NASCIO Staff Contact: Eric Sweden, esweden@amrms.com or (859) 514-9189.

Service Oriented Architecture: An Enabler of the Agile Enterprise in State Government

I. Executive Summary

Service Oriented Architecture (SOA) promises to be a significant innovation for state government. Imagine the ability to pick and choose business and technology services. To be able to trade out services based on organizational re-design, new strategic intent, legislative requirements, or business process modifications. To be able to reduce redundancy and improve data quality. SOA is not another new technology. It is a whole philosophy about sharing, decoupling business processes from technology, to enable a fluid enterprise that can change and change quickly. The vision that has been touted for so long within enterprise architecture regarding the *"spontaneous enterprise"*[1] now becomes possible. A number of states are just beginning their SOA efforts, or are in the planning stage for an SOA initiative. State government anticipates SOA is the path to extending legacy applications to handle business processes across government. Early applications of SOA include:

- ➤ Purchasing
- ➤ Integrating legacy applications
- ➤ Common payment engines

This research brief touches on aspects of SOA important to state government but it does not purport to be an exhaustive treatment of the subject. The references in the appendix provide additional resources.

II. Introduction

The purpose of this NASCIO Research Brief is to provide state CIOs a current overview of Service Oriented Architecture (SOA) as a tool in improving their state government operations. SOA is receiving much press and is a common term in the vernacular of business and information technology professionals across the globe .

Here in the United States, at the Federal level, the Office of Management & Budget (OMB) and the General Services Administration (GSA) have been early adopters of web services and SOA, and leaders in the development of the Federal Enterprise Architecture (FEA). For example, GSA and Unisys implemented a SOA-based architecture starting in

---

[1] See http://www.qualitydigest.com/sep99/html/sixsigma.html

2003 that leveraged legacy systems and associated databases and weaved together a J2EE and .NET based open standards component architecture.[2]

There are many factors driving this new emphasis that span a spectrum from the expectations of the coming generation to economic drivers to project management approaches to balancing time and cost. SOA is here to stay and it will prove to be one of the most significant events in the history of information technology and the connection between the vision for the *"agile enterprise"* and achieving operational efficiencies, and the associated enabling technologies. Some would consider SOA as significant as the advent of the assembly line by Henry Ford.

Whereas Henry Ford had demonstrated the value of *mass production*, *interchangeable parts*, and the *division of labor*, SOA has become the banner for demonstrating mass customization, composite solution development, reuse, reassembly, and dynamic approaches within information technology that enable the *agile enterprise*. Mr. Ford's success with the concepts of division of labor brought hallmark advances in organizational efficiencies. He slashed prices on the Model T and demonstrated that strategic lowering of prices could actually boost profitability.

> **CIO RECOMMENDATION:**
> *Take a leadership role in promoting the vision and concepts of SOA.*

The CIO should take the lead in establishing a vision for SOA, and evangelizing that vision among colleagues on the business side as well as the technical side of the organization. Executive buy-in is critical whether it is built through CIO relationships, executive order, or legislation. Further, the CIO should lead the development and continual evolution of a roadmap for delivering service oriented architecture for the enterprise that emphasizes business value. That roadmap must be dynamic, changeable as new learning occurs. We make that recommendation because there are new concepts and approaches developing in the world of SOA.

Service Oriented Architecture is not a replacement for enterprise architecture. Enterprise architecture is defined in the NASCIO Enterprise Architecture ToolKit[3] and the NASCIO report *Perspectives: Government Information Sharing – Calls to Action*[4] as a comprehensive management engineering operating discipline. SOA supports the overall enterprise architecture by enabling *agility* so the enterprise can indeed respond, and respond quickly to environmental trends, and disruptions such as market and regulatory changes.

- SOA influences the business architecture with well-defined, reusable business processes,
- influences the application architecture to use components and service interfaces,

---

[2] See IDC "eGovernment Case Study Analysis: Unisys Lays a Services-Oriented Architecture Foundation for the GSA," Sophie Mayo October, 2004 http://www.idc.com
[3] See http://www.nascio.org/nascioCommittees/EA/download.cfm?doc=toolkit
[4] See http://www.nascio.org/nascioCommittees/EA/download.cfm?doc=perspectives

- influences the data architecture to use XML, and
- influences the technical architecture with standards for infrastructure to support:
  - services,
  - consumers of those services,
  - services proxies, and
  - messaging infrastructure.

In fact, many would say, SOA is really not new. The objectives and ultimate outcome of successful SOA is already embedded in the philosophy of enterprise architecture. The concepts of sharing, and reuse within both the business and technology areas of the organization have been around for sometime. Maybe what is really going on with the "advent" of "SOA" is that there is finally an understanding of the *value* of architecture, reuse, and services. Maybe there is finally a motivation to abandon old paradigms regarding "not invented here". There is now availability of many enablers of the concepts of agility and the *service oriented enterprise* (SOE) that are now presented by governments' corporate partners. SOA provides flexibility, and the capability for adjustment of business processes.

We also have a new generation of managers, business professionals, technical professionals, coming up the ranks who have a different perspective on "how things are done." They aren't afraid to ask, "Why?" and, "are we ready to seek alternative means for solving problems?". Possibly the most significant contributor to the explosion of SOA activity is *organizational willingness*. Organizational culture is the most complex challenge in any management initiative. However, organizational culture is also the most powerful enabler of any management initiative – *once it is engaged.* And that is what is really happening now. The foundational concepts of SOA are not new. Someone once described SOA as *"old wine in new bottles."* What is new is the broad *organizational will* to share, reuse, and leverage capabilities inside and outside the organization. And, the *organizational will* to create new capabilities with "*reuse designed in.*" The concepts have existed, but not to any great success. We are now in a new era where services and business processes are seen as black boxes. There are a set of well defined inputs to get back a set of well defined outputs – but the process that delivers these outputs are of no concern to the consumer of these services and processes. Technical standards and components now make this activity technically easy.

