



Swiss Cloud Native Day 2025

Are you compliant?

This talk will describe the essential concepts of compliance frameworks and policies, specifically in the context of cloud-native infrastructure. Attendees will gain a comprehensive understanding of what compliance means, the role of various frameworks, and the importance of well-defined policies in maintaining regulatory and operational standards. The session will cover the fundamentals of compliance frameworks, provide examples of widely adopted standards, and delve into the technical controls that underpin these frameworks. Additionally, the presentation will include a live demonstration on how to evaluate compliance within cloud-native environments and highlight common challenges that organizations face in achieving and maintaining compliance.



Thursday, 18th September 2025
10:15 Uhr



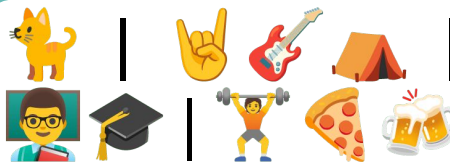
Daniel Drack
Senior DevOps Engineer



Daniel Drack
@DrackThor

Senior DevOps Engineer

Host @ Cloud Native Days Austria
Founder @ Cloud Native Austria
Organizer @ Cloud Native Chapter Graz



BSc | MA | MBA
Kubestronaut
SUSE | Exoscale | Snyk | GitLab | Scrum



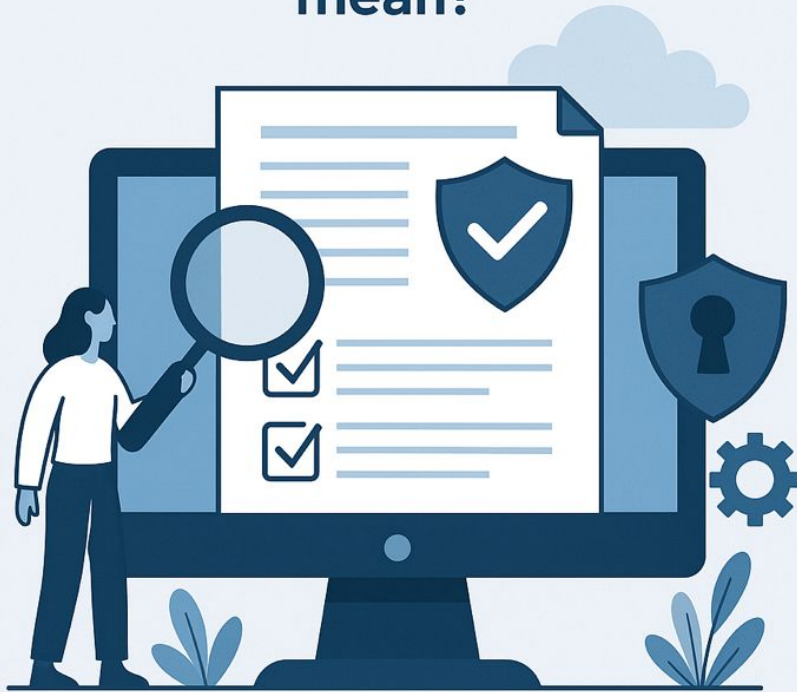
FullStackS
SOLUTION BRINGER

Are you
compliant?





What does 'Compliance' mean?



Compliance means **adhering to** applicable **specifications**.

Specifications can originate from inside or outside the organization.



Compliance != Security

GRC

ISO 27k
PCI DSS
TISAX

Quality

ISO 9k
ISO 25010
EFQM

Environment

ISO 14k
EMAS
GHG Protocol



Why does it matter? Outside View

- legal obligation
- competitive advantage (reputation!)
- business prerequisite (automotive, finance,...)

