

# SOA Meets Compliance: Compliance Oriented Architecture

*A conceptual framework for considering  
Documentum Retention Policy Services*

## Abstract:

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.

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.)

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

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC<sup>2</sup>, EMC, and where information lives are registered trademarks of EMC Corporation. Documentum is a registered trademark of EMC Corporation. All other trademarks used herein are the property of their respective owners. All other brand names are trademarks or registered trademarks of their respective owners.

60630305V1

# Table of Contents

<b>Introduction:</b> .....	<b>4</b>
Compliance, a Never Ending Story.....	4
Compliance in a Vacuum.....	5
<b>COA: An Architectural Approach</b> .....	<b>6</b>
What is Old is New Again .....	6
Business Requirements Distilled .....	6
Service Concerns.....	9
<b>RedMonk Take</b> .....	<b>9</b>
<b>About the Creative Commons License</b> .....	<b>10</b>
<b>About RedMonk</b> .....	<b>10</b>

## **Problem:**

- 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

## **Solution: a Service Oriented Architecture**

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

Compliance initiatives should not be restricted to preventing negative corporate behaviors, since there are quite often tangible business benefits to be received. Indeed, any compliance project team should consider the potential business benefits and market those internally. Compliance with the 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.

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

**What is Compliance?**

### What is Compliance?

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

## **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 research from the Economist Intelligence Unit (EIU), 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>

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)<sup>iii</sup> can provide the appropriate context for conducting such discussions with business executives.

*"The typical IT organization is addressing compliance reactively."*

# 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.

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.

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.

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

### **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.

## ***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—notation. 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.

*“Retention in one form or another is mentioned in nearly every important regulatory compliance act of the last 50 years.”*

We’ve distilled some of the most common compliance requirements from compliances standards large and small into a set of core services (See Table 1.) 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.<sup>1</sup>

**Table 1. COA Core Services**

<b>Service</b>	<b>Description</b>	<b>Example</b>
<b>Access Control</b>	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)
<b>Archive/Backup</b>	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>	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)

<sup>1</sup> 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.

<b>Service</b>	<b>Description</b>	<b>Example</b>
<b>Collaboration</b>	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>Destruction</b>	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)
<b>Disposition Management</b>	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>	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>Notarization</b>	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>Retention</b>	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	All employee I-9 forms must be retained in compliance with the Immigration and Nationality Act and H. R. 4306 stipulations (Human Resources)
<b>Retrieval</b>	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>Version Control</b>	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>	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)

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

## **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. 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. In any case, 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 the COA takes an asset and portfolio management approach. It is by no means necessary to 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>

*"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."*

## **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.

## 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 [sograd@redmonk.com](mailto:sograd@redmonk.com).

- ii "IT voices drowned in corporate governance rush," The Register, 4.22.2004
- iii "End-users tell of ILM compliance worries", Computer Reseller News, 5.24.2004
- v "Documentum's Next Step: EMC Division", RedMonk, 10.15.2003

**About EMC**

EMC Corporation (NYSE: EMC) is the world leader in information storage systems, software, networks, and services, providing automated networked storage solutions to help organizations get the maximum value from their information, at the lowest total cost, across every point in the information lifecycle. Information about EMC's products and services can be found at [www.EMC.com](http://www.EMC.com)

**About Documentum Software from EMC**

Documentum software from EMC Corporation includes enterprise content management solutions that enable organizations to unite teams, content, and associated business processes. With a single platform, EMC Documentum software enables people to collaboratively create, manage, deliver, and archive the content that drives business operations, from documents and discussions to e-mail, Web pages, records, and rich media. The Documentum enterprise content management platform makes it possible for companies to distribute all of this content in multiple languages, across internal and external systems, applications, and user communities. As a result of deploying Documentum, thousands of the world's most successful organizations are harnessing corporate knowledge, accelerating time to market, increasing customer satisfaction, enhancing supply chain efficiencies, reducing operating costs, and improving their overall competitive advantage.

For more information about Documentum enterprise content management, visit [www.emc.com/documentum](http://www.emc.com/documentum) or call **800.607.9546** (outside the U.S.: +1.925.600.6754).