SOA initiatives are reusing components of *legacy systems*. How much easier would SOA be realized if those legacy systems had been designed, anticipating exposure to broad reuse and re-assembly? *That is the future. Designing for reuse* will become more of the norm across industry and government.

> **CIO RECOMMENDATION:**
> *Embrace SOA as method for delivering business value*

Today we speak of the dynamic, adaptable enterprise - the fluid enterprise - "the spontaneous enterprise" - that changes over time in response to market and regulatory dynamics – and involves everyone from the top of the organization down to the most

granular level. There are many enablers that make this vision a reality. NASCIO believes that SOA is one of those enablers and encourages our CIOs to begin to develop a strategy for embracing SOA for delivering business value.

Even as Mr. Ford was continually learning, and seeking ways to improve, NASCIO believes there are new methods forthcoming to enable the vision of a dynamic, adaptable organization. Further, the enablers such as SOA will entail new methods, approaches and applications. One of Ford's maxims: *"Everything can always be done better than it is being done."* We expect that maxim applies to SOA as well. There will be new applications, new refinements.

With so much dialogue on the subject, we find that the term has multiple scopes of definition, applications, and approaches to implementation. Some professionals are more philosophical in their thinking about "services" and "architecture" and have a broader view of SOA

> *"Through 2006, SOA and "designing for integration" will represent the largest single innovation that reduces the cost and increases the effectiveness of integration projects in large enterprises."*
> Gartner Inc., 2003

that includes *business services*, *enterprise agility* and *business transformation*. Others restrict SOA to the application and technology architectures – i.e., treating it as strictly an information technology concept. Some focus even more equating SOA with Web Services. The more holistic thinkers see SOA as entailing a robust business strategy that is enabled by certain principles, frameworks, architectures – comprising an enterprise wide operating discipline approach to the scope of SOA.

In this introductory research brief on SOA, we won't debate the various views, for they all have something to offer. The focus of this research brief will be on the value of SOA making the point that indeed SOA is an essential tool in the CIO's portfolio of capabilities for enabling the strategic intent of the organization. Further, there are lessons to be learned from the pioneers and early adopters of SOA. Those lessons will be summarized.

Consistent with NASCIO's philosophy on enterprise architecture, the general perspective in this report is *holistic* and *comprehensive* in its treatment of SOA. We will make references to bodies of knowledge that present more in depth analysis of the dimensions of SOA. Our purpose here is to summarize in succinct fashion the essentials of SOA. NASCIO recognizes the significance of SOA and is fortunate to have as its corporate partners some of industry's most significant leaders. NASCIO is leveraging these partners by sponsoring a series of webinars on SOA to occur in May and June of 2006.[5]

Doing business in government today requires the communication and collaboration of all levels and branches of government. Business verticals in government consist of public services, social services, regulatory compliance, and government operations all working toward achieving the needs of constituents in the most effective way possible. Working across levels and branches of government is a complex and difficult undertaking that is

---

[5] See http://www.nascio.org/nascioCommittees/clc/webinarForm.cfm

further complicated by the governance and infrastructure that must exist to support it. The ability of government to connect at the business level, without ubiquitous supporting methods for execution, is frustrating and ineffective for business leaders. In today's world, government leaders expect to be able to move quickly, using all information appropriate to make effective choices that benefit constituents. Enablement of this expectation requires an organizational culture that embraces the sharing of assets and information.

Unfortunately, today's infrastructure is not well suited to responding to the demands for responsive interconnectivity. Simply re-aligning organizations will not achieve the requirement for governments to work across boundaries, either within existing layers, or across vertical levels. In the business of government, standard methods and processes govern common activities such as health care, finance, and public safety to ensure maximum efficiency and interoperability across business segments. Some states have created a Community of Practice (CoP) in these key areas to promote multiple agencies to work together in a collaborative and non-redundant manner. Information technology plays a significant role in helping to achieve this, but is limited in its ability to work across the many platforms and technology implementations that exist across the unique and autonomous entities that make up the government vertical.

As the information technology industry matures, its ability to meet the needs of government will be determined by its ability to become ubiquitous in cross-technology communications at high rates of speed, in a way that simplifies the ability of government to achieve requirements. SOA focuses IT on being *business driven*. The underlying assumption in SOA is that *not everything in technology can be the same*, so standard methods and processes must be defined to enable disparate technologies to communicate, *regardless of manufacturer or language*. In accomplishing this, technology becomes an effective tool for the business side of government to ride upon. The ability of government to use technology to achieve cross boundary activities is removed as an obstacle, and becomes an enabler. The simplification of the communication method, allows government to concentrate on the core business issue, and not consider the technical concerns of the past. This enables government to focus on streamlining business process, pushing decisions and information closer to constituents, and reducing the requirements for management processes and overhead between providers of services.

In summary, the value of SOA isn't in technology. It is in the ability of government to respond to change, and optimize services utilizing differing technologies as vehicles for maximizing constituent value. The Oracle Corporation received the following comments from some of its customers in a recent survey.