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um sicherzustellen und den **Nachweis dafür erbringen** zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

- <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679>



Why does it matter? Inside View

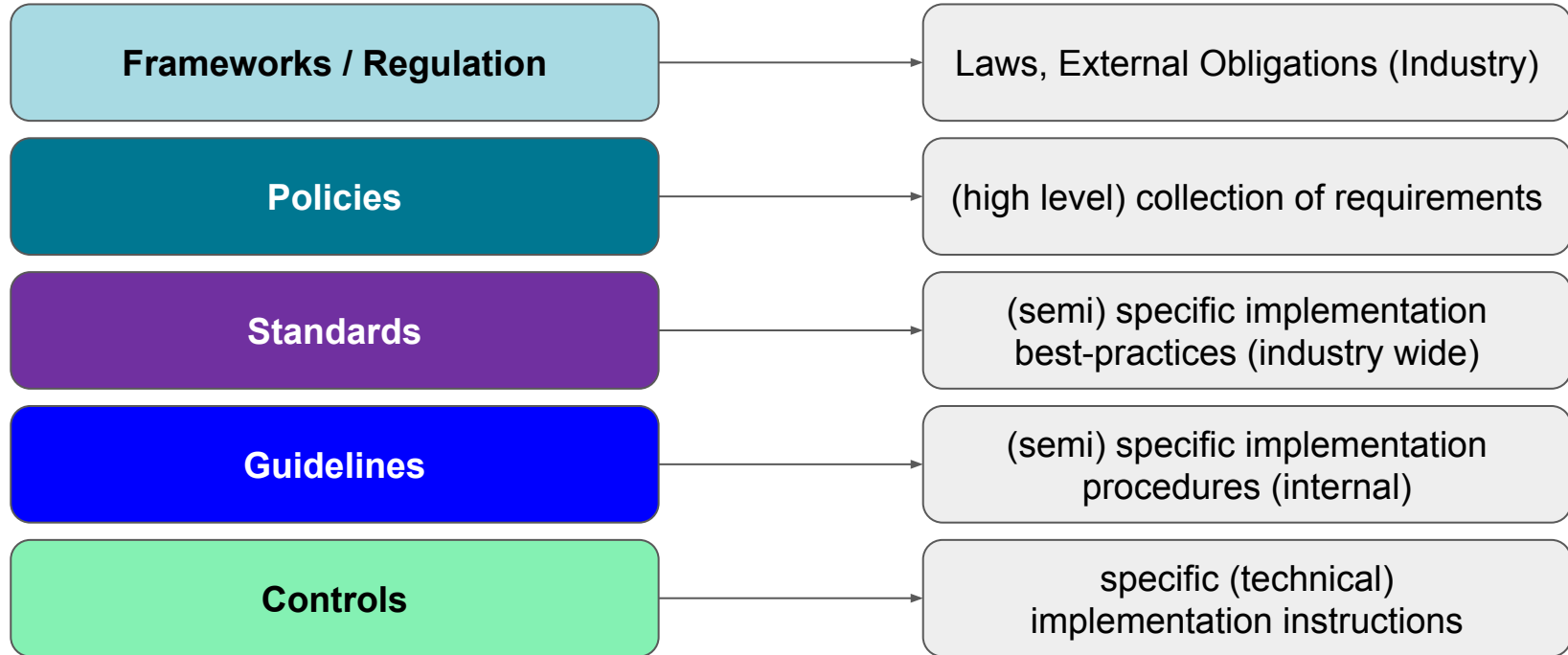
- improve system quality
- performance, transparency.. or **security**

**Process /
Organization**

**Technical
Best-Practices
and Requirements**



The compliance hierarchy





GDPR/DSGVO - Law/Regulation

Artikel 1

(Verfassungsbestimmung)

Grundrecht auf Datenschutz

§ 1. (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), [BGBl. Nr. 210/1958](#), genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

(3) Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;

2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

(Anm.: Abs. 5 aufgehoben durch [BGBl. I Nr. 51/2012](#))



NIST CSF - Policy

“It offers a taxonomy of highlevel cybersecurity outcomes [...] The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources [...]”

– <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

PROTECT (PR): Safeguards to manage the organization’s cybersecurity risks are used

- **Identity Management, Authentication, and Access Control (PR.AA):** Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access
 - **PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization
 - **PR.AA-02:** Identities are proofed and bound to credentials based on the context of interactions
 - **PR.AA-03:** Users, services, and hardware are authenticated
 - **PR.AA-04:** Identity assertions are protected, conveyed, and verified



BSI/ISO27k - Standards

“Im IT-Grundschutz-Kompendium werden standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Gebäude und Räume in IT-Grundschutz-Bausteinen beschrieben [..]”

