NIS2 & CIS Controls 2

Christian Frank (#473088)

September 7, 2025

Cyber Security Management: Sicherheitsstandards & Reifegradmodelle
Prof. Dr. Jan Hörnemann
FOM - Hochschule für Oekonomie & Management
SS 2025

In this paper, we will again examine the NIS2 security standard, review the mappings to the current set of CIS Controls v8.1, and evaluate the use of CSI benchmarks to assess the readiness of Kubernetes clusters for NIS2 and ensure ongoing compliance, thereby mitigating the risks of cyberattacks.

The paper is a revision of a previous paper that has been updated with new definitions and new aspects of legislation.

Contents

List of Figures

List of Tables

Listings

List of Abbreviations

AKS	Azure Kubernetes Service
APA	American Psychological Association
BCM	Business Continuity Management
BIA	Business Impact Analysis
BSIG	Gesetz über das BSI
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISA	Cybersecurity and Infrastructure Security Agency
CIS	Center for Internet Security
CNCF	Cloud Native Computing Foundation
CRA	Cyber Resilience Act
DORA	Digital Operational Resilience Act
EKS	Elastic Kubernetes Service
ENISA	European Union Agency for Cybersecurity
EU	European Union
GKE	Google Kubernetes Engine
IG	Implementation Group
K8s	Kubernetes
NIST	National Institute of Standards and Technology
NIS	Network and Information Security (Directive)
RIA	Risk Impact Analysis
SOC	Security Operations Center

1 Introduction

1.1 Cyber Security

Cybersecurity, also called information security or IT security, is the practice of protecting systems, networks, and programs from digital attacks. It aims to reduce the risk of these attacks and prevent the unauthorized exploitation of systems, networks, and technology.

Cybersecurity is an ongoing process because threats and attack vectors are constantly evolving. Organizations and individuals must proactively implement security measures and stay up-to-date on the latest threats.[1]

The CIA-Triad defines the key components of Information Security:

- Confidentiality
- Integrity
- Availability[2]

To address the availability of public infrastructure, our government has introduced the KRITIS designation, expanded the coverage of the BSI Act, and introduced the KRITIS-DachG.[3]

On a European level, NIS2 codifies this.

A lot has changed since the first version of the paper, especially regarding the mappings between CIS Controls and NIS2. The changes made it necessary to revisit the experiment and reevaluate the results.[4]

1.2 NIS2

NIS2, which stands for Network and Information Systems Directive II, is the EU's legislative act to strengthen cybersecurity across the European Union. It's essentially an update to the original NIS Directive implemented in 2016.

It sets stricter requirements for various sectors to improve security for essential entities. These entities include organizations in critical sectors like energy, transport, waste management, healthcare, and digital infrastructure providers.[5]

[1] See *Gemini (2024)*: What is Cyber Security. [22]
[2] See *Washington University (2025)*: The CIA Triad. [31]
[3] See *BSI (2024)*: What are Critical Infrastructures. [5]
[4] See *Frank, C. (2024)*: NIS2 and CIS Controls. [21]
[5] See *NIS 2 Compliant.org (2024)*: Comprehensive Guide to the NIS 2 Directive. [26]

Compared to the original directive, NIS2 applies to a broader range of businesses and organizations; it recognizes the importance of securing the supply chain and includes measures to address vulnerabilities in third-party vendors and suppliers.

It also emphasizes a risk-based approach to cybersecurity. Organizations must identify and assess their security risks and implement appropriate mitigation measures. Classical tools from Business Continuity Management, such as Risk Impact Analysis and Business Impact Analysis, are now essential parts of the cybersecurity toolkit.[6]

NIS2 entered into force on 16 January 2023, and the Member States had 21 months, until 17 October 2024, to transpose its measures into national law.[7]

As of the time of writing, the German government has just presented a proposal to the legislature to codify NIS2 into national law.[8]

1.3 CIS Controls and Benchmarks

CIS Controls, or CIS Critical Security Controls, are a prioritized set of best practices designed to improve an organization's cybersecurity posture. Developed by the Center for Internet Security (CIS), a non-profit organization, these controls are a widely trusted framework for defending against cyberattacks.[9]

CIS Benchmarks are configuration guides intended to harden various IT systems against cyberattacks based on the CIS' Critical Security Controls. They provide a set of best practices for securing specific operating systems, applications, and cloud platforms. Many of these Benchmarks have specific versions tied to the underlying software version.[10]

Most Kubernetes platform vendors provide automated tools to check against these benchmarks and report and enforce compliance as a first line of defense.

1.4 Kubernetes

Kubernetes, or K8s, is an open-source system designed to automate deploying, scaling, and managing applications built using containers. Containers package software in a standardized unit that includes all dependencies the software needs to run, like code, libraries, and settings. This makes them portable and efficient.

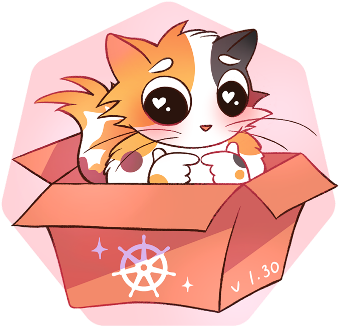
[6] See *BSI (2025)*: Business Impact Analysis. [3]
[7] See *Negreiro-Achiaga, M. (2023)*: The NIS2 Directive. [25]
[8] See *BSI (2025)*: NIS-2-Regierungsentwurf. [4]
[9] See *CIS (2024)*: Critical Security Controls. [12]
[10] See *CIS (2024)*: CIS Benchmarks List. [7]

Kubernetes helps manage these containers by grouping them logically. This makes it easier to track and manage complex applications with many containers. The original inspiration for Kubernetes came from Google's internal container orchestration system, Borg.[11]

In 2015, Kubernetes reached the 1.0 milestone, and in 2016, it was donated to the CNCF; the current release of Kubernetes is 1.33, codenamed Octarine. The cutest release was 1.30, codenamed Uwubernetes.