"Only 5 days to completely modify EAI project architected with SOA/BPEL (past experience: 2 months)." – *regarding an SOA based integration project at a western college*

"Never seen an IT project completed in less than 2 years; with SOA/BPEL core biz process automation delivered in <6 months." - *regarding composite SOA applications at*

a large financial institution

"SOA reduces bug fixing cycle from *3-4 months/30 people* to *3-4 weeks/5-8 people.*" - *regarding SOA Enabling the mainframe at a large insurance company*

BEA Systems, Inc. has found that where their government customers have been successful there has been a pragmatic start-small-approach. For example:

The City of Chicago's Business and Information Services (BIS) department, responsible for central IT services to various city departments, has taken a two phased approach over the last 3 years to their SOA implementations. In the first phase, they've started by selecting departments where they could see immediate cost savings and improvement to services out to end-users. In one case, building an integrated workflow and access management platform between four disparate legacy applications and data repositories coupled with a front-end portal for city contractors with the Public Building Commission, enabled them to leverage existing legacy investments yet build a front-end Java platform for exposing those systems as web services. Based on initial successes like this at a per department level, they began using the methodologies and practices learned to build core services consumable by multiple agencies around the city, for example, a payment engine to support tax collections using an Enterprise Service Bus and Data Services Platform. This particular project saw immediate return on investment in multiple departments, for example, an increase of 20% in parking permit revenues and collection of outstanding parking violation collections.

> **CIO RECOMMENDATION:**
> *Recognize SOA as an organizational change concept.*

The SOA perspective does not stop at web services, or application development in general. It is not restricted to technology. SOA brings with it a significant impact on *organizational change*. One of the best approaches to managing expectations and organization impact in through *clearly articulated service level agreements*. This will ensure everyone concerned understands expectations regarding capabilities, capacity and availability.

SOA promises to alleviate the past experience of business processes *shackled* to information management applications. How often have organizations been told that certain business processes, or certain differentiating business practices and terms would have to be eliminated or compromised – because the particular ERP system being implemented couldn't accommodate the existing business intent. The choices available to the organization included the following:

➢ Accept the approach prescribed by the ERP – without change. Change business processes and remove any market offerings that are too unique to be accommodated by the ERP –thus removing market differentiating business practices.

> ➢ Continue to build custom systems that fully implement those differentiating business practices.
> ➢ Customize the commercial ERP and enter into an ongoing version management challenge and frantic re-customization every time the vendor makes a change.

Some are claiming those days are gone. With SOA, not only is sharing emphasized, but also it is very possible that unique business practices can reenter. This anticipation is of course still dependent on the ability of the ERP system to accept the associated data and data rules. Additionally, there is the change in the vendor relationships. Some anticipate that vendor partners will eventually expose their software services so that functionality can be "rented" or "leased" as part of a state government composite application.

More importantly, SOA philosophy promises to facilitate transformation of the organization. This transformation involves the sharing and reusing of business and technology services. The source of such shared services can be another agency within the same jurisdiction, or another jurisdiction. It is conceivable that services will someday be shared among federal, state and local jurisdictions. Anticipate as well an Application Service Provider (ASP) model involving *service offerings*.

III. Definition of Service Oriented Architecture

CIO RECOMMENDATION:
Watch out for the "SOA Label"

There is much hype in this new term that accompanies and masks the real value. While it is recommended that state CIOs watch out for the hype, it is also recommended that they embrace the philosophy and concepts of SOA.

Among the myriad of definitions of SOA are the following:

> ➢ *Service Oriented Architecture is a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. (OASIS SOA Reference Model)[6]*
>
> ➢ *Contemporary SOA represents an open, agile, extensible, federated, composable architecture comprised of autonomous, QoS-capable, vendor diverse, interoperable discoverable and potentially reuseable services, implemented as Web services.*
>
> *SOA can establish an abstraction of business logic and technology that may introduce changes to business process modeling and technical architecture, resulting in a loose coupling between these models.*

---

[6] OASIS SOA Reference Model (DRAFT) see <http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm>

SOA is an evolution of past platforms, preserving successful characteristics of traditional architectures, and bringing with it distinct principles that foster service-orientation in support of a service-oriented enterprise [SOE].

SOA is ideally standardized throughout an enterprise, but achieving this state requires a planned transition and the support of a still evolving technology set. (Thomas Erl)[7]

➤ *. . . service-oriented architecture (SOA) is an approach to EA (enterprise architecture) where each major element is exposed as a "service." The result is a distributed computing environment with a high level of interoperability between systems. . . . SOA enables the enterprise architect to "defy the laws of gravity" and combine and recombine software elements without the necessity of spending substantial amounts of time or money, assuming it has been implemented intelligently. (Eric Pulier and Hugh Taylor)[8]*

➤ *SOA is based on a systems environment specifically architected to leverage freestanding units of functional code, each of which corresponds to a specific activity. An IT service, in this respect, is a self-describing software component that is accessible over a network and has a published interface that does not require knowledge of the technology used to create and deploy it. While SOA can be implemented without the use of Web services, Web services should be seen as the primary delivery model for this architecture. (IDC)[9]*

➤ *SOA is not a technology per se, but rather a set of principles and methodologies for designing and developing software "services" that can be deployed and managed across an enterprise network. These "services" are, in essence, software components-discrete pieces of code and/or data structures-that can be reused for different purposes. Reuse is possible because the components are packaged as self-contained, loosely coupled units, which enable developers to work with them without affecting other components. Because of their independent, modular nature, software components can be used like building blocks to develop a variety of new applications. They can also be made available externally to partners and suppliers for use in their applications. (Jean François Bissonnette)[10]*

➤ *. . . Services Orientation as well as SOA is an architectural style whose goal is to achieve loose coupling among interacting services. A service is a unit of work done by a service provider to achieve desired end results for a service consumer. Both provider and consumer are roles played by organizational units as well as software agents on behalf of their owners.*

---

[7] Thomas Erl, *Service-Oriented Architecture: Concepts,, Technology, and Design*, ISBN 0-13-185858-0, (New York, Prentice Hall, 2005), p. 54.

