

dash™

Guide to Continuous Compliance Monitoring



Table Of Contents

What is Continuous Compliance Monitoring?

02

Why Implement Continuous Compliance?

03

Security and Compliance in the Public Cloud

04

Architecting Secure Cloud Environment

06

Developing A Continuous Compliance Monitoring System

08

Continuous Compliance with Dash ComplyOps

16

What is Continuous Compliance Monitoring?

Continuous Compliance Monitoring is the process of scanning, monitoring, and assessing security and compliance standards across your IT infrastructure. This is typically done by first setting baseline security controls and then measuring security across cloud and IT environments.

Organizations, especially in regulated industries such as healthcare and finance are building continuous compliance processes in order to better manage their security process and ensure compliance across their applications and workloads.

Continuous compliance monitoring provides security teams with a real-time view into security and compliance concerns and enables teams to proactively find and resolve security concerns before they turn into problematic issues like breaches or violations. In this guide, we will walk through the steps to building a continuous compliance monitoring process for the cloud.

Dash ComplyOps provides [continuous compliance monitoring](#) capabilities so teams can gain insight into cloud security and ensure regulatory compliance.



Why Implement Continuous Compliance?

Organizations implement continuous compliance processes in order to meet numerous security objectives.



Increased Security Visibility

Unlike traditional point-in-time assessments and security audits, continuous compliance monitoring provides security teams with real-time security findings and better security insight into an organization's state of compliance.



Meet Regulatory Compliance Requirements

Many regulatory standards and compliance standards such as [HIPAA](#), [SOC 2](#) and PCI DSS require organizations to maintain security standards over time. Organizations build continuous compliance monitoring to ensure that IT infrastructure does not fall out of compliance with regulatory requirements even as their IT infrastructure undergoes changes.



Lower Overhead And Security Time Investment

Continuous compliance monitoring allows teams to automate security assessment and enables teams to evaluate security efforts with less time invested by security staff and consultants.



Faster Enterprise Security Procurement

Organizations selling to enterprises and regulated industries can utilize continuous compliance monitoring and reports as validation of security efforts in order to speed up enterprise security procurement and answer [security risk assessments \(SRAs\)](#).

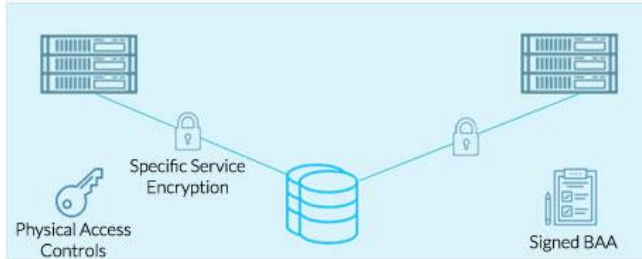
Security and Compliance in the Public Cloud



With the growth of public cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure, cloud security is an integral part for safeguarding applications and workloads. Consequently, teams should factor cloud security responsibilities into continuous compliance processes.

Security teams should understand the cloud shared responsibility model and cloud security requirements described below.

Cloud Shared Responsibility Model



Cloud Platform Responsibilities

Cloud platforms are responsible for security "OF" the cloud



Your Organization's Responsibilities

You are responsible for security "IN" the cloud

AS WELL AS

All Administrative controls and policies

Most cloud providers including Amazon Web Services (AWS) and Microsoft Azure follow a [shared responsibility model](#) for security and compliance. Under this model, security and compliance safeguards are a "shared responsibility". This means that while cloud service providers are responsible for specific physical safeguards and availability of certain services, it is up to the customer to implement all necessary administrative policies and technical safeguards within the cloud environment.

In other words, cloud service providers such as AWS provide physical and administrative “Security OF the Cloud”, whereas cloud customers are responsible for managing cloud service configuration, applications and “Security IN the Cloud”.

Cloud Provider Responsibilities

Cloud providers often manage all physical safeguards such as locking servers and restricting employee access to systems. Cloud providers also offer cloud customers with many cloud services and security configuration settings that security teams can leverage to implement technical security controls.

