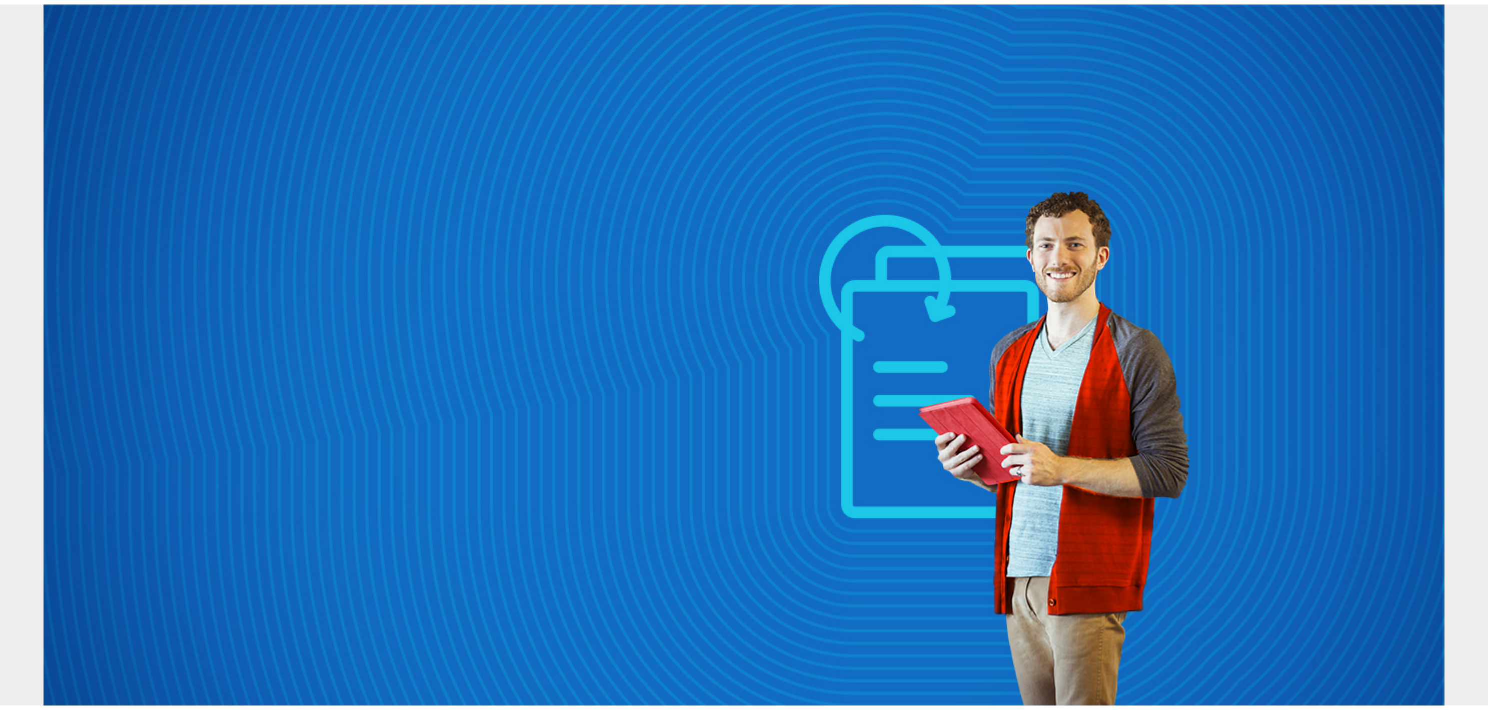
SOA COMPLIANCE



What is SOA?

SOA stands for service-oriented architecture, and it is an architecture that allows organizations to use services to achieve IT goals. Systems are designed over a network using a communications protocol, and using SOA as a framework can greatly simplify a variety of processes and reduce the costs of doing business. Additionally, SOA can make it easier for organizations to adhere to government regulations and meet service level agreements.