[8] Eric Pulier, Hugh Taylor, *Understanding Enterprise SOA,* ISBN 1-932394-59-1, (Connecticut, Manning, 2006), p 57.

[9] IDC "Why Are Services-Oriented Architectures Relevant to IT and Business Executives Alike?", Sophie Mayo, Marianne Hedin, November, 2004, www.idc.com

[10] See http://www2.cio.com/consultant/report3358.html

> *A Service is an implementation of a well-defined business functionality that operates independent of the state of any other Service defined within the system. Services have a well- defined set of interfaces and operate through a pre-defined contract between the client of the Service and the Service itself.*
>
> *Service-orientation presents an ideal vision of a world in which resources are cleanly partitioned and consistently represented. When applied to IT architecture, service-orientation establishes a universal model in which automation logic and even business logic conform to this vision. This model applies equally to a task, a solution, an enterprise, a community, and beyond (IFEAD).[11]*

There are many more definitions but the essence is in the words "service oriented." These words really speak to the perspective that must be adopted across the enterprise. That is a *service oriented perspective*. This requires adoption of a propensity to share, to look for an existing service that can be reused from within and outside of the immediate organization. Developing a service from the ground up becomes the exception. The potential for business transformation will require strong collaboration with the business to identify business services that can be shared.[12]

CIO RECOMMENDATION:
Describe the rationale for SOA as bringing business value

SOA is a path of choice for delivery business value, *quickly and effectively*. There is no stronger motivation. SOA has already proved itself within industry. Proponents cite ROI gained in a number of areas.

- ➢ Reducing cost to deliver solutions
- ➢ Reducing time to deliver solutions
- ➢ Reducing cost to maintain solutions
- ➢ Reduced time to market
- ➢ Increased utility from existing investments
- ➢ Increased number of features available to the business

However, be careful in quoting an ROI for SOA. The challenge is separating out that true ROI attributable to an SOA program or project deliverables while separating out the contributions from other initiatives.[13] This caution flag applies to the success stories we all read as well – be cautious. The value of SOA is recognized. But it shouldn't be oversold. Many other overlapping initiatives are contributing to the success of an organization as well including good project management, effective partnering, employee development, innovative technologies and implementations. However, these contributors to success must accompany effective *business strategies*.

---

[11] The Institute for Enterprise Architecture Developments http://www.enterprise-architecture.info/EA_Services-Oriented-Enterprise.htm
[12] See http://webservices.sys-con.com/read/164560_p.htm
[13] See http://blogs.zdnet.com/service-oriented/?p=388

> **CIO RECOMMENDATION:**
> *Establish a long term vision and strategy incorporating intermediate quick-wins.*

Successful implementers of SOA have developed a long term roadmap. They recognize that the development of a SOA will be a journey that starts small, but keeps the *ultimate outcome* in mind. That *ultimate outcome* is *enabled* by business agility.

This is achieved by starting with smaller projects with limited scope that can achieve a relatively high return on investment. Partner with a line of business champion to build that first shared service. Additional projects are defined that build toward the long term vision and provide incremental opportunities to develop expertise in identifying and implementing shared services.[14]

However, the *ultimate outcome* for government is the ability to meet changing demands from citizenry.

- Are streets safer?
- Are this nation's citizens healthier?
- Is healthcare available to those that need it?
- Is education available and effective in preparing our citizens for the opportunities and demands of a new economy?
- Is there the necessary economic development in this country to present employment, career, and personal development opportunities to our citizens?
- Are we able to respond quickly and effectively to national emergencies such as natural disasters, pandemics, terrorist threats and attacks?

This is a sample of the real outcomes we're trying to achieve in government. And they must be maintained in the forefront of any investment decisions, management initiatives, programs and projects. This same point has been made by NASCIO regarding enterprise architecture initiatives. We don't do enterprise architecture for the sake of enterprise architecture, methods and procedures, compliance with standards, etc. *Enterprise architecture is a path to government transformation – it is a method for accomplishing the mission of government.* It is only employed because it gets us to the goals presented in the previous bullets. The same perspective must be maintained regarding SOA.

> **CIO RECOMMENDATION:**
> *Establish SOA governance*

Establish SOA governance early in order to drive organizational behavior.[15] Without SOA governance in place, there is a high potential for developing redundant capabilities, regulatory noncompliance, and costly implementations.[16]

---

[14] See http://webservices.sys-con.com/read/164560_p.htm
[15] See http://www.weblayers.com/gcn/whitepapers/Introduction_to_SOA_Governance.pdf
[16] See http://www.gridtoday.com/grid/601213.html
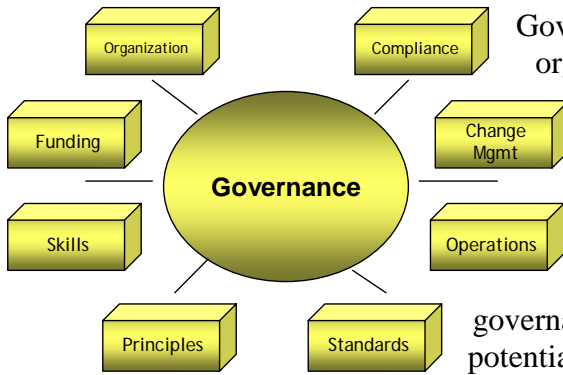
Governance is needed to ensure that an organization's SOA program is effectively planned and executed using defined standards, methods and procedures. Without governance, SOA will be fragmented, and ineffective. The result will be a flurry of activity that is less than effective over the long run. Without governance, there may be a few initial quick but potentially short-lived wins – e.g., rapidly developed web services providing limited utility. However, if this behavior continues, eventually the organization will experience cost overruns, project delays, and significant negative impact on the business.