Cloud service providers manage security settings such as:

- Specific agreements including service level agreements (SLAs) and [business associates' agreements \(BAA\)](#)
- Facility access, employee access, and locking servers
- Specific encryption settings

Cloud Customer Responsibilities

Organizations managing production services in the cloud are responsible for creating administrative policies and standard operating procedure as well as configuring security settings and technical standards such as:

- Audit logging
- Firewall and networking
- Anti-virus and anti-malware
- Security Configuration and Architecture
- Patch Management
- Backup and disaster recovery (DR)
- Intrusion detection systems (IDS)
- Vulnerability scanning

Building continuous compliance processes enables teams to ensure that cloud security standards and controls in these categories are maintained in the cloud environment.



Architecting Secure Cloud Environment



Developing Your Cloud Architecture

Organizations should keep security in mind when building cloud-based applications. Teams should consider architecting around the following principles.






Security – Applications and workloads should be architected with a high level of security. Teams should restrict access, based on the “principle of least privilege”, and ensure that users have only the minimum necessary permission to complete their tasks.

Reliability – Teams should build reliable systems that provide predictable performance, and deployments. Organizations should consider implementation of processes for change management and configuration management.

Availability – Teams should ensure that production systems are highly available, by architecting services across multiple regions, availability zones (AZs) and implementing standards for proper failover.

Protecting Against Cloud Security Issues

Teams must ensure they develop cloud security controls that protect their organization against security breaches. When operating in the cloud, there are some unique threats to an organization's security program. Security teams should work to build controls to protect against following types of issues:

-  **Permissions/Access Issues** - Improper users, roles, and permissions are at risk of privilege escalation and unauthorized access.
-  **Network Issues** – Public cloud platforms enable organizations to configure numerous network security settings. Teams with insecure networking settings around firewall, ports, and NACLs could end up with vulnerable networks.
-  **Availability Issues** – Organizations managing production workloads in the cloud typically build for high availability. Cloud service issues related to load balancers, NAT gateways, and issues with fail-over could lead to a potential service outage.
-  **Data Loss Issues** – Individual cloud services with improper security controls or settings may be vulnerable to hacking and may be accessed by unauthorized third parties.
-  **Compliance Issues** - Regulatory compliance standards such as HIPAA and cybersecurity standards such as SOC 2 require teams to maintain specific security standards for IT infrastructure. Missing protections, or changes to security configuration could lead to non-compliance.

Implementing Security Controls

In order to protect your organization from the types of cloud security issues listed above, your team should plan to implement cloud security controls to ensure the integrity of your cloud resources. Teams should implement technical security controls including:

- Encryption
- Audit Logging
- Access Control
- Backup and Disaster Recovery
- Firewall and Networking
- Intrusion Detection Systems (IDS)
- Vulnerability Scanning

Developing A Continuous Compliance Monitoring System



Defining Your Security Team and Security Roles

Before developing security and compliance programs, organizations should define their security team and key security roles responsible for security and compliance tasks. Teams should consider defining the following roles.

Security Officer – The staff member responsible for planning and implementing technical safeguards and baseline security controls across the IT environment. The Security Officer typically develops technical plans and manages security settings and solutions around standards such as access control, backup, and intrusion detection.

Privacy Officer – The staff member responsible for planning and implementing administrative safeguards. The Privacy Officer manages administrative tasks such as developing and updating administrative security policies and conducting employee security training.

DevOps Lead/Team – The team responsible for implementing and administering specific cloud and application security standards.

Security Incident Response Team (SIRT) – The team responsible for responding to, documenting, and resolving security incidents. This team is delegated power from the Privacy and/or Security Officer and should provide the organization feedback on possible improvements to the security plan.

Creating Security Policies

In order to measure security and compliance organizations should have established security policies and baseline controls to evaluate against. Security policies provide teams with a blueprint for how to manage security configuration.

Organizations should develop security policies and standard operating procedures and consider the follow best practices when writing security policies:

- ✓ Write policies in plain-English and ensure they are understandable by team members
- ✓ Set realistic security standards rather than idealistic standards
- ✓ Build standards around your technical stack and solutions
- ✓ Ensure policies fit your organizational structure
- ✓ Periodically review and update policies to ensure they are up to date

Connecting Policies to Baseline Security Controls

[Administrative policies](#) and procedures provide an outline for operating your company security program, but policies are only valuable if they are followed. Policies should be connected to baseline security controls to enforce security standards.

