Microsoft

cloudneeti

Digital stewardship: automating finserv regulatory compliance with Azure

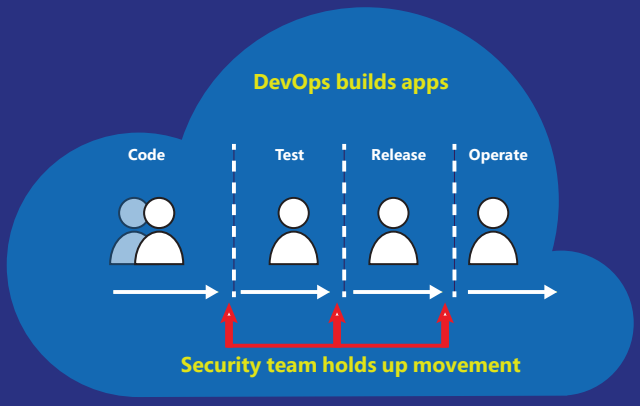
Howard Bush, Principal Program Manager
Sidney Higa, Senior Business Manager
Gururaj Pandurangi, CEO Cloudneeti

Spring 2019

Microsoft

Digital stewardship: automating finserv regulatory compliance with Azure

Digital stewardship requires compliance with many regulatory rules. It's a goal that can be achieved with a combination of two strategies. First, build compliance into the solution. Then employ a SaaS solution to achieve and maintain compliance.



Problem

Financial services (finserv) tech enterprises are required to prove and maintain compliance to various regulatory standards and laws. They often separate application development roles (DevOps) from Information Security (InfoSec). DevOps is built for agility, and InfoSec for enforcing policies; but security teams are not educated on cloud technologies. This disparity causes DevOps teams to attempt to deploy software that is vulnerable and non-compliant. Then the InfoSec team holds up the release and pushes for traditional host and network scanning. That doesn't work when software uses diverse cloud native technologies—IaaS, PaaS, serverless, containers, SaaS integrations and so on.

The root problem is that compliance is a **shared responsibility**. Many assume that just because something is built on Azure, in the cloud, it is automatically "safe" or "compliant." In fact, compliance is shared between the customer (the enterprise) and Azure. Some items are the responsibility of Azure (like physical security of Azure datacenters) and some are owned by the enterprise (such as encryption of data stores). And both the security and DevOps teams need a way to understand and track all compliance work. A few other issues complicate this:

- Enterprises are often built with Office 365 and Azure. Azure networking and workloads must be seamlessly integrated with Office 365 identities.
- Security teams are used to auditing an on-premises network once a year (or less). If the right safeguards are in place, no more compliance work needs to be done. But on the cloud, compliance must be continually monitored. In contrast, the DevOps team makes code changes frequently and they must get the security team to understand and approve.
- DevOps can build on new architectures such as serverless functions or containers. The security team doesn't need to understand these technologies, but they must ensure compliance. Unless the compliance task is abstracted away from the actual architecture, confusion and misunderstanding can occur.

Building on Azure solves these problems.

Solution

The remedy lies in integrating continuing compliance through automation. This results in:

- achieving compliance
- maintaining compliance

This is a two-part strategy: First, build a solution that includes built-in compliance capabilities (discovery, reporting, and remediation).

Second, employ a purpose-built service to monitor and enforce compliance at every step in the DevOps cycle. Such a service accommodates the architectural complexities (such as serverless functions and containers) and lets DevOps and security teams focus on compliance as a list of tasks.

Benefits

Automated compliance gives you these benefits:

- Confidentiality, availability and integration are applied in the cloud.
- Centralized visibility and control over a high-volume workload.
- Information security is in step with DevOps.
- Compliance controls are applied across all stages of DevOps.

Microsoft

Part 1: Ground up strategy

Start with a blueprint, add DevOps, automate compliance*

To build a fully automated compliant solution there are three stages, as outlined below. The results are cumulative: a single solution with automated compliance.

* Note that there are two areas that must be covered: security and compliance. These are two different disciplines that do not share the same concerns or language. For example, security relies on "best-practice guidelines," while compliance uses "controls and policies."

Stage 1: start with blueprints

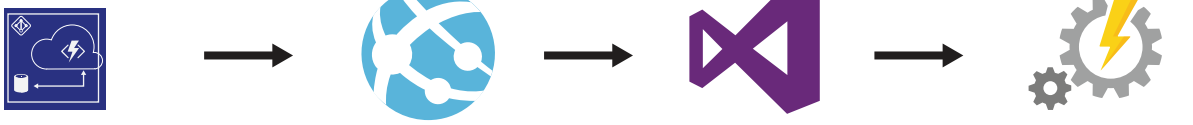
Microsoft has published a series of **blueprints**, which is a set of artifacts and documents that give you a reference architecture that includes the components for managing compliance. The documentation instructs and exemplifies how to understand and implement full compliance. This is especially vital as Microsoft can only own some of the compliance controls (such as security built into the Azure datacenter). One vital part of any blueprint is the Azure Resource Manager template. The template is used to automate deployment of any set of Azure services, saving time, especially in a CI mode.