"For the people who built it, for the people who release it, and for the furries who keep all of our clusters online, we present to you Kubernetes v1.30: Uwubernetes, the cutest release to date."[12]

Figure 1: Kubernetes 1.30 Release Logo



1.5 Research Question & Method

This paper will examine the new NIS2 security standards, compare them to the current CIS v8 controls, and attempt to map them with a focus on using the CSI Benchmarks. Once we've established a helpful relationship, we will evaluate using CSI benchmarks to check Kubernetes clusters for NIS2 compliance. We will also check whether CIS Benchmarks can provide information about the level of compliance for Kubernetes clusters and offer actionable insights into reaching NIS2 compliance for the relevant controls.

To do this, we will perform an Experiment and check the findings of the Kubernetes CIS Benchmarks on a generic Kubernetes cluster.[13] For this experiment, we will select Microsoft's Azure Kubernetes Service (AKS) as the target Kubernetes implementation.

The goal of this paper is to determine if CIS Kubernetes Benchmark results can indicate whether a Kubernetes cluster is NIS2-compliant on the platform level.

[11] See *Gemini (2024)*: What is Kubernetes. [23]
[12] *Dsouza, A. (2024)*: Kubernetes 1.30. [13]
[13] See *Genau, L. (2020)*: Ein Experiment in deiner Abschlussarbeit durchführen. [24]

1.6 Gender-neutral Pronouns

Our society is becoming more open, inclusive, and gender-fluid, and now I think it's time to think about using gender-neutral pronouns in scientific texts, too. Two well-known researchers, Abigail C. Saguy and Juliet A. Williams, both from UCLA, propose to use the singular they/them instead: "The universal singular they is inclusive of people who identify as male, female, or nonbinary."[14] The aim is to support an inclusive approach in science through gender-neutral language.

In this paper, I'll attempt to follow this suggestion and invite all my readers to do the same for future articles. Thank you!

If you're not sure about the definitions of gender and sex and how to use them, have a look at the definitions by the American Psychological Association.[15]

1.7 Climate Emergency

As Professor Rahmstorf puts it: "Without immediate, decisive climate protection measures, my children currently attending high school could already experience a 3-degree warmer Earth. No one can say exactly what this world would look like—it would be too far outside the entire experience of human history. But almost certainly, this earth would be full of horrors for the people who would have to experience it."[16]

[14] *Saguy, A. (2020)*: Why We Should All Use They/Them Pronouns. [30]

[15] See *APA (2021)*: Definitions Related to Sexual Orientation. [1]

[16] *Rahmstorf, A. (2024)*: Climate and Weather at 3 Degrees More. [29]

2 NIS2 & CIS

2.1 The Network and Information Security Directive

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy at the end of 2020, the second version of the Network and Information Security Directive (NIS2).[17]

We will first examine some key components newly introduced with the directive and then compare this to an already established industry framework.

2.1.1 EU Cybersecurity Agency ENISA

The European Union Agency for Cybersecurity (ENISA) is a key player in ensuring high cybersecurity across Europe. Established in 2004 and empowered by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, promotes trustworthy Information and Communications Technology products and services, collaborates with Member States and EU bodies, and prepares Europe for future cyber threats. By sharing knowledge, building capacity, and raising awareness, ENISA works with stakeholders to strengthen trust in the connected economy, boost resilience, and safeguard Europe's society and citizens in the digital age.[18]

2.1.2 EU Cybersecurity Act

The EU Cybersecurity Act is the central legislation strengthening the EU's cybersecurity capabilities. It enhances the role of ENISA, the EU Agency for Cybersecurity, and establishes a robust certification framework for products and services.

Key provisions of the EU Cybersecurity Act:

- Strengthened ENISA: The Act grants ENISA a permanent mandate, increases its resources, and assigns it new responsibilities.
- Certification framework: ENISA will play a pivotal role in establishing and maintaining a European cybersecurity certification framework.
- Public information: ENISA will provide information on certification schemes and issued certificates through a dedicated website.

[17] See *EU (2023)*: Cybersecurity Policies. [16]

[18] See *EU (2025)*: Who we are. [20]

- Operational cooperation: ENISA will facilitate cooperation between EU Member States in handling cybersecurity incidents and coordinating responses to large-scale cross-border attacks.[19]

2.1.3 EU Cyber Resilience Act

The Cyber Resilience Act (CRA) is a significant step towards safeguarding consumers and businesses from cybersecurity vulnerabilities. By introducing mandatory cybersecurity requirements for manufacturers and retailers, the CRA addresses the issue of inadequate security features in products and software. It also aims to empower consumers and businesses by providing them with clear information about the cybersecurity of products and ensuring that they are designed and maintained with security in mind. The CRA's key benefits include:

- Harmonized rules: Consistent rules for products with a digital component.
- Cybersecurity framework: Requirements for planning, design, development, and maintenance of products.
- Duty of care: Obligation to ensure product security throughout its lifecycle.
- Consumer protection: Improved ability for consumers to make informed choices.
- Business security: Enhanced protection for businesses using digital products.[20]

2.1.4 EU Cyber Solidarity Act

The Act seeks to improve preparedness, detection, and response to significant cybersecurity threats by establishing a European Cybersecurity Alert System and a comprehensive Cybersecurity Emergency Mechanism.

Key features of the EU Cyber Solidarity Act:

- European Cybersecurity Alert System: This system will consist of interconnected Security Operation Centers (SOCs) across the EU, using advanced technologies like AI and data analytics to detect and share threat warnings.
- Cybersecurity Emergency Mechanism: This mechanism will provide a framework for coordinated responses to large-scale cyberattacks and crises.

[19] See *EU (2023)*: The EU Cyber Security Act. [17]
[20] See *EU (2024)*: Cyber Resiliency Act. [18]

- Enhanced capacities: The Act will strengthen the EU's capacity to detect, prepare for, and respond to cybersecurity incidents.

The European Cybersecurity Shield, a component of the Act, is a pilot initiative involving three cross-border Security Operations Center consortia. Launched in November 2022, this pilot project aims to test and refine the concept of a networked system of SOCs for early threat detection and sharing.[21]

2.2 Bundesamt für Sicherheit in der Informationstechnik

The BSI in Germany refers to the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security). It's Germany's national cybersecurity authority and was established in 1991.

