TREND MICRO

EBOOK

Banking on Cloud Governance

How financial services organizations can design and implement cloud management and governance solutions to accelerate cloud adoption

aws partner network

Table of contents

A governance framework to propel your cloud journey

Cloud technology has transformed the financial services industry (FSI). From improved customer engagement solutions, enhanced risk modeling, and agile infrastructure, cloud services have enabled FSI organizations to differentiate and adapt to a changing market. While many of these companies have begun to adopt cloud technologies, those with strong governance controls in place have been able to accelerate their migration journeys.

If you're going to migrate, do it well.

Cloud governance ensures people, processes, and technology work together to achieve the best outcomes from cloud services. Governance should not simply be in response to a complex regulatory environment or security challenges—it should make good business sense.

Without robust cloud governance, FSI teams may lack the roadmap to navigate the complexity of new services and solutions added to their technology stacks. Tasks like onboarding, monitoring, and evidence collection should stick to a formalized approach so they are addressed completely and consistently.

A solid cloud governance framework encompasses three main areas:

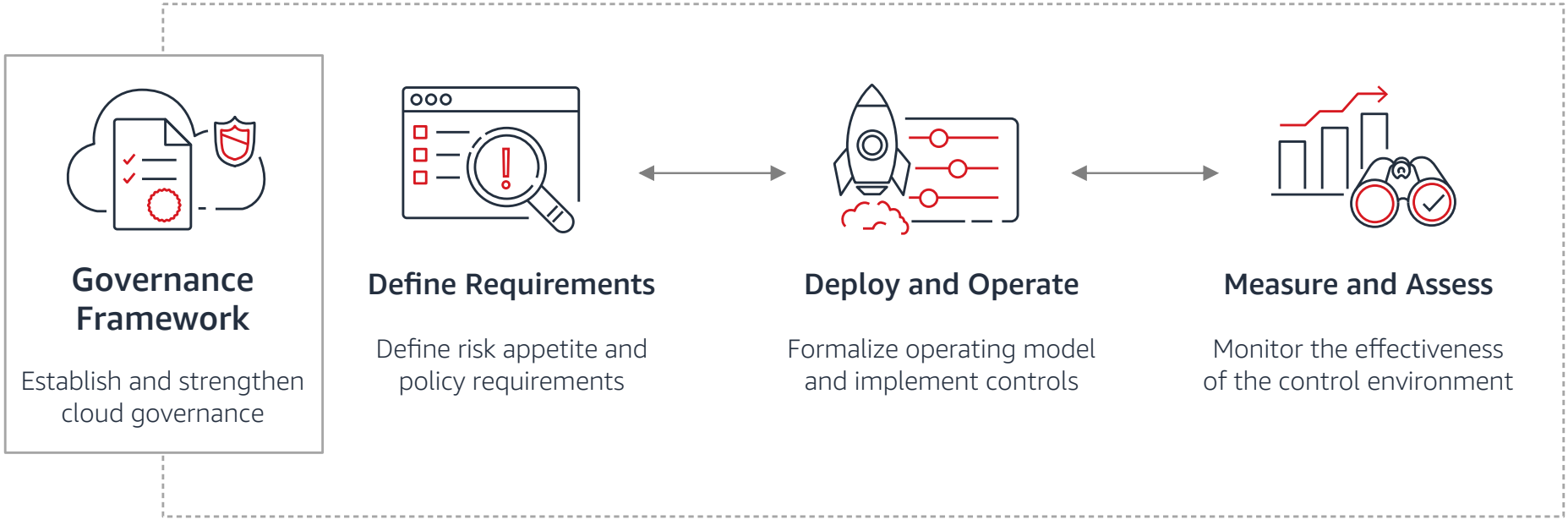
- **People**—formalize your organizational structure to support cloud migration and operation
- **Processes**—determine best practices to design and engineer security controls and guardrails
- **Technology**—establish a streamlined assessment process for adoption and onboarding of new cloud services

Cloud governance is foundational to your organization. It ensures technology investments are sustainable and that they propel strategic objectives forward.

AWS approach to cloud governance

The AWS approach to cloud governance is an actionable framework designed for FSI organizations to improve their control implementation and operation, as well as assessment practices that validate control effectiveness.

Together, Amazon Web Services (AWS) and Trend Micro can help you enhance your cloud governance for more successful cloud adoption.



Define requirements

Cloud migration offers the opportunity to evolve your organization's management and governance processes. You will benefit from proactively validating requirements and obligations to optimize for the cloud.

You know you're in trouble when...

