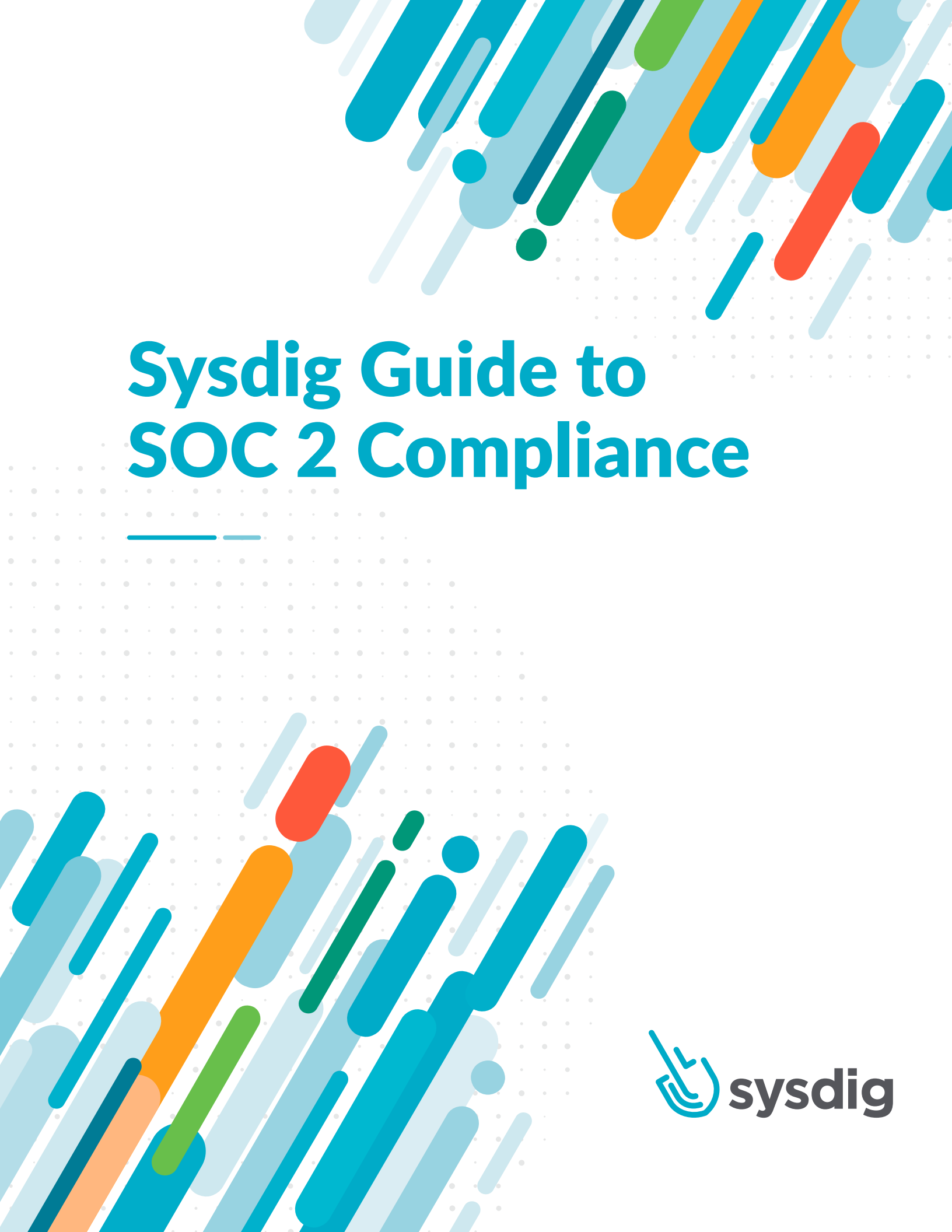
Sysdig Guide to SOC 2 Compliance



Contents

Introduction

All organizations want to be seen as trustworthy in the eyes of their customers and partners. There are many ways a company can instill trust in their brand, but a surefire way to lose credibility — and business — is by not protecting customer data. Instances of customer personal data theft have taken a massive toll on the companies that have had their technology resources attacked. As more data is pushed to the cloud and used in rapidly developed applications, it's a business imperative for that data to be protected.

Modern organizations are prioritizing the security of customer data as a top issue, and a major effort is happening within most companies to ensure that their technology resources are protected against data theft and misuse. Supporting this effort is the SOC 2 framework which provides guidance and requirements to ensure service providers securely manage customer data to protect the interests of the organization and the privacy of its clients. It is intended to provide specific controls and best practices that shape how a company safeguards the security and privacy of customer data..