The BSI is headquartered in Bonn and operates under the Federal Ministry of the Interior. It plays a crucial role in Germany's national cybersecurity strategy and works closely with international partners such as NIST on cybersecurity matters.

Among other things, the current draft bill provides for an amendment to the BSI Act (BSIG) and an expansion of the group of regulated organizations to include the categories of important and particularly important institutions.[22]

In its new role, the BSI will in the future supervise around 29,500 institutions that will be subject to new legal obligations in the area of IT security.

2.3 Center for Internet Security

All the institutions mentioned above are part of the EU's attempt to provide a legal and regulatory framework for cybersecurity. However, several established frameworks are already available within the private sector, one of which is CISecurity.

CISecurity is an acronym for the Center for Internet Security. It's a non-profit organization that helps individuals, businesses, and governments protect themselves from cyber threats. Their key offerings are CIS Controls and CIS Benchmarks.

The Center for Internet Security was founded 20 years ago in Washington, D.C., in response to increased cyberattacks. It has established itself as the go-to resource for computer security, but unlike ENISA, CISecurity is not a government organization.

[21] See *EU (2024)*: Cyber Solidarity Act. [19]

[22] See *BSI (2025)*: NIS-2-Regierungsentwurf. [4]

Its funding comes from various government and non-profit grant programs designed to improve the overall cybersecurity posture of the U.S., as well as through the sale of various cybersecurity best practices tools and resources, such as CIS SecureSuite Membership and CIS Hardened Images, and cybersecurity services like CIS Endpoint Security Services.

2.3.1 CIS Controls

CIS Controls are actionable and prioritized recommendations that provide organizations with a cybersecurity defense strategy and improve their cybersecurity posture.[23]

CIS Controls are organized into Implementation Groups:

- IG1 is a minimum standard of information security aimed at all enterprises.
- IG2 focuses on enterprises dealing with sensitive client or company information.
- IG3 focuses on the impact of zero-day attacks and targeted attacks from sophisticated adversaries and might not be suitable for all enterprises.

Implementation groups are cumulative; i.e., to implement IG2, you would also need to implement IG1.

Entities in the particularly important category will most likely need to implement IG3.

The CIS Controls are a standalone toolset. There are mappings available for other security and compliance requirements, such as NIS2, DORA, ISO 27001, NIST CSF, or NIST SP 800-53.[24]

2.3.2 CIS Benchmarks

CIS Benchmarks are detailed configuration guidelines for operating systems, hardware, and software. These can be validated and monitored automatically using specialized tools.

The Benchmark itself addresses the CIS Controls safeguards of Secure Configurations and maintaining a Secure Configuration Process without individual mappings to these safeguards.[25]

In CIS Controls v8, this would be Control 4.1, "Establish and Maintain a Secure Configuration Process"; in CIS Controls v7, it was Control 5.1, "Establish Secure Config-

[23] See *CIS (2025)*: Critical Security Controls. [12]
[24] See *CIS (2025)*: Critical Controls Mappings. [9]
[25] See *CIS (2024)*: Benchmark List. [7]

urations." Both Controls are part of the Implementation Group IG1 in their respective version.

The CIS Benchmarks do not address other controls.[26] For the remainder of this paper, we will focus on the CIS Benchmarks applicable to Kubernetes and the CIS Controls that can be monitored through CIS Benchmarks and link these to the NIS2 Directive.

2.4 CIS Benchmarks on Kubernetes

To validate the compliance of Kubernetes clusters with a selected CIS Benchmark, Aqua Security maintains the kube-bench toolset.

For Kubernetes, the most common way of running kube-bench is to create a job on the cluster that needs to be analyzed.[27]

[26] See *CIS (2024)*: CIS Critical Security Controls FAQ. [8]

[27] See *Aqua Securites (2025)*: Running kube-bench. [2]

Listing 1: Kube-bench Job

```
apiVersion: batch/v1
kind: Job
metadata:
  name: kube-bench
spec:
  template:
    spec:
      hostPID: true
      containers:
        - name: kube-bench
          image: docker.io/aquasec/kube-bench:latest
          command:
            ["kube-bench", "run", "--benchmark", "aks-1.7"]
      restartPolicy: Never
```

After the job has finished, the CIS Benchmarks results will become available within the pod logs.

In the next chapter, we will examine the mapping between CIS Controls and NIS2 and then break it down to match elements from the CIS Kubernetes Benchmark.

3 NIS2 Exploration

3.1 Mapping between NIS2 and CIS Controls 8.1

To support NIS2 compliance, CISecurity released in April 2025 a mapping for the CIS Controls v8.1 and the NIS2 Directive.[28]

CISecurity uses its in-house methodology to map the individual provisions of a given compliance directive, in this case NIS2, to the individual CIS Controls. The mapping sheet covers all CIS Controls and consists of directly mapped entries and unmapped entries from either direction.

The directive items in the mapping refer directly to the current NIS2 Technical Implementation Guidance and can be easily verified in either direction.[29]

3.2 CIS Benchmarks on AKS

As a first step, we extract the CIS Controls that are covered in the Benchmark from the most current version of the AKS Benchmark:

[28] *CIS (2025)*: CIS Controls v8.1 Mapping to NIS2 Directive. [11]

[29] See *ENISA (2025)*: Technical Implementation Guidance. [14]

Table 1: CIS Controls in AKS Benchmark v1.7

ID	Auto	Description
2.5	N	Allowlist Authorized Software
3.3	Y	Configure Data Access Control Lists
3.10	Y	Encrypt Sensitive Data in Transit
3.11	Y	Encrypt Sensitive Data at Rest
3.12	Y	Segment Data Processing and Storage Based on Sensitivity
4.1	Y	Establish and Maintain a Secure Configuration Process
4.4	Y	Implement and Manage a Firewall on Servers
4.5	Y	Implement and Manage a Firewall on End-User Devices
4.6	N	Securely Manage Enterprise Assets and Software
4.7	Y	Manage Default Accounts on Enterprise Assets and Software
5	N	Account Management
5.4	Y	Restrict Administrator Privileges to Dedicated Administrator Accounts
5.6	N	Centralizes Account Management
6	Y	Access Control Management
6.8	N	Define and Maintain Role-Based Access Control
7.5	Y	Perform Automated Vulnerability Scans of Internal Enterprise Assets
7.6	Y	Perform Automated Vulnerability Scans of External Enterprise Assets
8.1	N	Establish and Maintain an Audit Log Management Process
8.2	Y	Collect Audit Logs
8.5	Y	Collect Detailed Audit Logs
13.4	Y	Perform Traffic Filtering Between Network Segments
16.5	N	Use Up-to-Date and Trusted Third-Party Software Components

The CIS Benchmark tools can automate some of the tests for these CIS Controls and thus can automate regular compliance checks.

