

# Definitive Guide™

to

## Cloud Compliance Automation

The fastest way to make cloud  
applications secure and compliant



**Jon Friedman**

**FOREWORD BY:**

**Richard Stiennon**

*Compliments of:*

**ANITIAN**

## **About Anitian**

Anitian delivers the fastest path to application security and compliance in the cloud. [Anitian's SecureCloud for Compliance Automation](#) and [SecureCloud for Enterprise Cloud Security](#) help high-growth companies get their SaaS applications to the cloud and market quickly, so they can unlock revenue in weeks, not months or years. Our automated cloud application security platforms deliver a full suite of security controls – both pre-engineered and pre-configured to meet rigorous security standards such as FedRAMP, CMMC, DoD SRG, StateRAMP, PCI, SOC 2, and more. Anitian's pre-built environment and platforms use the full power and scale of the cloud to accelerate time-to-production, time-to-market, and time-to-revenue so you can start secure, start compliant, and stay ahead. Find out more at [www.Anitian.com](http://www.Anitian.com).

# **DefinitiveGuide™**

**to**

# ***Cloud Compliance Automation***

The fastest way to make cloud applications  
secure and compliant

**Jon Friedman**

Foreword by Richard Stiennon

IT industry analyst, author, and columnist

With contributions from

Scott Emo, Emily Cummins, and John Vecchi



**CYBEREDGE**  
P R E S S

# Definitive Guide™ to Cloud Compliance Automation

Published by:

**CyberEdge Group, LLC**

1997 Annapolis Exchange Parkway

Suite 300

Annapolis, MD 21401

(800) 327-8711

[www.cyber-edge.com](http://www.cyber-edge.com)

Copyright © 2021, CyberEdge Group, LLC. All rights reserved. Definitive Guide™ and the CyberEdge Press logo are trademarks of CyberEdge Group, LLC in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.

Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, without the prior written permission of the publisher.

Requests to the publisher for permission should be addressed to Permissions Department, CyberEdge Group, 1997 Annapolis Exchange Parkway, Suite 300, Annapolis, MD, 21401 or transmitted via email to [info@cyber-edge.com](mailto:info@cyber-edge.com).

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or [info@cyber-edge.com](mailto:info@cyber-edge.com).

ISBN: 978-1-948939-21-8 (Paperback)

ISBN: 978-1-948939-22-5 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

---

## Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

**Editor:** Susan Shuttleworth

**Graphic Design:** Debbi Stocco

**Anitlan Contributors:** Scott Emo, Emily Cummins, and John Vecchi

# Table of Contents

---

Foreword .....	v
Introduction .....	vii
Chapters at a Glance .....	vii
Helpful Icons .....	viii
Chapter 1: Compliance Automation for Cloud Applications .....	1
The Drivers of Cloud Compliance Automation .....	1
Introducing Compliance Automation .....	4
Compliance Automation Addresses Five Challenges .....	4
The Benefits of Compliance Automation .....	10
Chapter 2: Setting up a Secure, Compliant Infrastructure .....	11
A Secure Infrastructure Is a Prerequisite for Compliance .....	11
Challenges for Creating a Secure Cloud Infrastructure .....	12
Steps for Creating a Secure Cloud Infrastructure .....	13
The Pre-engineered Cloud Security Infrastructure Option .....	20
Chapter 3: Building Compliance into Development and Test .....	21
Compliance in the Pipeline .....	21
Compliant Code from the Start .....	22
Security and Compliance Shift Left .....	23
Chapter 4: Integrating the Application and Documenting Compliance .....	25
Integrate the Application into the Environment .....	26
Define Processes .....	26
Document Compliance .....	28
Validate Compliance .....	30
Chapter 5: Staying Compliant with Automation and Standardization .....	31
Stuff Happens .....	31
Continuous Monitoring .....	32
Ongoing Assessment .....	33
Remediation .....	33
Software Development Life Cycle Management and Testing .....	34
Reporting and Dashboards .....	34
Prepare Once, Audit Many .....	35
Outcomes of Standardization .....	36

Chapter 6: Audit Ready in Weeks: A Case Study .....	37
Is This Stuff Real? .....	37
Case Study: SentinelOne and FedRAMP Certification .....	38
Chapter 7: Compliance Automation Platforms .....	41
The Big Reasons for Compliance Automation .....	41
Compliance Automation Platforms .....	42

# Foreword

If you are investigating the emerging discipline of compliance automation, you probably have many questions.

You probably *don't* have to ask about the need for streamlining compliance activities. By now I think we all know what a slow, expensive, and risky undertaking it is to certify a software application as compliant with standards such as PCI DSS, FedRAMP, and GDPR. We are also finding out how costly compliance-related delays and errors can be, postponing returns on application development projects by months, or even years. Clearly, accelerating cloud security and compliance activities can only be a very good thing.

But you may have questions about the scope of compliance automation. It goes far beyond integrating security testing into DevOps pipelines and finding templates of compliance documents. It starts with setting up a security and management infrastructure that meets regulatory requirements, includes automating security and compliance testing and documentation, and extends to continuous monitoring and change control. To appreciate the potential impact of compliance automation, you need to understand the variety of opportunities for improvement that it offers.

You may also have questions about tools and resources that can support compliance automation. These range from utilities offered by cloud platform providers to security products from third-party vendors, DevOps and test solutions, automated configurators and documentation generators, compliance dashboards, and resources for ongoing compliance assessments.

This *Definitive Guide to Cloud Compliance Automation* will help you learn about the wide scope of compliance automation and about many of the resources and tools available to implement it. It describes how compliance automation helps enterprises address five major challenges related to making

software applications secure and compliant on cloud platforms and keeping them that way over time. It includes a case study

that illustrates how compliance automation can be deployed and some of the major benefits. It also provides a very brief introduction to the idea of a pre-engineered compliance platform, a concept pioneered by Anitian, the guide's sponsor.

In short, if you are investigating the emerging discipline of compliance automation, the *Definitive Guide to Cloud Compliance Automation* is a great place to start.

**Richard Stiennon**  
**IT Industry Analyst, Author, Columnist, and**  
**Member, Board of Directors, Anitian**



# Introduction

any technology professionals think that the activities required to deploy a software application on a cloud platform, make it secure, and document compliance *must necessarily be manual*. Applications are unique, so surely how they are protected and the reports you must produce to comply with regulations will differ. And where processes vary, it follows that standardization and automation can only play small roles, right?

Well, no. In fact, cloud compliance automation typically shortens from one or two years down to a few months the time it takes to deploy an application in the cloud, protect it from attack, and produce a full set of compliance documentation. Applications have been made “audit-ready” in as little as eight weeks for complex standards such as FedRAMP, PCI DSS, and HIPAA.

This guide explains how you can achieve results like that. You will learn the value of setting up a secure, compliant cloud environment that can be used by many applications with only minor adjustments. You will explore ways to build security and compliance into coding and testing processes. You will find suggestions on how to automate compliance documentation and keep applications secure and compliant over time.

We hope this information will be useful, and that by the end of the guide you will agree that cloud compliance automation is an idea whose time has come.

## Chapters at a Glance

**Chapter 1**, “Compliance Automation for Cloud Applications,” introduces cloud compliance automation and its benefits.

reviews the steps for creating and configuring a secure infrastructure for cloud applications.

**Chapter 3, “Building Compliance into Development and Test,”** explores ways to promote secure coding and integrate security testing into DevOps pipelines.

**Chapter 4, “Integrating the Application and Documenting Compliance,”** suggests ways to automate processes that integrate applications into cloud environments and document compliance.

**Chapter 5, “Staying Compliant with Automation and Standardization,”** outlines strategies for keeping applications secure and compliant over time.

**Chapter 6, “Audit Ready in Weeks: A Case Study,”** presents a case study that illustrates the advantages of a compliance automation platform.