- Your organization lacks a cloud migration strategy
- There is no point-person responsible for cloud governance
- Your risk and compliance teams are not engaged in defining the requirements for your cloud migration

> According to Gartner, NIST CSF will be **used by 50%** of US private sector organizations by 2020[1]

Define risk appetite and policy requirements

Simply operating in a highly regulated industry means FSI organizations are obligated to maintain strict oversight of their technology environments, identify risks, and assess the effectiveness of their risk management strategies. However, in many cases, companies have internal policies and processes that are not optimized for cloud computing, making it extremely difficult to determine whether existing controls will satisfy internal and regulatory expectations.

By redefining development, operational, and oversight processes as part of your AWS migration, you can lay the groundwork for ongoing evidence of sound governance.

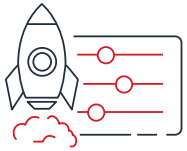
Leverage solutions that align with the NIST framework

The NIST Cybersecurity Framework (CSF) provides a foundation for cloud security and an accelerated path to cloud adoption. AWS and Trend Micro utilize this foundation to build solutions that support the five risk management functions: identify, protect, detect, respond, and recover.

NIST FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities	Develop and implement appropriate safeguards to ensure delivery of critical services	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

[1] NIST, Cybersecurity framework



Deploy and operate

The most effective control environment is one that encompasses a combination of directive, preventative, detective, and responsive security measures that mitigate identified risks.

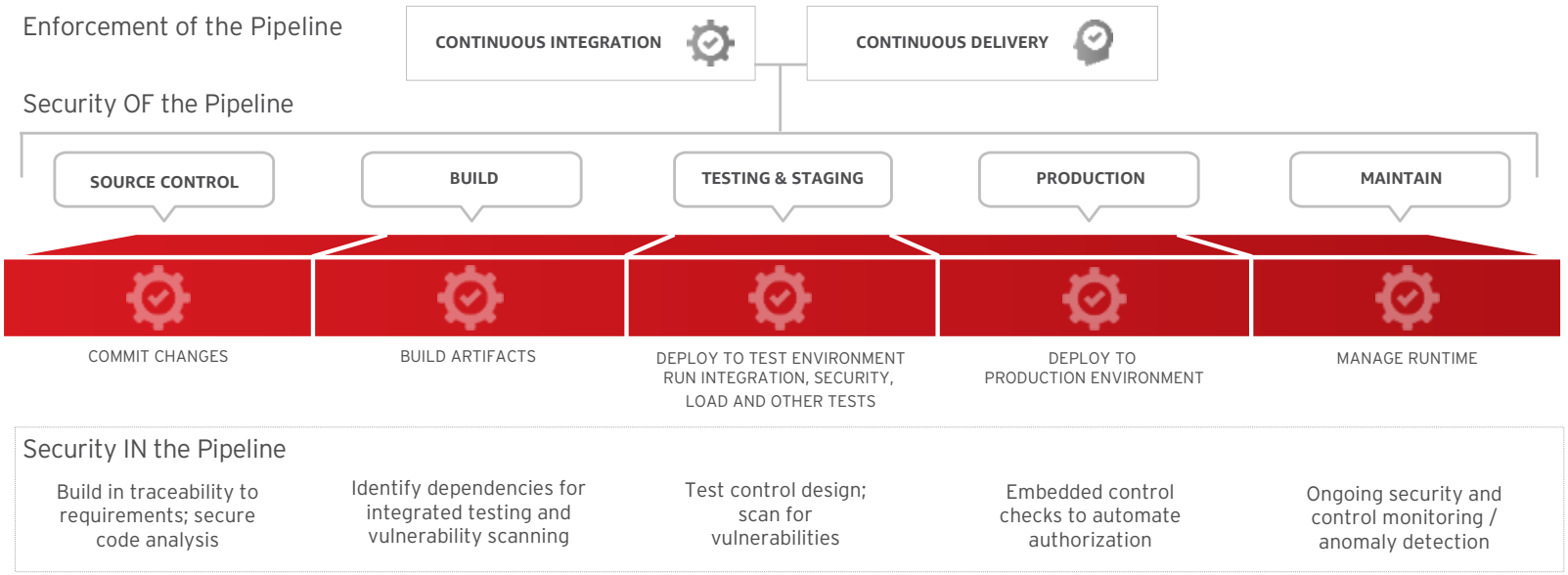
You know you're in trouble when...

- You're not enforcing a CI/CD pipeline as part of your cloud development requirements
- You haven't established the minimum security and operational requirements for your AWS environments
- You don't have a defined cloud incident management process

By formalizing controls and security measures around automated deployment, production operation, ongoing monitoring, and independent assessment, you can continue to substantiate your governance framework while fostering modernized development practices and innovation.

