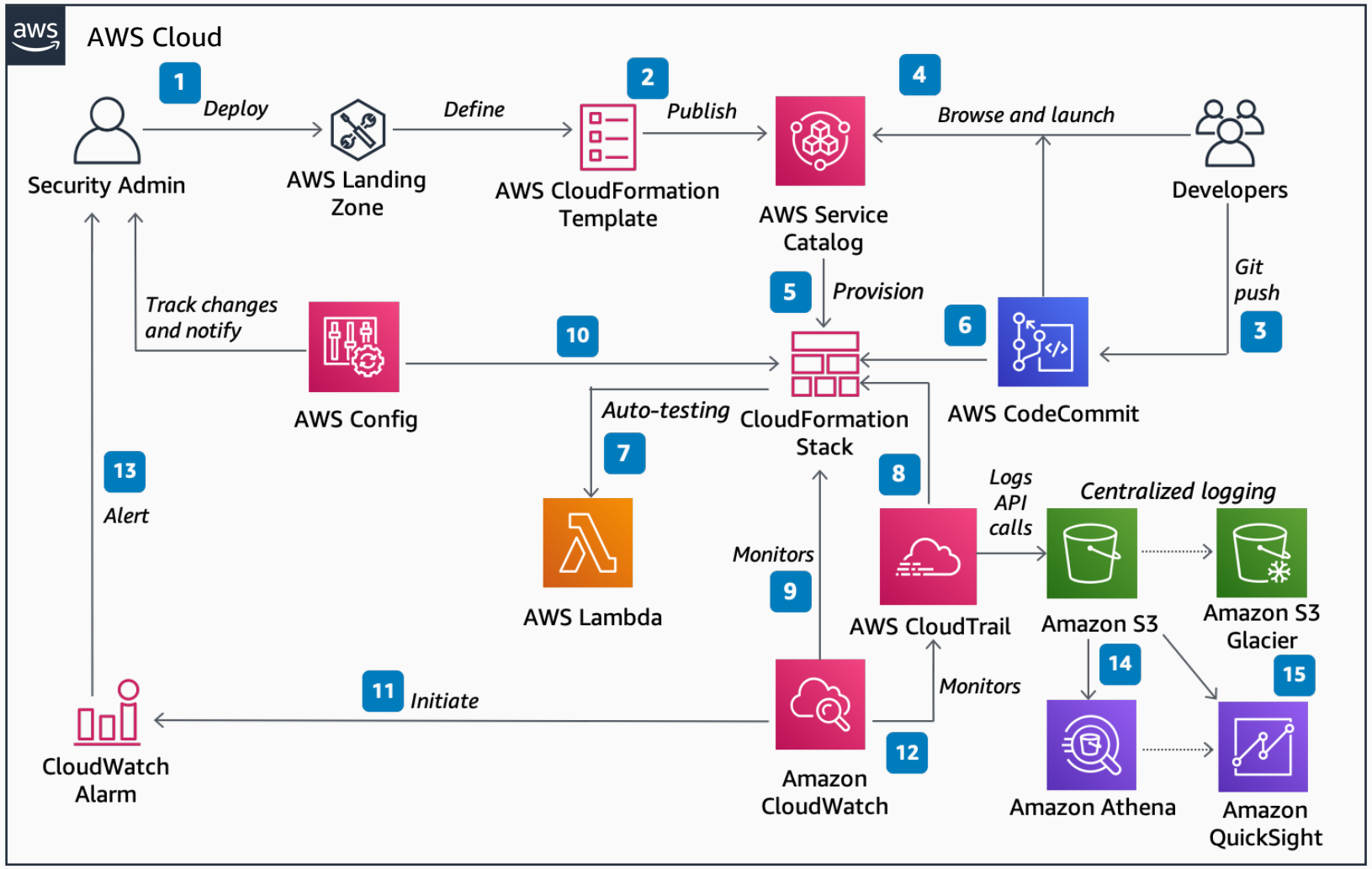
GxP Compliance Automation

Building a Secure and Compliant GxP Workload on AWS



1 **AWS Landing Zone** allows the security administrator to automate the set-up of an environment for running secure and scalable workloads. Security admin defines an **AWS Service Catalog** product (for example, a GxP application) using **AWS CloudFormation** templates.

2 Security admin publishes the template for developers in the **AWS Service Catalog**. Developers use this framework to further enhance the template based upon the application requirements.

3 Developers take the framework and modify applications to further enhance it under **Git** source control and use **AWS CodeCommit** to fully manage the private code repository.

4 Developer deploys the modified code from **CodeCommit** to their GxP infrastructure, using **AWS Service Catalog** to launch the product they need as an **AWS CloudFormation stack**.

5 The stack automatically provisions the necessary AWS resources based on what has been committed to the code repository as specified by the developer.

6 **AWS Service Catalog** is at the center of this architecture, so developers can release their source code without needing to access to any underlying resources or go through security administrators.

7 Automate the testing/Installation qualification process using **AWS Lambda** or Python program and create a test summary/ qualification report automatically in an **Amazon S3** bucket .

8 All individual CloudTrail logs, VPC flow logs, and **AWS Config** changes are aggregated into a centralized S3 bucket in a separate AWS account.

9 The security administrator configures, monitors, and sets up automated alerts on changes and on the health of the stack via **Amazon CloudWatch**.

10 When the stack is changed, change events are recorded and tracked through AWS Config. Out of compliance events are displayed in dashboard.

11 To indicate that something may be out of compliance, **CloudWatch** can initiate alarms based on rules that you design.

12/13 **CloudTrail** monitors API calls made against the AWS environment. The administrator is notified/alerted by **CloudWatch Events** when something changes that could cause the system to be non-compliant.

14/15 Log Data is queried and converted into a human readable format like CSV using **Amazon Athena**, for any audit purpose. Visualize **CloudTrail Logs** using **Amazon QuickSight**.

AWS Reference Architecture