The vision for SOA will not be achieved, resulting in limited reusability in highly focused applications. Therefore, establish governance, and establish it early.

> *"SOA Governance is critical to achieving SOA success," stated Eric A. Marks, President and CEO of AgilePath Corporation, "and it cannot be reduced to a software tool or a vendor product suite. SOA governance is all about organization, process and enforcing policies to achieve a consistent behavioral model. This SOA Governance Reference Model frames SOA governance in this context."[17]*

Most of the failures experienced thus far in implementing a SOA is the lack of governance.[18]

The essential elements of SOA governance include[19] [20]:
  - Organizational Design
  - Funding
  - Management of Associate Development
    - Knowledge, Skills, and Experience
  - Principles
  - Standards
  - Operational Processes and Tools
  - Change Management
  - Risk Management
  - Compliance and Performance Metrics

Governance will include answers to the following questions[21]
  - Who defines and *modifies systems*?

---

[17] See http://www.agile-path.com/news/agilepath_soa_gov_ref_model_feb_21_2006_v1.pdf
[18] See http://dev2dev.bea.com/blog/steviebennett/archive/2005/11/soa_myth_or_hyp_1.html
[19] See http://www-128.ibm.com/developerworks/webservices/library/ws-soa-govern/
[20] See http://dev2dev.bea.com/blog/steviebennett/archive/2006/03/is_2006_the_yea_1.html
[21] See http://dev2dev.bea.com/pub/a/2006/02/soa-long-term.html

> ➢ Who is allowed *access to the services*?
> ➢ What *quality of service* must we provide?
> ➢ Who will *pay for building* the services?
> ➢ Who will *pay for service infrastructure*?
> ➢ How will the *interdependencies of services be managed*?
> ➢ How do we *expose services* to outside parties?
> ➢ How will we *measure the success* of SOA?

The establishment of governance will determine whether the SOA for state government will be a haphazard set of activities with no common purpose, or a program that is managed for long term sustainable success.[22]

CIO RECOMMENDATION:
See SOA as a program not a project

SOA must be seen as a program not a project. SOA will prove to be a journey and includes establishing all the necessary components of a program.

Selecting the first project within an SOA program is equally important. That first project must be successful in order to gain and maintain support for the rest of the program. The first project should have a very limited scope but also contribute toward the long term goals of the program. Current statistics on project success are rather bleak. It is important to prepare in advance to avoid the often encountered pitfalls of many IT related projects.

Scope   Time   Cost
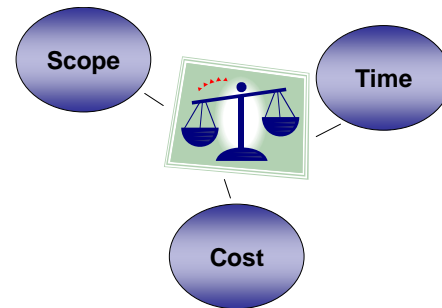
The Standish Group reports the following statistics related to the incidence of project failure in general without regard to the type of project – SOA or otherwise. These results were presented at the 2006 Symposium on Justice and Public Safety Information Sharing - *Strategic Planning Principles, Effective Funding, and Oversight Session.* [23]

- 52% of projects will cost 189% of original estimates
- Large organizations net only 42% of the original features and functions in the end product
- 31% of IT projects are canceled before completion
- 16% of large scale projects are completed on time and within budget

The message is clear from these statistics – use proper project management discipline in planning and executing your SOA project.

---

[22] See http://www.dmreview.com/article_sub.cfm?articleID=1051396
[23] See
http://www.search.org/conferences/2006symposium/presentations/Tuesday_Day%202/PLANNING%20Strategic%20Planning/Strat%20Plan%20Session%203.14.06.ppt

If state SOA initiatives are not run as programs, involving all the discipline that has been promoted within enterprise architecture, state government will be saddled with a new legacy of web services applications. The business and technology gains promised by SOA will not be realized.

"In 2006, enterprises worldwide will have spent nearly $3 billion on failed and redesigned Web services projects because of poorly implemented service-oriented architectures"[24]

Understand that as a program matures more success stories will result. It will take some time for state SOA to mature to the point where tangible benefits are accumulating. Recent studies show that many SOA efforts are not producing the results first touted. The root cause is organizational dynamics and the fact that SOA is still maturing. A recent survey of 1,000 organizations indicated only 21% were actually sharing services. Clearly this presents implications relative to managing expectations, effective communication, managing organizational dynamics and incentives, and the fact that realization of the benefits of SOA are slowly growing.[25]

> **CIO RECOMMENDATION:**
> *Achieve real time control by integrated business intelligence and SOA*

SOA enables real time control when integrated with business intelligence capabilities. This capability can take the form of an Executive Digital Dashboard (EDD) that provides the agency executive with real-time metrics on performance.[26] Establishing better visibility into the business operations provides management with the ability to detect problems and quickly intervene. Whereas, EAI solutions tend to be expensive and inflexible, an SOA solution using loosely coupled web services can provide the ability to communicate with multiple business applications dynamically.

One approach to analyzing business processes is Business Activity Monitoring (BAM). BAM can provide real time analysis by monitoring ongoing computer operations that are tied to business processes. SOA provides a simplification towards business process monitoring by providing the follow advantages[27]:

- Flexible and economic integration approach
- Business process optimization through logical process modeling
- Not reliant on proprietary interfaces
- No need for an expensive message bus/broker
- Shorter timeframes for implementing

---

[24] Beware of Opportunistic Web Services Projects (Gartner, Inc. 2003); See http://www.weblayers.com/gcn/whitepapers/Introduction_to_SOA_Governance.pdf
[25] See http://blogs.zdnet.com/service-oriented/
[26] See http://webservices.sys-con.com/read/114125.htm
[27] Eric Pulier, Hugh Taylor, *Understanding Enterprise SOA,* ISBN 1-932394-59-1, (Connecticut, Manning, 2006), p 95.