Ensure DevOps includes security

DevOps is an approach that combines cultural philosophies, practices, and tools so that organizations can automate development processes, achieve more stable production, and enforce security consistently. Through DevOps, teams integrate and automate preventive, detective, and responsive security controls.

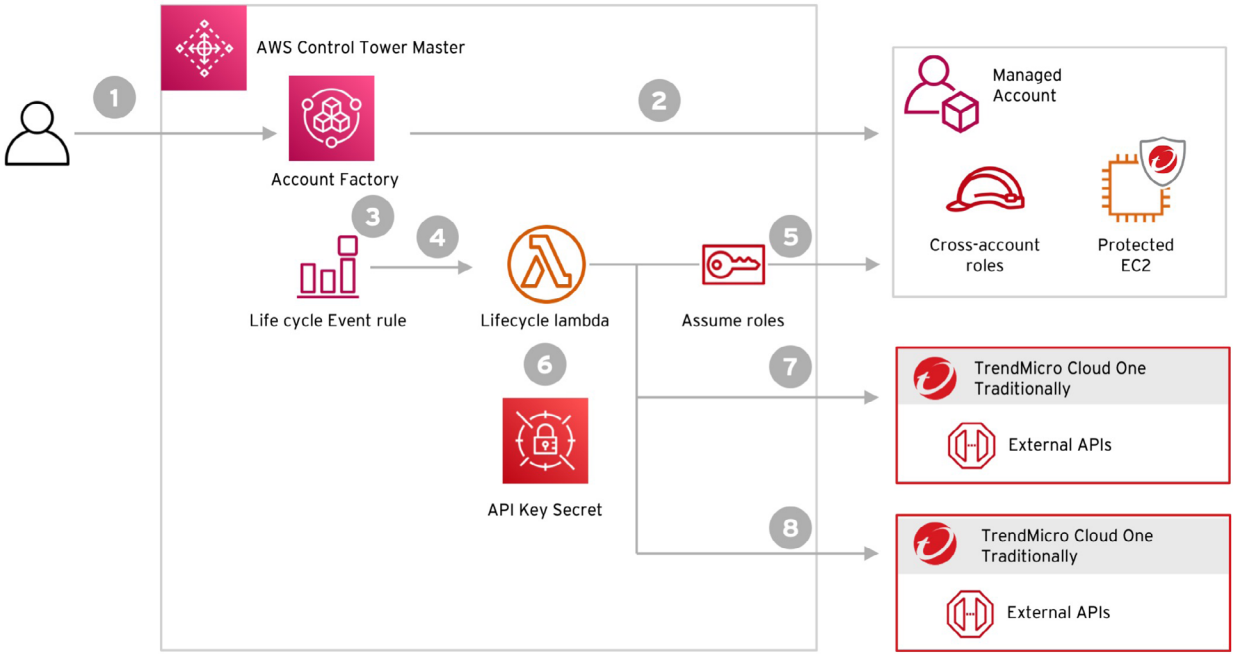


Automate security in DevOps with Trend Micro Cloud One™

To ensure cloud environments are secure, development teams should automate tasks, such as deployment, discovery, and auto scaling. The security-as-a-code framework of Trend Micro Cloud One allows developers to easily include security layers in their build pipelines and practice continuous integration and continuous delivery (CI/CD). In addition, RESTful APIs enable teams to change policies, check the status of security controls, and automate reporting. To maintain regulatory compliance, Trend Micro Cloud One automatically checks cloud infrastructure against industry standards, 600+ cloud best practices, and frameworks like NIST and the General Data Protection Regulation (GDPR).

Enable more control with Trend Micro Cloud One and AWS Control Tower

AWS Control Tower provides a systematic way to set up and govern multi-account AWS environments. When a new account is created, AWS Control Tower automates the setup and provides ongoing policy management. Because Trend Micro Cloud One integrates with AWS Control Tower, any new AWS account will automatically be configured with Trend Micro Cloud One security.



The Trend Micro Cloud One integration with AWS Control Tower:

- Reduces friction in setting up key security tools
- Delivers immediate visibility into your environment
- Helps streamline your CI/CD pipeline through automated checks against compliance standards, security controls, and non-regulatory frameworks like NIST

Measure and assess

A strong validation process included as part of your governance framework ensures consistent improvement and oversight. In parallel, the ability to effectively measure and assess your cloud program, including details on the overall governance processes and the technical implementations of your cloud control framework will promote a common understanding and offer evidence of effective governance.

You know you're in trouble when...

- You have not defined success criteria and metrics for your cloud program
- There is not a defined process to assess the security and control of your cloud environment

Practice good reporting and metrics

The key to successfully engaging internal and external stakeholders, such as auditors, is the ability to measure and assess your cloud program. With a formalized approach to reporting, you should be able to provide details on the overall governance processes and the technical implementations of your cloud control framework.