**Chapter 7, “Compliance Automation Platforms,”** examines the idea of a compliance automation platform.

## Helpful Icons

TIP



Tips provide practical advice that you can apply in your own organization.

DONT FORGET



When you see this icon, take note as the related content contains key information that you won't want to forget.

CAUTION



Proceed with caution because if you don't it may prove costly to you and your organization.

TECH TALK



Content associated with this icon is more technical in nature and is intended for IT practitioners.

ON THE WEB



Want to learn more? Follow the corresponding URL to discover additional content available on the web.

# Chapter 1 **Compliance**

# **Automation for Cloud**

# **Applications**

## In this chapter

- Understand why compliance automation is such an important topic right now
- Learn the five key challenges for businesses that it addresses
- Review the benefits of compliance automation

*“To change something, build a new model that makes the existing model obsolete.”*

— Buckminster Fuller

---

# The Drivers of Cloud Compliance Automation

Today, every business and government organization of any size needs to get better at complying with industry standards and government regulations. Four reasons stand out.

First, the potential costs of non-compliance can be staggering. The direct and indirect costs of data breaches, regulatory fines, lawsuits, and damaged reputations can quickly reach millions of dollars. A survey of multinational corporations by the Ponemon Institute found the average annual cost of non-compliance to be \$14.8 million, an increase of 45 percent between 2011 and 2018.

Second, the cost of becoming and staying compliant is escalating rapidly. In 2021, a survey by Hyperproof found that



percent of organizations plan to increase spending on IT risk management and compliance. Of all respondents, 37 percent expected their total compliance budget to rise 25 to 50 percent over the next 12-24 months.



For more data on the costs of compliance and non-compliance, read the Ponemon Institute survey, [The True Cost of Compliance with Data Protection Regulations](#), and the Hyperproof [2021 IT Compliance Benchmark Report](#).

Third, compliance efforts often stretch out time-to-market, resulting in major opportunity costs. Organizations often face new regulatory challenges when they want to introduce new products and services, sell to new customers in regulated industries, and enter new markets. They must:

- ▢ Design and implement new security controls
- ▢ Tighten up policies and procedures
- ▢ Produce voluminous reports and plans documenting compliance

Meeting these challenges can take many months or even years, leading to foregone revenue and sometimes loss of competitive advantage.

Finally, forward-thinking enterprises are moving software applications to cloud platforms, such as Amazon Web Services (AWS) and Microsoft Azure, so they can scale operations, reduce capital costs, and react more quickly to changing demand. But in moving to cloud platforms, they must give up many of the familiar security, management, compliance, analytics, and reporting tools used in their data centers. They face a lengthy process of evaluating, selecting, licensing, learning, integrating, and configuring a cohesive set of alternative products that run on their cloud platform and meet all regulatory and security requirements.

## When slow compliance processes affect the bottom line

When slow compliance processes delay the acquisition's IT rollout of new software systems, the entire enterprise up to corporate standards for security and compliance, they can't be integrated with those of the parent company.

- A software vendor plans to expand its business into regulated industries such as moving a critical application to a cloud platform to reduce capital expenses and free up revenues administrators for other tasks. It can't start generating revenues until the cloud product meets their security standards. a compliance audit.

- In all four scenarios, the organizations cannot generate new revenue or reduce costs until their applications have been audited and validated as compliant with the relevant standards and regulations.
- A global manufacturer is making a strategic acquisition.

---

## *The drive for agility*

Many enterprises today are also working hard to increase business agility. They want to shorten software release cycles so they can bring new products to market sooner and respond more quickly to evolving customer needs. To achieve these objectives, they are investing in DevOps and Agile product development practices and in software orchestration, automation, and reporting (SOAR) products.

Unfortunately, complex, manual, error-prone compliance processes can act as a brake on agility, resulting in:

- ≡ Longer software release cycles
- ≡ Postponed product releases
- ≡ Failed compliance audits

# Introducing Compliance Automation

Compliance automation is a relatively new field that focuses on how to make software applications compliant and secure, and how to keep them that way over time. It covers techniques and technologies that accelerate, automate, and standardize compliance processes. Its goals are to:

- ≡ Avoid data breach costs and fines by ensuring that the right security controls and processes are in place to block attacks and demonstrate compliance with regulatory policies
- ≡ Reduce the cost of becoming and staying compliant by eliminating repetitive manual tasks
- ≡ Dramatically accelerate time-to-market for new software solutions and for products that depend on new software, by slashing the time required for applications to become compliant
- ≡ Speed up cloud transformations by enabling organizations to quickly replace their data center security and management tools with equal or better cloud-based and cloud-native alternatives



- ☰ Enhance rather than hinder business agility by
  - integrating compliance into software development life cycles and supporting DevOps tools

## Compliance Automation Addresses Five Challenges

Compliance automation helps organizations address five major challenges, as illustrated in Figure 1-1. We review them briefly here and discuss them in depth in other chapters of this guide.



---

**Figure 1-1:** Compliance automation helps organizations address five major challenges.

### *Setting up a secure, compliant infrastructure*

Industry standards and government regulations require applications and data to be protected from outside attack, insider threats, inadvertent disclosure of personal information, and many other bad outcomes. Some mandate specific security and compliance technologies, while others set forth general directives and leave implementation decisions entirely to the enterprise. However, the impact is the same: to be compliant, applications must be supported by an infrastructure that includes a wide range of security, compliance, management, reporting, and analytics products.

At first glance, you might not think this is a great challenge. Enterprises already run security, compliance, management, and analytics solutions in their data centers. But many of their current products aren't available on cloud platforms, do not translate well there, or don't work well with the cloud versions of other third-party software packages or the native services of platforms such as AWS and Azure.

Also, many organizations embrace DevOps practices when they move application development to the cloud. But legacy security products often don't fit with short development and delivery cycles. In this situation, bringing familiar security tools forward can cause security and compliance to become impediments to rapid code development and cause conflict between security and DevOps organizations.

Most enterprises recognize the need to move to a new set of tools to handle security and compliance in the cloud. But they face a lengthy process of evaluating, selecting, licensing, learning, and integrating a cohesive set of best-of-breed products that run on their cloud platform. These tasks can take months, even years, for complex standards like PCI DSS, FedRAMP, HIPAA, CMMC, and GDPR.



**TIP** Some people think that compliance activities start only *after* an infrastructure is in place and application coding is almost complete. In fact, a secure, compliant infrastructure is a *prerequisite* for accelerating the development, deployment, and enhancement of compliant applications. You can't do a good job architecting and coding a compliant application without knowing early on the security-related tools and services available in the infrastructure.

### ***Building compliance into development and testing***

Creating compliant software applications involves much more than just educating developers on secure coding standards. Development organizations need to build compliance into every phase of the application development and DevOps lifecycles, including:

- ▢ Requirements assessment
- ▢ Application design
- ▢ Coding
- ▢ Testing and verification
- ▢ Maintenance and enhancement

A variety of methods and tools can be used to automate and accelerate the work in these phases, and to ensure that nothing is missed in the hand-offs from one stage to the next. In particular:

- ▢ Security and compliance frameworks, threat models, reference architectures, and sample security policies can accelerate requirements assessment and the design of compliant applications.
- ▢ DevOps and automated software testing tools ensure that applications are tested for security issues and policy violations early in the development process, when they are easiest to fix, and continuously thereafter.

## ***Integrating the application and documenting compliance***

After an application is coded and tested for security and compliance, it must be deployed in the cloud infrastructure and integrated with the security and management tools there. For example, firewall and intrusion prevention system (IPS) rules need to be tuned and access control policies defined based on the characteristics of the application. Templates and examples can speed up this process and ensure consistency.

