

1 critical to fix, 30 warnings. Biggest lever: drop privileged:true.



HEADLINE FINDINGS

- > **CRITICAL** kube-system container "kube-proxy" is privileged 0.33
- > **WARN** big-monolith no pods found matching service labels (map[app:hunger-check]) 1.00
- > **WARN** default no pods found matching service labels (map[app:build-code]) 1.00
- > **WARN** default no pods found matching service labels (map[app:health-check]) 1.00
- > **WARN** default no pods found matching service labels (map[app:internal-proxy]) 1.00

AUDIT CONTEXT

Cluster .test, audited 2026-05-05 07:55. Posture score **14/100** (prior: 14/100). dump SHA-256: 6b181a0c2f43426a...

Findings are fused across **0 scanner source(s)** spanning **0 categories** (no scanners). When multiple independent sources flag the same resource with the same issue class, we collapse them into one finding and increase its confidence score (shown as a bar, 0.0–1.0). The posture score is confidence-weighted — low-confidence findings deduct proportionally fewer points.

Scoring per finding: CRITICAL –12 pts, WARN –4 pts, INFO –1 pt, each multiplied by the finding's confidence. Floor 0, ceiling 100.

This audit is based on cluster state collected via Ephemera's collect-cluster-data.sh script (read-only kubectl get calls), then scanned offline by 0 independent tools. Secrets, JWTs, AWS keys, and PEM blocks are redacted at collection time and again before printing.

Every signal, with source attribution.

Rows are deduplicated across scanners: when multiple tools independently flag the same (namespace, resource, issue), they collapse into one row. The **Sources** column shows which tools agreed, and **Confidence** reflects how corroborated the finding is — higher bars = more independent tools converged.

| ID | SEV | NAMESPACE | RESOURCE | FINDING | SOURCES | CONF |
|------|--|------------------|-----------------------------------|--|------------------------------|--|
| F-01 | CRITICAL | kube-system | DaemonSet/kube-proxy | container "kube-proxy" is privileged | config scan | <div style="width: 33%;"><div style="background-color: #000; height: 10px;"></div></div> 0.33 |
| F-02 | WARN | big-monolith | Service/hunger-check-service | no pods found matching service labels (map[app:hunger-check]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-03 | WARN | default | Service/build-code-service | no pods found matching service labels (map[app:build-code]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-04 | WARN | default | Service/health-check-service | no pods found matching service labels (map[app:health-check]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-05 | WARN | default | Service/internal-proxy-api-ser... | no pods found matching service labels (map[app:internal-proxy]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-06 | WARN | default | Service/internal-proxy-info-ap... | no pods found matching service labels (map[app:internal-proxy]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-07 | WARN | default | Service/kubernetes-goat-home-s... | no pods found matching service labels (map[app:kubernetes-goat-home]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-08 | WARN | default | Service/metadata-db | no pods found matching service labels (map[app:kubernetes.io/instance: | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-09 | WARN | default | Service/poor-registry-service | no pods found matching service labels (map[app:poor-registry]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-10 | WARN | default | Service/system-monitor-service | no pods found matching service labels (map[app:system-monitor]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-11 | WARN | default | Service/wordpress-1776847905 | no pods found matching service labels (map[app:kubernetes.io/instance: | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-12 | WARN | default | Service/wordpress-1776847905-m... | no pods found matching service labels (map[app:kubernetes.io/component | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-13 | WARN | default | Service/wordpress-1776847905-m... | no pods found matching service labels (map[app:kubernetes.io/instance: | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-14 | WARN | secure-middlewre | Service/cache-store-service | no pods found matching service labels (map[app:cache-store]) | config scan runtime check | <div style="width: 100%;"><div style="background-color: #000; height: 10px;"></div></div> 1.00 |
| F-15 | WARN | default | Service/kubernetes | service has no selector specified | config scan | <div style="width: 85%;"><div style="background-color: #000; height: 10px;"></div></div> 0.85 |
| F-16 | WARN | kube-system | Service/kube-dns | no pods found matching service labels (map[k8s-app:kube-dns]) | config scan | <div style="width: 85%;"><div style="background-color: #000; height: 10px;"></div></div> 0.85 |
| F-17 | WARN | default | Deployment/wordpress-1776847905 | Repeated warning events: Unhealthy (13x) | runtime check | <div style="width: 33%;"><div style="background-color: #000; height: 10px;"></div></div> 0.33 |
| F-18 | WARN | default | Job/batch-check-job | The container "batch-check" is using an invalid container image, "madh | config scan | <div style="width: 33%;"><div style="background-color: #000; height: 10px;"></div></div> 0.33 |
| F-19 | WARN | default | Job/batch-check-job | container "batch-check" does not have a read-only root file system | config scan | <div style="width: 33%;"><div style="background-color: #000; height: 10px;"></div></div> 0.33 |