Stage 2: Automate through DevOps

The DevOps process results in continuous integration (CI). But such a process does not include the security rules or compliance controls. If you start with the blueprint, you will gain the knowledge about security and compliance that is vital to the strategy. With that knowledge, you can add the correct components to the RM template that may be required to secure the solution according to specific regulations, or to set the controls for specific compliances. This is is automation through the DevOps cycle, sometimes called **DevOpsSec**.

Stage 3: Automated compliance

With automation built into the DevSecOps structure, the last stage can be reached. The nature of security and compliance means rules and controls are ever-evolving. And the changes demand some effort. For example, specific compliances such as those from the National Institute of Standards and Technology have controls that must understood. Then measuring (aka continuous assessment) is needed, ususally through APIs. This gives visibility into the current status versus the regulation—you must see the gaps. Finally, you need enforcement—which comes from understanding the gap—to ensure compliance. The result is a solution with APIs built in to assess, report, and apply compliance controls.



Azure blueprint
Start with an Azure blueprint to begin creating a solution

Build a basic compliant app
Build your app with the basic components to assure compliance

Integrate with DevOps
Automate compliance integration using Resource Manager templates

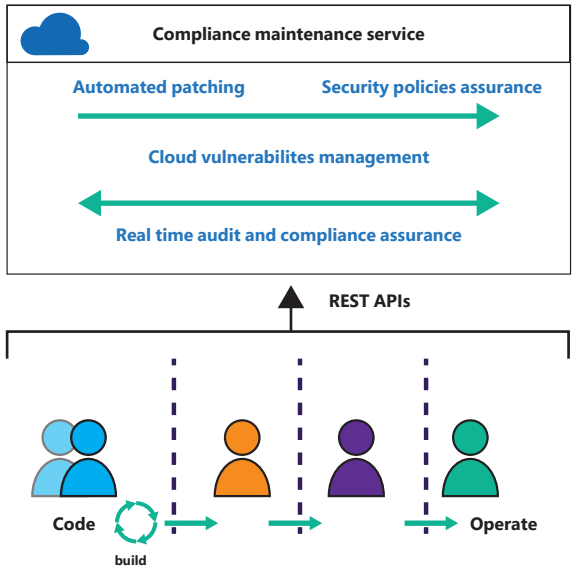
Automate compliance
Build APIs for continuous assessment, reporting, and remediation

Part 2: Employ a compliance service

Achieving and maintaining compliance is a full-time job on the cloud. Use an an API based cloud-native service to perform continuous monitoring of an enterprise's security and compliance posture. The purpose-built service performs these functions:

- Discovery of services (taking inventory of existing assets)
- Establish a baseline of your security and compliance posture: understand the existing assets
- For each asset, or asset type, adjust posture through the DevOpsSec process (security orchestration and automated response).
- Report statuses and suggest remediations.

Search the Azure marketplace for a compliance automation service, such as **cloudneeti.com**.



Microsoft

Resources

Compliance offerings: Lists the compliances enforced by Azure

Azure Security and Compliance Blueprints: Overview of Azure security and compliance blueprints

Azure Blueprints service: Enables teams to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements

Simplify compliance: Provides an overview of compliance offerings.

DevOps service: Automates software delivery

Azure Resource Manager overview: Primary method to deploy, monitor and manage solutions as a group

Azure security management and monitoring: Explains how to monitor and manage Azure virtual machines

Cloud Adoption Framework (CAF): Outlines a new approach to cloud architecture

CAF governance: Explains the concept of governance

Best practices for maintaining compliance: Summarizes methods to keep in compliance

Partners

Need it now? Our partners are ready to engage and help you with their services.

cloudneeti

Organizations and government agencies leveraging Azure cloud platform are trying to grasp the complexity associated with cloud. Often times, security, governance and compliance are top concerns for cloud adoption. Cloudneeti, a Microsoft Azure certified partner, enables customers for an easy, effective and efficient transformation to automated security and compliance monitoring of Azure and Office 365 workloads. Cloudneeti has a strong Financial services focus and they directly collaborated with Microsoft and global partners in creating various Azure Security and Compliance Blueprints - PCI DSS, FFIEC and more. Their SaaS product is available on Azure Marketplace.

Reach out to them for a trial on **www.cloudneeti.com**

Find your perfect solution on Martketplace

The Marketplace is the premier destination for all your industry partner needs—certified and optimized to run on Azure. Find the industry solutions across finance and banking, trial the technology and get directly in-touch with the partners to accelerate your evaluation.

Find a partner >