Documenting and verifying compliance are major tasks, especially for enterprises encountering a new standard or regulation. Most development groups today depend on checklists, spreadsheets, playbooks, and manual processes to document conformance with regulations. Similarly, they rely on largely manual code reviews to verify compliance and prepare for audits. These approaches are slow and prone to errors, particularly when organizations are unfamiliar with a regulation or new to cloud platforms.

In fact, the prospect of producing all the required documents and reports can be so daunting that enterprises may be persuaded to pay outside consultants hundreds of thousands or millions of dollars to design, configure, and deploy the computing infrastructure and produce the necessary documentation.

Automated workflows and resources like sample report libraries, artifact repositories, and document generators can dramatically reduce the effort and time required to document compliance and prepare for audits. They can also reduce the risk of failed audits and eliminate high professional service fees for outside consultants.

### ***Standardizing the compliance and security environment***

Compliance automation is not just about automating compliance. It concerns automating *and standardizing* compliance and security.

Why is standardization important? It's because development organizations tend to deploy applications to cloud platforms in an ad hoc manner, each with its own enabling environment and compliance processes based on a different set of security solutions, management and reporting tools, and analytics products. It is not unusual for an IT organization to become saddled with several application firewalls, IPSs, SIEMs, endpoint security tools, container security technologies, log inspection tools, etc., or to have applications with different tools and workflows for validating, documenting, and monitoring compliance.



Duplication and overlap in infrastructure result in inefficiencies, higher costs, information silos, and an inability to share expertise across applications.

To avoid these problems, organizations must not only create a cloud infrastructure with a full set of security, management, reporting, and other services. They should also *enforce their use* across application development groups. That doesn't mean that every application will use the same services in the same way, but they should draw from the same set of options.

The same logic applies to using a common set of tools and workflows for managing compliance. When all applications take advantage of one enabling environment and one set of compliance processes, everyone can focus on making that environment and those processes as automated, flexible, and consistent as possible. As a result, security and compliance can reinforce business agility instead of impeding it.

## ***Keeping applications secure and compliant over time***

Stuff happens. New threats emerge. Enterprises enhance software applications and deploy new ones. They explore new technologies. They enter new markets that require adherence to additional standards and regulations. Standards and regulations themselves evolve.

Organizations need processes to monitor and respond to these changes. The responses may include:

- ▢ Updating compliance documentation and generating monthly reports
- ▢ Remediating vulnerabilities and reconfiguring security controls to bring applications back into compliance
- ▢ Implementing new security controls

- ☐ Going through all the work involved in complying with an additional standard or regulation

Continuous compliance automation can help these processes run smoothly. It can also free up resources for strategic projects such as adding value to applications and strengthening the security posture of the enterprise.

Also, continuous scanning for vulnerabilities and policy violations, automated workflows for change management, and compliance documentation generators can automate and accelerate many of the processes involved. Integration between compliance tools and DevOps pipelines can ensure that application enhancements and new software releases are fully tested for compliance. Dashboards and analytics tools can illustrate trends related to compliance and security and show progress toward goals in those areas.

## The Benefits of Compliance Automation

At an operational level, compliance automation can help organizations:

- ☐ Shorten software release cycles
- ☐ Release more feature enhancements faster
- ☐ Increase productivity by reducing time spent documenting compliance and preparing for audits

Compliance automation can also help organizations achieve business goals such as:

- ☐ Eliminating drawn-out and failed audits
- ☐ Avoiding data breaches
- ☐ Speeding up time-to-market and time-to-revenue for new products
- ☐ Entering profitable new markets much sooner

## Seven signs your organization needs compliance automation

1. Software releases are being delayed by compliance and each type of security and management tool on your cloud platform.
2. You depend on checklists, spreadsheets, and playbooks to verify compliance. Your compliance and security tools aren't integrated into your DevOps pipeline.
3. You rely on expensive professional services consultants to teach you how to create a compliant environment for your new product or entry into a target market is delayed by 18-24 months while you build cloud application(s).
4. You use a different process every time you prepare for a regulatory audit.
5. You have more than one type of security and management tool on your cloud platform.
6. Your compliance and security tools aren't integrated into your DevOps pipeline.
7. A new product or entry into a target market is delayed by 18-24 months while you build cloud application(s).

# Chapter 2 **Setting up a Secure, Compliant Infrastructure**

## In this chapter

- Understand why a secure cloud infrastructure is a prerequisite for compliance
- Review the steps for creating and configuring a secure cloud infrastructure
- Learn about the pre-engineered infrastructure option

*“The loftier the building, the deeper must the foundation be laid.”*

– Thomas à Kempis

---

## **A Secure Infrastructure Is a Prerequisite for Compliance**

Compliance automation cannot succeed without a cloud infrastructure that includes a reliable, scalable computing platform and a variety of security technologies. Without such an infrastructure, applications cannot be compliant and automation cannot be effective.

### ***Standards demand security***

Most industry standards and government regulations take one of two approaches to defining security requirements:



- ☐ Explicitly mandating the use of specific security technologies such as firewalls, multi-factor authentication, SIEMs, and data encryption
- ☐ Setting out general directives such as “ensure the protection and privacy of personal data” or “develop and maintain secure systems and applications”

In practice, the second approach has about the same effect as the first, since the general directives cannot be met without the same or similar technologies. No application is going to be compliant unless it is protected by a series of security, management, and reporting products.

### ***Automation requires stability and consistency***

Organizations should plan ahead to create a stable infrastructure. If they don't think about their requirements in advance and identify solutions early on, they will find themselves continuously changing services, revising parameters, and introducing new tools. These changes will, in turn, force them to make frequent alterations to application code, DevOps processes, and compliance documentation that slow down new releases and introduce errors and defects.

Similar problems occur when applications are built on different cloud services and tools. In that case code, processes, and documentation will be inconsistent across the applications, which also makes compliance automation difficult.

## **Challenges for Creating a Secure Cloud Infrastructure**

Even enterprises that have established a stable, consistent infrastructure in their data centers face serious challenges when they start deploying applications on cloud platforms like AWS and Azure.

First, they are forced to largely abandon the familiar system software, utilities, middleware, and management tools used in their data centers and adjust to the tools and utilities supplied by the cloud platform providers.

Second, they need to decide whether to replace the on-premises versions of security, analytics, and reporting tools with:

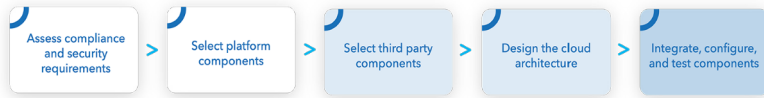
- ☐ Cloud versions of the same products
- ☐ Cloud-native substitutes offered by the platform provider
- ☐ Alternative cloud-based solutions from other vendors

Third, these enterprises must integrate the components of the new security and compliance solution stacks and revise their processes accordingly.

## Steps for Creating a Secure Cloud Infrastructure

The steps for creating a secure infrastructure are shown in Figure 2-1. At first glance, these steps appear to be fairly simple:

1. Assess security requirements in the relevant standards and regulations.
2. Select components offered by the cloud platform provider.
3. Select security, management, and reporting tools from third-party vendors.
4. Design a cloud architecture that optimizes security and simplifies administration.
5. Deploy, integrate, configure, and test the component tools.



**Figure 2-1:** Steps to create a secure infrastructure


However, moving through these steps can take months, especially when organizations are just building up their knowledge of compliance requirements and cloud-based security and management tools.


## ***Assess compliance and security requirements***

Most major industry standards and government regulations attempt to give enterprises leeway in selecting the security technologies and tools that best address the threats they face and the needs of their specific industries. Many also make provisions for “compensating controls,” which are alternative technologies or procedures for providing the same level of security when typical controls are impractical.

This flexibility is welcome, but it also puts a burden on the organization to understand not only the intent of the relevant standard(s) and regulation(s) but also how auditors and government agencies have been interpreting them in practice.