| Year | Country | Value | Unit | Source |
|------|---------|-------|------|--------|
| 2000 | Algeria | 1.0 | kg | FAO |
| 2001 | Algeria | 1.0 | kg | FAO |
| 2002 | Algeria | 1.0 | kg | FAO |
| 2003 | Algeria | 1.0 | kg | FAO |
| 2004 | Algeria | 1.0 | kg | FAO |
| 2005 | Algeria | 1.0 | kg | FAO |
| 2006 | Algeria | 1.0 | kg | FAO |
| 2007 | Algeria | 1.0 | kg | FAO |
| 2008 | Algeria | 1.0 | kg | FAO |
| 2009 | Algeria | 1.0 | kg | FAO |
| 2010 | Algeria | 1.0 | kg | FAO |
| 2011 | Algeria | 1.0 | kg | FAO |
| 2012 | Algeria | 1.0 | kg | FAO |
| 2013 | Algeria | 1.0 | kg | FAO |
| 2014 | Algeria | 1.0 | kg | FAO |
| 2015 | Algeria | 1.0 | kg | FAO |
| 2016 | Algeria | 1.0 | kg | FAO |
| 2017 | Algeria | 1.0 | kg | FAO |
| 2018 | Algeria | 1.0 | kg | FAO |
| 2019 | Algeria | 1.0 | kg | FAO |
| 2020 | Algeria | 1.0 | kg | FAO |
| 2021 | Algeria | 1.0 | kg | FAO |
| 2022 | Algeria | 1.0 | kg | FAO |
| 2023 | Algeria | 1.0 | kg | FAO |
| 2024 | Algeria | 1.0 | kg | FAO |
| 2025 | Algeria | 1.0 | kg | FAO |
| 2026 | Algeria | 1.0 | kg | FAO |
| 2027 | Algeria | 1.0 | kg | FAO |
| 2028 | Algeria | 1.0 | kg | FAO |
| 2029 | Algeria | 1.0 | kg | FAO |
| 2030 | Algeria | 1.0 | kg | FAO |
| 2031 | Algeria | 1.0 | kg | FAO |
| 2032 | Algeria | 1.0 | kg | FAO |
| 2033 | Algeria | 1.0 | kg | FAO |
| 2034 | Algeria | 1.0 | kg | FAO |
| 2035 | Algeria | 1.0 | kg | FAO |
| 2036 | Algeria | 1.0 | kg | FAO |
| 2037 | Algeria | 1.0 | kg | FAO |
| 2038 | Algeria | 1.0 | kg | FAO |
| 2039 | Algeria | 1.0 | kg | FAO |
| 2040 | Algeria | 1.0 | kg | FAO |
| 2041 | Algeria | 1.0 | kg | FAO |
| 2042 | Algeria | 1.0 | kg | FAO |
| 2043 | Algeria | 1.0 | kg | FAO |
| 2044 | Algeria | 1.0 | kg | FAO |
| 2045 | Algeria | 1.0 | kg | FAO |
| 2046 | Algeria | 1.0 | kg | FAO |
| 2047 | Algeria | 1.0 | kg | FAO |
| 2048 | Algeria | 1.0 | kg | FAO |
| 2049 | Algeria | 1.0 | kg | FAO |
| 2050 | Algeria | 1.0 | kg | FAO |
| 2000 | Algeria | 1.0 | kg | FAO |
| 2001 | Algeria | 1.0 | kg | FAO |
| 2002 | Algeria | 1.0 | kg | FAO |
| 2003 | Algeria | 1.0 | kg | FAO |
| 2004 | Algeria | 1.0 | kg | FAO |
| 2005 | Algeria | 1.0 | kg | FAO |
| 2006 | Algeria | 1.0 | kg | FAO |
| 2007 | Algeria | 1.0 | kg | FAO |
| 2008 | Algeria | 1.0 | kg | FAO |
| 2009 | Algeria | 1.0 | kg | FAO |
| 2010 | Algeria | 1.0 | kg | FAO |
| 2011 | Algeria | 1.0 | kg | FAO |
| 2012 | Algeria | 1.0 | kg | FAO |
| 2013 | Algeria | 1.0 | kg | FAO |
| 2014 | Algeria | 1.0 | kg | FAO |
| 2015 | Algeria | 1.0 | kg | FAO |
| 2016 | Algeria | 1.0 | kg | FAO |
| 2017 | Algeria | 1.0 | kg | FAO |
| 2018 | Algeria | 1.0 | kg | FAO |
| 2019 | Algeria | 1.0 | kg | FAO |
| 2020 | Algeria | 1.0 | kg | FAO |
| 2021 | Algeria | 1.0 | kg | FAO |
| 2022 | Algeria | 1.0 | kg | FAO |
| 2023 | Algeria | 1.0 | kg | FAO |
| 2024 | Algeria | 1.0 | kg | FAO |
| 2025 | Algeria | 1.0 | kg | FAO |
| 2026 | Algeria | 1.0 | kg | FAO |
| 2027 | Algeria | 1.0 | kg | FAO |
| 2028 | Algeria | 1.0 | kg | FAO |
| 2029 | Algeria | 1.0 | kg | FAO |
| 2030 | Algeria | 1.0 | kg | FAO |
| 2031 | Algeria | 1.0 | kg | FAO |
| 2032 | Algeria | 1.0 | kg | FAO |
| 2033 | Algeria | 1.0 | kg | FAO |
| 2034 | Algeria | 1.0 | kg | FAO |
| 2035 | Algeria | 1.0 | kg | FAO |
| 2036 | Algeria | 1.0 | kg | FAO |
| 2037 | Algeria | 1.0 | kg | FAO |
| 2038 | Algeria | 1.0 | kg | FAO |
| 2039 | Algeria | 1.0 | kg | FAO |
| 2040 | Algeria | 1.0 | kg | FAO |
| 2041 | Algeria | 1.0 | kg | FAO |
| 2042 | Algeria | 1.0 | kg | FAO |
| 2043 | Algeria | 1.0 | kg | FAO |
| 2044 | Algeria | 1.0 | kg | FAO |
| 2045 | Algeria | 1.0 | kg | FAO |
| 2046 | Algeria | 1.0 | kg | FAO |
| 2047 | Algeria | 1.0 | kg | FAO |
| 2048 | Algeria | 1.0 | kg | FAO |
| 2049 | Algeria | 1.0 | kg | FAO |
| 2050 | Algeria | 1.0 | kg | FAO |