Understanding the implications of SOC 2

SOC 2 came about as part of the reporting guidelines from the American Institute of CPAs, and was part of their effort to establish guidelines for the privacy of operating with customer data. It operates as an auditing procedure that gives organizations a security framework for the minimal requirements when considering a SaaS provider.

While not a comprehensive, nor prescriptive, list of requirements, SOC 2 identifies and lays out the necessary criteria to ensure development and ongoing management of security behaviors for an organization as they relate to the handling and management of customer information. The language explains specific controls in detail, but each organization has some degree of flexibility in how they adapt and apply SOC 2.

The framework is formed around five categories around which organizations need to ensure trusted compliance when working with user data, including:

- **Security** relates to protection of information and systems from unauthorized access. The intent of this category is to identify and address issues of IT security infrastructures, such as firewalls, multi-factor authentication, and other measures that can help prevent unauthorized access to data.

  The access controls addressed in this category are intended to prevent abuse of systems and technology resources, theft or unauthorized removal of data, and non-allowed usage, alteration, or exposure of data.

- **Availability** addresses the IT and operational environment of an organization, which includes the software, infrastructure, and other resources that store, use, or maintain data. It pertains to the availability and operability of the controls for operation, monitoring, and maintenance. This criteria concerns whether, and how, an organization maintains minimal acceptable network performance levels and assesses and mitigates potential external threats.

  This principle involves security-related criteria that may affect availability, but does not pertain to system functionality and usability.

- **Processing integrity** ensures that processes and systems operate as intended and are devoid of error, omission, delay, and/or unauthorized usage or transactions. The purpose of this element of SOC 2 is to provide the proper data processing operations and ensure they operate in a way that is authorized, complete, and accurate.

  For this principle, it's important to note that processing integrity does not imply data integrity. Any errors contained with data when they are added to systems cannot be addressed as part of the SOC 2 controls.

- **Confidentiality** is about an organization's processes for restricting access to data to specific individuals, or groups of people who are specifically identified within (and external to) the organization. It relates to client data and confidential company information that is restricted. Also, it includes things like strategic plans and intellectual property, as well as data required to be protected by law, regulations, contracts, or agreements.

- **Privacy** criteria is about an organization's ability to safeguard private customer data from unauthorized access. This is typically information like name, social security, or address information, or other identifiers such as race, ethnicity, or health information.

The importance of SOC 2 compliance for security-minded organizations

Compliance with SOC 2 is determined through an audit with a third-party organization that rigorously analyzes the orchestration of controls and how they are applied, creating a more secure environment for data. Much like all compliance standards, adherence is based on how an organization applies controls in a manner that suits their unique needs and those of their clients/customers.

The compliance review process can cover a six-to-12-month timeframe, and the results of audits are intended to both identify general security posture, and specific areas of concern that might indicate security holes or potential for risk within the organization.

Organizations that achieve SOC 2 compliance can assure customers that their data is governed by processes, technologies, and behaviors that are designed to provide the highest degree of protection from within and outside of the enterprise. Compliant organizations can tout that they:

- Understand and operate according to normal operations, and continuously monitor for malicious and/or unauthorized activity. All of this is documented to identify and report on system configuration changes and abnormal behavior.
- Apply tools that recognize and alert on security threats, and can identify where within systems those issues exist so they can be addressed.
- Have access to the most updated and relevant information on security incidents so systems and processes can be improved and remediated to avoid issues in the future.

How Sysdig Secure helps validate SOC 2 compliance

It's also important to note that validating compliance is the **number one blocker** to faster application delivery. Regulators are increasingly enforcing financial penalties for failure to comply.

Studies have shown that:

- Annual cost of non-compliance to businesses runs an average of $14.8 million.
- The cost of compliance, on the other hand, was found to average $5.5 million.

Modern organizations are increasingly using Kubernetes for application development, which is helping them build products and solutions faster. But the dynamic nature of Kubernetes creates an environment in which it's difficult to detect when assets fall out of SOC 2 compliance. Without a clear mapping of SOC 2 guidelines to this new environment, your teams won't be able to prove they meet compliance requirements. As a result, meeting a SOC 2 audit becomes an expensive fire drill, slowing down application delivery for cloud and security teams. Kubernetes compliance requires a new approach.

SOC 2 compliance for workloads and cloud

While SOC 2 controls cover most aspects of a modern IT environment, only some are related to containers, hosts and Kubernetes security. Also, SOC2 framework applies to cloud-native infrastructure. Sysdig Secure validates SOC2 compliance, covering specific controls for workloads and AWS cloud environment.