This means that teams should translate policy standards into configuration management and further infrastructure controls. Consider the following examples for how baseline controls are defined and how security standards are enforced.

Example Policy Standard	Baseline Security Control
<p>Disaster Recovery Policy</p> <p><i>“Company ABC creates backups of production services on a daily basis.”</i></p>	<p>Security teams must configure settings for snapshots and automated backups and test that backup functions continue to work as designed.</p>
<p>System Access Policy</p> <p><i>“Company ABC reviews users, roles, and permissions and removes unnecessary permissions on a weekly basis.”</i></p>	<p>Security teams must create a process for manual or automatic reviews of cloud permissions, IAM users/roles, and update permissions as required.</p>

As you can see, teams must handle security configuration for defined security standards. Additional testing, auditing, and/or manual review is often required to ensure that baseline security controls are properly configured.

Connecting Scanning and Monitoring to Compliance

Just as security controls are connected to policies, organizations dealing with regulatory requirements and cybersecurity standards, should connect compliance standards to [baseline security controls](#).

Security teams may consider creating a “crosswalk” between compliance standards and security standards enabled across IT infrastructure.

Example crosswalk for cloud security controls		
SSH port is open to all	<p>HIPAA Security Rule</p> 	<p>164.308(a)(5)(ii)(B) - Protection from Malicious Software</p> <p>164.308(a)(4)(ii)(A) - Isolation Health Clearinghouse Functions</p> <p>164.312(c)(1) - Integrity</p>
	<p>SOC 2</p> 	<p>CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p>
	<p>HITRUST</p> 	<p>01.v - Information Access Restriction</p> <p>09.v - Electronic Messaging</p> <p>09.m - Network Controls</p> <p>09.x - Electronic Commerce Services</p>

EC2 Security Group(s) opens SSH port to all Ec2

35 of 79 Active Issue Item(s) Resolved First Occurrence: 4 months ago
3 Active Issue Item(s) Ignored Most Recent Occurrence: 6 days ago

High Priority

Compliance Standards:

- HIPAA Controls**
- NIST Controls
- HITRUST Controls
- SOC2 Controls

ADMIN-17 - : 164.308(a)(5)(ii)(B) - *Protection from Malicious Software*
Procedures to guard against malicious software

ADMIN-12 - : 164.308(a)(4)(ii)(A) - *Isolation Health Clearinghouse Functions*
Policies and procedures to separate PHI from other operations

TECH-7 - : 164.312(c)(1) - *Integrity*
Policies and procedures to safeguard PHI unauthorized alteration

Scanning and Monitoring the Cloud Environment

To automate baseline security controls and enforce policy standards, teams must implement security scanning. Unlike traditional vulnerability scanning or intrusion detection, continuous compliance monitoring and scanning is focused on [scanning infrastructure](#) and applications for policy violations.

Cloud security settings can change as applications scale, new resources are added, or additional staff members join the organization. The goal of compliance scanning is to automate the security audit process and find security issues across IT infrastructure as they occur, so they can be quickly resolved.

Teams may consider implementing scanning and monitoring for security configuration including the following:

- ✓ Check access control settings
 - Scan for users, roles, and permissions that may lead to privilege escalation
 - Scan for key rotation
- ✓ Check networking firewall configuration
 - Scan for open ports (SSH, FTP, DB, etc)
 - Scan for public ally available cloud services
- ✓ Check encryption standards
 - Scan for data volume encryption
 - Scan for forced SSL settings
- ✓ Check backup settings
 - Scan for snapshot settings
 - Scan for backup retention settings

When security issues are found they should be resolved by the appropriate security team members and updated in configuration management. Organizations can turn to solutions such as [Dash ComplyOps](#) to conduct [security compliance scanning](#) of cloud environments and find security issues related to infrastructure and compliance standards.

The screenshot shows the 'dash' Compliance Center interface. On the left is a dark sidebar with navigation options: Dashboard, Policy Center, Compliance Center (selected), Compliance Overview, Compliance Issues, Action Center, Report Center, and Settings. The main content area is titled 'Compliance Center' and features a table of 'Compliance Issues Detected During Dash Scan'. The table has columns for Priority, Name, Assigned To, Account, Source, Service, Items, and Date. The issues listed include various security configurations for AWS accounts, such as NACLs, S3 bucket logging, flow logs, and Security Group rules. A right-hand sidebar contains filters for Issue Status, Issue Priority, AWS Accounts, Source, Service, My Issues, and Remediation Available. At the bottom right, it indicates 'Issues - 45'.