Management Accounting for Decision Making

Chapter 1: Introduction to Management Accounting

Management accounting provides information for internal use to help managers make decisions. It is different from financial accounting, which provides information for external users like investors and creditors. Management accounting is more detailed and focuses on specific areas of the business.

Chapter 2: Cost Accounting and Cost Control

Cost accounting is a branch of management accounting that tracks and records the costs of production. It helps managers control costs and improve efficiency. There are different types of costs, such as direct and indirect costs.

| Cost Type | Description | Example |
|---------------|---|---|
| Direct Cost | Costs that can be directly traced to a specific product or service. | Raw materials, direct labor |
| Indirect Cost | Costs that cannot be directly traced to a specific product or service but are necessary for production. | Factory overhead, utilities, depreciation |

| Cost Type | Description | Example |
|---------------|---|-----------------------------|
| Variable Cost | Costs that change in proportion to the level of production. | Raw materials, direct labor |
| Fixed Cost | Costs that do not change with the level of production. | Factory rent, depreciation |

| Cost Type | Description | Example |
|-----------------|---|--------------------------------|
| Prime Cost | The sum of direct materials and direct labor costs. | Raw materials, direct labor |
| Conversion Cost | The sum of direct labor and manufacturing overhead costs. | Direct labor, factory overhead |

| Cost Type | Description | Example |
|---------------|--|-------------------------------------|
| Standard Cost | A predetermined cost for a unit of product, used for comparison with actual costs. | Standard cost for a unit of product |
| Actual Cost | The actual cost incurred for a unit of product. | Actual cost for a unit of product |












| Cost Type | Description | Example |
|------------------------|--|--|
| Cost Variance | The difference between standard cost and actual cost. | Cost variance for a unit of product |
| Cost Variance Analysis | The process of identifying the causes of cost variances. | Cost variance analysis for a unit of product |

| ID | SEV | FINDING | FRAMEWORK REFERENCES | CONF |
|------|------|--|---|------|
| | | | CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | |
| F-06 | WARN | no pods found matching service labels (map[app:internal-proxy]) | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-07 | WARN | no pods found matching service labels (map[app:kubernetes-goat-home]) | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-08 | WARN | no pods found matching service labels (map[app.kubernetes.io/instance:me | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-09 | WARN | no pods found matching service labels (map[app:poor-registry]) | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-10 | WARN | no pods found matching service labels (map[app:system-monitor]) | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-11 | WARN | no pods found matching service labels (map[app.kubernetes.io/instance:wo | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-12 | WARN | no pods found matching service labels (map[app.kubernetes.io/component:p | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 | 1.00 |

| ID | SEV | FINDING | FRAMEWORK REFERENCES | CONF |
|------|------|--|--|------|
| | | | CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | |
| F-13 | WARN | no pods found matching service labels (map[app.kubernetes.io/instance:wo | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-14 | WARN | no pods found matching service labels (map[app:cache-store]) | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 1.00 |
| F-15 | WARN | service has no selector specified | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 0.85 |
| F-16 | WARN | no pods found matching service labels (map[k8s-app:kube-dns]) | NIS2: 21.2.b GDPR: 32.1.b DORA: 10.1 CRA: I.1.2.h, I.1.2.i CER: 13.1.c ISO27001: A.8.16 SOC2: CC7.2 NIST-CSF: DE.CM-09 OWASP-K8s: K05 | 0.85 |
| F-17 | WARN | Repeated warning events: Unhealthy (13x) | NIS2: 21.2.b, 21.2.c GDPR: 32.1.b DORA: 11.6 CRA: I.1.2.h CER: 13.1.c ISO27001: A.5.30, A.8.16 SOC2: A1.2 NIST-CSF: DE.CM-09 | 0.33 |
| F-18 | WARN | The container "batch-check" is using an invalid container image, "madhua | NIS2: 21.2.d, 21.2.e GDPR: 32.1.d DORA: 8.2, 9.4.d CRA: I.2.1, I.2.7 ISO27001: A.8.9, A.8.19 CIS-K8s: 6.1.1 SOC2: CC6.8, CC8.1 NIST-CSF: ID.RA-01, GV.SC-05 MITRE: T1525 OWASP-K8s: K02 NSA-CISA: PS-9, UA-4 | 0.33 |
| F-19 | WARN | container "batch-check" does not have a read-only root file system | NIS2: 21.2.e, 21.2.g GDPR: 32.1.b | 0.33 |

| | |
|---|---|
| <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> | <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> |
| <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> | <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> |
| <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> | <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> |
| <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> | <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> |
| <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> | <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> |
| <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> | <p>1. Introduction</p> <p>2. Methodology</p> <p>3. Results</p> <p>4. Discussion</p> <p>5. Conclusion</p> |

