact that compliance standards are designed to meet the needs of radically different businesses.

It's becoming apparent however, that there is actually very little new in the new regulations. Instead, time-tested concepts are being applied to new business procedures. Records retention is an excellent example. Retention in one form or another is mentioned in nearly every important regulatory compliance act of the last 50 years. The specifics vary widely but the premise of record retention is fairly universal - that a given asset must be retained in unaltered form for a predetermined time period. HIPAA's policies describe retention in terms such as patient age, while the SEC uses calendar years, but despite this difference the core service of retention - the ability to preserve a specific record in an unaltered form - is a common link between the two. Sarbanes Oxley's focus on documented, controlled processes meanwhile is very similar to SEI's CMMI methodology, which requires adhering organizations to demonstrate documented, repeatable procedures.

---

"It's becoming apparent however, that there is actually very little new in the new regulations."

---

We've distilled the most common compliance challenges from compliances standards large and small into a set of core services (See Table 1.) Like the amino acids that make up DNA, we believe that the following services assembled in varying combinations can address the majority of enterprise and governmental compliance challenges. By breaking down the barriers between disparate compliance requirements and distilling out a core set of services, organizations can organize their thinking around compliance specific services; implementing them according to their own unique needs. While critical to compliance, basic enterprise services such as basic identity and application runtimes are omitted, as they need to be present for IT enterprise function and as such are not included as compliance-specific component services.

**Table 1 - COA Core Services**

Service	Relevant Vendors	Description	Example
<b>Access Control</b>	BMC CYA IBM Netegrity Novell Oblix PSS Systems Sun	Establishes control over access to specific assets and resources according to established rules and processes via authentication and authorization elements; prevents unauthorized access and changes	Patient records are accessible only to authorized care providers for HIPAA compliance (Health Care)

---

“Like the amino acids that make up DNA, we believe that the following services assembled in varying combinations can address the majority of enterprise and governmental compliance challenges.”

---

<b>Analytics</b>	Business Objects Cartesis Cognos Fair Isaacs Microstrategy Movaris Oversight Paisley SAS Wall Street Systems	Suite of functions encompassing tasks such as data mining and drill down, reporting, querying, measurement, etc	Operational data is monitored and analyzed according to Basel II metrics (Finance)
<b>Archive/Backup</b>	Anacomp Connected EMC FivePoints iLumin Iron Mountain KVS Sector ZANTAZ	Stores long-term data for cost, convenience, or disaster recovery purposes	Figures such as Work In Progress (WIP) and inventory metrics are transferred to offsite tape to prevent loss in the event of an event affecting the primary datacenter (Manufacturing)
<b>Auditing</b>	Documentum FileNet Interwoven Lumigent Open Text Vignette	Establishes and maintains precise asset history, including creation, alteration, renaming, date copied, etc.	Can be used for forensic purposes to establish a document’s chain of custody (Legal)
<b>Collaboration</b>	Documentum FileNet IBM Open Text Vignette	Enables synchronous or asynchronous communication between individuals, teams or organizations working on the same or related business tasks	For public companies, internal finance workers collaborate with external auditing and legal staff members to produce SEC filing documents such as a 10K (Legal/Government)
<b>Conflict Resolution</b>	Not Available	Mechanism by which conflicting requirements are automatically identified and resolved according to preset requirements, or if necessary escalated for external manual review.	Addresses situations such as when HIPAA mandates that its retention schedule supersedes those mandated by a US State, except in cases where state requirements exceed HIPAA’s (Healthcare)
<b>Destruction</b>	Iron Mountain	Provides for secure destruction of materials that have reached the end of their useful and/or mandated lifespan	At the end of the SEC mandatory retention period, broker/dealer orders are securely destroyed (Finance)

---

“These services represent a foundation for modular compliance initiatives.”