Below is a comprehensive table where each of the compliance controls apply:

Family ID	Control ID	Family	SOC2-workload	SOC2-AWS
CC3	CC3.2	Risk Assessment	✓	✓
CC5	CC5.1	Control Activities	✓	
CC5	CC5.2	Control Activities	✓	✓
CC6	CC6.1	Logical and Physical Access Controls	✓	
CC6	CC6.2	Logical and Physical Access Controls	✓	✓
CC6	CC6.6	Logical and Physical Access Controls	✓	✓
CC6	CC6.8	Logical and Physical Access Controls	✓	
CC7	CC7.1	System Operations	✓	✓
CC7	CC7.2	System Operations	✓	✓
CC7	CC7.5	System Operations	✓	
CC8	CC8.1	Change Management	✓	
CC9	CC9.1	Risk Mitigation	✓	

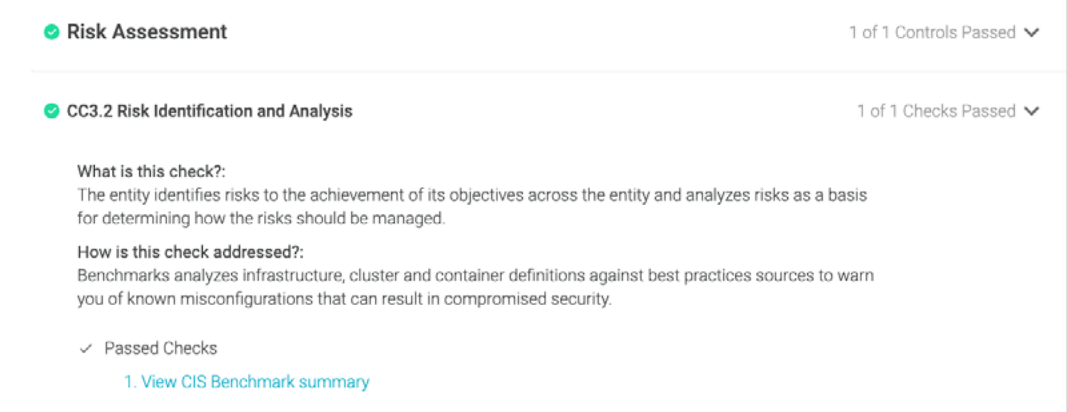
To better understand the extent of SOC 2 and its relevance to your overall security posture and approach, the following is a list of controls, grouped by control family, that Sysdig Secure can help you monitor and manage.

Sysdig compliance controls for SOC 2

CC3 | Risk Assessment

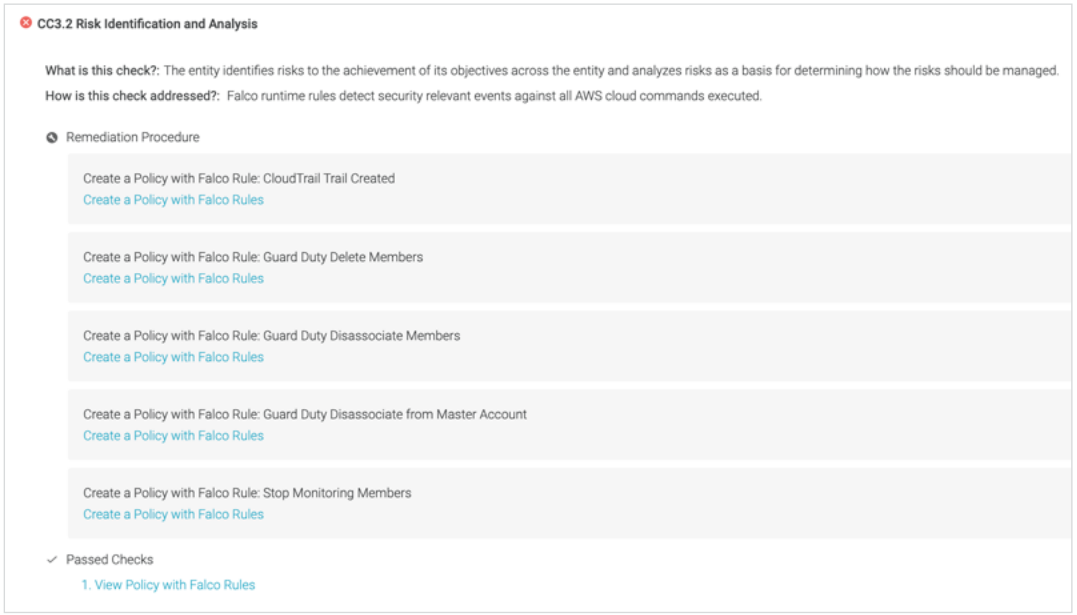
The criteria under CC3 covers COSO Principles 6-9, which address an organization's assessment of risks. It also relates to how risk impacts the organization's operations and the plans and processes the organization develops and applies in order to mitigate those risks.

