# Introduction

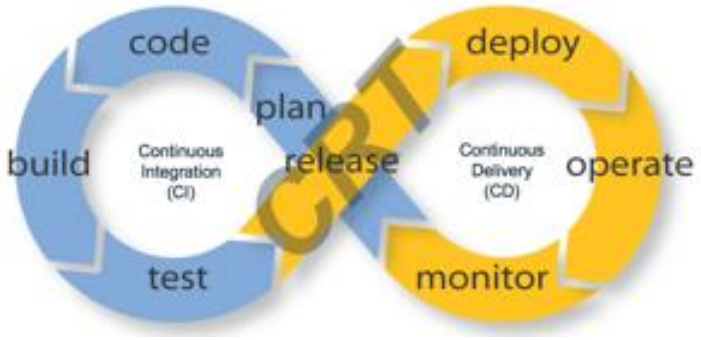
The AWS Security Automation and Orchestration (SAO) program and methodology enables AWS customers and partners to constrain, track and publish continuous risk treatments (CRT), configurations and assimilates DevOps routines (e.g. **continuous integration** (**CI**) and **continuous delivery** (**CD**)) into a "Type Accredited"[1] secure AWS architecture. This architecture is configured to converge across common security frameworks (e.g. FedRAMP, PCI-DSS, DoD SRG, CJIS, HIPPA, and others) through the use of security as code practices.

The goal of AWS SAO it to exchange existing manual configurations of systems and services with automated and auditable Security as Code practices. AWS SAO will also align comprehensive DevOps orchestrations by automating simple to complex tasks such as securing systems configuration, patching and validations of service alignment to a stated security perimeter and/or ATO requirements. Within AWS SAO, orchestration is the connective layer which streamlines security processes. It also powers security automation for organizations to easily implement modern defense-in-depth capabilities based on their internal and external requirements.

With AWS SAO, organizations can rely on their technology deployment to not only provide a trusted operational environment, but also ensure that any security tools and technologies leveraged can also be dependable as user, systems and service change operationally.

The results will create a real-time risk management capability in alignment with DevOPS CI/CD processes to maintain operational certification and accreditation (e.g. ATO) know as Continuous Risk Treatment (CRT). CRT is a modernized continuous monitoring process and technology approached which is designed to detect, maintain and in selected cases correct security and compliance deviations and threats associated with an organization's solution and service deployment within their operational cloud environment as new security requirements or cyber threats emerge.

CRT processes monitor security controls in real-time to ensure the risk and/or threat treatment (Control Intent) is working as designed or at least within an intended margin of acceptance base on "guard rails" or configuration rules built into the control to allow for business operations. Through continuous risk treatments of the operational security controls, design changes and/or improperly implemented security controls can be adjusted and/or replaced as part of an organization's continuous delivery and integration processes. The result is an enhanced risk management capability which can monitor, react to and remediate operational security risk automatically.




[1] A form of accreditation which is used to authorize multiple instances of a system in approved locations with the same type of computing environment. A type accreditation will satisfy **Certification and Accreditation (C&A)** requirements by using a repeatable configuration approach for integrations, deployments and risk treatments which are pre-tested, validated and documented against common security frameworks.

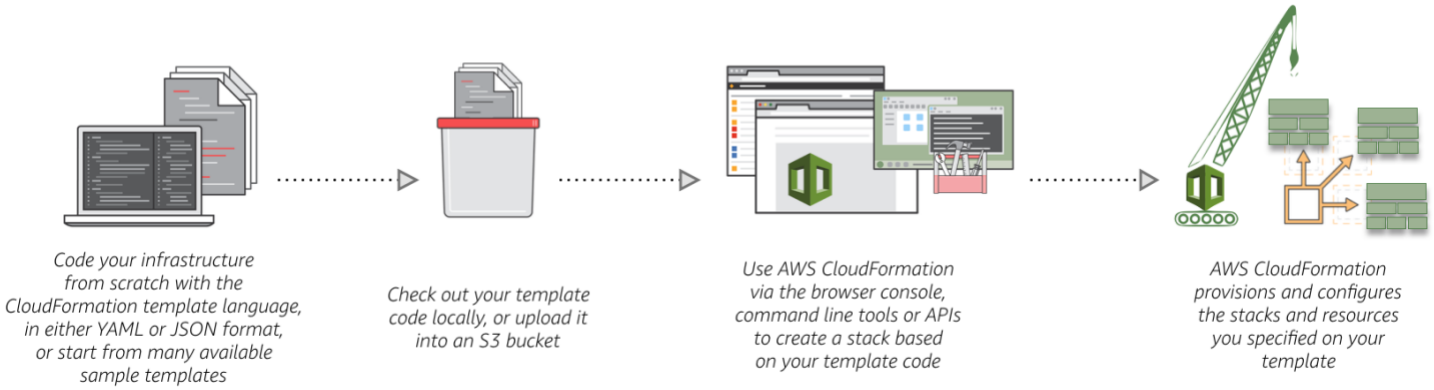
## Understanding Automated Compliance

AWS allows for rule-based, automated compliance. When you are creating infrastructure for a particular project or campaign, you can create reusable templates that provide a consistent environment for development, testing, production, and validation activities. Once deployed, AWS has tools to continually test, monitor, and log events that occur. You can use these tools to rapidly detect deviations from enterprise policy and sound alarms when deviations occur.