---

<b>Disposition Management</b>	Documentum FileNet IBM Interwoven MDY Open Text Vignette	Mechanism for determining the disposition – or requirements – for a particular asset	Workers can designate a file as a record, and assign it a disposition in years to satisfy DoD 5015.2 (Government)
<b>Indexing</b>	iLumin IBM Legato Google	Crawls through asset stores and indexes them for easier browsing, search and retrieval	Retained drawings, requirements and specifications for a manufactured component are crawled and indexed to ease the litigation discovery process (Manufacturing)
<b>Information Integration</b>	Actuate (Nimble) BEA Composite Context Media IBM Ipedo MetaMatrix Venetica	Provides the ability to unify disparate data sources and types to create a virtual data source composed of two or more data sources of record	Different data sources and repositories are connected and accessed to provide the customer information profile as required by the PATRIOT Act (Insurance)
<b>Monitoring</b>	Akonix Facetime IBM IMLogic Lumigent Mercury Interactive Micromuse Microsoft Net IQ TIBCO Oracle Oversight	Watch specific assets or resources for specific actions, events or conditions, often using an agent-based approach.	For public companies, data stores are monitored for unauthorized and/or inappropriate access indicative of fraud (Publicly Held Firms)
<b>Notarization</b>	Adobe Meridio Surety	Attests to and certifies basic asset creation elements such as author, date created	FDA submissions may be notarized prior to their submission for the purposes of complying with Title 21 CFR 11 (Pharmaceutical)
<b>Policy Engine</b>	IBM	Translates human language policy information into machine readable and actionable instructions and rule sets	Firms can ensure that Gramm-Leach-Bliley compliant privacy policies are implemented and adhered to across their infrastructure (Finance)

“To avoid integration problems...enterprises should implement a flexible and dynamic architecture that consumes compliance services as required.”

<b>Process Registry</b>	Adobe BEA CapeClear IBM Iona Infravio Microsoft Novell SAP Sun Systinet TIBCO Vitria	A directory of available compliance related services and the compliance problems they map to; the registry should allow for automated discovery and description of compliance functions. UDDI and or ebXML will potentially underpin the registry approach.	Patient record application can seek out and access retention services dynamically for compliance storage purposes (Health Care).
<b>Retention</b>	Documentum FileNet Iron Mountain IBM Interwoven MDY Open Text Veritas Vignette	Ensures that assets are retained at a minimum for their required lifespan, and are not deleted, lost or corrupted prior to their scheduled end of life	Agencies can comply with DoD 5015.2 regulations regarding document retention and disposition (Government)
<b>Retrieval</b>	Autonomy Google Microsoft Overture Verity	Supported by Indexing and Tagging, provides for retrieval of asset based search or browse based retrieval as required	Firms can comply with email discovery by retrieving only assets related to the specific request made (Legal)
<b>Tagging</b>	Documentum FileNet IBM Interwoven Logic Library Open Text Vignette	Mechanism for attaching and storing metadata to assets for later consumption and manipulation	CAD/CAM drawings may be tagged with descriptive metadata including date created, product usage, raw material type, etc (Engineering)
<b>Version Control</b>	Catalyst CA Documentum FileNet IBM Infravio Interwoven Open Text Serena Vignette	For iteratively developed assets, provides for documented version capture of asset at each stage in its lifecycle	For public companies, provides capture at each stage of collaboratively developed assets like SEC submissions (Publicly Held Firms)
<b>Workflow</b>	IBM Sonic Software TIBCO webMethods	Implements established business processes to provide clear, repeatable procedures that can be controlled	Provides clear, repeatable process for processing Criminal Offender Record Information (CORI) requests (Education)

---

“The trouble with ILM however is that it doesn’t exist as a deliverable.”

---

These services represent a foundation for modular compliance initiatives. To avoid integration problems, rather than implementing monolithic applications designed to tackle a single regulatory challenge, enterprises should implement a flexible and dynamic architecture that consumes compliance services as required.

The COA approach has numerous benefits, including:

- Reduced licensing costs due to fewer redundant purchases
- Increased productivity through service reuse
- Enhanced service by reducing project time to completion
- Improved management efficiencies by streamlining service portfolio
- The architectural flexibility to grow and change with regulatory requirements

### ***Don't Believe the Hype: Information Lifecycle Management***

These notions of ongoing management, control and improvement are reflected in key compliance concepts such as the term popularized by the storage industry, Information Lifecycle Management (ILM).