Control	Description	How Sysdig helps
CC3.2 workload	The entity identifies risks to the achievement of its objectives across the entity, and analyzes risks as a basis for determining how they should be managed.	Sysdig analyzes infrastructure, cluster and container definitions against best practices sources to warn you of known misconfigurations that can result in compromised security.



CC3.2 for workload

Control	Description	How Sysdig helps
CC3.2 AWS	The entity identifies risks to the achievement of its objectives across the entity, and analyzes risks as a basis for determining how they should be managed.	Sysdig's runtime rules detect security relevant events against all AWS cloud commands executed.

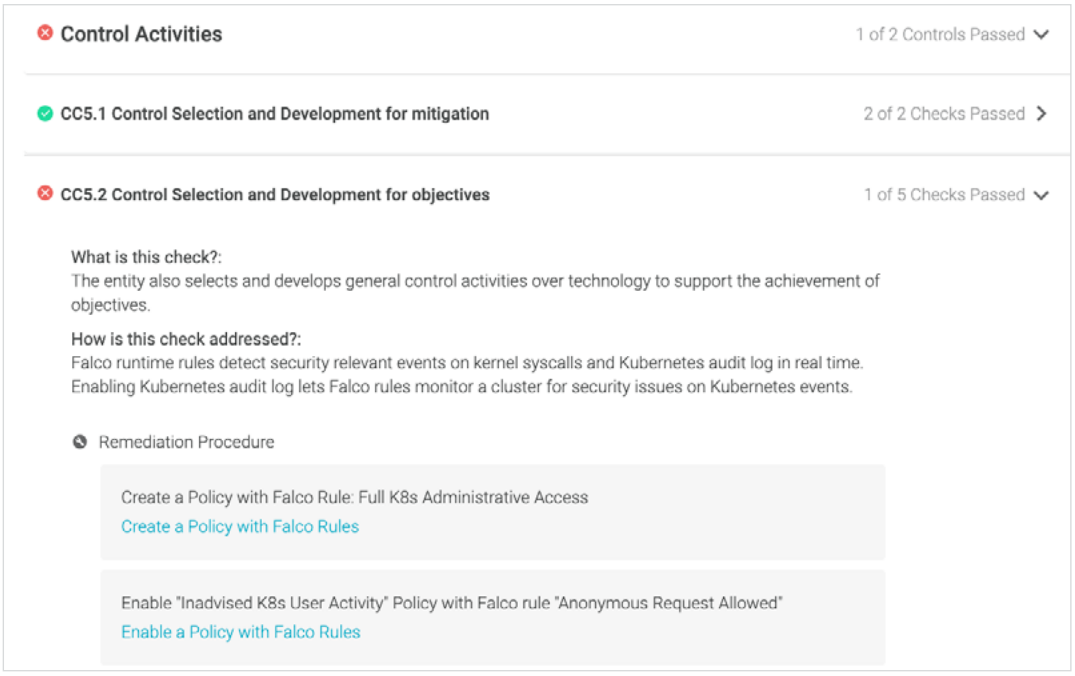


CC3.2 for AWS

CC5 | Control Activities

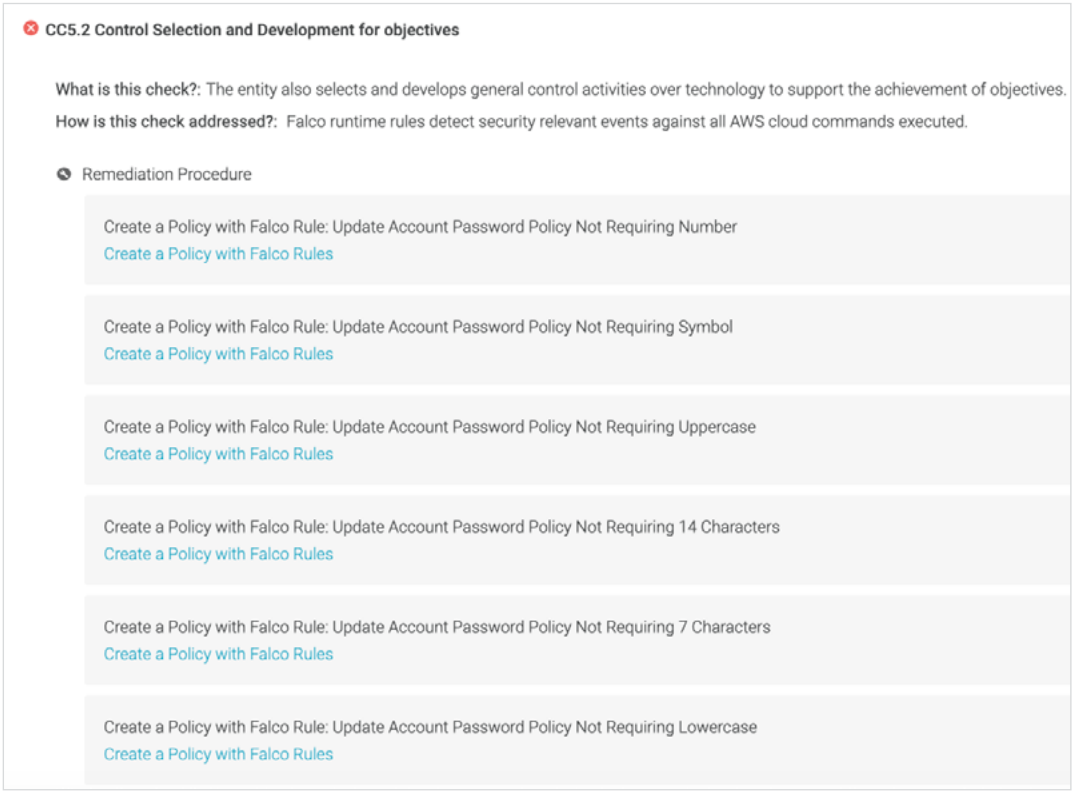
The criteria under CC5 selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control	Description	How Sysdig helps
CC5.1 workload	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Sysdig analyzes infrastructure, cluster and container definitions against best practices sources to warn you of known misconfigurations that can result in compromised security, detecting static and runtime security issues, getting capture data for audit, and preventing and blocking insecure situations.
CC5.2 workload	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Sysdig's runtime rules detect security relevant events on kernel syscalls and Kubernetes audit log in real time.



CC5.1 and CC5.2 for workload

Control	Description	How Sysdig helps
CC5.2 AWS	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Sysdig's runtime rules detect security relevant events against all AWS cloud commands executed.