SOA allows organizations to create a framework that works for their needs. As with other IT architectures, there is no set way of doing things, just a guide for figuring out how to do them. The thing that sets SOA apart from other architectures is that it involves making services work together within programs and processes to create a framework. There are several definitions, but, generally speaking, a service is a self-contained unit that provides a function, such as handling currency exchanges or collecting data put in by a user.

Working together, services can be combined to make larger applications function, and they are able to share data across computers and systems. Services can share data between each other automatically, so they are able to be used by a wide variety of users and programs. Using the same set of services in a large number of programs can represent an enormous savings in terms of time and development efforts for an organization.

SOA compliance involves following processes put in place by the organization that created the framework, and compliance with SOA can allow businesses to also be in compliance with government regulations. For instance, if a law requires businesses to maintain a change log that is updated whenever a particular file is modified, the business can set their SOA framework up to require that a service perform this task. By complying with the SOA, the business will also be complying with the government regulation.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Who uses SOA?

Large businesses and the government tend to be the most common users of SOA, and this is often due to the need to both follow a variety of regulations and share data across a wide range of users and systems. Initially, businesses were the first to take advantage of SOA, but in the last decade or so, the government has made a concerted effort to use SOA in both state and federal systems.

As mentioned, one of the strong points of SOA is that it uses services to create functionality. Government entities are required to share vast amounts of data with other entities on a regular basis. Take state licensing systems. Even within the same state, there are several offices that are responsible for different tasks but need the same data to accomplish them. Counties will often handle data gathering and distribution of driver's licenses, but state offices are normally the ones that revoke people's driving privileges.

Without a framework like SOA, each county may have its own program that collects and stores data about citizens and their driving records, and the state may have yet another. This can create enormous amounts of redundancy and problems getting databases to communicate properly. However, with SOA, all involved organizations can use the same services to collect, maintain and access data.

Businesses with a variety of locations and divisions benefit from SOA for many of the same reasons. Data sharing is often much simpler since it is coming from the same services and programs instead of being patch-worked together. This also means that if there are problems, it's easy to determine where they are coming from. Maintaining security and handling upgrades are also less challenging when applications are using the same services.

Businesses frequently make use of SOA to follow guidelines put in place either by the business itself or the government. There are numerous IT regulations that different industries must follow, and there are not architectures for many of them. The health care industry, for example, has to follow a range of rules and requirements for handling medical records.

SOA allows businesses to create a framework with security measures and data protections built in, which can make the process of proving compliance with government standards much easier. Businesses are able to provide their framework to auditors and then demonstrate that they are following the framework they set up. Reporting mechanisms can be made a part of the architecture, making the compliance process a relatively simple and transparent one.

Implementing SOA

While there are a number of benefits to using SOA to create a framework for an organization, there is a variety of potential pitfalls as well. For SOA to work effectively, it requires discipline in implementation, and usage. While the architecture is one that can be applied in a slow and progressive manner (one service at a time), it is not one that will work properly if it is used piecemeal. If the goal is not to eventually end up with a system that complies with SOA architecture, the result is usually a mishmash of services and programs that don't fit together well or live up to expectations.

The majority of businesses and organizations that are currently adopting SOA are ones that already have a framework in place. There are few cases where an organization can completely eliminate their current framework and start from scratch, so SOA adoption is almost always a transition, with the exception being new organizations that have nothing in place.

As with most architectures, it is necessary to establish what an organization needs to accomplish. From there, it's a matter of determining which functions are a priority and accomplishing goals and integrations in a set order. In cases where a business has an established and functioning framework, the analysis may be focused on determining where the most overlap is and then prioritizing the creation of services that can be used the largest number of applications.

SOA components

SOA is mostly built on a variety of parts that allow services to work together. Some of the major components that SOA relies upon are:

Service Oriented Enterprise (SOE): The SOE lists the processes and procedures that are used to create and maintain the SOA. This also frequently includes the names of the individuals who make the rules for running a SOA and who is responsible for ensuring that goals are met.