Reporting and metrics to focus on include:

- AWS service usage
- Application migration status
- Regulatory mapping status

Continually validate controls

All cloud governance participants should regularly assess the coverage and effectiveness of controls across AWS environments to ensure they are optimized for business activities and satisfy external obligations. By establishing a strong validation process, your organization can work toward continuous improvement and ongoing oversight.

Considerations for validating controls:

- Integrate cloud controls into Risk Control Self-Assessment (RCSA) for ongoing assessment
- Train internal audit teams on the AWS environment and provide detailed code samples
- Make control evidence available in an immutable form to enable the appropriate reviews

Automate security and compliance checks

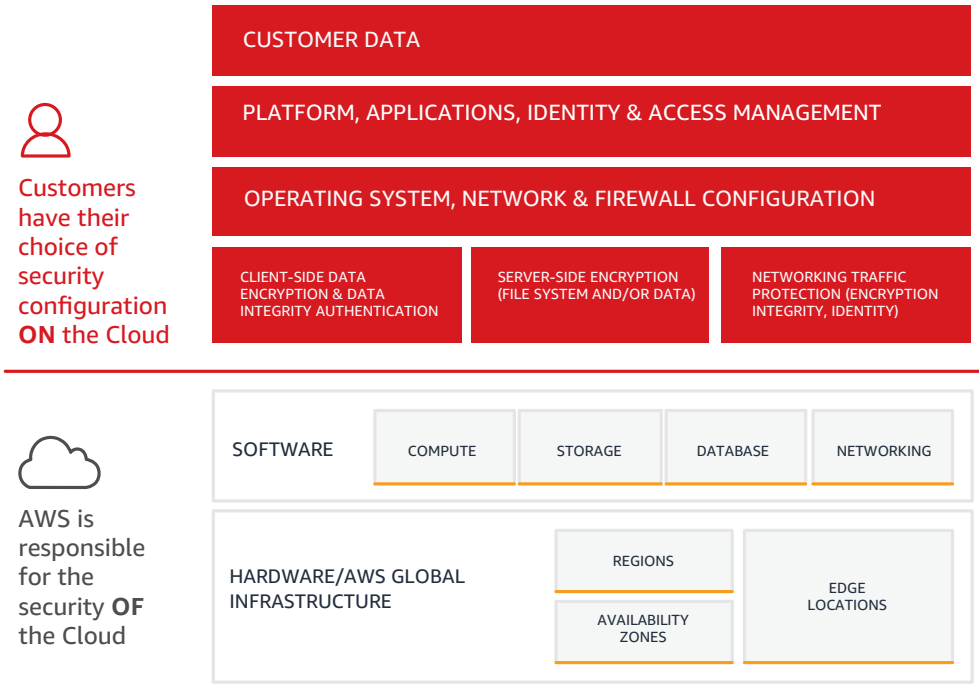
Trend Micro Cloud One™ – Conformity automatically checks your AWS investments against compliance standards, security controls, and non-regulatory frameworks, like NIST, to help your team continually monitor the effectiveness of your governance structure. These hundreds of automated checks will help you achieve a more holistic understanding of your overall security and compliance posture.

Enhancing cloud governance with Trend Micro

By combining the AWS approach to cloud governance with security solutions from Trend Micro, you can securely manage and govern your AWS workloads and ultimately accelerate your cloud migration. While AWS provides a secure cloud infrastructure, through the Shared Responsibility Model, organizations are responsible for securing the workloads, applications, and data that run on AWS—that's where Trend Micro can help.

Trend Micro Cloud One helps you map to the AWS Well-Architected Framework, automate security tasks, and implement the Shared Responsibility Model to gain the flexibility and control you need to build in the cloud.

As an Advanced Technology partner in the Amazon Partner Network, Trend Micro works with AWS to ensure your security is optimized for current and future AWS services. Trend Micro stays on top of new technology services, and has released integrations for services like Amazon GuardDuty, Amazon Detective, Amazon Appflow, Amazon VPC Ingress Routing, and offers CPPO/SPPO – Channel/Solution Partner Private Offers through the AWS Marketplace.



Take the next step

An effective cloud governance approach can help you capitalize on cloud opportunities, ensuring your FSI organization benefits from the agility, scalability, and security of cloud infrastructure. Learn more about the Shared Responsibility Model and the AWS Cloud Governance for Financial Services, or start a free, 60-day trial of Trend Micro Cloud One™ – Conformity.

Discover how Trend Micro can strengthen your security posture with solutions available in the AWS Marketplace.