3.3 CIS AKS Benchmarks Mappings

From the controls covered by the Benchmark, we extract the ones that have direct NIS2 implementation mappings.

Table 2: NIS2 Mappings in AKS Benchmark v1.7

ID	Type	Item	Description	Directive
3.3	Subset	11.1	Access control policy	11.1.1
3.12	Subset	11.4	Administration systems	11.4.2
4.1	Subset	6.3	Configuration management	6.3.1-3
5.4	Subset	11.3	Authentication	11.3.2
	Subset	11.6	Authentication	11.6.2
6.8	Superset	1.2	Roles, responsibilities and authorities	1.2.6
	Subset	11.1	Access control policy	11.1.1
	Subset	11.2	Access control policy	11.2.3
	Subset	11.3	Access control policy	11.3.3
7.5, 7.6	Subset	6.10	Vulnerability handling and disclosure	6.10.2
8.1	Equivalent	3.2	Monitoring and logging	3.2.1
	Superset	3.2	Monitoring and logging	3.2.2, 3.2.7
8.2	Subset	3.2	Monitoring and logging	3.2.1
8.5	Subset	3.2	Monitoring and logging	3.2.3

Counting the number of automated tests, CIS Control 04, Secure Configuration of Enterprise Assets and Software, emerges as the most promising candidate of the CIS Benchmark for NIS2 compliance that corresponds to the NIS2 implementation guidance.

3.4 CIS Controls

The CIS Controls in the current version (v8) consist of 18 controls:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data

12. Network Infrastructure
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider
16. Application Software Security
17. Incident Response
18. Penetration Testing[30]

As with the NIS2 articles, many of these controls are procedural and cannot be automated. Control 04, however, Secure Configuration of Enterprise Assets and Software, is of particular importance for individual IT systems, such as Kubernetes clusters.

Control 04 consists of several subcontrols:

1. Establish and Maintain a Secure Configuration Process
2. Establish and Maintain a Secure Configuration Process for Network Infrastructure
3. Configure Automatic Session Locking on Enterprise Assets
4. Implement and Manage a Firewall on Servers
5. Implement and Manage a Firewall on End-User Devices
6. Securely Manage Enterprise Assets and Software
7. Manage Default Accounts on Enterprise Assets and Software
8. Uninstall or Disable Unnecessary Services on Enterprise Assets and Software
9. Configure Trusted DNS Servers on Enterprise Assets
10. Enforce Automatic Device Lockout on Portable End-User Devices
11. Enforce Remote Wipe Capability on Portable End-User Devices
12. Separate Enterprise Workspaces on Mobile End-User Devices[31]

Control 4.1 strongly emphasizes the configuration process, as the default configuration for enterprise software is typically geared toward ease of deployment and use rather than security.

[30] See *CIS (2024)*: Critical Security Controls v8. [12]
[31] See *CIS (2024)*: Critical Security Controls v8 - Control 04. [12]

CIS Control 4.1 maps to the NIS2 implementation guidance 6.3, which clearly states that maintaining a Secure Configuration Process is essential.

Leaving default configurations unchecked might result in some of these security risks:

- Exposed Services and Ports
- Default Accounts and Passwords
- Pre-configured DNS Settings
- Older or Vulnerable Protocols
- Pre-installed Unnecessary Software[32]

To mitigate these, the CIS Benchmarks provide a security baseline for enterprise software, such as Kubernetes, covering all aspects of CIS Control 4.1 and a matching IT Security Policy.[33]

3.5 NIS2 Article 21

The NIS2 directive itself is a legal document organized into Chapters and Articles. It has a pan-European scope and targets critical businesses. NIS2 applies to many entities that provide essential services to the European economy and society, such as Operators of Essential Services (OES) and Digital Service Providers (DSPs). While NIS2 primarily targets medium and large enterprises, smaller entities may still be affected, depending on the services they provide.

As we've seen, much of the content concerns reporting requirements and EU-wide cooperation and institutions, which we will not analyze further in this paper.[34]

Article 21, however, defines the required Cybersecurity risk-management measures for critical infrastructure. In paragraph 2, point (g), NIS2 calls for basic cyber hygiene practices and cybersecurity training.

Any entity covered by the directive must, thus, have an IT Security Policy to implement basic cyber hygiene.[35] To strengthen their security postures, entities could rely on one of the major frameworks and standards, such as the NIST SP 800 series, ISO/IEC 27001, Mitre Att&ck, or CIS Controls.[36]

[32] See *CIS (2024)*: Ibid. [12]

[33] See *CIS (2024)*: CIS Benchmarks List. [7]

[34] See *EU (2022)*: NIS2 Directive. [15]

[35] See *NIS 2 Compliant.org (2024)*: List of Policies Required by NIS 2 Directive. [27]

[36] See *NIS 2 Compliant.org (2024)*: Requirements Checklist for NIS 2. [28]

CIS Control 4.1, as linked to the implementation guidance 6.3, is the prime candidate to support and evaluate NIS2 Article 21 2(g) as it covers basic cyber hygiene and IT security policy.

The requirements in Article 21 are much broader than those of CIS Control 04, but a secure configuration process is a fundamental element.

Fulfilling CIS Control 04 does not imply compliance with Article 21, but noncompliance with CIS Control 04 does imply noncompliance with Article 21.

The CIS Benchmarks can thus indicate whether an IT system is potentially NIS2 compliant. Evaluating and running the CIS Benchmarks regularly will support NIS2 compliance checking and defense against cyber attacks.