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf

SYS.1.6.A17 Ausführung von Containern ohne Privilegien (S)

Die Container-Runtime und alle instanziierten Container SOLLTEN nur von einem nicht-privilegierten System-Account ausgeführt werden, der über keine erweiterten Rechte für den Container-Dienst und das Betriebssystem des Host-Systems verfügt oder diese Rechte erlangen kann. Die Container-Runtime SOLLTE durch zusätzliche Maßnahmen gekapselt werden, etwa durch Verwendung der Virtualisierungserweiterungen von CPUs.

Sofern Container ausnahmsweise Aufgaben des Host-Systems übernehmen sollen, SOLLTEN die Privilegien auf dem Host-System auf das erforderliche Minimum begrenzt werden. Ausnahmen SOLLTEN angemessen dokumentiert werden.

SYS.1.6.A7 Persistenz von Protokollierungsdaten der Container (B)

Die Speicherung der Protokollierungsdaten der Container MUSS außerhalb des Containers, mindestens auf dem Container-Host, erfolgen.



PCI DSS - Standards

“ [...] PCI DSS provides a baseline of technical and operational requirements designed to protect account data. [...]”

- https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Requirements and Testing Procedures		Guidance
5.2 Malicious software (malware) is prevented, or detected and addressed.		
Defined Approach Requirements	Defined Approach Testing Procedures	Purpose
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	5.2.1.a Examine system components to verify that an anti-malware solution(s) is deployed on all system components, except for those determined to not be at risk from malware based on periodic evaluations per Requirement 5.2.3.	There is a constant stream of attacks targeting newly discovered vulnerabilities in systems previously regarded as secure. Without an anti-malware solution that is updated regularly, new forms of malware can be used to attack systems, disable a network, or compromise data.
Customized Approach Objective	5.2.1.b For any system components without an anti-malware solution, examine the periodic evaluations to verify the component was evaluated and the evaluation concludes that the component is not at risk from malware.	Good Practice It is beneficial for entities to be aware of "zero-day" attacks (those that exploit a previously unknown vulnerability) and consider solutions that focus on behavioral characteristics and will alert and react to unexpected behavior. Definitions System components known to be affected by malware have active malware exploits available in the real world (not only theoretical exploits).



CIS Benchmarks - Controls

“This document provides prescriptive guidance for establishing a secure configuration posture for Kubernetes v1.29 - v1.32.[..]”

- <https://workbench.cisecurity.org/benchmarks/21709>

1.2.1 Ensure that the `--anonymous-auth` argument is set to false

Audit Procedure

Run the following command on the Control Plane node:

```
ps -ef | grep kube-apiserver
```

Verify that the `--anonymous-auth` argument is set to `false`.

Alternative Audit

```
kubectl get pod -nkube-system -lcomponent=kube-apiserver -o=jsonpath='{range .items[*]}{.spec.containers[*].command} {"\n"}{end}' | grep '--anonymous-auth' | grep -i false
```