Service Oriented Infrastructure (SOI): This is the environment that the services run on. The environment is responsible for ensuring that services are able to connect and communicate properly. In a very general sense, the SOI can be likened to an operating system for services and processes to run on.

Service registry: This is a critical part of the SOA in that it lists all services that are available. It includes information about what they do and how they can be used via service metadata. A service registry prevents redundancy and makes it easier to determine which processes need to be built.

Business processes: These are what allow services to function together to complete tasks. An example of a business process is when customers are emailed a monthly statement. One service collects customer data, another service pulls an individual's transactions for the last 30 days and yet another service sends out the automated emails; a business process is what makes them all work together.

Master data management (MDM) hub: An MDM hub is used to take information and data from a variety of sources and standardize how it is stored and accessed. There are several ways that MDM hubs can be set up, but their goal is to eliminate duplicate data, provide formatting standards and ensure that data is accurate and accessible by services that need to use it.

Data management: Handling and sharing data are easier with services that limit the number of input sources, but a robust data management plan is still a necessary part of SOA. In addition to the fact that a variety of services may be used to collect different types of data, data may also be coming from outside of an organization. As such, data management is used to create policies for handling, tracking and securing data.

Enterprise service bus (ESB): The ESB allows services in a framework to communicate with each other across different applications and processes. It is frequently used by the MDM hub to access data and messages from applications, so it is a system that enables communication, not one that manages data.

SOA compliance

Adhering to SOA governance is a way of ensuring that an organization's systems continue to work properly, and doing so can be a start of verifying compliance to legal regulations. It is also often used as a way of demonstrating that information is secure, something that may be important to users and stakeholders or investors.

An SOA audit will mean different things for different organizations depending on what their goals are. However, common topics include ensuring that security protocols are in place and that services are created and managed properly. Audits will normally rely on reporting to verify that systems are working correctly, and they may also include ensuring that a framework is addressing the needs and obligations of an organization.

Although security is often easier to establish with an SOA framework because there are often fewer working parts, that doesn't mean it's not a major concern. SOA still requires that organizations put user authentications in place across applications and environments as well as ensure that services and applications are not easily accessed by unauthorized parties.

Reporting systems are also essential to providing an organization with information about how well a framework is performing. Quality of service and error reporting are key to verifying that services are working quickly and without problems, and they may also help to prove that SLAs are being met. Reporting helps an organization determine if and where there are problems as well as demonstrating to outside parties that a framework and organization are doing their jobs properly.

Coupled with the importance of reporting is going over requirements for a system on a regular basis and ensuring that they are being tracked and met. The government frequently refines or clarifies regulations that organizations must meet, so SOA governance will need to be updated to reflect these changes. Additionally, requirements or obligations for an organization may change based on new SLAs or expectations from stakeholders. An SOA will not remain viable if it is not being updated to address the needs of an organization.

Service creation and management are another critical part of SOA governance because they are issues that are at the heart of the architecture. If services are not managed properly, it defeats the purpose of using SOA to create a framework. It is crucial that services are created and made available in such a way that there is as little redundancy as possible. Services should also be reused rather than having new ones created, and to help this process, documentation and information about services should be readily available and robust.

Services must also be properly maintained and monitored to ensure that they are able to meet user demands. When there are a large number of users involved, scalability can turn into a problem that results in errors, slow response times, corrupted data and failure to meet SLAs or government regulations.

A major part of ensuring that SOA governance requirements are being met is having specific guidelines and processes for creating services, ensuring interoperability and maintaining the framework, and specific people need to be named as responsible for making this happen. Without having named individuals in charge of making choices, it can be difficult for companies to make changes that are needed to address problems or make needed alterations to their SOA framework and governance.

As with other architectures, complying with procedures and ensuring that objectives are being met is an ongoing process. In addition to the fact that networks and systems are constantly changing, creating nearly endless opportunities for things to go wrong, business obligations are also frequently in flux. New innovations, requests from users and the ever present issues of security prevent organizations from ever being done with ensuring compliance with SOA.