In the next chapter, we will conduct our experiment and validate our findings by examining the benchmark results from an AKS cluster.

4 NIS2 Analysis

4.1 Running the CIS Benchmarks

To examine the results of a CIS Benchmark, we will create a Kubernetes cluster on Microsoft Azure with the following versions:

- Microsoft AKS v1.32
- CIS AKS Benchmark v1.7
- kube-bench v0.11.2
- SUSE Rancher v2.11.3
- Terraform v1.12

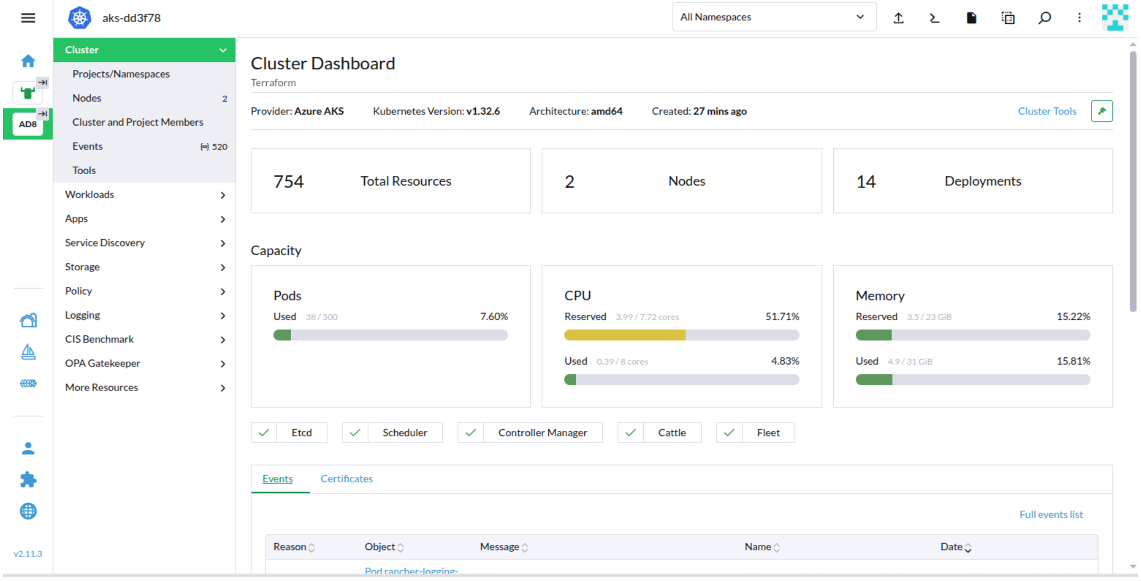
We will create the cluster with a default node pool and without hardening to get reproducible results that will be relevant for most environments:

Listing 2: Terraform Plan

```
# AKS cluster
resource "azurerm_kubernetes_cluster" "cluster_az" {
  name                = "aks-${random_id.instance_id.hex}"
  location            = var.az-region
  resource_group_name = var.az-resource-group
  kubernetes_version  = var.k8version
  dns_prefix          = "aks-${random_id.instance_id.hex}"
  web_app_routing {
    dns_zone_ids = []
  }
  local_account_disabled = "false"
  default_node_pool {
    name       = "agent${random_id.instance_id.hex}"
    node_count = var.numnodes
    vm_size    = var.type
  }
  identity {
    type = "SystemAssigned"
  }
}
```

This is the resulting AKS cluster that we will use for our test:

Figure 2: AKS Cluster Dashboard



Cluster Dashboard
Terraform

Provider: Azure AKS   Kubernetes Version: v1.32.6   Architecture: amd64   Created: 27 mins ago

754 Total Resources | 2 Nodes | 14 Deployments

Capacity

Pods — Used 38 / 500 — 7.60%

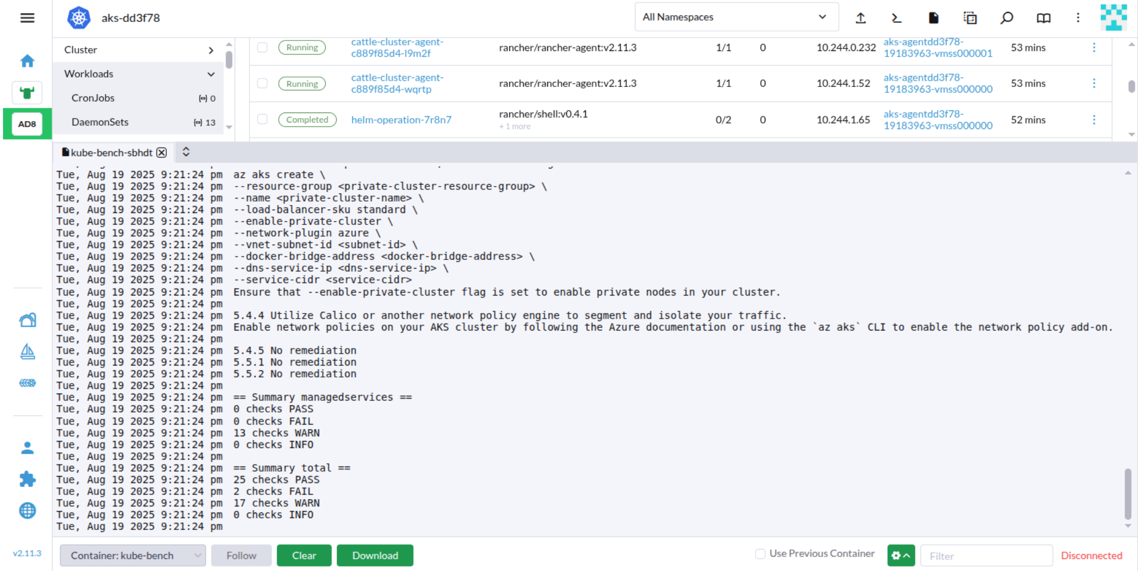
CPU — Reserved 3.99 / 7.72 cores — 51.71%; Used 0.39 / 8 cores — 4.83%