If the exit code is '1', then the control isn't present / failed

Remediation Procedure

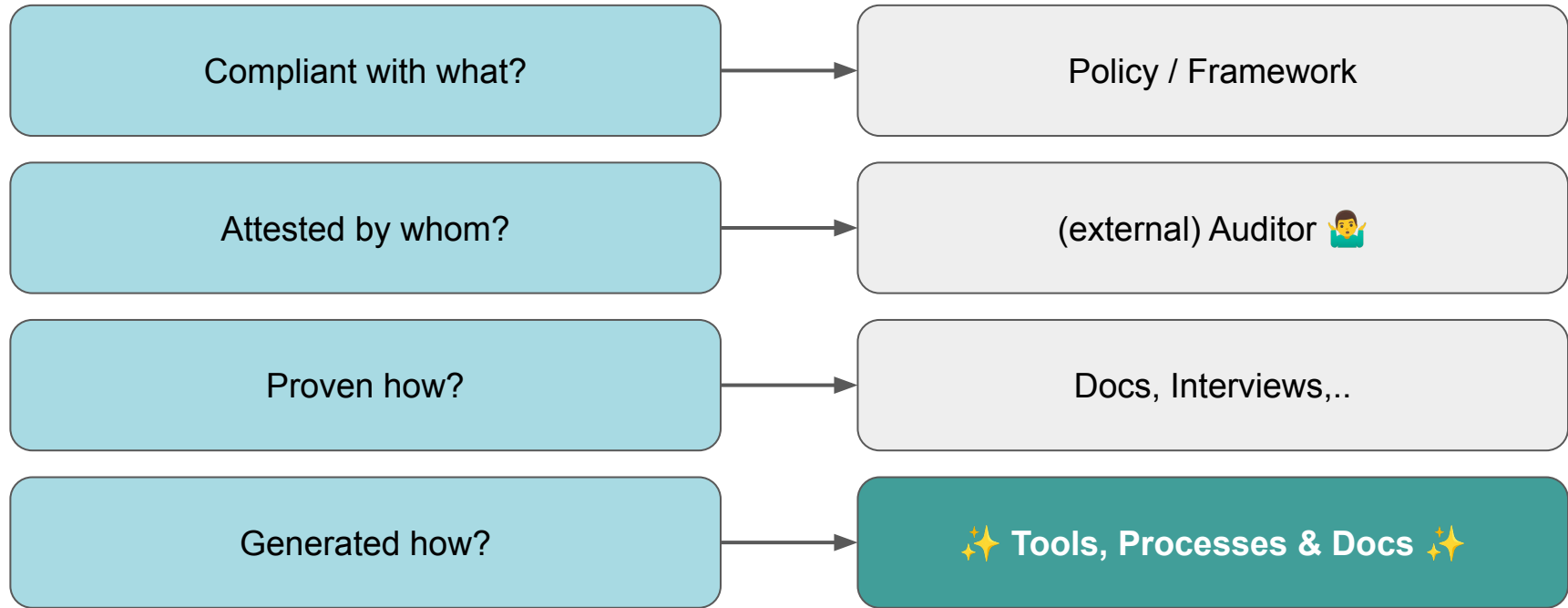
Edit the API server pod specification file `/etc/kubernetes/manifests/kube-apiserver.yaml` on the Control Plane node and set the below parameter.

```
--anonymous-auth=false
```



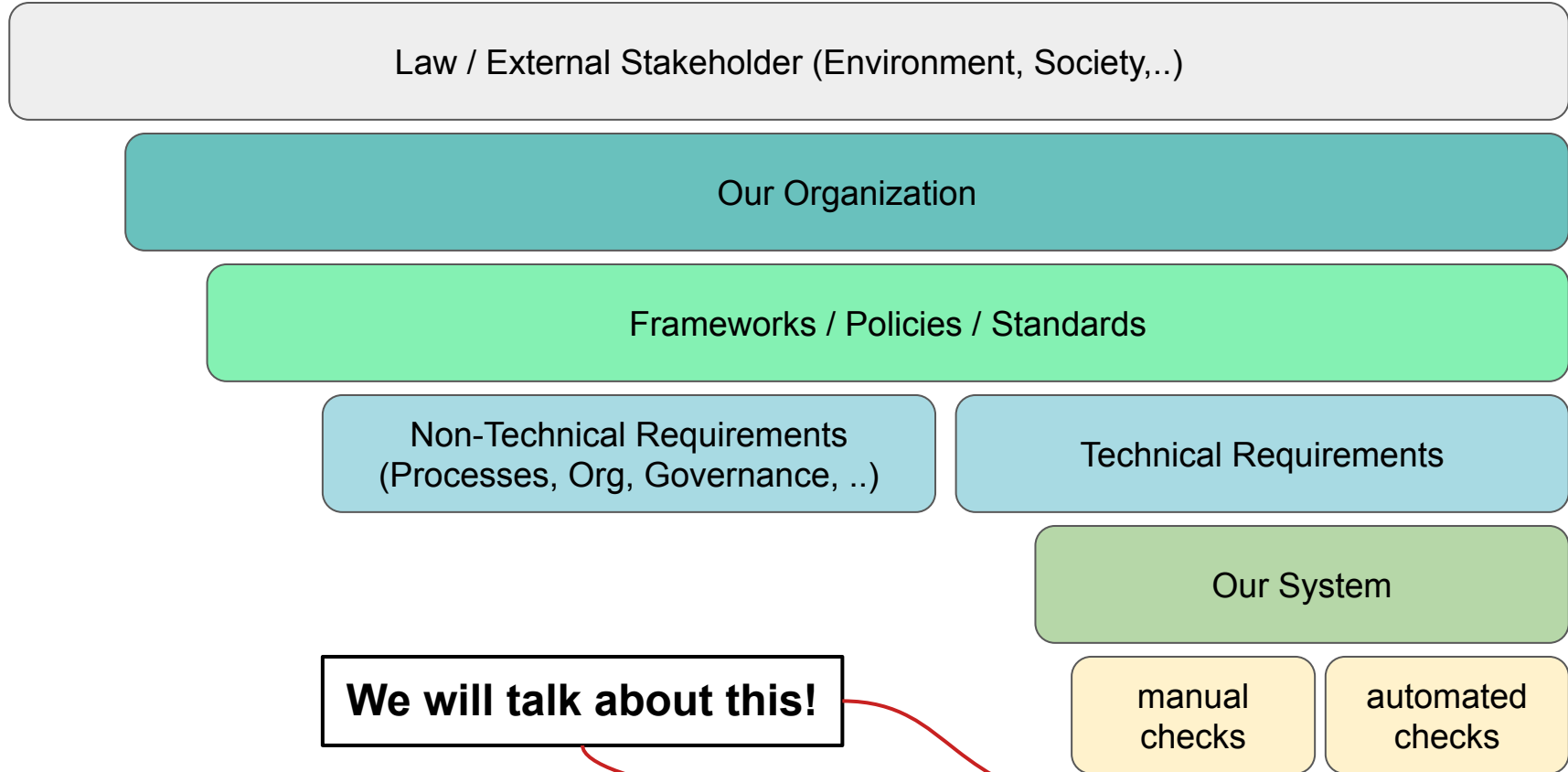
Are you compliant?