Priority	Name	Assigned To	Account	Source	Service	Items	Date
Medium	Subnet(s) with allow all ingress NACLs		AWS Account	scan	vpc	64	3 months ago
Medium	Subnet(s) with allow all egress NACLs		AWS Account	scan	vpc	64	3 months ago
High	S3 Bucket(s) have access logging disabled		AWS Account	scan	s3	56	4 months ago
High	S3 bucket(s) do not have logging enabled		AWS Account	configservice	s3	49	a month ago
Medium	Subnet(s) detected without a flow log	NH	AWS Account	scan	vpc	47	4 months ago
Medium	EC2 Security Group(s) opens TCP port to all		AWS Account	scan	ec2	45	4 months ago
Medium	Versioned S3 bucket(s) without MFA delete		AWS Account	scan	s3	44	4 months ago
High	EC2 Security Group(s) opens SSH port to all	NH	AWS Account	scan	ec2	44	4 months ago
Low	EC2 default Security Group(s) in use with rules		AWS Account	scan	ec2	40	4 months ago
Medium	S3 Bucket(s) do not have versioning enabled		AWS Account	scan	s3	34	4 months ago

Resolving Cloud Security Issues

Identifying security findings is one part of the security process. Teams must work to resolve security issues and ensure that issues remain resolved.

Creating Security Reports

The first step to resolving cloud security issues is to create a list of security issues based on findings from cloud scans and monitoring. Teams should outline discovered security issues, relevant policy and security control violations, and helpful metadata.

Teams may use these security reports to prioritize issues, determine remediation tasks and plan next steps for resolving issues. Reports that accurately inventory security controls and issues provide teams with validation of security standards.

The screenshot displays the Dash Report Center interface. On the left is a dark sidebar with the 'dash' logo and navigation menu items: Dashboard, Policy Center, Compliance Center, Action Center, Compliance History, Report Center, and Settings. The main content area is titled 'Report Center' and shows a list of security issues. The issues are grouped into two sections: 'Administrative Safeguards' (green header) and 'Technical Safeguards' (orange header). Each issue is listed with a status indicator (green or red dot), a right-pointing arrow, and a description.

Category	Issue ID	Description	Status
Administrative Safeguards	164.308(a)(1)(i)	Security Management Process - ADMIN-1	Resolved (Green)
	164.308(a)(1)(ii)(A)	Risk Analysis - ADMIN-2	Resolved (Green)
	164.308(a)(1)(ii)(B)	Risk Management - ADMIN-3	Resolved (Green)
	164.308(a)(1)(ii)(C)	Sanction Policy - ADMIN-4	Resolved (Green)
	164.308(a)(2)	Assigned Security Responsibility - ADMIN-5	Resolved (Green)
Technical Safeguards	164.312(a)(1)	Access Control - TECH-1	Open (Red)
	164.312(a)(2)(i)	Unique User Identification - TECH-2	Open (Red)
	164.312(a)(2)(ii)	Emergency Access Procedure - TECH-3	Resolved (Green)

Connecting to your Security Workflow - JIRA, Trello, SIEM Platform



Teams may consider integrating security findings into existing workflow tools and security solutions. In order to manage tasks related to security issues, organizations may track issues in a task management solution such as JIRA or Trello.

Additionally, your team may consider connecting security findings and events into a SIEM solution like Splunk to better query and analyze security findings.

Performing DevOps Tasks

Once a team has identified potential security findings, the team must perform the necessary remediation tasks. These security tasks are generally assigned to DevOps team members. Teams should take the following steps when performing DevOps tasks and remediation actions.

Resolve cloud security settings – Implement the appropriate changes to cloud security settings to resolve the cloud security issue(s).

Test cloud services and applications - Test to ensure that all services are running properly and that remediation actions have not broken any service dependencies.

Change configuration management settings – Make any relevant changes to configuration management systems to ensure that future services do not have the same security issue.

Document resolution actions – Document any actions that are taken to resolve the security issue(s). Update tasks that are managed within your workflow tool.