As a result, a team or task force needs to master the requirements and translate them to specific products and solutions that will provide a secure, compliant environment for the organization’s applications. The team could be

staffed by:  Current members of the IT and compliance organizations (if they have enough experience with the pertinent regulations and with cloud-based security and management tools)

 New hires with the right experience and skills



- ☐ Contractors from consulting or system integration firms
  - ☐ A service provider with a pre-engineered cloud compliance platform (discussed below)

Don't approach your first compliant cloud application as a one-off exercise. It is tempting to do "just enough" to meet the needs of the first application. However, you will probably find that the second and third applications require a different architecture or more-comprehensive tools. Some organizations end up with multiple web application firewalls (WAFs), encryption tools, SIEMs, log management solutions, etc. With a little extra analysis and planning you can build or license a secure, compliant infrastructure that will meet the needs of multiple applications. This approach will lower costs, reduce errors, and generally make life simpler in the long run (and usually much sooner than that).

### ***Select components from the platform provider***

The next step in the process is to look at the management, security, and reporting tools offered by the cloud platform provider and determine which ones address the security and compliance requirements that have been identified. For example, Figure 2-2 lists some of the cloud-native products offered by Amazon that enhance reliability, availability, security, and visibility in an AWS environment.

<b>Component</b>	<b>Function</b>
<b>Amazon CloudWatch</b>	A service for monitoring and logging AWS cloud resources and applications
<b>AWS CloudTrail</b>	A service for monitoring account activities on AWS
<b>AWS IAM</b>	AWS Identity and Access Management service for controlling access to AWS services and resources
<b>Amazon S3</b>	A highly reliable and secure data storage infrastructure

<b>AWS Secrets Manager</b>	A service to secure and manage database credentials, API keys, and other secrets for access and encryption
<b>AWS GovCloud</b>	AWS regions designed to host regulated workloads and controlled unclassified information (CUI)
<b>AWS VPC</b>	A virtual private cloud area in AWS that isolates applications to control access

**Figure 2-2:** Examples of Amazon security and management tools

### *Select components from third-party vendors*

Cloud platform providers such as Amazon and Microsoft offer excellent tools for managing and monitoring their own infrastructure, but they don't always offer customers all the software technologies needed to comply with complex security standards and regulations like PCI DSS, HIPAA, GDPR, CMMC, and FedRAMP. Also, some of the products they offer are not as feature rich as similar solutions provided by vendors that specialize in those areas.

As a result, secure cloud environments often incorporate security, management, DevOps, and analytics tools from third-party vendors. Figure 2-3 highlights components of a secure, compliant infrastructure that are sometimes sourced from third parties.

<b>Component</b>	<b>Function</b>
<b>Web application firewall</b>	Monitors traffic to web applications and detects web-based application attacks
<b>Vulnerability management</b>	Scans systems for vulnerabilities and misconfigurations
<b>SIEM</b>	Provides central log storage, alert management, event correlation, and security analytics

<b>Encryption</b>	Ensures that applications use encryption modules and settings compliant with standards such as FIPS 140-2
<b>Container security</b>	Provides security and access control for containers and their contents
<b>Endpoint security</b>	Provides anti-malware, incident detection and prevention, file integrity monitoring, and other security services for endpoints and networked components
<b>Multi-factor authentication (MFA)</b>	Provides FIPS-compliant authentication with two or more credentials for applications
<b>Identity repository</b>	Manages user and system identities and permissions
<b>Configuration management</b>	Automates and orchestrates processes for building, testing, and releasing compliant applications
<b>Certificate authority</b>	Manages digital certificates for public key encryption

**Figure 2-3:** Examples of components sometimes sourced from third-party vendors




Most large enterprises need to comply with three or more major standards. To avoid making short-sighted decisions, evaluate third-party products on their ability to meet the security and compliance requirements of all the regulations affecting you now, plus additional ones you may want or need to comply with in the future.


### ***Design the cloud architecture***

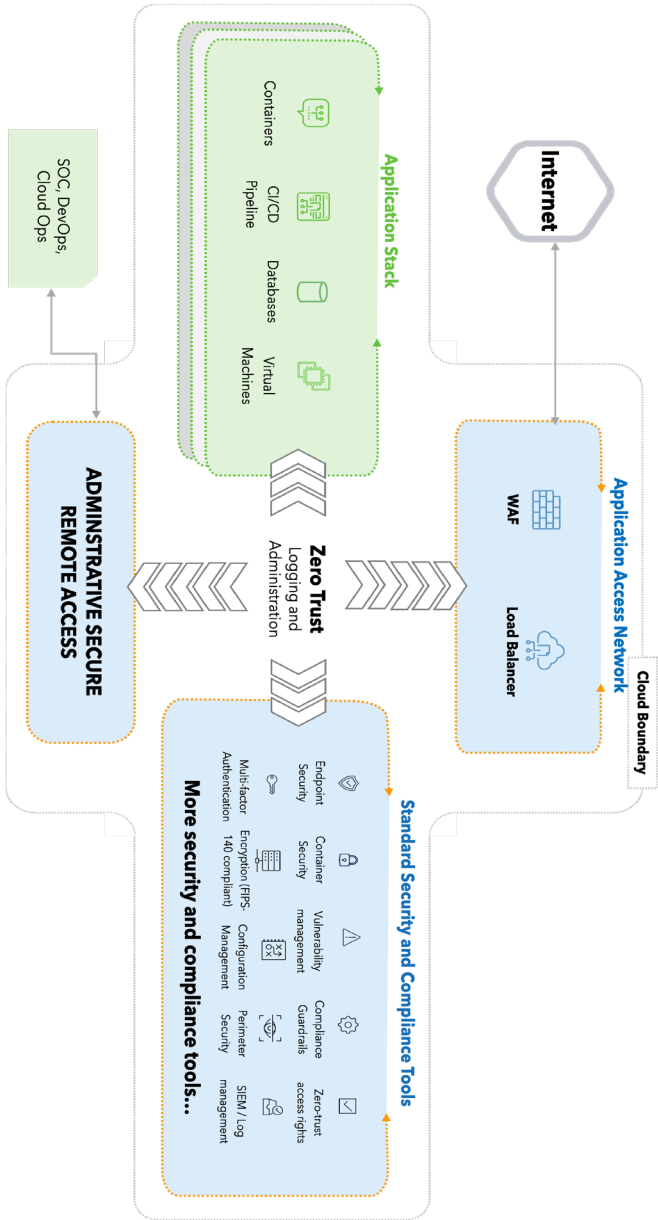
A secure, compliant cloud infrastructure needs a cloud architecture that optimizes security and simplifies administration. For instance, it is a best practice to configure the application, the application access controls, and the security and compliance tools in their own virtual private

cloud (VPC) on AWS or in their own virtual network (VNet) on Azure. Connections between these areas can be tightly controlled based on the principles of zero trust network access, as illustrated in Figure 2-4.