ILM describes the process by which an asset is controlled over a period of time from creation to destruction, according to a set of external requirements. A key narrative for customers and vendors alike, ILM has emerged as an important requirement in many compliance efforts. The trouble with ILM however is that it doesn’t exist as a deliverable; no single vendor can package an easily implemented system that permits management of more than one or two asset types. The goal of managing all of a company’s information assets - regardless of type – is still on the distant horizon, although EMC’s acquisition of Documentum and Legato is pushing it in that direction rapidly.

Marcus Hill from BT Retail says customers are confronted with this reality: "ILM *per se* is a myth; a destination at best."<sup>iv</sup>

Integration is the primary reason that ILM still needs fleshing out. ILM tends to be a siloed, either/or proposition: meaning application or asset type oriented. Does a three letter acronym failing to deliver expected value due to its inability to integrate across people, process and technology silos sound familiar? The problem isn’t new. For years Customer Relationship Management (CRM) projects have tried and failed to build a "360 degree view of the customer" – a single profile that aggregates all information an organization owns about a particular customer, whether it's from an ERP system, a billing system, or a sales force automation (SFA) system. The ILM challenge is significantly more complex than that faced by CRM, as the scope of information that must be integrated is substantially wider.

### ***Service Concerns***

Similar to Web services implementations, many firms will cringe at the thought of a services-led approach, believing that this necessitates massive system integration expenditures and long, complex projects. The legacy of traditional

integration and Enterprise Application Integration (EAI) headaches casts a long shadow. Enterprises accustomed to buying packaged applications, for example, will probably feel their IT staff is simply not capable of assembling and delivering a COA. While this may or may not be a valid assumption, depending on the complexity of the needs, that line of thinking is ultimately irrelevant.

There is no need for an organization to assemble a COA by itself using its own internal resources. By implementing COAs within their own product lines, ISVs and even Systems Integrators can make the purchasing of a COA as simple to enterprises as buying a solution package. Hosted or managed service type solutions are another possible COA deployment scenario (automated backup and archiving of corporate email for example). Organizations with greater resources may wish to assemble a COA from scratch. The COA approach is as viable for an ISV as it is for an enterprise; a few vendors are already moving in that direction. Pervasive, for example, is a database company that caters to application vendors and it's explicitly building out services to enable its ISV customer to deliver compliance services such as audit and information integration through their application to their end-users.

---

"On the contrary, a COA approach looks at existing core services and identifies whether they are extensible and can be used in a COA context."

---

Many services - collaboration, for one - will consist of packaged or hosted applications, rather than homegrown ones, in the vast majority of cases. Organizations should focus on achieving a COA with the approach that best fits their existing resources and budget; there's no one "true" path to compliance.

It is also crucial to note that COA takes an asset and portfolio management approach. It is by no means necessary to rip and replace existing technologies. On the contrary, a COA approach looks at existing core services and identifies whether they are extensible and can be used in a COA context. COA is a framework that can be built out incrementally using a range of different technologies. Each enterprise can define the parameters of their own COA implementation. This isn't about wholesale replacement, nor is it a windfall opportunity for vendors. As with SOA discipline, however, rationalization and consolidation are good first steps to delivering reuse and cost effective, flexible services.<sup>v</sup>

COA is simply a rational approach to solving a set of challenges.

### **COA In Action: Geisinger Health**

We're seeing more and more organizations using COA-style approaches. Geisinger Health System, as an example, has recently won plaudits for its use of IT; it has been cited by the Wall Street Journal, and won the Association for Information and Image Management (AIIM) Best Practices Award 2004 for its creation of a comprehensive HIPAA-compliant electronic patient records system.

Geisinger's approach to compliance is services-based, requiring the creation of a dedicated patient records organization and the associated architecture to serve the needs of the other business divisions. This patient records organization provides, for example, central scanning services for branch office partners.

Geisinger has broken down its own organizational silos, not just technical ones. Thus, the legal department was instrumental in justifying the IDM investment, projecting litigation savings of hundreds of thousands of dollars a year.

---

" 'For any function we do, the system has an audit trail. It protects patient records from business people and business accounts from caregivers.' "

---

The organization's definition of patient records covers a range of data types such as patient photos, cardiogram videos, electronic reports from medical lab systems, benefits statements, claims forms, patient survey forms, e-mail and so on. All of these

data types must be indexed and stored according to formal policies. A first step to compliance was bringing all records under management.

