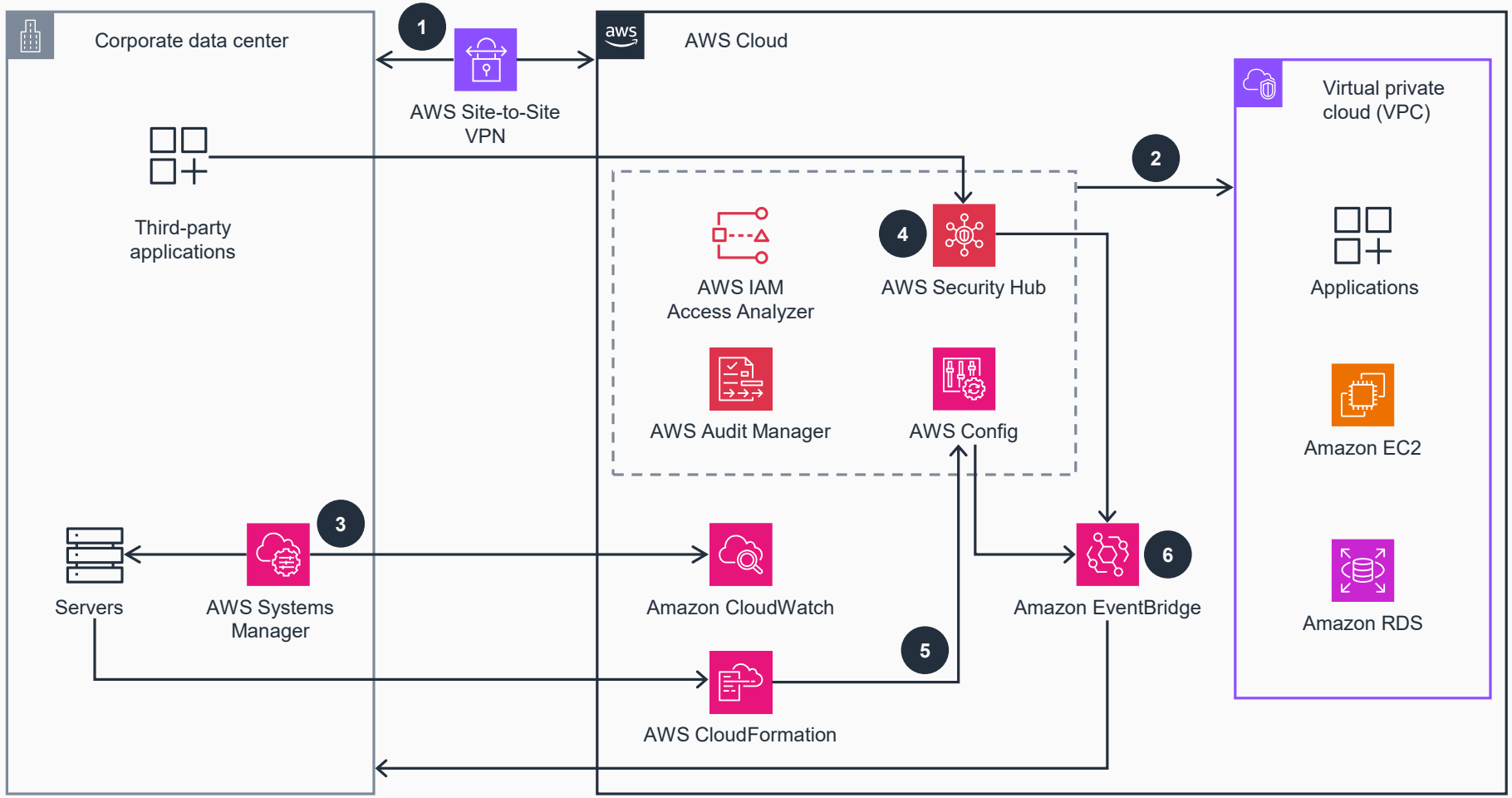
Guidance for Credit Unions to Evaluate FFIEC Compliance on AWS

This architecture diagram shows how nonprofit financial services organizations can evaluate their Federal Financial Institutions Examination Council (FFIEC) workloads on AWS.



1. Use an **AWS Site-to-Site VPN** connection for secure communication between the on-premises corporate data center and AWS.

2. **AWS IAM Access Analyzer**, **AWS Audit Manager**, **AWS Security Hub**, and **AWS Config** are applied to the AWS cloud environment. These services evaluate compliance standards for applications running on services hosted on AWS like **Amazon Elastic Compute Cloud (Amazon EC2)** and **Amazon Relational Database Service (Amazon RDS)**. **IAM Access Analyzer** helps identify external access to AWS resources and validates permission policies. **Audit Manager** automates evidence collection by running framework assessments against AWS resources. **Security Hub** and **AWS Config** help assess whether resources adhere to compliance best practices.

3. To evaluate on-premises environments, install an **AWS Systems Manager** agent on the on-premises servers to collect logs, which are stored in **Amazon CloudWatch**.

4. **Security Hub** integrates with third-party products and aggregates security findings for centralized viewing.

5. **AWS CloudFormation** registers the on-premises servers as custom resources in AWS. **AWS Config** rules and conformance packs can then be applied.

6. **Amazon EventBridge** invokes a custom action to manage the configuration of on-premises servers and remediate any security risks that **Security Hub** and **AWS Config** find.

Reviewed for technical accuracy September 22, 2023

AWS Reference Architecture