This technique:  Enables the implementation of zero-

trust security principles  Helps meet the access control requirements of many standards

 Simplifies administration by allowing the DevOps team to manage and update the application, the security or DevOps team to manage and use the security tools, network administrators to handle load balancing and network security, and so forth, without needing assistance or approval from other groups



**Figure 2-4:** Example of an architecture that isolates the application on the cloud platform and uses zero trust network access principles to control access. (Source: Anitian)



## ***Integrate, configure, and test the components***

The final step is to integrate and configure the components and test that they work together. The process might include:

- ☐ Hardening host systems and services with secure configurations
- ☐ Turning off unnecessary network and cloud platform services
- ☐ Defining virtual routing and switching rules and security groups to rout network traffic in conformance with zero trust network access principles
- ☐ Creating firewall, next-generation firewall (NGFW) and WAF rules that restrict connectivity to VPCs, VNets, systems, applications, and data stores
- ☐ Configuring security tools so their behavior maps to the controls required by security standards and regulations
- ☐ Ensuring that all traffic between tools is being encrypted and decrypted properly ☐ Verifying that the SIEM can capture and analyze event data and alerts

from all perimeter, endpoint, and other security tools in the infrastructure

Design, integration, and configuration activities can take weeks, even months. However, the process can be accelerated with resources such as:

- ▢ Reference architectures that diagram secure, compliant, and manageable environments on cloud platforms
- ▢ Reference images of hardened systems
- ▢ Documented firewall, NGFW, and WAF rules that minimize connectivity to resources
- ▢ Templates of rules and policies for security tools



Set up a process to capture and log implementation artifacts such as architecture and data flow diagrams, system images, firewall rule sets, access control and security policies, and scripts. A library of these artifacts will speed up your deployment of subsequent applications.

## The Pre-engineered Cloud Security Infrastructure Option

As we noted earlier, it can take months, or even years, to analyze requirements for a secure cloud infrastructure, select components, and integrate and test the components. These tasks are especially difficult for organizations that lack experience with the security and management tools available on their cloud platform.

Many enterprises faced with this challenge end up hiring large teams of consultants or system integrators. This approach

reduces the risk of failing audits, but it doesn't speed up the process much and can cost millions of dollars.

An alternative is to utilize a pre-engineered cloud security and compliance platform that contains all necessary security, management, and analytics tools, already integrated and ready to deploy on a cloud platform.

The advantages of a pre-engineered platform far outweigh the disadvantage of being unable to choose the components of the infrastructure. These advantages include:

- ⇒ Having a secure, compliant cloud environment available in days instead of months or years
- ⇒ Dramatically reducing the risk of failing the first (or any) audit
- ⇒ Eliminating the cost of hundreds of hours of staff time and contractor fees to analyze requirements, evaluate tools, select components, and integrate and test the environment
- ⇒ Offloading to the compliance platform provider the work of managing and enhancing the environment

ON THE WEB



For an example of a pre-engineered compliance platform, view the [Anitian SecureCloud for Compliance Automation Solution Brief](#).

# Chapter 3 **Building Compliance into Development and Test**

## In this chapter

- Explore ways to build secure coding practices into design and development processes from the start
- Learn about integrating security and compliance testing into DevOps pipelines

*“If you don’t have time to do it right, when will you have time to do it over?”*

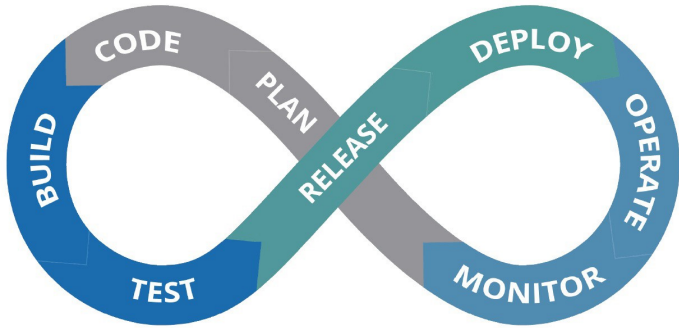
– John Wooden

---

## **Compliance in the Pipeline**

DevOps is an approach to software development that integrates and automates the processes for coding, building, testing, releasing, and maintaining applications (Figure 3-1). DevOps principles and practices enable development, test, and IT operations teams to work together to deliver frequent releases of high-quality code.

However, in many organizations application security and compliance are not integrated into DevOps processes. They remain islands of ad hoc tasks, relying on manual code reviews and intermittent testing. Reviews and tests are performed only in the final stages of development. Predictably, outcomes often include failed audits, extensive reworking of code, and delayed releases of applications into production.



**Figure 3-1:** DevOps integrates and automates code, build, test, release, and other phases in the software development life cycle.

Compliance automation addresses those challenges by:

- ▣ Building secure coding practices into design and development processes from the start
- ▣ Integrating security and compliance testing into automated continuous integration/continuous delivery (CI/CD) DevOps pipelines

## Compliant Code from the Start

One of the goals of compliance automation is to ensure that security and compliance features are built into applications early in the development process, rather than bolted on at the end as an afterthought.

Partly this involves organizational adjustments, such as providing training to DevOps teams on security requirements and giving developers responsibility for testing their own code for security and compliance. Often application security and test teams are asked to serve as consultants who train and support developers, rather than coding and testing security features themselves.

Secure DevOps and compliance teams can also accelerate development and delivery processes and promote consistency by creating and sharing artifacts such as:



A comprehensive set of compliance requirements

### Chapter 3: Building Compliance into Development and Test | 23



Diagrammed security architectures documenting the required environment and integration points



Standardized libraries of secure code



Code samples of security features



Test plans and test scripts to validate that security- and compliance-related features work as required



Store the templates, code samples, test plans, and other artifacts in your code repository and tag them based on the specific standards and regulations they address. That way, it will be easy to find the items you need when starting to develop the next application.

## Security and Compliance Shift Left

It is an axiom in the software development community that it is far more costly to fix defects discovered late in the development lifecycle than early. This insight has prompted development organizations to integrate testing into their DevOps pipelines.



For an estimate of how dramatically the cost of fixing bugs escalates over time, see Table 5-1 and Figure 5-3 in the classic NIST white paper, [The Economic Impacts of Inadequate Infrastructure for Software](#).

### *Test early and often*

DevOps tools orchestrate and automate the tasks involved in integrating, testing, and delivering working software. They initiate automated testing every time code is completed and committed to a repository, ensuring that testing begins early

in the development process and is never overlooked. The types of testing might include:

- ▢ Static Application Security Testing (SAST), which parses application source code to find defects and vulnerabilities
- ▢ Dynamic Application Security Testing (DAST), which probes running applications from the outside by simulating the actions of threat actors
- ▢ Interactive Application Security Testing (IAST), which places a software agent within applications to test components for weaknesses

Organizations can also automate processes that: ▢  
Ingest data from application security testing tools

- ▢ Analyze test data and create prioritized lists of defects and vulnerabilities that need to be remediated
- ▢ Feed data and remediation suggestions into bug tracking and ticketing systems

## ***Standardize tools and processes***

As in other areas we have discussed, software development testing benefit greatly from a standardized environment, where the same tools and processes are used for all applications. If the standardized environment includes good development and testing tools that are integrated with each other and other elements of the infrastructure, all software

development groups will have an incentive to use them. If one group creates processes to build security into applications from design to deployment, other groups can (and will) take advantage of that work. Good tools and common processes lead to greater consistency, repeatability, and application quality.

## Chapter 4 Integrating the Application and Documenting Compliance

### In this chapter

- Review the activities involved in integrating the application into the environment
- Examine tasks to document and validate compliance
- Learn how these tasks can be accelerated and automated

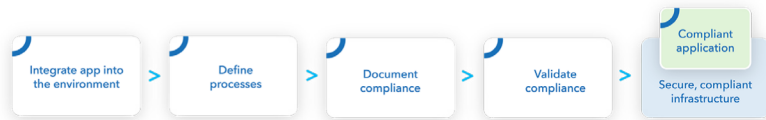
*“We can lick gravity, but sometimes the paperwork is overwhelming.”*

– Wernher von Braun, rocket scientist

---

We have set up a secure environment on a cloud platform and finished coding a compliant application. The next phase of the project involves hooking the application into the environment, defining security processes, documenting compliance, and validating successful compliance. The end result is a compliant application running on a secure, infrastructure, as illustrated in Figure 4-1.