... and how to figure that out?





Scope is everything.





Two Examples

PCI DSS

—

**semi specific
multiple systems
different testing
docs & procedures**


CIS Controls

—

**very specific
single system
fixed testing
defined configs**



PCI DSS Scope & Segmentation

- “PCI DSS is intended for **all entities** that **store, process, or transmit cardholder data (CHD)** [..].” → 
- PCI DSS requirements apply to:
 - The cardholder data environment (CDE), which is comprised of:
 - **System components**, people, and processes that store, **process**, or transmit **cardholder data and/or sensitive authentication data**, and,
 - **System components** that may not store, process, or transmit CHD/SAD but have **unrestricted connectivity** to system components that store, process, or transmit CHD/SAD.
 - AND **System components**, people, and processes **that could impact the security of cardholder data and/or sensitive authentication data**.
- “**System components**” include network devices, servers, computing devices, **virtual components, cloud components, and software**.



PCI DSS Testing Methods

- **Examine**: The assessor critically evaluates data evidence. Common examples include **documents (electronic or physical)**, screenshots, **configuration files**, **audit logs**, and data files.
- **Observe**: The assessor watches an action or views something in the environment. Examples of observation subjects include **personnel performing a task or process**, **system components performing a function** or responding to input, environmental conditions, and physical controls.
- **Interview**: The assessor converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.



6. Findings and Observations

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements and Testing Procedures	Reporting Instruction	Reporting Details: Assessor's Response	Summary of Assessment Findings (check one)				
			In Place	In Place w/ CCW	N/A	Not Tested	Not in Place
1.1 Establish and implement firewall and router configuration standards that include the following:							
1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:							
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations.			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all:	Identify the document(s) reviewed to verify procedures define the formal processes for:						
• Network connections, and	• Testing and approval of all network connections.	<Report Findings Here>					
• Changes to firewall and router configurations.	• Testing and approval of all changes to firewall and router configurations.	<Report Findings Here>					
1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.	Identify the sample of records for network connections that were selected for this testing procedure.	<Report Findings Here>					
	Identify the responsible personnel interviewed who confirm that network connections were approved and tested.	<Report Findings Here>					
	Describe how the sampled records verified that network connections were:						
	• Approved	<Report Findings Here>					
	• Tested	<Report Findings Here>					
1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	Identify the sample of records for firewall and router configuration changes that were selected for this testing procedure.	<Report Findings Here>					
	Identify the responsible personnel interviewed who confirm that changes made to firewall and router configurations were approved and tested.	<Report Findings Here>					
	Describe how the sampled records verified that the firewall and router configuration changes were:						