Updating Security Policies

As teams continue to grow and infrastructure and cloud services are added and modified, it is important to periodically review and update existing administrative policies.

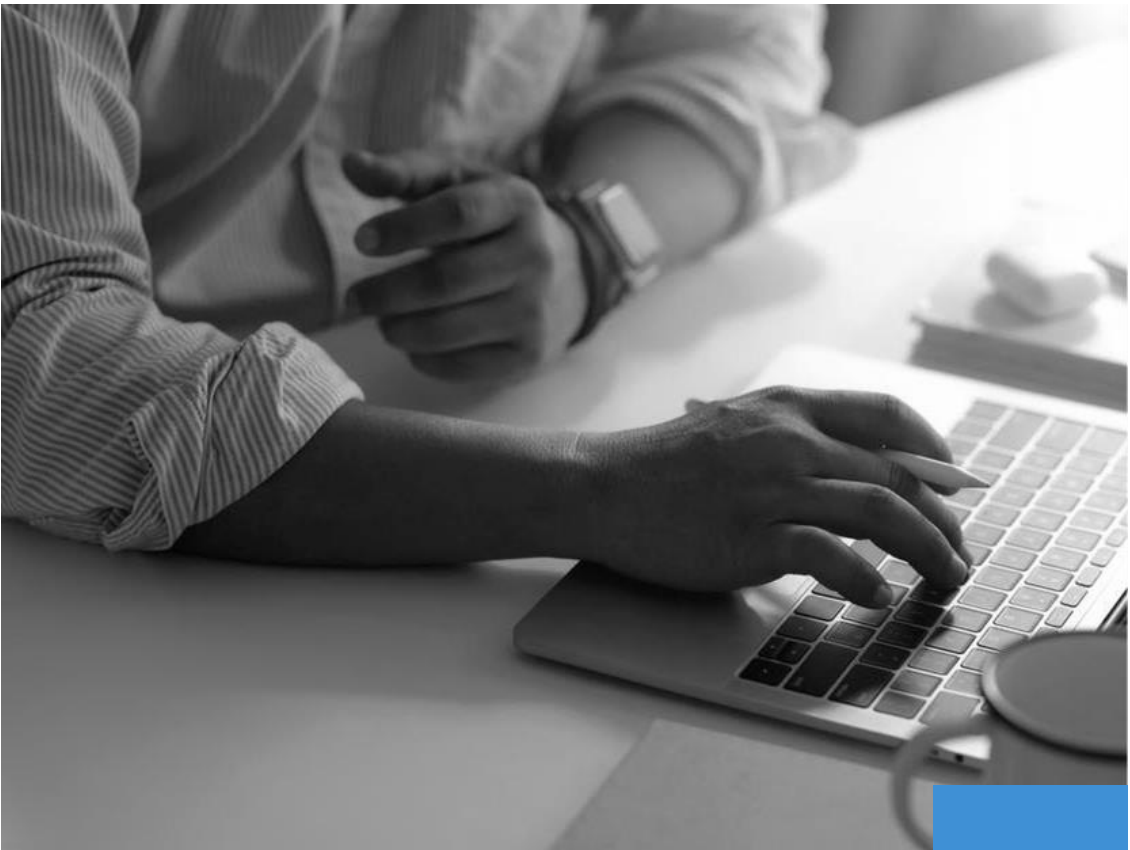
Policies should be updated to reflect changes with staff and roles, new technologies, and new processes. Having a set of up-to-date administrative policies will make it easier for teams to maintain cloud security standards and understand the overall security process.

Having a mechanism that checks policies against your baseline controls will allow teams to better maintain accurate policy documents.

Automating the Process / Maintaining Compliance

While teams may initially manage much of the cloud security and compliance process manually, organizations may look at automating the compliance process in order to make a more effective security program.

Teams will want to look at automating the processes for identifying cloud compliance issues, mapping compliance standards, and building reports and cloud compliance workflow. Tools such as the [Dash ComplyOps](#) platform to build, manage and maintain compliance standards across cloud services.



Continuous Compliance with Dash ComplyOps

7. Configuration Management Policy

Company ABC standardizes and automates configuration management through Ansible, as well as documentation of all changes to production systems and Ansible automatically configure all Company ABC systems according to established policies and are used as part of our Disaster Recovery plan and process.