**Figure 4-1:** Steps to integrate the application and document compliance.

## Integrate the Application into the Environment

When the application has been coded and tested, it can be stood up in its own VPC or VNet on the cloud platform (see Figure 2-4). The next step is to integrate it with the security and management tools in the environment. This involves configuring the tools and defining policies based on the characteristics and use cases of the application.

Integration activities include:

- ▢ Defining access control policies based on the needs of users, subject to regulatory requirements and the principle of least privilege
- ▢ Creating firewall and IPS rules based on the application’s data flows and security needs
- ▢ Setting up policies for multi-factor authentication
- ▢ Configuring endpoint detection and response (EDR) agents and distributed them to all endpoints

### Standardization speeds integration

In Chapter 1 we outlined the one EDR, etc. Second, they can create advantages of a standardized com- ate templates of rules and policies, pliance and security environment. and in some cases write scripts to These certainly play out when deploy them automatically. These it comes to integrating applica- types of standardization eliminate tions. First, security and DevOps days or weeks of work integrating teams only need to learn how to applications and reduce errors configure tools and create policies that can undermine security and for one firewall, one IPS, one SIEM, compliance.

## Define Processes

Many standards and regulations require organizations to define and document policies and procedures in areas like:

- ▢ Configuration management and system maintenance

Chapter 4: Integrating the Application and Documenting Compliance |

27

---

- ▢ Software patching and updating
- ▢ Logging and auditing
- ▢ Incident response
- ▢ Software development life cycle (SDLC) management
- ▢ Risk assessment
- ▢ Security awareness and training for employees

Some policies and procedures can be carried over from data centers, but most need to be substantially revised or completely redeveloped because:

- ▢ The architecture, management and reporting tools, and security solutions in the cloud environment differ substantially from those used in the data center.
- ▢ Complex and changing standards require more flexible processes and increasingly detailed documentation.

### Log data ingestion and distribution

An example of a process that needs converting it to standard to be rethought when an organization starts deploying compliant searching, analysis, and audit applications on a cloud platform is log data ingestion and distribution.

Administrators need to:

- Set up alerts that send data to SIEMs and other security tools
- Identify all the systems and tools that produce log and event data that is useful for distribute appropriate data to attack detection, incident management dashboards, anaresponse, security forensics, lytics tools, and governance, anomaly detection, trend risk management, and complianalysis, and audits. ance systems.
- Create processes for capturing and deduplicating data,

## ***Accelerating and automating process definition***

A variety of resources can be used to accelerate the job of defining and documenting policies and procedures for a secure, compliant cloud environment.

- ⇒ Diagrams, flow charts, and “playbooks” of processes already developed for the cloud platform and the same or similar security tools
- ⇒ Templates of policy settings that define the processes
- ⇒ Code snippets and scripts that help acquire, reformat, store, and distribute the data

In addition, DevOps and security orchestration, automation, and response (SOAR) tools can automate many processes after they have been defined.

## **Document Compliance**

Creating documentation for compliance can be a very laborintensive task involving extensive research, many documents and plans, and months of work by specialists. The required documentation for many standards is voluminous indeed.

For example, FedRAMP certification requires:

- ☐ A System Security Plan (SSP)
- ☐ A Configuration Management Plan ☐ A Contingency Response Plan ☐ An Incident Response Plan.
- ☐ An additional 34 documents describing 17 control family plans and procedures.

In some cases, the standards group or government agency offers a standard form or template that specifies the information and artifacts needed to document compliance. Examples include the FedRAMP SSP and the PCI DSS Report on Compliance (ROC). More often, however, required documents

Chapter 4: Integrating the Application and Documenting Compliance | 29

---

are named (e.g.: a “personal data protection policy,” an “incident response plan,” “access control policy and procedures”) but the detail is left to the enterprise and its auditors. These general mandates offer flexibility, but place a burden on the organization to decide, “What detail is expected, and how much is enough?”

In addition, several important standards require enterprises to produce assessments that describe gaps in their current security and compliance controls and to produce a monthly remediation plan or a “Plan of Action and Milestones (POA&M)” that outlines planned corrective actions and improvements.



Compliance documentation is never static. Documents and plans need to be updated on a regular basis as applications change and your compliance program matures. We will discuss this in the next chapter.

## ***Automating compliance documentation***

There are several ways to simplify and automate the creation of compliance documentation.

You can find templates that illustrate the structure and content of documents and plans that have been used in the past to achieve compliance. Some are offered by standards bodies, government agencies, and compliance specialists.

You can also turn to providers of solutions that automate the creation of compliance documentation. They offer document generators that capture data from different sources and prepopulate sections of forms and reports. For example, a document generator might discover a list of the servers and other systems in the environment and automatically insert the list into the relevant documents.



**TIP** When considering compliance automation options, give careful consideration to those that employ an “*enter once, populate everywhere*” approach to documentation. It can save hundreds of hours of work. In fact, it is one of the factors that enable pre-engineered cloud security platforms to make applications audit ready 80 percent faster than conventional compliance processes.

## **Validate Compliance**

Different standards bodies and government agencies have different approaches to validating compliance. Typically, an audit is conducted by a licensed individual or company, sometimes called a Qualified Security Assessor (QSA) or a Third-Party Assessment Organization (3PAO). Successful completion of the audit can lead to an official certification, “authority to operate” (ATO), or other formal recognition of compliance.

In some cases, organizations certify themselves through a review, assessment, or audit conducted by an internal auditor, a “data protection officer” (DPO), or an outside consultant.



Reviews and assessments may be less expensive and timeconsuming than formal audits, but they are not an excuse for slacking off. The penalties for failure can be quite severe if the U.S. Department of Health and Human Services’ Office for

Civil Rights (OCR) or the European Union's Information Commissioner's Office (ICO) decides to audit you for compliance (with HIPAA or with the GDPR, respectively). The fines for noncompliance with the GDPR can reach up to 10 million euros or 2 percent of annual revenue for some infringements, and up to 20 million euros or 4 percent of annual revenue for major violations.

## ***Accelerating validation***

There isn't much that organizations can do to accelerate the audit itself, but several activities prior to an assessment or audit can and should be automated. These activities identify weaknesses in technology and processes that could cause the enterprise to fail a review or audit. They include:

- ☐ Vulnerability scans, to find vulnerabilities and misconfigurations in systems and networks
- ☐ Penetration (pen) testing, to uncover weaknesses and policy violations in systems, networks, platforms, applications, and security tools
- ☐ Piloting of key processes, to identify shortcomings in workflows, data acquisition and analysis, and analyst and administrator training

# Chapter 5 **Staying Compliant with Automation and Standardization**

## In this chapter

- Learn about strategies for keeping applications secure and compliant over time
- Review the advantages of standardization and a “prepare once, audit many” approach

*“Every successful organization has to make the transition from a world defined primarily by repetition to one primarily defined by change.”*

– Bill Drayton

---

## **Stuff Happens**

**H**eraclitus’ maxim, “The only thing that is constant is change,” certainly applies to the world of security and compliance. Computing infrastructures continuously evolve, driven by changing business needs and new technologies. New cyberthreats emerge and inspire new defenses. Standards and regulations grow more detailed and comprehensive, and new ones appear. Organizations need to adopt several strategies to cope with these different challenges and maintain security and compliance over time.

# Continuous Monitoring

## *Threat detection*

Many standards explicitly require continuous monitoring of the computing environment to detect indicators of compromise (IOCs) and other signs of ongoing attacks. Typically, monitoring involves collecting data from a wide variety of security tools, correlating and analyzing the data using SIEMs and security analytics tools, and executing incident response workflows to analyze and respond to attacks.

These activities are time sensitive and involve massive amounts of data. Making them effective requires three types of automation:

1. Integrating the security and security analytics tools in the cloud environment and automating the process of collecting data from many sources
2. Automating the filtering and analysis of the data, often using machine learning and other artificial intelligence techniques to detect anomalies
3. Automating the incident response and threat analysis workflows

## *Threat hunting*

Threat hunting is another important form of continuous monitoring. It involves using threat intelligence to determine likely attacks on the enterprise, then proactively looking for indicators of those attacks.