PCI DSS
v3.2.1 ROC
Template

1: Install and Maintain Network Security Controls



1.1.1: All security policies and operational procedures that are identified in Requirement 1 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

Defined Approach Testing Procedures:

- **Examine documentation** and **interview personnel** to verify that security policies and operational procedures identified in Requirement 1 are managed in accordance with all elements specified in this requirement.

→ no automation here, sorry 🙄🙄

1: Install and Maintain Network Security Controls



2.2.4: Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.

Defined Approach Testing Procedures:

- Examine **system configuration standards** to verify necessary services, protocols, daemons, and functions are **identified and documented**.
- **Examine system configurations** to verify the following:
 - All unnecessary functionality is removed or disabled.
 - Only required functionality, as documented in the configuration standards, is enabled.

→ some automation here, yey 🎉



CIS Benchmarks - Controls

“prescriptive configuration recommendations”

in total: 1253

Product Families:

Cloud Providers: 11

Desktop Software: 7

Mobile Devices: 3

Network Devices: 9

Operating Systems: 26

Server Software: 20

1.2.1 Ensure that the `--anonymous-auth` argument is set to false

Audit Procedure

Run the following command on the Control Plane node:

```
ps -ef | grep kube-apiserver
```

Verify that the `--anonymous-auth` argument is set to `false`.

Alternative Audit

```
kubectl get pod -nkube-system -lcomponent=kube-apiserver -o=jsonpath='{range .items[*]}.{spec.containers[*].command} {"\n"}{end}' | grep '\--anonymous-auth' | grep -i false
```

If the exit code is '1', then the control isn't present / failed

Remediation Procedure

Edit the API server pod specification file `/etc/kubernetes/manifests/kube-apiserver.yaml` on the Control Plane node and set the below parameter.

```
--anonymous-auth=false
```



CIS benchmark compliance check tools



- The Good: 😇 kube-bench
- The (not so) Bad: 🤘 cnspec
- The Ugly: 😞 openScap

**Aqua
Security**

Apache-2.0

k8s



**rudimentary
custom
query
language
(YAML)**

**go cli ||
container**

**purpose
built**


**NIST
RedHat**

LGPL-2.1

**OS
apps**

**complex
XML based
query
language**

- XCCDF
- OVAL
- CPE
- DS

**terrible but
still heavily
used** 

Mondoo

BSL

k8s
OS
SaaS
...

**powerful yet
“simple”
query
language**

**go cli ||
container**

**multiple
integrations**



Daniel, Demo Time 🙏



The Good, The Bad & The Ugly

kube-bench

- easy to use
- vendor backed
- k8s only
- fine for nerds 🧐
- adaptable

open-scrap

- big community
- (vendor backed)
- VERY complicated 😬
- nice reports
- “adaptable”

cnspec

- small community
- vendor backed
- VERY powerful 💪
- nice query language
- DIY or enterprise



TL;DR - Finishing Note

- **you still need to maintain documentation**
 - use docs as code (+AI?)
 - integrates to IaC/Config as Code
 - version history and IAM out of the box
 - cheap 💰💰
- **use fitting tools** like..
 - Sprinto / Vanta ← (Enterprise) Compliance Platform
 - Mondoo ← Exposure Management and Compliance Platform
- implement **processes & best-practices**
 - proper processes and architecture ← docs and metrics!
 - everything as code (IaC, config, docs,..)
 - system specific best practices ← CIS benchmarks

Links



- kube-bench: <https://github.com/aquasecurity/kube-bench>
- openscap: <https://github.com/openscap/openscap>
 - OpenScap SSG (scan profiles)
 - <https://complianceascode.readthedocs.io/>
 - User Manual:
 - https://static.open-scap.org/openscap-1.3/oscap_user_manual.html
- cnspec: <https://github.com/mondoohq/cnspec>
 - policies: <https://github.com/mondoohq/cnspec/tree/main/content>