Memory — Reserved 3.5 / 23 GiB — 15.22%; Used 4.9 / 31 GiB — 15.81%

✓ Etcd ✓ Scheduler ✓ Controller Manager ✓ Cattle ✓ Fleet

We then execute the kube-bench job as defined in Chapter 2, and the Benchmark results will become available in the job output:

Figure 3: Kube-bench Job Output



Running	cattle-cluster-agent-c889f85d4-l9m2f	rancher/rancher-agent:v2.11.3	1/1	0	10.244.0.232	aks-agentdd3f78-19183963-vmss000001	53 mins
Running	cattle-cluster-agent-c889f85d4-wqrtp	rancher/rancher-agent:v2.11.3	1/1	0	10.244.1.52	aks-agentdd3f78-19183963-vmss000000	53 mins
Completed	helm-operation-7r8n7	rancher/shell:v0.4.1 + 1 more	0/2	0	10.244.1.65	aks-agentdd3f78-19183963-vmss000000	52 mins

```
Tue, Aug 19 2025 9:21:24 pm  az aks create \
Tue, Aug 19 2025 9:21:24 pm  --resource-group <private-cluster-resource-group> \
Tue, Aug 19 2025 9:21:24 pm  --name <private-cluster-name> \
Tue, Aug 19 2025 9:21:24 pm  --load-balancer-sku standard \
Tue, Aug 19 2025 9:21:24 pm  --enable-private-cluster \
Tue, Aug 19 2025 9:21:24 pm  --network-plugin azure \
Tue, Aug 19 2025 9:21:24 pm  --vnet-subnet-id <subnet-id> \
Tue, Aug 19 2025 9:21:24 pm  --docker-bridge-address <docker-bridge-address> \
Tue, Aug 19 2025 9:21:24 pm  --dns-service-ip <dns-service-ip> \
Tue, Aug 19 2025 9:21:24 pm  --service-cidr <service-cidr>
Tue, Aug 19 2025 9:21:24 pm  Ensure that --enable-private-cluster flag is set to enable private nodes in your cluster.
Tue, Aug 19 2025 9:21:24 pm
Tue, Aug 19 2025 9:21:24 pm  5.4.4 Utilize Calico or another network policy engine to segment and isolate your traffic.
Tue, Aug 19 2025 9:21:24 pm  Enable network policies on your AKS cluster by following the Azure documentation or using the `az aks` CLI to enable the network policy add-on.
Tue, Aug 19 2025 9:21:24 pm
Tue, Aug 19 2025 9:21:24 pm  5.4.5 No remediation
Tue, Aug 19 2025 9:21:24 pm  5.5.1 No remediation
Tue, Aug 19 2025 9:21:24 pm  5.5.2 No remediation
Tue, Aug 19 2025 9:21:24 pm
Tue, Aug 19 2025 9:21:24 pm  == Summary managedservices ==
Tue, Aug 19 2025 9:21:24 pm  0 checks PASS
Tue, Aug 19 2025 9:21:24 pm  0 checks FAIL
Tue, Aug 19 2025 9:21:24 pm  13 checks WARN
Tue, Aug 19 2025 9:21:24 pm  0 checks INFO
Tue, Aug 19 2025 9:21:24 pm
Tue, Aug 19 2025 9:21:24 pm  == Summary total ==
Tue, Aug 19 2025 9:21:24 pm  25 checks PASS
Tue, Aug 19 2025 9:21:24 pm  2 checks FAIL
Tue, Aug 19 2025 9:21:24 pm  17 checks WARN
Tue, Aug 19 2025 9:21:24 pm  0 checks INFO
Tue, Aug 19 2025 9:21:24 pm
```

4.2 Benchmarks Findings

Let's inspect the detailed results from the CIS Benchmark scan, beginning with the worker node security:

Table 3: CIS Benchmark Scan - Worker Node

State	ID	Description
[PASS]	3.1.1	Ensure that the kubeconfig file permissions are set to 644 or more restrictive (Automated)
[PASS]	3.1.2	Ensure that the kubelet kubeconfig file ownership is set to root:root (Automated)
[PASS]	3.1.3	Ensure that the azure.json file has permissions set to 644 or more restrictive (Automated)
[PASS]	3.1.4	Ensure that the azure.json file ownership is set to root:root (Automated)
[PASS]	3.2.1	Ensure that the –anonymous-auth argument is set to false (Automated)
[PASS]	3.2.2	Ensure that the –authorization-mode argument is not set to AlwaysAllow (Automated)
[PASS]	3.2.3	Ensure that the –client-ca-file argument is set as appropriate (Automated)
[PASS]	3.2.4	Ensure that the –read-only-port is secured (Automated)
[PASS]	3.2.5	Ensure that the –streaming-connection-idle-timeout argument is not set to 0 (Automated)
[PASS]	3.2.6	Ensure that the –make-iptables-util-chains argument is set to true (Automated)
[PASS]	3.2.7	Ensure that the –eventRecordQPS argument is set to 0 or a level which ensures appropriate event capture (Automated)
[PASS]	3.2.8	Ensure that the –rotate-certificates argument is not set to false (Automated)
[PASS]	3.2.9	Ensure that the RotateKubeletServerCertificate argument is set to true (Automated)

As expected, a default installation of a Microsoft AKS cluster will pass all tests for node security, including the important CIS Benchmark test 3.2.1 for anonymous access to the Kubelet server. The CIS Benchmark documentation states the obvious for this test: "You should rely on authentication to authorize access and disallow anonymous requests."[37]

[37] *CIS (2023)*: CIS AKS Benchmark, 3.2 Kubelet. [6]

Next, we'll examine the results for the policies:

Table 4: CIS Benchmark Scan - Policies

State	ID	Description
[FAIL]	4.1.1	Ensure that the cluster-admin role is only used where required (Automated)
[PASS]	4.1.2	Minimize access to secrets (Automated)
[PASS]	4.1.3	Minimize wildcard use in Roles and ClusterRoles (Automated)
[PASS]	4.1.4	Minimize access to create pods (Automated)
[PASS]	4.1.5	Ensure that default service accounts are not actively used (Automated)
[FAIL]	4.1.6	Ensure that Service Account Tokens are only mounted where necessary (Automated)
[PASS]	4.2.1	Minimize the admission of privileged containers (Automated)
[PASS]	4.2.2	Minimize the admission of containers wishing to share the host process ID namespace (Automated)
[PASS]	4.2.3	Minimize the admission of containers wishing to share the host IPC namespace (Automated)
[PASS]	4.2.4	Minimize the admission of containers wishing to share the host network namespace (Automated)
[PASS]	4.2.5	Minimize the admission of containers with allowPrivilegeEscalation (Automated)
[WARN]	4.4.1	Ensure latest CNI version is used (Manual)
[PASS]	4.4.2	Ensure that all Namespaces have Network Policies defined (Automated)
[PASS]	4.5.1	Prefer using secrets as files over secrets as environment variables (Automated)
[WARN]	4.5.2	Consider external secret storage (Manual)
[WARN]	4.6.1	Create administrative boundaries between resources using namespaces (Manual)
[WARN]	4.6.2	Apply Security Context to Your Pods and Containers (Manual)
[PASS]	4.6.3	The default namespace should not be used (Automated)

In this section, we encounter two failures due to excessive admin access usage and four warnings concerning network and workload configuration, which should be remedied with the appropriate hardening.

As the final step, we'll examine the results for managed services:

Table 5: CIS Benchmark Scan - Managed Services

State	ID	Description
[WARN]	5.1.1	Ensure Image Vulnerability Scanning using Microsoft Defender for Cloud (MDC) (Manual)
[WARN]	5.1.2	Minimize user access to Azure Container Registry (ACR) (Manual)
[WARN]	5.1.3	Minimize cluster access to read-only for Azure Container Registry (ACR) (Manual)
[WARN]	5.1.4	Minimize Container Registries to only those approved (Manual)
[WARN]	5.2.1	Prefer using dedicated AKS Service Accounts (Manual)
[WARN]	5.3.1	Ensure Kubernetes Secrets are encrypted (Manual)
[WARN]	5.4.1	Restrict Access to the Control Plane Endpoint (Manual)
[WARN]	5.4.2	Ensure clusters are created with Private Endpoint Enabled and Public Access Disabled (Manual)
[WARN]	5.4.3	Ensure clusters are created with Private Nodes (Manual)
[WARN]	5.4.4	Ensure Network Policy is Enabled and set as appropriate (Manual)
[WARN]	5.4.5	Encrypt traffic to HTTPS load balancers with TLS certificates (Manual)
[WARN]	5.5.1	Manage Kubernetes RBAC users with Azure AD (Manual)
[WARN]	5.5.2	Use Azure RBAC for Kubernetes Authorization (Manual)

All tests in this section are set to warning level, as they mainly deal with systems outside of the Kubernetes cluster, such as the container registry. Also, in the remediations for this section, we can find the recommendation to move from public AKS to private AKS and private endpoints, which would significantly reduce the attack surface.

4.3 Relevance for NIS2 Article 21

The identified failures in the scan are both linked to the NIS2 technical implementation guidance 6.3, which generally calls for a "deny-all, permit-by-exception policy."[38]

Following the principle of least privilege is part of basic cyber hygiene. It should be standard for all critical IT systems that follow established principles for good governance.

To fully comply with the requirements of the NIS2 Directive, additional hardening measures would need to be taken for our cluster by implementing the requirements outlined in the CIS AKS Benchmark results.

[38] See *ENISA (2025)*: Technical Implementation Guidance. [14]

4.4 Implications for DORA compliance

To support DORA compliance, CIS Security released in April 2025 a mapping for the CIS Controls v8.1 and DORA.[39]

The mappings seem to be very similar to the mappings for the NIS2 Directive; a detailed analysis could be the subject of a further paper, with a similar outcome likely.

4.5 Overall Compliance and Risk Mitigation

We have seen Microsoft's Azure Kubernetes Engine partly pass the AKS CIS Benchmark v1.7 and might need additional hardening for full compliance. The other major hosted versions of Kubernetes, Google's Kubernetes Engine (GKE) and Amazon's Elastic Kubernetes Service (EKS), also offer CIS compliance and remediation guidance to their customers.

On-premise Kubernetes distributions, such as SUSE's Rancher or Red Hat's OpenShift, offer optional CIS compliance and hardening, too.

Ensuring that an IT system, such as a Kubernetes cluster, scores a passing grade on the CIS Benchmarks supports basic cyber hygiene and should be part of any IT Security Policy.

4.6 Outlook

Article 21 of the NIS 2 Directive outlines the cybersecurity risk-management measures essential entities must implement to protect their networks and information systems. These measures are designed to prevent and minimize the impact of cyber incidents on both the entities and their customers. It outlines critical cybersecurity practices that every business under the NIS2 regulations must have in place.

One mandatory cybersecurity measure under Article 21 is basic cyber hygiene practices and training, as described in paragraph 2(g).

This requirement is where NIS2, the CIS Controls, and the CIS Benchmarks intersect. The CIS Benchmarks outline and implement procedures to fulfill CIS Control 04, Secure Configuration, a crucial requirement for basic cyber hygiene and part of any IT Security Policy.

[39] *CIS (2025)*: CIS Controls v8.1 Mapping to DORA. [10]

As we've seen above, CIS Benchmarks can be used to enforce good security practices by automatically checking for deviations and issues. CIS Benchmarks can also recommend the necessary steps for remediation.

We can conclude that a passing result for the appropriate CIS Benchmark can serve as a good indicator of whether the Kubernetes cluster is NIS2 compliant.

Passing the CIS Benchmark alone is not a sufficient indicator, though, as the NIS2 Directive includes many more aspects than the basic cyber hygiene outlined in Article 21; however, failing the CIS Benchmark, as in our case, will be a clear indicator that the Kubernetes cluster as part of the IT platform is not NIS2 compliant.

NIS2 is a legal framework, and compliance will be mandatory for European critical entities, ensuring widespread adoption. Unlike the CISecurity or ISO 27001 frameworks, adherence to the NIS2 Directive's requirements is not optional for entities classified as important or particularly important; it will be mandated by law.