Threat hunting requires careful thinking by experienced security analysts. However, many tasks can be automated, such as collecting and filtering threat intelligence, matching external threat intelligence with information from the enterprise's information systems, and searching for IOCs on the network and in the cloud environment.



For a broad perspective on continuous monitoring and ongoing security assessments, see the [Conducting Continuous Monitoring](#) page on the FedRAMP.gov website.



---

## Ongoing Assessment

To cope with changes in cloud environments and with new threats, organizations need to conduct ongoing assessments of their systems, networks, and security controls. These assessments may take the form of:

- ⇒ Updating inventories of information system and cloud components, to identify new assets that need to be protected

- ⇒ Conducting vulnerability scans, to find vulnerabilities and misconfigurations in systems and networks

- ⇒ Testing security controls, to validate their effectiveness (for example, ensuring that authentication is being performed correctly based on the organization's policies)



- ⇒ Performing pen testing, to uncover weaknesses and policy violations by replicating the methods used by attackers

All ongoing assessment processes should be automated as much as possible. Most of them involve repetitive tasks that can be scripted and handled by automated tools.

## Remediation

After attacks and vulnerabilities are identified, many clean-up and remediation tasks can be automated. These include:

- ▢ Distributing and applying software patches
- ▢ Fixing configuration errors in servers, endpoints, and network devices
- ▢ Updating policies in security tools



Set up explicit processes for “control tuning”: periodically analyzing the performance of security tools and optimizing their settings. That means, for example, adjusting policies and parameters to filter out false positives and to prioritize indicators of the attacks that pose the greatest risk to the enterprise.

## Software Development Life Cycle Management and Testing

In Chapter 3 we discussed how to build compliance and security into the software development life cycle so security- and compliance-related defects can be uncovered and corrected sooner.

Tools and techniques like automated DevOps pipelines and continuous deployment are critical for ongoing compliance. Just as it is important to prevent compliance issues from delaying the delivery of new software applications, so it is vital that compliance automation support fast enhancements over the life of existing applications.

## Reporting and Dashboards

Most major standards and regulations require ongoing reports of various kinds, including:

- ⇒ Monthly, quarterly, or annual assessments of security controls and processes, covering subjects like account management, access controls, software patching, data protection and privacy, firewall configurations, data encryption, and incident reporting
- ⇒ Remediation plans and plan of action and milestone (POAM) reports detailing how the organization will address known vulnerabilities and flaws in security controls
- ⇒ Change control and impact assessment reports that document changes in applications, infrastructure, and processes, in system and device configurations and rules, and in security and privacy policies
- ⇒ Risk assessments that identify internal and external risks, evaluate the organization's overall security posture, and measure progress toward compliance

Organizations can automate the collection of data for these reports and assessments and speed up the production of the documents themselves using tool such as:

- ⇒ Change control and configuration management systems

---

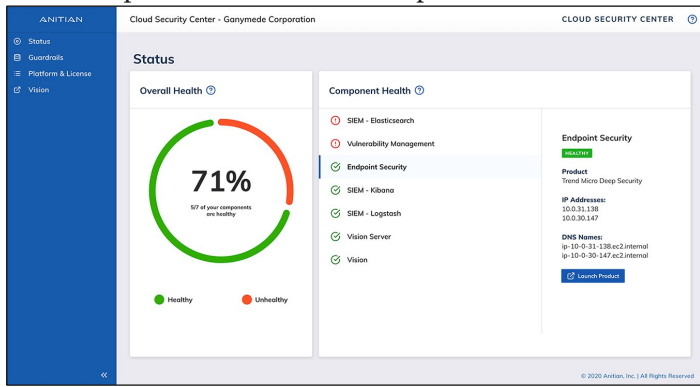
## Chapter 5: Staying Compliant with Automation and

Standardization | 35 ⇒ Secure repositories to collect and manage completed compliance documents, security and network logs, the output of security analysis and forensics reports, and other security and compliance artifacts

- ☰ Report and document templates
- ☰ Report generators

## Compliance dashboards

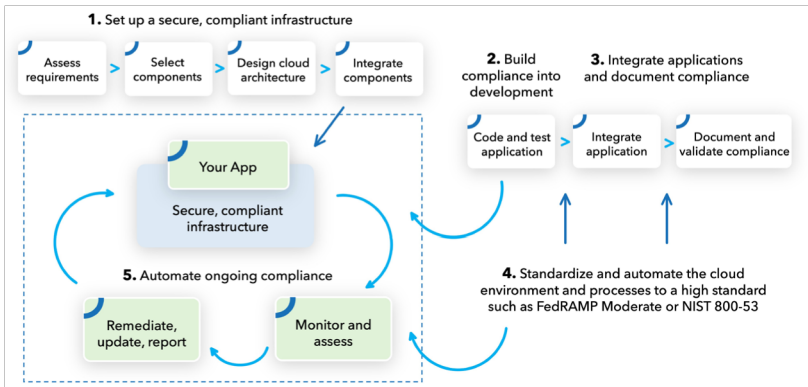
A compliance dashboard is an excellent tool to help manage compliance over time. It can show progress toward meeting overall compliance goals and pinpoint weak spots that could potentially result in failed assessments and audits. Figure 5-1 is an example of a screen from a compliance dashboard.



**Figure 5-1:** Example of a screen from a compliance dashboard, showing progress toward meeting FedRAMP requirements. (Source: Anitian)

## Prepare Once, Audit Many

Enterprises covered by multiple standards should start by creating a standard environment and processes designed to handle one of the more demanding regulations such as FedRAMP or NIST 800-53. Afterwards, this same environment can support additional, less-demanding regulations with little modification. Figure 5-2 illustrates this “prepare once, audit many” approach, which reduces costs and compliance-related delays over time.



**Figure 5-2:** A standardized environment and automated processes enable organizations to protect more applications and satisfy additional regulations with little incremental effort.

## Outcomes of Standardization

The advantages of a standardized cloud infrastructure and standardized processes include:

- ☐ Faster time-to-compliance and time-to-revenue, because applications can be dropped into a secure, compliant environment and compliance can be documented with much less effort
- ☐ Easier management and faster response, because all the security, compliance, and management tools are integrated
- ☐ Lower license and administrative costs, because the organization only needs to license and learn one set of tools

The improvements can be striking. Some organizations have:

- ☐ Shortened time-to-market for a new software product by 80 percent
- ☐ Reduced the cost of compliance by 50 percent

In the next chapter we look at real-life examples of organizations that are achieving outcomes like these.

## Chapter 6 **Audit Ready in Weeks: A Case Study**

### In this chapter

- Review a case study of compliance automation and its benefits for an industry-leading cybersecurity company
- Find links to case studies about simplifying FedRAMP, PCI DSS, HIPAA, and GDPR compliance for cloud applications

*“One eye-witness is worth more than ten hearsays.”* –  
Plautus

---

### Is This Stuff Real?

Some claims made for compliance automation can sound like hype: *new cloud applications made audit ready in weeks rather than months or years...organizations with minimal in-house knowledge of cloud security and compliance smoothly migrating applications to cloud platforms...companies entering new markets months earlier than expected.* But experience has proved that results like these occur on a regular basis.

In this chapter we present one case study and provide links to three others that illustrate some of the advantages of a compliance automation platform.

# Case Study: SentinelOne and FedRAMP Certification

## *About SentinelOne*

SentinelOne is a cybersecurity solutions company based in Mountain View, California. It has more than 800 employees and almost 5,000 customers. The company's flagship Singularity Platform combines an autonomous endpoint protection platform (EPP), endpoint detection and response (EDR), IoT security, and cloud workload protection (CWPP). Its solutions meet the requirements of some of the world's most demanding government and defense agencies and enterprises in healthcare, finance, energy, retail, and other fields.