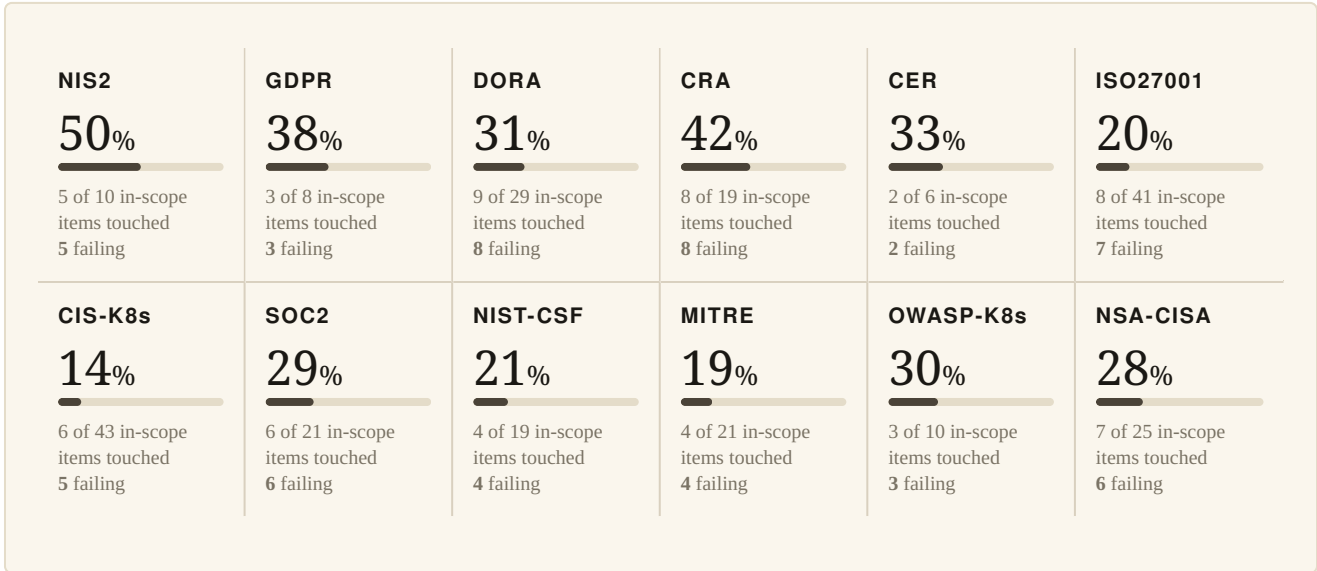
| Date | Description | Debit | Credit |
|------|-------------|---------|---------|
| 1900 | To Balance | | 100.00 |
| 1901 | By Cash | 50.00 | |
| 1902 | To Cash | | 25.00 |
| 1903 | By Cash | 75.00 | |
| 1904 | To Cash | | 100.00 |
| 1905 | By Cash | 150.00 | |
| 1906 | To Cash | | 200.00 |
| 1907 | By Cash | 300.00 | |
| 1908 | To Cash | | 400.00 |
| 1909 | By Cash | 500.00 | |
| 1910 | To Cash | | 600.00 |
| 1911 | By Cash | 700.00 | |
| 1912 | To Cash | | 800.00 |
| 1913 | By Cash | 900.00 | |
| 1914 | To Cash | | 1000.00 |
| 1915 | By Cash | 1100.00 | |
| 1916 | To Cash | | 1200.00 |

| ID | SEV | FINDING | FRAMEWORK REFERENCES | CONF |
|------|------|---|--|---|
| | | | SOC2: A1.2 NIST-CSF: DE.CM-09 | |
| F-32 | INFO | Standalone Job does not specify ttlSecondsAfterFinished | — |  0.33 |
| F-33 | INFO | container "batch-check" has cpu request 0 | NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 OWASP-K8s: K01 |  0.33 |
| F-34 | INFO | container "batch-check" has memory limit 0 | NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 |  0.33 |
| F-35 | INFO | Standalone Job does not specify ttlSecondsAfterFinished | — |  0.33 |
| F-36 | INFO | container "hidden-in-layers" has cpu request 0 | NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 OWASP-K8s: K01 |  0.33 |
| F-37 | INFO | container "hidden-in-layers" has memory limit 0 | NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 |  0.33 |
| F-38 | INFO | unhealthyPodEvictionPolicy is not explicitly set | — |  0.33 |
| F-39 | INFO | unhealthyPodEvictionPolicy is not explicitly set | — |  0.33 |
| F-40 | INFO | container "kube-proxy" is Privileged hence allows privilege escalation. | NIS2: 21.2.e, 21.2.g GDPR: 32.1.b DORA: 9.2, 9.4.a CRA: I.1.2.b, I.1.2.k ISO27001: A.8.2, A.8.9 CIS-K8s: 5.2.5 SOC2: CC6.1 NIST-CSF: PR.PS-01 MITRE: T1548 OWASP-K8s: K01 NSA-CISA: PS-4 |  0.33 |
| F-41 | INFO | container "kube-proxy" has cpu request 0 | NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 OWASP-K8s: K01 |  0.33 |
| F-42 | INFO | container "kube-proxy" has memory limit 0 | NIS2: 21.2.c DORA: 7.c ISO27001: A.8.6 |  0.33 |