7.1 Configuration Management Policies

1. Company ABC uses Ansible to standardize and automate configuration management.
2. No systems are deployed into Company ABC environments without approval from the Company ABC VP of Engineering.
3. All changes to production systems, network devices, and firewalls are approved by the Company ABC VP of Engineering before they are implemented to ensure they comply with business and security requirements.

* What individual role or team will handle risk related decisions and reporting for compliance purposes?:

CTO

- CTO
- VP of Engineering
- Senior Management
- Other

* What security scanning tool do you use with your systems?:

OpenVAS

- OpenVAS
- Qualys FreeScan
- Nessus Scanner
- Other

Create cloud security policies by answering simple questions

Set Cloud Security Policies

Dash provides organizations with a set of custom [security and compliance policies](#) built around public cloud best practices and compliance standards including HIPAA, SOC 2, and HITRUST. Teams can utilize answer plain-English questions about their organization, technology, and staff to build robust policies and cloud security controls. Policies include:

- Employee Training Policy
- Facility Management Policy
- Breach Policy
- Configuration Management Policy
- Roles Policy
- Auditing Policy
- System Access Policy

Setup Continuous Compliance Monitoring

Dash enables teams to enforce set security policies across their cloud environment. Dash provides an automated process for scanning and monitoring your cloud environment for security issues across individual resources and cloud services. Compliance issues are automatically identified and are mapped to relevant compliance frameworks.

For example – Dash will identify services with unencrypted data volumes, open SSH ports, missing backup settings and more.

Dash [Continuous Compliance Monitoring](#) allows your team to enforce all security controls defined in your policies. Teams can customize security controls and identify potential security issues before they turn into serious security breaches.

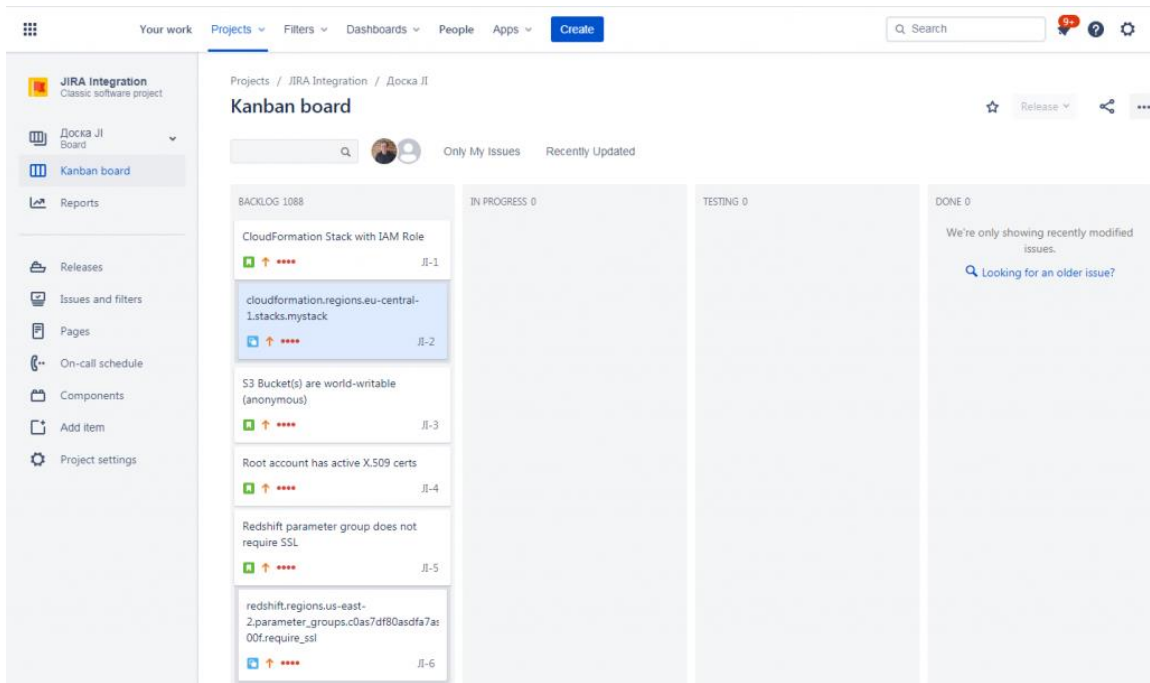
The screenshot displays the Dash Compliance Center interface. On the left is a dark sidebar with navigation options: Dashboard, Policy Center, Compliance Center (selected), Action Center, Report Center, and Settings. The main content area is titled 'Compliance Center' and shows a specific issue: 'EC2 Security Group(s) opens SSH port to all'. The issue status is '35 of 79 Active Issue Item(s) Resolved', with '3 Active Issue Item(s) Ignored'. It includes a 'High Priority' badge and an AWS Account ID: 187515304745. The 'Compliance Standards' section lists HIPAA Controls (ADMIN-17 and ADMIN-12), NIST Controls (ADMIN-12), HITRUST Controls, and SOC2 Controls (TECH-7). Below this, 'Related Policies' includes Data Integrity Policy, Configuration Management Policy, Auditing Policy, and System Access Policy. The 'Issue' section states: 'Exposing SSH port (22) to the public may allow unauthorized access and compromise AWS services via bruteforce, compromised credentials or other attacks.' The 'Recommendation' is: 'For affected EC2 Security Group(s) - Remove or replace Inbound Rules where SSH Port (22) has a Source = Any or 0.0.0.0/0.' On the right, the 'Issue Timeline' shows 'Issue Assigned - EC2 Security Group(s) opens SSH port to all' on Wed Jan 29 2020 16:49:25 GMT+0000 (UTC) and 'Issue Opened' on Thu Jan 16 2020 15:44:34 GMT+0000 (UTC) by user: johnsmith. The 'Event History' section shows three events: '4 months ago' (55 Objects(s) Affected), '3 months ago' (56 Objects(s) Affected), and '3 months ago' (51 Objects(s) Affected).