However, as Eric Pulier and Hugh Taylor point out, using business process management to justify SOA can have its challenges. It can be very political because it involves turf. And business process management can be subjective. Therefore, proceed cautiously – ensuring the proper business knowledge and business process improvement expertise is employed.

> **CIO RECOMMENDATION:**
> *See services as assets that must be managed*

Recognize that services are organizational assets and they need to be managed over an inherent lifecycle. Like any other organizational asset, services will need to be created, purchased or leased. They will have a useful life with appropriate asset management.
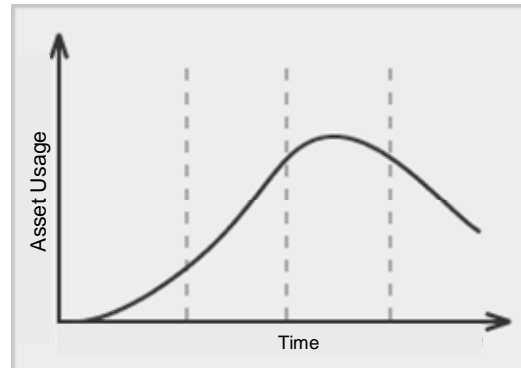
Services asset management should include a catalog of derived SOA assets that is accessible by developers and managers. The catalog should provide the capability to trace service assets including:

- What is the service?
- How can it be employed?
- Where is it located?
- What project or initiatives are currently using this service?
- What business processes are associated with this service?

"A good Asset Management strategy and supporting tool can therefore help make SOA related materials available and understandable throughout the organization."[28]

> **CIO RECOMMENDATION:**
> *Establish a security policy*

Security is a significant challenge when embarking on a SOA program. It can be anticipated that in most cases SOA implementation in the application and technical layers of architecture will involve web services (WS). The good news is that WS is easy to use, and is open. However, WS also opens state government to attack. iSEC Security Partners states, *"Like all good security, it really needs to be baked into the product by the engineers closest to the work."[29]*

Jeremy Bennett, Software Architect with Symantec states,

---

[28] See http://www.ebizq.net/topics/systems_management/features/5463.html
[29] See http://www.isecpartners.com/

"Today's web services are the modern generation's version of RPC/DCOM/CORBA. They have the same issues that the previous generation failed to solve with the added "benefit" of using HTTP as the common transport. Many enterprises have been trained to believe that the HTTP protocol must be allowed through the firewall and exempted from most filtering policy, because it's "business critical." Startups who have attempted to "secure web services" by moving the firewall up a layer and provide some sort of transactional control have come and gone. On the surface these are great ideas, until you begin to notice that not many of the interfaces or transactions are standardized and these solutions need to be customized for every deployment."

Authorization and authentication become critical elements when exposing applications and organizational information via web services. Establish a security policy within a federated services environment. As pointed out by Eric Pulier and Hugh Taylor, although security is a formidable challenge, the CIO shouldn't let that stop an SOA initiative – rather establish the appropriate SOA security policy. Part of the challenge is that in an SOA environment, security includes machine to machine interactions. Software pirates can emulate a friendly machine fairly easily.[30]

As services are exposed for reuse, there are additional risk management issues that must be addressed in advance.

Daniel Ingevaldson, Technology Strategy Director with Internet Security Systems states,

"SOA promises to deliver to the end-user unprecedented access to information via Web-based applications in ways that were simply not possible before. However, CIOs must understand that the advantages provided by SOA such as code reuse, interoperable services, and accelerated development also create new and challenging problems. The power of SOA, in that it can connect previously inaccessible sources of data directly to the Web with relative ease, also represents its greatest risk. A simple question such as, "Is username and password authentication enough?" takes on a new significance. It is important that risks associated with the rapid deployment of powerful new Web applications with SOA are both carefully evaluated and patiently addressed."
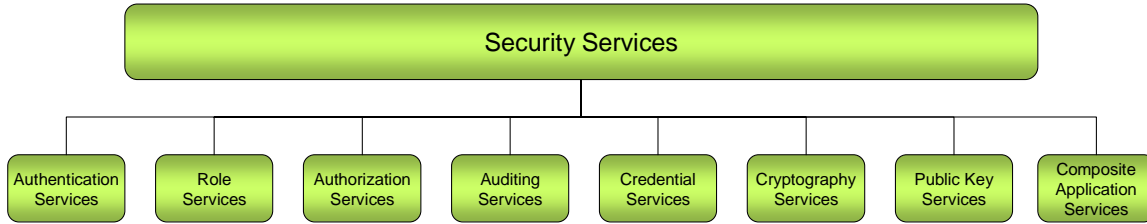
The goal regarding SOA security includes activities intended to disallow unauthorized access to web services; prohibit unwarranted listening, intercepting, and modification of messages; maintenance of the privacy and integrity of messages.

Shared services includes shared information. If information can be effectively shared, a possible result is a reduction in the volume of information that must be secured. If information is *stored once used many times* there is an improved ability to audit access. There is the potential to simplify the entire environment adding to the ability to more easily secure it.

---

[30] Eric Pulier, Hugh Taylor, *Understanding Enterprise SOA,* ISBN 1-932394-59-1, (Connecticut, Manning, 2006), Chapter 9

Interestingly, security and the various associated supportive concepts can themselves be treated as services. The components of security include:

```
                          ┌─────────────────────────────┐
                          │      Security Services       │
                          └─────────────────────────────┘
```

| Authentication Services | Role Services | Authorization Services | Auditing Services | Credential Services | Cryptography Services | Public Key Services | Composite Application Services |

The Open Web Application Security Project (OWASP) identified the top ten Most Critical Web Application Security Vulnerabilities. These are still top priorities.[31]

1	Un-validated Input	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
2	Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
3	Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
4	Cross Site Scripting (XSS) Flaws	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
5	Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.