Framework references are indicative and should be reviewed with your compliance team. Covers: NIS2 (EU 2022/2555), GDPR (EU 2016/679), DORA (EU 2022/2554), CRA (EU 2024/2847), CER (EU 2022/2557), ISO/IEC 27001:2022, MITRE ATT&CK for Containers, OWASP K8s Top 10, and NSA/CISA K8s Hardening Guide v1.2.

Which regulations this cluster speaks to.

Each of the six frameworks below defines dozens or hundreds of requirements, only a subset of which are addressable through Kubernetes cluster state. The percentages show how many of the **in-scope** items (excluding purely organisational/physical controls) are exercised by findings in this report. A high percentage is not good news — it means findings are landing across many control domains.



The per-framework breakdown on the following pages shows every section and subsection. **Primary** = cluster state is the main source of evidence. **Partial** = cluster contributes but is insufficient alone. **Contextual** = informs but is not main evidence. **Out of scope** means Kubernetes cannot provide evidence — handled by policies, training, supply chain controls, and incident response processes.

HOW TO READ THIS

For each framework item, the table shows: the requirement, its Kubernetes relevance, the number of distinct findings that touched it, the highest severity hit, and which finding IDs map to it. Finding IDs link back to the findings table on page 2 so you can trace each compliance gap to a concrete remediation.

This is a technical coverage view, not a compliance attestation. Real compliance requires documented policies, organisational controls, supply chain audits, personnel training, and incident response procedures that a cluster scanner cannot assess. What this report does is surface the Kubernetes-level evidence you can contribute toward each framework's technical requirements.

Section 1: Introduction

This document provides a comprehensive overview of the project's objectives and scope.

Section 2: Project Objectives

The primary goal of this project is to develop a robust system that meets the following requirements:

1. High performance and scalability.

2. User-friendly interface and intuitive navigation.

3. Data security and privacy protection.

4. Integration with existing systems and data sources.

5. Regular updates and maintenance support.

6. Comprehensive documentation and user training.

7. Flexibility to adapt to changing requirements.

8. Cost-effectiveness and efficient resource utilization.

9. Reliability and high availability.

10. Compliance with industry standards and regulations.

11. Scalability to handle future growth.

12. Support for multiple platforms and devices.

13. Clear communication and collaboration among team members.

14. Regular progress reporting and transparency.

15. Proactive risk management and mitigation strategies.

16. Strong leadership and team motivation.

17. Effective time management and scheduling.

18. Regular communication and stakeholder engagement.

19. Clear roles and responsibilities for team members.

20. Regular feedback loops and continuous improvement.

21. Strong project governance and oversight.

22. Regular risk assessments and updates.

23. Clear communication channels and protocols.

24. Regular team meetings and status updates.

25. Strong project management and organizational skills.

| Year | Country | Value |
|------|---------|-------|
| 2010 | China | 1.2 |
| 2011 | China | 1.3 |
| 2012 | China | 1.4 |
| 2013 | China | 1.5 |
| 2014 | China | 1.6 |
| 2015 | China | 1.7 |
| 2016 | China | 1.8 |
| 2017 | China | 1.9 |
| 2018 | China | 2.0 |
| 2019 | China | 2.1 |
| 2020 | China | 2.2 |
| 2021 | China | 2.3 |
| 2022 | China | 2.4 |
| 2023 | China | 2.5 |
| 2024 | China | 2.6 |
| 2025 | China | 2.7 |
| 2026 | China | 2.8 |
| 2027 | China | 2.9 |
| 2028 | China | 3.0 |
| 2029 | China | 3.1 |
| 2030 | China | 3.2 |
| 2031 | China | 3.3 |
| 2032 | China | 3.4 |
| 2033 | China | 3.5 |
| 2034 | China | 3.6 |
| 2035 | China | 3.7 |
| 2036 | China | 3.8 |
| 2037 | China | 3.9 |
| 2038 | China | 4.0 |
| 2039 | China | 4.1 |
| 2040 | China | 4.2 |
| 2041 | China | 4.3 |
| 2042 | China | 4.4 |
| 2043 | China | 4.5 |
| 2044 | China | 4.6 |
| 2045 | China | 4.7 |
| 2046 | China | 4.8 |
| 2047 | China | 4.9 |
| 2048 | China | 5.0 |
| 2049 | China | 5.1 |
| 2050 | China | 5.2 |
| 2051 | China | 5.3 |
| 2052 | China | 5.4 |
| 2053 | China | 5.5 |
| 2054 | China | 5.6 |
| 2055 | China | 5.7 |
| 2056 | China | 5.8 |
| 2057 | China | 5.9 |
| 2058 | China | 6.0 |
| 2059 | China | 6.1 |
| 2060 | China | 6.2 |
| 2061 | China | 6.3 |
| 2062 | China | 6.4 |
| 2063 | China | 6.5 |
| 2064 | China | 6.6 |
| 2065 | China | 6.7 |
| 2066 | China | 6.8 |
| 2067 | China | 6.9 |
| 2068 | China | 7.0 |
| 2069 | China | 7.1 |
| 2070 | China | 7.2 |
| 2071 | China | 7.3 |
| 2072 | China | 7.4 |
| 2073 | China | 7.5 |
| 2074 | China | 7.6 |
| 2075 | China | 7.7 |
| 2076 | China | 7.8 |
| 2077 | China | 7.9 |
| 2078 | China | 8.0 |
| 2079 | China | 8.1 |
| 2080 | China | 8.2 |
| 2081 | China | 8.3 |
| 2082 | China | 8.4 |
| 2083 | China | 8.5 |
| 2084 | China | 8.6 |
| 2085 | China | 8.7 |
| 2086 | China | 8.8 |
| 2087 | China | 8.9 |
| 2088 | China | 9.0 |
| 2089 | China | 9.1 |
| 2090 | China | 9.2 |
| 2091 | China | 9.3 |
| 2092 | China | 9.4 |
| 2093 | China | 9.5 |
| 2094 | China | 9.6 |
| 2095 | China | 9.7 |
| 2096 | China | 9.8 |
| 2097 | China | 9.9 |
| 2098 | China | 10.0 |
| 2099 | China | 10.1 |
| 2100 | China | 10.2 |

DORA · DORA

Regulation (EU) 2022/2554 — Digital Operational Resilience Act

29 in-scope items · 9 touched · 8 failing

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|---|--|--------------|-------------------|---|
| Art.5 · Governance and organisation | | | | |
| 5.1 | Management body approves ICT risk management framework | out-of-scope | — | |
| Art.6 · ICT risk management framework | | | | |
| 6.2 | Strategies, policies, procedures, protocols and tools protecting all ICT assets | primary | — | |
| 6.8 | Digital operational resilience strategy within framework | partial | — | |
| Art.7 · ICT systems, protocols and tools | | | | |
| 7.a | Appropriate to magnitude of operations | contextual | — | |
| 7.b | Reliable | primary | — | |
| 7.c | Sufficient capacity for data processing, peak load, stress | primary | 6 INFO | F-33, F-34, F-36, F-37, F-41, F-42 |
| 7.d | Technologically resilient to adequately deal with additional needs under stress | primary | — | |
| Art.8 · Identification | | | | |
| 8.1 | Identify, classify and document ICT-supported business functions | partial | — | |
| 8.2 | Identify information and ICT assets, their interconnections | primary | 2 WARN | F-18, F-21 |
| 8.3 | Identify and document all processes dependent on ICT 3rd parties | partial | — | |
| 8.4 | Risk assessment on each major change to infrastructure | contextual | — | |
| 8.7 | Assess ICT concentration risk and interdependencies | partial | — | |
| Art.9 · Protection and prevention | | | | |
| 9.1 | Continuously monitor and control security + functioning of ICT systems | primary | — | |
| 9.2 | Minimise impact of ICT risk via appropriate security tools | primary | 9 CRITICAL | F-01, F-19, F-20, F-22, F-23, F-25 (+3) |
| 9.3 | Design, procure and implement ICT security policies, procedures, protocols, tools | primary | 1 CRITICAL | F-01 |
| 9.4.a | Availability, authenticity, integrity, confidentiality of data | primary | 6 CRITICAL | F-01, F-20, F-23, F-25, F-27, F-40 |
| 9.4.b | Security of data in use, in transit, at rest | partial | — | |
| 9.4.c | Policies preventing information leakage | primary | — | |
| 9.4.d | Network connection security + software/firmware up to date | primary | 2 WARN | F-18, F-21 |
| 9.4.e | Physical and logical access control to ICT assets | primary | 4 CRITICAL | F-01, F-20, F-23, F-27 |
| 9.4.f | Strong authentication mechanisms + key management | partial | — | |
| Art.10 · Detection | | | | |
| 10.1 | Detect anomalous activities, including ICT network performance + incidents | primary | 15 WARN | F-02, F-03, F-04, F-05, F-06, F-07 (+9) |
| 10.2 | Multiple layers of control, alert thresholds, criteria | primary | — | |
| 10.3 | Automated alert mechanisms for staff responsible for response | partial | — | |
| Art.11 · Response and recovery | | | | |