## How Automation works in AWS

AWS CloudFormation provisions your resources in a safe, repeatable manner, allowing you to build and rebuild your infrastructure and applications, without having to perform manual actions or write custom scripts. CloudFormation takes care of determining the right operations to perform when managing your stack, and rolls back changes automatically if errors are detected.

By provisioning, configuring, and managing your AWS infrastructure resources using code and templates, you are able to monitor and enforce infrastructure compliance. AWS CloudFormation give organization an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. You can use AWS CloudFormation's sample templates or create your own templates.




## Bringing DevOps and Security together to form AWS SAO

Transitioning to DevOps requires a change in culture and mindset. At its simplest, DevOps is about removing the barriers between traditionally siloed teams; development, operations and security. In some organizations, there may not even be separate development, operations and security teams; engineers may do both. With DevOps, the two disciplines work together to optimize both the productivity of developers and the reliability of operations.

The alignment of development and operations teams has made it possible to build customized software and business functions quicker than before, but security teams continue to be left out of the DevOps conversation. In a lot of organizations, security is still viewed as or operates as roadblocks to rapid development or operational implementations, slowing down production code pushes. As a result, security processes are ignored or missed as the DevOps teams view them as a road block toward their pending success. As part of your organization strategy towards a security, automated and orchestrated cloud deployment and operations and you will need to unite the DevOPS and SecOps teams in an effort to fully support and operationalize your organizations cloud operations. Below are the DevOPS and Security practices which make up AWS SAO:

### Continuous Integration (CI)

Continuous Integration is a software development practice where developers regularly merge their code changes into a central repository, after which automated builds and tests are run. The key goals of continuous integration are to find and address bugs quicker, improve software quality, and reduce the time it takes to validate and release new software updates.

## Continuous Delivery (CD)

Continuous Delivery is a software development practice where code changes are automatically built, tested, and prepared for a release to production. It expands upon continuous integration by deploying all code changes to a testing environment and/or a production environment after the build stage. When continuous delivery is implemented properly, developers will always have a deployment-ready build artifact that has passed through a standardized test process.

## Continuous Risk Treatment (CRT)

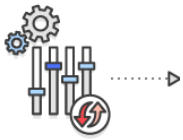
Continuous Risk Treatment is a modernized continuous monitoring process and technology approached which is designed to detect, maintain and in selected cases correct security, compliance and threats associated with an organization's solution and service deployment within their operational cloud environment as new needs or cyberthreats emerge.

## Microservices

The Microservices architecture is a design approach to build a single application as a set of small services. Each service runs in its own process and communicates with other services through a well-defined interface using a lightweight mechanism, typically an HTTP-based application programming interface (API). Microservices are built around business capabilities; each service is scoped to a single purpose. You can use different frameworks or programming languages to write microservices and deploy them independently, as a single service, or as a group of services.

## Infrastructure as Code

Infrastructure as Code is a practice in which infrastructure is provisioned and managed using code and software development techniques, such as version control and continuous integration. The cloud's API-driven model enables developers and system administrators to interact with infrastructure programmatically, and at scale, instead of needing to manually set up and configure resources. Thus, engineers can interface with infrastructure using code-based tools and treat infrastructure in a manner similar to how they treat application code. Because they are defined by code, infrastructure and servers can quickly be deployed using standardized patterns, updated with the latest patches and versions, or duplicated in repeatable ways.



## Configuration Management

Developers and system administrators use code to automate operating system and host configuration, operational tasks, and more. The use of code makes configuration changes repeatable and standardized. It frees developers and systems administrators from manually configuring operating systems, system applications, or server software.

## Policy as Code

With infrastructure and its configuration codified with the cloud, organizations can monitor and enforce compliance dynamically and at scale. Infrastructure that is described by code can thus be tracked, validated, and reconfigured in an automated way. This makes it easier for organizations to govern changes over resources and ensure that security measures are properly enforced in a distributed manner (e.g. information security or compliance with FedRAMP, PCI-DSS or HIPAA). This allows teams within an organization to move at higher velocity since non-compliant resources can be automatically flagged for further investigation or even automatically brought back into compliance.

## Compliance as code

AWS and Amazon Partners allows you to codify your compliance with custom rules in AWS Lambda that define your internal best practices and guidelines for resource configurations. Using AWS SAO resources, you can automate assessment of your resource configurations and resource changes to ensure continuous compliance and self-governance across your AWS infrastructure.

## Continuous audit and compliance

AWS SAO is designed to help you assess compliance with your internal policies and regulatory standards by providing you visibility into the configuration of your AWS resources, and evaluating resource configuration changes against your desired configurations continuously through the integration AWS services and Amazon Partner Network solutions.

# How SAO works

AWS provides several security capabilities and services to increase security and control network access. Our approach is to leverage automation as a force-multiplier for organizations which are operating leaner and need to be more responsive to new lines of business, while maintaining more complex infrastructure with the same (or fewer) staff.

The program includes support, guidance, and resources for ISVs who aspire to obtain an ATO on AWS of targeted compliance frameworks for solutions running on AWS. The focus is on helping customers, independent software vendors (ISVs) and partners, significantly accelerate the process and reduce costs of obtaining an ATO under required compliance frameworks. The result, increased speed to market, which enables more customers while accelerating the process of getting a compliance certification. This is all accomplished while maintaining security across the operational system.