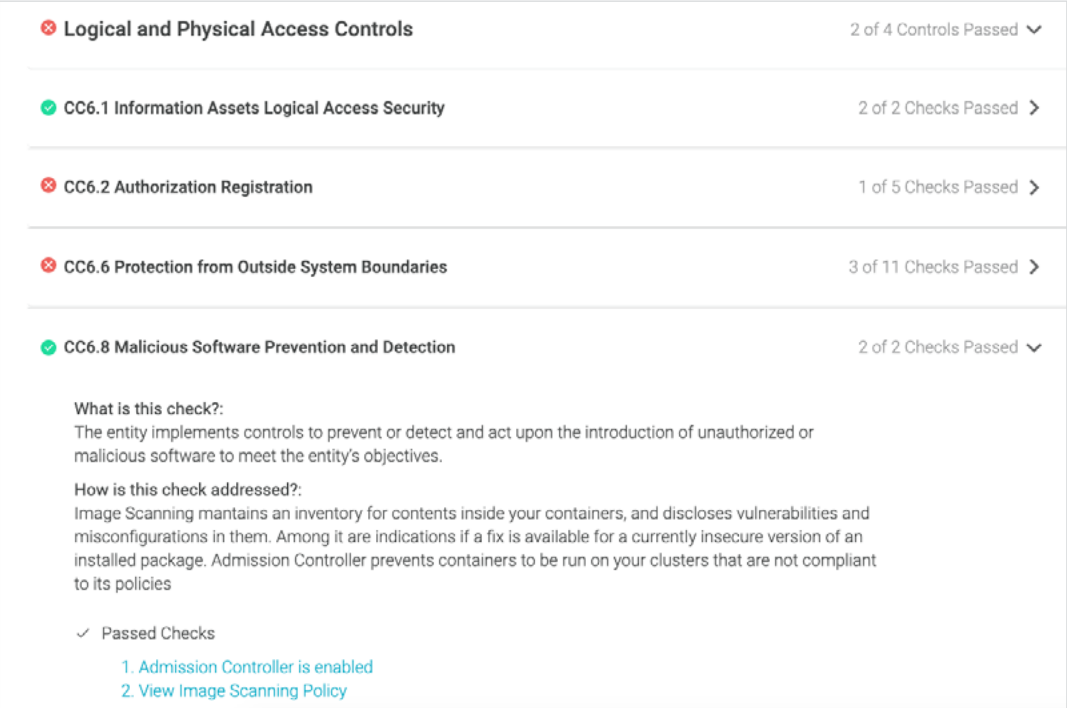


CC5.2 for AWS

CC6 | Logical and Physical Access Controls

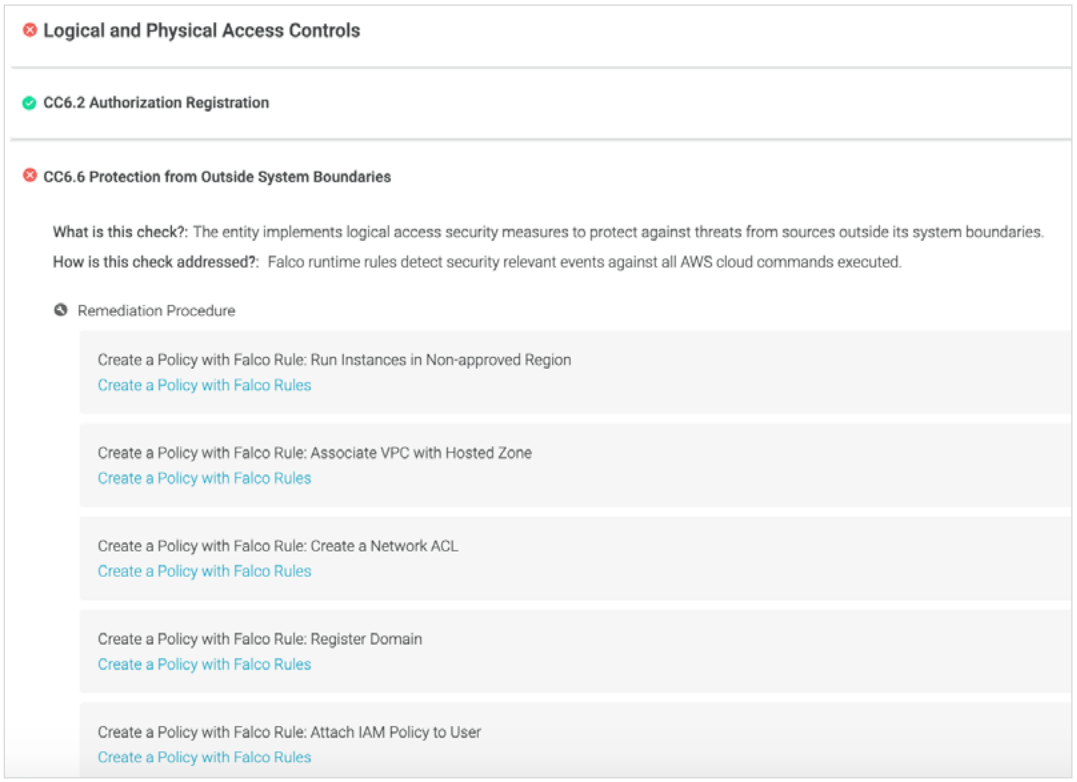
The criteria in CC6 relates to logical access to physical security of an organization's buildings, structures, and resources, and access to security software, software infrastructure, and software architectures in order to protect them from security risks.

Control	Description	How Sysdig helps
CC6.1 workload	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Sysdig's image profiling analyzes a running container image for network ports open and running processes to create a snapshot state, then you can detect deviations from it.
CC6.2 workload	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Sysdig's runtime rules detect security relevant events on kernel syscalls and Kubernetes audit log in real time. Enabling Kubernetes audit log lets Sysdig's runtime rules monitor a cluster for security issues on Kubernetes events.
CC6.6 workload	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network Security feature gives you information on network topology real data flow, helps you propose and visualize existing network security bounds, and create and edit Kubernetes Network Policies to enforce them.
CC6.8 workload	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Image Scanning maintains an inventory for contents inside your containers, and discloses vulnerabilities and misconfigurations in them. Among them are indications if a fix is available for a currently insecure version of an installed package. Admission Controller prevents containers to be run on your clusters that are not compliant to its policies



CC6.1, CC6.2, CC6.6 and CC6.8 for workload

Control	Description	How Sysdig helps
CC6.2 AWS	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Sysdig's runtime rules detect security relevant events against all AWS cloud commands executed.
CC6.6 AWS	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Sysdig's runtime rules detect security relevant events against all AWS cloud commands executed.