In addition to Article 21, the NIS2 Directive also contains Article 23, which outlines the requirements for EU-wide incident reporting. Article 23 defines what constitutes an incident, the mandatory reports, and the content required in these reports. With pan-European reporting of cyber attacks, a coordinated response should become much more manageable.

5 Summary

The Center of Internet Security offers benchmarks for testing a Kubernetes cluster against. Aqua Security provides the kube-bench implementation for the CIS Benchmark scans and can support mitigating the findings. Major on-premise Kubernetes platforms, such as SUSE's Rancher, integrate kube-bench and CIS Benchmark scans into their offering.

The CIS Benchmarks cover multiple sections of the CIS Controls v8.1, NIS2 Technical Implementation Guidance, and Article 21 2(g) of the Network and Information Systems Directive II.

From our experiment and analysis, we conclude that the CIS Benchmarks will help enterprises fulfill and monitor the requirements for basic cyber hygiene as outlined in Article 21 2(g). The CIS Benchmarks can help determine whether a Kubernetes cluster is NIS2-compliant on the platform level and are a good complement to ENISA's Technical Implementation Guidance.

Upcoming legislation, such as the KRITIS-DachG ("Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen"), together with the NIS-2-Regierungsentwurf, will further strengthen the security posture of IT systems in Germany and the EU.

Regardless of future developments, governance, risk management, and regulatory compliance will remain critical topics in Enterprise IT, and the CIS Benchmarks are a good tool for monitoring IT systems compliance.

The Terraform plan files for the downstream cluster used in this paper are on my GitHub.

References

[1] APA. (2021) Definitions related to sexual orientation. [Access 2021-04-06]. [Online]. Available: https://www.apa.org/pi/lgbt/resources/sexuality-definitions.pdf

[2] Aqua Securities. (2025) Running kube-bench. [Access 2025-08-15]. [Online]. Available: https://github.com/aquasecurity/kube-bench/blob/main/docs/running.md

[3] BSI. (2025) Business impact analysis. [Access 2025-08-14]. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/3_BusinessImpactAnalysieren/BIA_node.html

[4] BSI. (2025) It-sicherheitsrecht nis-2-regierungsentwurf. [Access 2025-08-11]. [Online]. Available: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2025/250730_NIS-2-Regierungsentwurf.html

[5] BSI. (2025) What are critical infrastructures? [Access 2025-05-29]. [Online]. Available: https://www.bsi.bund.de/EN/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

[6] CIS. (2023) Cis aks benchmark. [Access 2025-05-14]. [Online]. Available: https://www.cisecurity.org/cis-benchmarks

[7] CIS. (2024) Cis benchmarks list. [Access 2025-05-14]. [Online]. Available: https://www.cisecurity.org/cis-benchmarks

[8] CIS. (2024) Cis critical security controls faq. [Access 2025-08-14]. [Online]. Available: https://www.cisecurity.org/controls/cis-controls-faq

[9] CIS. (2025) Cis controls mappings. [Access 2025-08-19]. [Online]. Available: https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/mapping-and-compliance-with-the-cis-controls

[10] CIS. (2025) Cis controls v8.1 mapping to dora. [Access 2025-08-19]. [Online]. Available: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-dora

[11] CIS. (2025) Cis controls v8.1 mapping to nis2 directive. [Access 2025-08-19]. [Online]. Available: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-1-mapping-to-nis2-directive-2022-2555

[12] CIS. (2025) Cis critical security controls. [Access 2025-05-29]. [Online]. Available: https://www.cisecurity.org/controls

[13] A. Dsouza and K. Martin. (2024) Kubernetes v1.30. [Access 2025-08-12]. [Online]. Available: https://kubernetes.io/blog/2024/04/17/kubernetes-v1-30-release/

[14] ENISA. (2025) Technical implementation guidance. [Access 2025-08-19]. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

[15] European Union. (2022) Nis2 directive. [Access 2025-08-14]. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27

[16] European Union. (2023) Cybersecurity policies. [Access 2025-08-14]. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[17] European Union. (2023) The eu cybersecurity act. [Access 2025-08-14]. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[18] European Union. (2024) Cyber resiliency act. [Access 2025-08-14]. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[19] European Union. (2024) The eu cyber solidarity act. [Access 2025-08-14]. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

[20] European Union. (2025) Who we are. [Access 2025-08-14]. [Online]. Available: https://www.enisa.europa.eu/about-enisa/who-we-are

[21] C. Frank. (2024) Nis2 and cis controls. [Access 2025-05-29]. [Online]. Available: https://storage.googleapis.com/bucket.chfrank.net/NIS2-CIS-Controls.pdf

[22] Gemini. (2024) What is cyber security. [Access 2024-04-18]. [Online]. Available: https://gemini.google.com

[23] Gemini. (2024) What is kubernetes. [Access 2024-04-18]. [Online]. Available: https://gemini.google.com

[24] L. Genau. (2022) Ein experiment in deiner abschlussarbeit durchführen. [Access 2024-04-15]. [Online]. Available: https://www.scribbr.de/methodik/experiment/

[25] M. D. M. Negreiro-Achiaga. (2023) The nis2 directive. [Access 2025-08-14]. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[26] NIS 2 Compliant.org. (2024) Comprehensive guide to the nis 2 directive. [Access 2025-08-14]. [Online]. Available: https://nis2compliant.org/

[27] NIS 2 Compliant.org. (2024) List of policies required by nis 2 directive. [Access 2025-08-14]. [Online]. Available: https://nis2compliant.org/

[28] NIS 2 Compliant.org. (2024) Requirements checklist for nis 2. [Access 2025-08-14]. [Online]. Available: https://nis2compliant.org/

[29] S. Rahmstorf, *Climate and Weather at 3 Degrees More*. Cham: Springer Nature Switzerland, 2024, pp. 3–17.

[30] A. Saguy and J. Williams. (2020) Why we should all use they/them pronouns. [Access 2020-05-20]. [Online]. Available: https://blogs.scientificamerican.com/voices/why-we-should-all-use-they-them-pronouns/

[31] Washington University. (2025) The cia triad. [Access 2025-05-29]. [Online]. Available: https://informationsecurity.wustl.edu/guidance/confidentiality-integrity-and-availability-the-cia-triad/