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|--|--|---------------------|----------------------|------------------------------------|
| 11.2 | Comprehensive ICT business continuity policy | partial | — | |
| 11.4 | ICT response and recovery plans: RTO, RPO | partial | — | |
| 11.6 | Redundant ICT capacities with resources, capabilities + functionalities | primary | 6 WARN | F-17, F-24, F-28, F-29, F-30, F-31 |
| Art.12 · Backup policies and procedures, restoration and recovery | | | | |
| 12.1 | <i>Policies specifying scope of data covered by backup</i> | <i>contextual</i> | — | |
| 12.2 | <i>Backup systems able to activate in accordance with backup policies</i> | <i>contextual</i> | — | |
| 12.3 | <i>Restoration and recovery procedures and methods regularly tested</i> | <i>contextual</i> | — | |
| Art.13 · Learning and evolving | | | | |
| 13.1 | <i>Review ICT-related incidents + root-cause analysis</i> | <i>out-of-scope</i> | — | |
| Art.14 · Communication | | | | |
| 14.1 | <i>Crisis communication plans enabling responsible disclosure</i> | <i>out-of-scope</i> | — | |

| Year | Country | Value |
|------|---------|-------|
| 2000 | China | 1.00 |
| 2001 | China | 1.00 |
| 2002 | China | 1.00 |
| 2003 | China | 1.00 |
| 2004 | China | 1.00 |
| 2005 | China | 1.00 |
| 2006 | China | 1.00 |
| 2007 | China | 1.00 |
| 2008 | China | 1.00 |
| 2009 | China | 1.00 |
| 2010 | China | 1.00 |
| 2011 | China | 1.00 |
| 2012 | China | 1.00 |
| 2013 | China | 1.00 |
| 2014 | China | 1.00 |
| 2015 | China | 1.00 |
| 2016 | China | 1.00 |
| 2017 | China | 1.00 |
| 2018 | China | 1.00 |
| 2019 | China | 1.00 |
| 2020 | China | 1.00 |
| 2021 | China | 1.00 |
| 2022 | China | 1.00 |
| 2023 | China | 1.00 |
| 2024 | China | 1.00 |
| 2025 | China | 1.00 |
| 2026 | China | 1.00 |
| 2027 | China | 1.00 |
| 2028 | China | 1.00 |
| 2029 | China | 1.00 |
| 2030 | China | 1.00 |
| 2031 | China | 1.00 |
| 2032 | China | 1.00 |
| 2033 | China | 1.00 |
| 2034 | China | 1.00 |
| 2035 | China | 1.00 |
| 2036 | China | 1.00 |
| 2037 | China | 1.00 |
| 2038 | China | 1.00 |
| 2039 | China | 1.00 |
| 2040 | China | 1.00 |
| 2041 | China | 1.00 |
| 2042 | China | 1.00 |
| 2043 | China | 1.00 |
| 2044 | China | 1.00 |
| 2045 | China | 1.00 |
| 2046 | China | 1.00 |
| 2047 | China | 1.00 |
| 2048 | China | 1.00 |
| 2049 | China | 1.00 |
| 2050 | China | 1.00 |
| 2051 | China | 1.00 |
| 2052 | China | 1.00 |
| 2053 | China | 1.00 |
| 2054 | China | 1.00 |
| 2055 | China | 1.00 |
| 2056 | China | 1.00 |
| 2057 | China | 1.00 |
| 2058 | China | 1.00 |
| 2059 | China | 1.00 |
| 2060 | China | 1.00 |
| 2061 | China | 1.00 |
| 2062 | China | 1.00 |
| 2063 | China | 1.00 |
| 2064 | China | 1.00 |
| 2065 | China | 1.00 |
| 2066 | China | 1.00 |
| 2067 | China | 1.00 |
| 2068 | China | 1.00 |
| 2069 | China | 1.00 |
| 2070 | China | 1.00 |
| 2071 | China | 1.00 |
| 2072 | China | 1.00 |
| 2073 | China | 1.00 |
| 2074 | China | 1.00 |
| 2075 | China | 1.00 |
| 2076 | China | 1.00 |
| 2077 | China | 1.00 |
| 2078 | China | 1.00 |
| 2079 | China | 1.00 |
| 2080 | China | 1.00 |
| 2081 | China | 1.00 |
| 2082 | China | 1.00 |
| 2083 | China | 1.00 |
| 2084 | China | 1.00 |
| 2085 | China | 1.00 |
| 2086 | China | 1.00 |
| 2087 | China | 1.00 |
| 2088 | China | 1.00 |
| 2089 | China | 1.00 |
| 2090 | China | 1.00 |
| 2091 | China | 1.00 |
| 2092 | China | 1.00 |
| 2093 | China | 1.00 |
| 2094 | China | 1.00 |
| 2095 | China | 1.00 |
| 2096 | China | 1.00 |
| 2097 | China | 1.00 |
| 2098 | China | 1.00 |
| 2099 | China | 1.00 |
| 2100 | China | 1.00 |