Dash scans your cloud environment and identifies issues related to compliance standards

Automate Cloud Security and Compliance

Dash provides security teams with the ability to connect compliance monitoring and security findings to other components of your security process. Teams can set up notifications and alerts across email, Slack, and similar services.

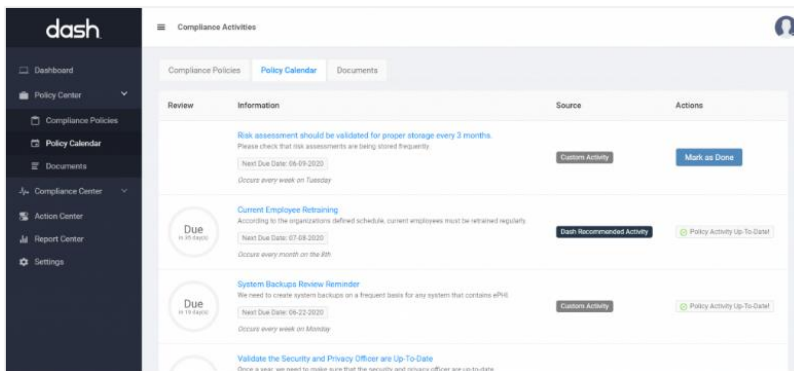
Teams can also connect Dash compliance findings to workflow tools and ticketing systems such as JIRA and Trello. In this way teams can track cloud compliance issues and security programs in the productivity tools they already use. Security and DevOps staff can easily view, assign and track the status of compliance issues.