---

[31] See http://www.owasp.org/documentation/topten.html

6	Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
7	Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
8	Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
9	Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
10	Insecure Configuration Management	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

IV. Summary

The following is a summary of recommendations coming from some of NASCIO's corporate partners that currently provide consulting services relative to SOA.

√ Make sure your business drivers match your ambition. Don't have the ambition to expand agency capability and a driver to lower IT cost.

√ Establish a verifiable business case for your SOA project(s) that includes operations cost reduction, potential new revenue streams, more effective business processes. But verify that the expectations are realized. If not fully realized, analyze for lessons learned so future projects will be more successful.

√ Don't tie SOA governance to a complex project. Keep the governance outside of any project to avoid SOA going down with a failed or troubled project.

√ When you set up governance for SOA, keep a distinction between the governance of the architecture, operations, and strategy - all have different viewpoints, responsibilities, and expectations.

√ Governance must ensure re-use of services. Without that focus, SOA will not realize its benefits.

√ Manage the culture change. Avoid the belief that SOA is nothing new. SOA *is* different from past processes.

√ New skills are needed. Developers need to learn more than just the wizards. Architecture teams, operations teams, and business teams all need training and new skills.

√ Match the services to the business organization. You must have a clear point of ownership for common services. Infrastructure must be owned by information technology. Services are owned by the appropriate business groups.

√ Don't equate SOA with web services. You can't just replace existing application program interfaces (APIs) with web services without a proper architecture. Services need to be business-aligned.

√ Don't rush into building a SOA. You must show value to business.
Develop a viable SOA transition plan and a defined SOA business
case.

√ Develop a roadmap for proper introduction of technology in support
of the business and have the business-side of the organization
support it.

√ Apply good service modeling to create your services. Your goal is
component reuse.

√ Establish an SOA lab to develop the end-to-end SOA ecosystem,
realize the governance in an infrastructure, establish best practices,
and develop patterns.

√ Communicate, communicate, communicate. Use an internal website,
blogs, and discussion boards.

√ Understand the organizational forces that are pushing for SOA
adoption and the forces resisting the adoption. Determine the level
of risk to the SOA adoption. Make plans to overcome the resistance.

√ Make sure total environment is ready to accept SOA:
  - *Management is committed*
  - *Funding*
  - *IT environment is ready*
  - *Technical staff willing to learn and use SOA*
  - *Acceptable and realistic ROI*
  - *IT and business organizations are in agreement and
    working together.*

Contributors:

Jeremy Bennett World Headquarters Symantec Corporation 20330 Stevens Creek Blvd. Cupertino, CA 95014 jbennett@symantec.com (408) 517-8000	Lewis Carr Director, Public Sector Marketing BEA Systems, Inc. Corporate Office, USA 2315 North First Street San Jose, CA 9513 lcarr@bea.com (408) 570-8180
Pam Carr Symantec Corporation National Business Development State & Local Govt, Academic, and Healthcare 4820 Carondelet St New Orleans, LA 70115 pcarr@symantec.com (504) 202-0067	Chris Dunlap SOA Sales Strategist BEA Systems, Inc. 700 State Highway 121 ByPass Suite 100 Lewisville, TX 75067 cdunlap@bea.com (469) 528-4815
Lauren Farese Senior Manager, Sales Consulting Oracle Corporation P.O. Box 139 Hamptom, NJ 08827 lauren.farese@oracle.com (908) 612-1434	Randy Hughes State Technical Architect CIO Office Department of Technology Services 6000 State Office Bldg SLC, UT 84114 randyhughes@utah.gov (801) 537-9071
Katie Ignaszewski Director Government Affairs Internet Security Systems Inc 12950 Worldgate Dr Ste 100 Herndon, VA 20170 kignaszewski@iss.net (703) 456-9106	Daniel Ingevaldson Director, Technology Strategy Internet Security Systems Inc 6303 Barfield Road Atlanta, GA 30328 dsi@iss.net 404-236-3160
Robert Jansen Area Sales Manager - Public Sector Business Interaction Division 3460 Preston Ridge Road Suite 225 Alpharetta, GA 30005 robert.jansen@bea.com (404) 467-422	Drew Mashburn Chief Enterprise Architect Arkansas Office of the Executive CIO 124 W. Capitol - Suite 990 Little Rock, AR 72201-3709 drew.mashburn@arkansas.gov (501) 682-5256

Stephen Newell IT Architect IBM 2401 W Jefferson St Springfield, IL 62702-3495 srnewel@us.ibm.com (217) 793-5825	Doug Robinson Executive Director NASCIO 201 East Main St., Suite 1405 Lexington, KY 40507 drobinson@AMRms.com (859) 514-9153
Mike Spillers Marketing Manager, Americas Sales Internet Security Systems 6303 Barfield Road Atlanta, GA 30328 mspillers@iss.net 404-236-2750	Chris Walls Senior Website & Publications Coordinator AMR Management Services 201 E. Main St., Suite 1405 Lexington, KY 40507 (859) 514-9174 cwalls@AMRms.com

Resources:

NASCIO *www.nascio.org*	*Enterprise Architecture: The Path to Government Transformation* *http://www.nascio.org/nascioCommittees/EA/* *Calendar of scheduled webinars on SOA from NASCIO Corporate Partners* *http://www.nascio.org/nascioCommittees/clc/webinarForm.cfm* *Archived NASCIO webinars on SOA* *http://www.nascio.org/nascioCommittees/EA/webinars06/webinar06Archive.cfm* *Call for Action, A Blueprint for Better Government: The Information Sharing Imperative* *http://www.nascio.org/washwatch/NASCIOww/calls_for_action.cfm* *Catalog of Collaborative Information Exchange* *http://www.nascio.org/nascioCommittees/EA/catalog/* *Washington Watch* *http://www.nascio.org/washwatch/index.cfm*

	PERSPECTIVES: Government Information Sharing Calls to Action *http://www.nascio.org/publications/index.cfm#perspectives* *In Hot Pursuit: Achieving Interoperability Through XML* *http://www.nascio.org/publications/index.cfm#xml* *We Need to Talk: Governance Models to Advance Communications Interoperability* *http://www.nascio.org/nascioCommittees/interoperability/Interop.%20Gov.%20Research%20Brief%20Final.pdf* *A National Framework for Collaborative Information Exchange: What is NIEM?* *http://www.nascio.org/nascioCommittees/EA/#niem* *List of NASCIO Corporate Partners* *http://www.nascio.org/aboutNascio/corpProfiles/* *List of NASCIO Publications* *http://www.nascio.org/publications/index.cfm* *List of NASCIO Committees* *http://www.nascio.org/nascioCommittees/index.cfm*
Department of Justice, Office of Justice Programs	*DOJ's Global Justice Information Initiative GJXDM Knowledge Base and Help Desk* *http://www.it.ojp.gov/gjxdm/helpdesk/* *Global Justice Information Sharing Initiative* *http://it.ojp.gov/topic.jsp?topic_id=8* *A Framework for Justice Information Sharing: Service-Oriented Architecture (SOA)* *https://it.ojp.gov/documents/20041209_SOA_Report.pdf* *Additional Global reports related to SOA* *http://it.ojp.gov/index_results.jsp?start=0&count=10&words=SOA&order=date*
State Government websites	*NASCIO State Profiles* *http://www.nascio.org/aboutNascio/profiles/* *State of California Enterprise Architecture* *http://www.cio.ca.gov/ITCouncil/Committees/ArchStandards.html*

	• *SOA (Service Oriented Architecture) Details (updated 4/20/2006)* *http://www.cio.ca.gov/ITCouncil/Committees/PDFs/SOA_ Details_2006-04-21.pdf* • *SOA Presentation (updated 3/29/2006)* *http://www.cio.ca.gov/ITCouncil/Committees/PDFs/SOA_ Presentation_2006-03-29.pdf*
The IJIS Institute	*IJIS Institute Technology Assistance Program – Guidelines for Technology Assistance* *http://www.ijis.org/traction/read?proj=Public&sdate=20060 214&edate=all&type=single&rec=25&side=1* *Information Exchange Package Documentation Guidelines V1.1* *http://www.ijis.org/traction/read?proj=XMLComm&sdate=2 0060214&edate=all&type=single&rec=130&side=1*
Center for Technology in Government	*Service Oriented Architecture: Making Collaborative Government Work* *http://www.centerdigitalgov.com/center/fileReg.php*
SOA Related Web sites	*SOA Pipeline http://www.soa-pipeline.com/* *Enterprise Decision Management* *http://edmblog.fairisaac.com/weblog/2005/11/soa_business_i n.html* *SOA Web Services http://webservices.sys- con.com/read/category/1153.htm* *Executive Digital Dashboards http://webservices.sys- con.com/read/114125.htm* *BEA Systems – SOA Building Blocks* *http://www.bea.com/content/files/solutions/resource/soa/BEA _buildblock_SOA_success.pdf* *Institute For Enterprise Architecture Developments* *http://www.enterprise-architecture.info/EA_Services- Oriented-Enterprise.htm (See this site for many other aspects of EA as well as SOA)*

Reports	*OASIS SOA Reference Model:* *http://www.oasis- open.org/committees/tc_home.php?wg_abbrev=soa-rm*

	Forrester Reports • *Integration In A Service-Oriented World by Ken Vollmer and Mike Gilpin* *Gartner* • *A number of reports and podcasts available, subscription required* • *"Guidelines for Implementing Service Oriented Architectures in Government" by Greg Kreizman, March 2005*

Books	Understanding Enterprise SOA by Eric Pulier, Hugh Taylor, ISBN 1-932394-59-1, (Connecticut, Manning, 2006), orders@manning.com, 242 pages Service-Oriented Architecture : A Field Guide to Integrating XML and Web Services by Thomas Erl, ISBN 0-13-142898-5 , (New Jersey, Prentice-Hall, Pearson Education, 2005), www.phptr.com, 534 pages Service-Oriented Architecture : Concepts, Technology, and Design by Thomas Erl, ISBN 0-13-185858-0, (New Jersey, Prentice-Hall, Pearson Education, 2005), www.phptr.com, 760 pages Enterprise SOA: Service-Oriented Architecture Best Practices by Dirk Krafzig, Karl Banke, Dirk Slama, ISBN 0-13-146575-9, (New Jersey, Pearson Education, 2005), www.phptr.com, 382 pages

This report and the NASCIO Enterprise
Architecture Program are funded by a grant
from the Bureau of Justice Assistance, Office
of Justice Programs, U.S. Department of
Justice.

The opinions, findings, conclusions, and
recommendations contained in this publication
are those of the contributors, and do
not necessarily reflect the official positions
or policies of the Department of Justice.

Disclaimer

NASCIO makes no endorsement, express or implied, of any products, services, or websites contained herein, nor is NASCIO
responsible for the content or the activities of any linked websites. Any questions should be directed to the administrators of the
specific sites to which this publication provides links. All critical information should be independently verified.