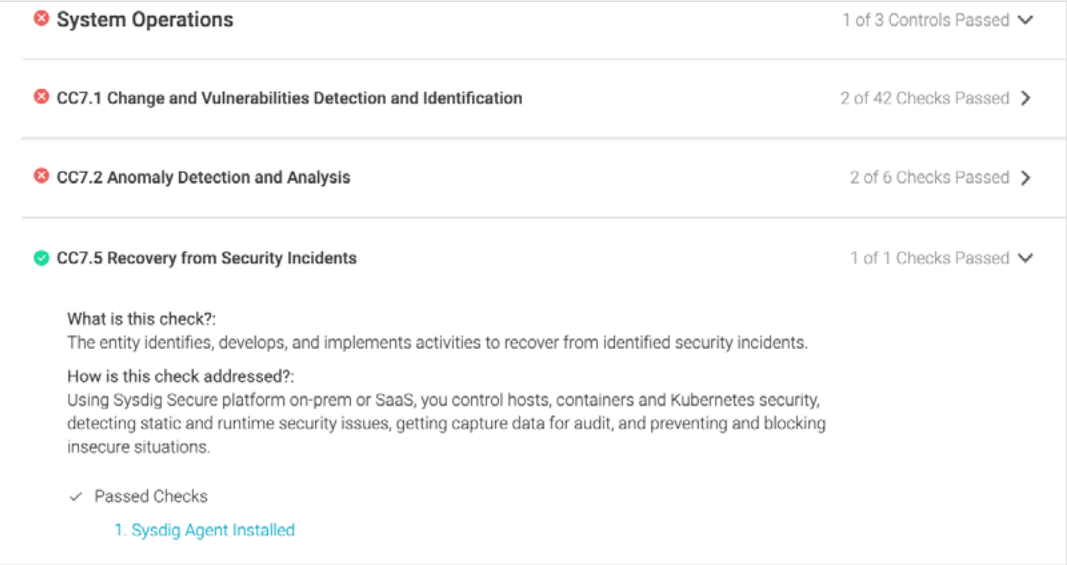


CC6.2 and CC6.6 for AWS

CC7 | Monitoring Activities

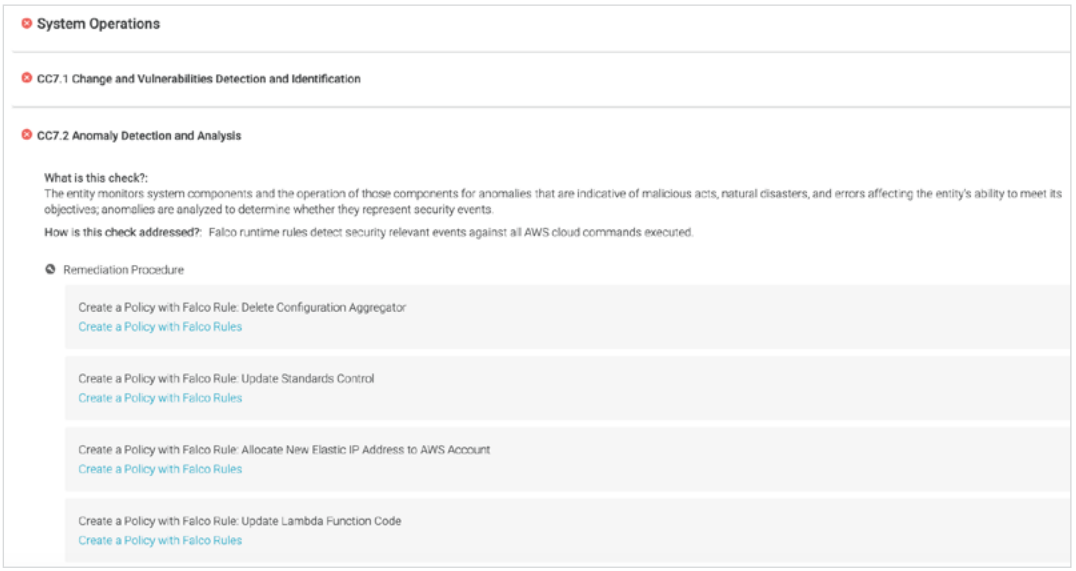
CC7 covers “system operations”, which is a wide range of criteria that is inclusive of the underlying operational procedures and processes that drive systems related to security. It includes the detection, analysis, response, and remediation of security-related activities and events.

Control	Description	How Sysdig helps
CC7.1 workload	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Image Scanning maintains an inventory for contents inside your containers, and discloses vulnerabilities and misconfigurations in them. Among them are indications if a fix is available for a currently insecure version of an installed package. Enabling Kubernetes audit log let Sysdig’s runtime rules monitor a cluster for security issues on Kubernetes events. Sysdig’s runtime rules detect security relevant events on kernel syscalls and Kubernetes audit log in real time.
CC7.2 workload	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Profiling analyzes a running container image for network ports open and running processes to create a snapshot state, then you can detect deviations from it. Enabling Kubernetes audit log let Sysdig’s runtime rules monitor a cluster for security issues on Kubernetes events. Sysdig’s runtime rules detect security relevant events on kernel syscalls and Kubernetes audit log in real time.
CC7.5 workload	The entity identifies, develops, and implements activities to recover from identified security incidents.	Using Sysdig Secure platform on-prem or SaaS, you control hosts, containers and Kubernetes security, detecting static and runtime security issues, getting capture data for audit, and preventing and blocking insecure situations.