SentinelOne is often recognized as an industry pacesetter. It was named a leader in the 2021 Gartner Magic Quadrant for EPPs and is the only EDR vendor ever to achieve 100 percent visibility in a MITRE Engenuity ATT&CK evaluation. The company has been named to the Forbes AI 50 List, the CNBC Disruptor 50, and the Deloitte Fast 500.

## *Certification stalled*

The company's cloud-based technology is very complex and cutting edge, featuring distributed AI and enterprise-scale data analytics. It works across Linux and Windows servers in Amazon EC2 environments and workloads in Docker and Kubernetes containers, as well as on a wide variety of endpoints.

SentinelOne was anxious to achieve FedRAMP Moderate certification and have its solutions hosted in Amazon AWS GovCloud regions so it could grow its footprint in the U.S. federal government and defense marketplace. The outside consultant hired to lead the certification effort wasn't moving fast enough to meet the company's goals.

## ***Solution: A pre-engineered cloud security infrastructure***

When investigating alternatives, the chief information security officer (CISO) of SentinelOne came across information about a cloud automation platform offered by Anitian (<https://www.anitian.com/>).

The platform included a cloud security infrastructure with a complete stack of security and compliance technologies and controls, integrated with each other and with native tools of the AWS cloud platform. The CISO verified that this infrastructure had already enabled several companies to achieve FedRAMP certification and was therefore “a known good commodity.” His team would not have to spend time researching FedRAMP requirements, designing a compliant environment, and evaluating security products. They could simply “wire up” their application into the infrastructure designed by Anitian.

SentinelOne already had a lot of the basic documentation needed for FedRAMP certification, but Anitian was able to help the company quickly update it to take the new platform into account.

## ***Business impact***

Compliance automation dramatically shortened the wait time to achieve FedRAMP certification and begin generating revenue from U.S. federal government and defense agencies. SentinelOne’s application was ready for the audit for FedRAMP moderate certification (which requires demonstrating compliance with 325 controls) just 10 weeks after beginning the project with Anitian. It obtained Authority to Operate (ATO) in only 8 months.

The company’s EPP product is now hosted on the FedRAMP.gov website, and is being used by several U.S. federal agencies

FedRAMP authorization has given SentinelOne credibility not only with federal agencies, but also with a wide variety of organizations that serve government customers. They include defense contractors and their suppliers, research labs, managed services providers (MSPs), managed security service providers (MSSPs), and managed detection and response (MDR) companies.



## Certification as a competitive advantage

“With limited budget and staff, puts SentinelOne in a position of federal agencies rely heavily on strength as we look to help more their technology partners to help agencies improve their cyberdethem overcome both cybersecurity fenses and protect themselves and other technology challenges. – and US citizens – against ever

Government entities desperately  
a product roadmap to help

increasing cyberattacks.” need

determine which vendors to

Patty Trexler, Vice President, them

The FedRAMP designation

Government, Healthcare, and trust.

Education, SentinelOne.

ON THE WEB



You can find more compliance automation case studies at: <https://www.anitian.com/resources/case-studies/>. Examples include: [Smartsheet](#) (ready for a FedRAMP moderate certification audit in under 60 days and received ATO in under 4 months), [World Web Technologies](#) (PCI DSS compliance), and [Orion Health](#) (HIPAA, HITRUST, GDPR, and PCI DSS compliance).

# Chapter 7 Compliance Automation Platforms

## In this chapter

- Review the reasons for adopting compliance automation
- Examine the idea of a compliance automation platform

*“Don’t try to reinvent the wheel. Just learn from the guys who have already done it well.”*

– George Foreman

---

## The Big Reasons for Compliance Automation

In this guide we have outlined how compliance automation helps organizations address five challenges: setting up a secure, compliant cloud infrastructure, building compliance into development and test, integrating applications into the environment and documenting compliance, standardizing the compliance and security environment, and keeping applications compliant over time. The key benefits include:

- ☐ Better IT and cloud application security
- ☐ Reduced security and compliance costs
- ☐ Quicker time-to-market for enterprises serving or selling to regulated industries ☐ Increased business

agility and faster migration of applications to cloud platforms.

## Compliance Automation Platforms

Organizations that recognize the value of compliance automation should investigate compliance automation platforms such as the one provided by Anitian, the sponsor of this guide. A robust compliance automation platform offers features such as:

- ⇒ A pre-engineered security and compliance environment with a full set of integrated security and management tools
- ⇒ Templates and tools that accelerate the processes of integrating applications into the environment and documenting compliance with specific standards
- ⇒ Tools and services to monitor applications and keep them secure and compliant over time
- ⇒ Integration with DevOps pipelines and processes

The advantages of implementing compliance automation through such a platform include:

- ⇒ Eliminating the work of assessing, purchasing, deploying, and integrating cloud-based security and management tools and designing a cloud architecture
- ⇒ Slashing the time and cost required to integrate applications into a secure environment, document compliance, pass audits, and achieve certifications
- ⇒ Implementing a “prepare once, audit many” approach that increases the odds of certifying compliance the first time through and passing multiple audits after
- ⇒ Significantly reducing the costs and resources (staff and consultants) needed to implement and manage cloud security and compliance
- ⇒ Achieving a stronger security posture and avoiding data breaches.

ON THE WEB



For a brief introduction to compliance automation platforms, read the [SecureCloud for Compliance Automation Solution Brief](#).

# ANITIAN

Get to cloud and market 80% faster.  
**Do it for 50% of the cost.**



Simple. Fast. Secure. Compliant.

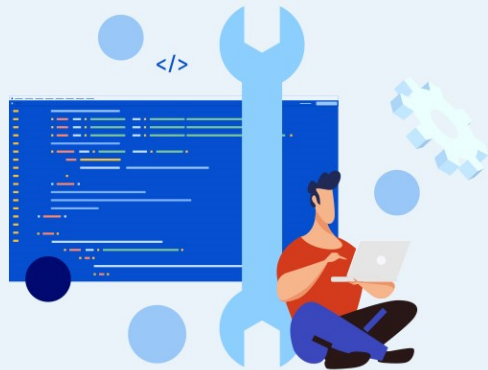
## FOR COMPLIANCE AUTOMATION

FedRAMP audit-ready in 60 days at 50% of the cost.

## FOR ENTERPRISE CLOUD SECURITY

Secure your applications from cloud to production.

## Industry Awards



# Learn how to make cloud applications FedRAMP, PCI, CMMC, or StateRAMP audit-ready in weeks and keep them secure and compliant over time.

Building security and compliance into cloud applications doesn't have to be a slow, manual, error-prone process. Discover how automation and standardization enable you to quickly and accurately set up a secure, compliant cloud environment, build security and compliance into code, and produce and update compliance documentation.

- **Compliance automation for cloud applications** — understand the concept and the business problems it solves
- **Creating an infrastructure** — learn how to build a cloud infrastructure that meets security and compliance requirements
- **Building compliance into development** — review how to promote secure coding and testing for DevSecOps
- **Automating compliance documentation** — examine ways to generate documents for auditors and regulators
- **Staying compliant** — explore strategies for keeping applications continuously secure and compliant
- **Real life examples** — see how organizations have saved months releasing cloud applications and entering new markets

## ***About the Author***

Jon Friedman has over 20 years experience in industry analysis and marketing roles at software and IT services companies. He has described cutting-edge technologies and their business benefits for more than 40 high-tech companies. Jon has a BA from Yale and an MBA from Harvard.



**CYBEREDGE**  
PRESS

Not for resale

ISBN 978-1-948939-21-8



9 781948 939218 >