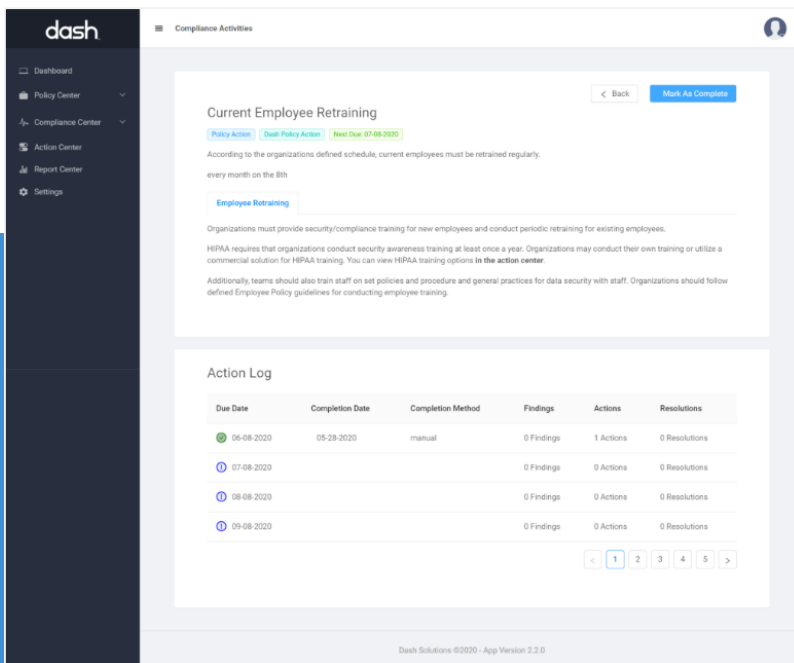
Manage Administrative Tasks

Dash provides tracking of [administrative security](#) and compliance tasks. Dash automatically generates a Compliance Calendar and enables your team to document findings, actions, and remediation steps. Teams can use Dash to store all compliance evidence and reference artifacts in-case of a security assessment or security audit.

Additionally, security staff can access all security documents provided by the cloud provider and may upload any security documents and vendor agreements to consolidate them in a central location.



Administrative compliance tasks are automatically tracked by the Dash Policy Calendar

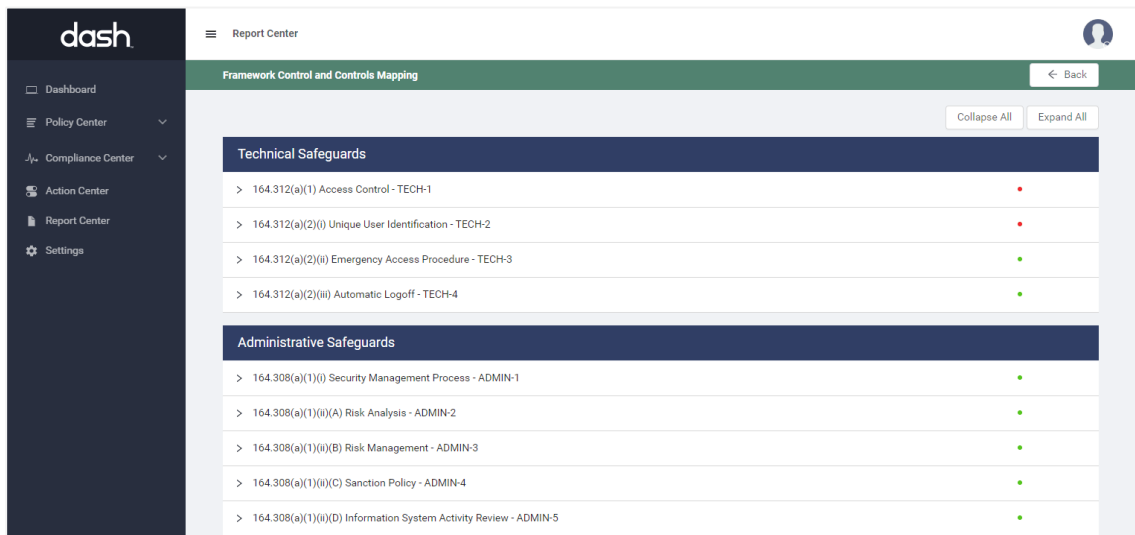


Dash provides next steps for administrative tasks and evidence collection

Generate Security Reports and Validate Security Efforts

Dash provides robust [compliance reporting](#) for validating security efforts internally and during security assessment. Organizations can use Dash reports to answer security risk assessments (SRAs), identify potential security issues, and provide security validation to potential customers and auditors.

Dash Compliance Framework Reports give your team a complete inventory of security as they relate to individual compliance standards for standards such as HIPAA, SOC 2, and HITRUST. Teams can see their current compliance status as related to applicable cybersecurity frameworks and regulatory standards.



Dash report provides an inventory and status of compliance controls



Learn how dash helps organizations manage compliance standards such as HIPAA, SOC 2, and NIST 800-53 in the public cloud

[Tour Dash ComplyOps](#)



dash™

Copyright © 2020 Dash Solutions. All rights reserved.