CC7.1, CC7.2 and CC7.5 for workload

Control	Description	How Sysdig helps
CC7.1 AWS	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Sysdig's runtime rules detect security relevant events against all AWS cloud commands executed.
CC7.2 AWS	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Sysdig's runtime rules detect security relevant events against all AWS cloud commands executed.

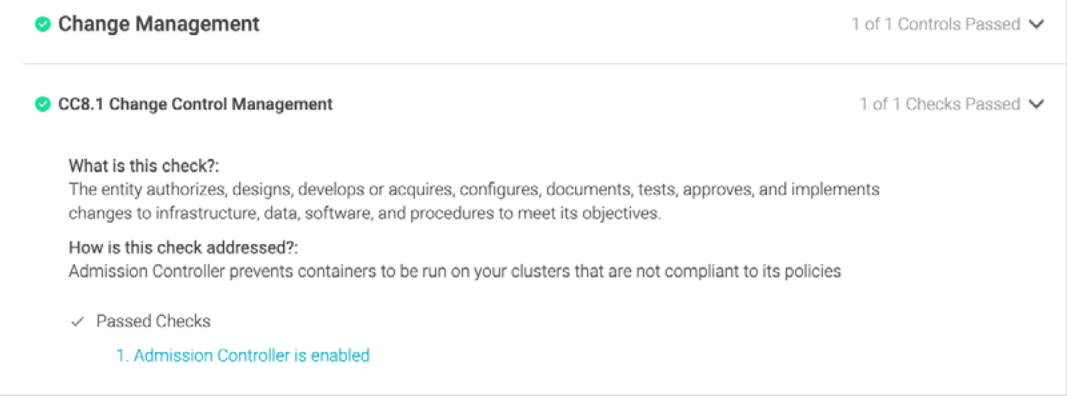


CC7.1 and CC7.2 for AWS

CC8 | Change Management

The criteria within CC8 pertains to changes, and the processes that guide changes, to systems within an organization that make use of security controls.

Control	Description	How Sysdig helps
CC8.1 workflow	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives..	Admission Controller prevents containers to be run on your clusters that are not compliant to its policies.

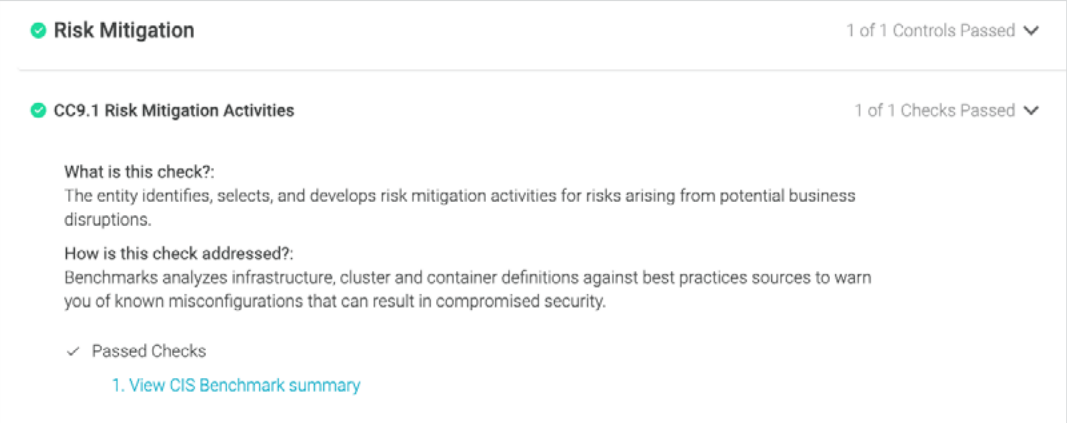


CC8.1 for workload

CC9 | Risk Mitigation

The CC9.0 criteria is focused on the holistic risk mitigation processes and systems within an organization.

Control	Description	How Sysdig helps
CC9.1 workflow	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Benchmarks analyzes infrastructure, cluster and container definitions against best practices sources to warn you of known misconfigurations that can result in compromised security.



CC9.1 for workload

Security and CloudOps teams need to have a clear mapping of controls to their containerized workloads, as well as the ability to continuously track compliance over time. This will let them be confident in their ability to manage security risk and pass security audits. In the course of doing this, compliance efforts should not hinder cloud adoption, but rather go hand-in-hand as companies increase their usage of the cloud and Kubernetes for application development.

To learn more about how Sysdig Secure validates compliance visit
https://sysdig.com/products/secure/cloud-and-container-compliance/

You can also sign-up for a Sysdig Secure free 30-day trial at
https://sysdig.com/company/free-trial/

www.sysdig.com