Before Geisinger installed IDM its records were in filing cabinets, doctors' offices, local hard drives,

and in some cases even digital pictures on memory sticks. The dermatology department, for example, had 10,000 35 mm slides in storage. With its new approach, however, Geisinger provides a simple import mechanism for records from any desktop, according to defined policies.

Geisinger Details	
<b>Compliance Requirements:</b>	HIPAA, Pennsylvania Insurance Department Guidelines for Retention, Centers for Medicare & Medicaid Services (CMS), Internal Revenue Service (IRS), National Committee for Quality Assurance (NCQA)
<b>Hardware:</b>	EMC Clariion 10 Terabyte Storage Area Network
<b>Software:</b>	Vignette Integrated Document Management (IDM), TIBCO Staffware, EpicCare
<b>Applications Supported by COA:</b>	Billing, Claims Processing, Clinical, Medical Laboratory, Picture Archiving, document imaging and report management

According to David Partsch, Program Director for Geisinger, compliance is not the challenge it once was: "For any function we do, the system has an audit trail. It protects patient records from business people and business accounts from caregivers."

The next focus areas for its compliance efforts are to standardize on a content management and collaboration platform, and to tie its customer-facing portal to its COA records-management services. Geisinger is already planning for what happens after HIPAA's initial phases, with regulators already planning to call for a unique identifier for every national healthcare provider. This legal framework will take information sharing to a new level, with all the data management challenges that implies.

### RedMonk Take

In an ideal world, customers would be able to dynamically mix and match all component services. Unfortunately, that's not the current reality. While some services such as archive/backup, auditing, retention and workflow are mature enough to be integrated, and in some cases are already established as available monitored services, many others are nascent.

But COA thinking is inevitable. The first COA-like constructions are already emerging in the area of ILM where the pain associated with retention and asset management has been festering for years. Indeed, ISV and storage suppliers' ongoing attempts at addressing ILM requirements via acquisitions or a combination of broad partnerships<sup>vi</sup> only validates the difficulty of the point-to-point integration route. Customers need more than just loosely coupled partnership integrations, or closed single vendor approaches. Vendors and their customers need to think architecturally, in terms of standards and embracing a service-centric approach to compliance.

Given the steady progress of related technologies such as Web services and SOAs, the path towards COAs is evident and gaining momentum. At the same time, the demand for compliance continues its inexorable march into industry after industry. Organizations not currently confronted by compliance challenges will be shortly. Put all of that together, and COAs look more and more like a mandatory response to the escalating problem of compliance. The question of how to align business and IT is as old as the industry. COA is an approach that begins to do just that - align business policies with IT capabilities, without pouring concrete on the solution.

---

“COA is an approach that begins to do just that - align business policies with IT capabilities, without pouring concrete on the solution.”

---

# About the Creative Commons License

---

This work is licensed under the Creative Commons Attribution-ShareAlike License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/2.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

## About RedMonk

---

RedMonk is a research and advisory services firm that assists enterprises, vendors, systems integrators and corporate finance analysts in the decision making process around today's enterprise software stacks. We cover the industry by looking at integrated software stacks, focusing on business and operational context rather than speeds and feeds and feature tick-lists.

Founded by James Governor and Stephen O'Grady, and headquartered in Bath, Maine, RedMonk is on the web at [www.redmonk.com](http://www.redmonk.com). If you would like to discuss this report email [sogrady@redmonk.com](mailto:sogrady@redmonk.com).

---

---

<sup>i</sup> "Auditors' experience with material irregularities: Frequency, nature, and detectability", J.K Loebbecke, M.M. Eining, and J.J. Willingham, Jr, Auditing: A Journal of Practice & Theory, Fall 1989

<sup>ii</sup> " IT voices drowned in corporate governance rush," The Register, 4.22.2004

<sup>iii</sup> "End-users tell of ILM compliance worries", Computer Reseller News, 5.24.2004

<sup>iv</sup> "BEA, SOA, UML ,“ MonkChips blog, June 8 2004:

<sup>v</sup> "Documentum's Next Step: EMC Division", RedMonk, 10.15.2003