ISO27001 · ISO/IEC 27001:2022

ISO/IEC 27001:2022 — Information security management systems

41 in-scope items · 8 touched · 7 failing

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|---|--|---------------------|---------------|------------------------------------|
| A.5 · Organizational controls (37) | | | | |
| A.5.1 | <i>Policies for information security</i> | <i>out-of-scope</i> | — | |
| A.5.2 | <i>Information security roles and responsibilities</i> | <i>out-of-scope</i> | — | |
| A.5.3 | Segregation of duties | partial | — | |
| A.5.7 | <i>Threat intelligence</i> | <i>contextual</i> | — | |
| A.5.8 | <i>Information security in project management</i> | <i>out-of-scope</i> | — | |
| A.5.9 | Inventory of information and other associated assets | partial | — | |
| A.5.10 | <i>Acceptable use of information and assets</i> | <i>out-of-scope</i> | — | |
| A.5.15 | Access control | primary | — | |
| A.5.16 | Identity management | primary | — | |
| A.5.17 | Authentication information | partial | — | |
| A.5.18 | Access rights | primary | — | |
| A.5.19 | Information security in supplier relationships | partial | — | |
| A.5.20 | <i>Addressing information security in supplier agreements</i> | <i>out-of-scope</i> | — | |
| A.5.21 | Managing information security in the ICT supply chain | partial | — | |
| A.5.23 | Information security for use of cloud services | primary | — | |
| A.5.24 | Information security incident management planning | partial | — | |
| A.5.25 | Assessment and decision on information security events | partial | — | |
| A.5.26 | <i>Response to information security incidents</i> | <i>out-of-scope</i> | — | |
| A.5.27 | <i>Learning from information security incidents</i> | <i>out-of-scope</i> | — | |
| A.5.29 | Information security during disruption | partial | — | |
| A.5.30 | ICT readiness for business continuity | primary | 6 WARN | F-17, F-24, F-28, F-29, F-30, F-31 |
| A.5.33 | Protection of records | partial | — | |
| A.5.35 | <i>Independent review of information security</i> | <i>out-of-scope</i> | — | |
| A.5.36 | Compliance with policies, rules and standards for infosec | primary | — | |
| A.5.37 | <i>Documented operating procedures</i> | <i>out-of-scope</i> | — | |
| A.6 · People controls (8) | | | | |
| A.6.1 | <i>Screening</i> | <i>out-of-scope</i> | — | |
| A.6.2 | <i>Terms and conditions of employment</i> | <i>out-of-scope</i> | — | |
| A.6.3 | <i>Information security awareness, education and training</i> | <i>out-of-scope</i> | — | |
| A.6.6 | <i>Confidentiality or non-disclosure agreements</i> | <i>out-of-scope</i> | — | |
| A.6.7 | Remote working | partial | — | |
| A.6.8 | <i>Information security event reporting</i> | <i>out-of-scope</i> | — | |
| A.7 · Physical controls (14) | | | | |
| A.7.1 | <i>Physical security perimeters</i> | <i>out-of-scope</i> | — | |
| A.7.2 | <i>Physical entry</i> | <i>out-of-scope</i> | — | |
| A.7.4 | <i>Physical security monitoring</i> | <i>out-of-scope</i> | — | |
| A.7.8 | <i>Equipment siting and protection</i> | <i>out-of-scope</i> | — | |
| A.7.9 | <i>Security of assets off-premises</i> | <i>out-of-scope</i> | — | |

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|--|--|----------------|------------------------------|--|
| A.7.10 | Storage media | out-of-scope | — | |
| A.7.11 | Supporting utilities | out-of-scope | — | |
| A.7.12 | Cabling security | out-of-scope | — | |
| A.7.13 | Equipment maintenance | out-of-scope | — | |
| A.7.14 | Secure disposal or re-use of equipment | out-of-scope | — | |
| A.8 · Technological controls (34) | | | | |
| A.8.1 | User endpoint devices | partial | — | |
| A.8.2 | Privileged access rights | primary | 5 CRITICAL | F-01, F-20, F-23, F-27, F-40 |
| A.8.3 | Information access restriction | primary | — | |
| A.8.4 | Access to source code | out-of-scope | — | |
| A.8.5 | Secure authentication | primary | — | |
| A.8.6 | Capacity management | primary | 6 INFO | F-33, F-34, F-36, F-37, F-41, F-42 |
| A.8.7 | Protection against malware | partial | — | |
| A.8.8 | Management of technical vulnerabilities | primary | — | |
| A.8.9 | Configuration management | primary | 11 CRITICAL | F-01, F-18, F-19, F-20, F-21, F-22 (+5) |
| A.8.10 | Information deletion | partial | — | |
| A.8.12 | Data leakage prevention | partial | — | |
| A.8.13 | Information backup | contextual | — | |
| A.8.14 | Redundancy of information processing facilities | primary | — | |
| A.8.15 | Logging | partial | — | |
| A.8.16 | Monitoring activities | partial | 21 WARN | F-02, F-03, F-04, F-05, F-06, F-07 (+15) |
| A.8.17 | Clock synchronization | out-of-scope | — | |
| A.8.18 | Use of privileged utility programs | partial | — | |
| A.8.19 | Installation of software on operational systems | partial | 2 WARN | F-18, F-21 |
| A.8.20 | Networks security | primary | — | |
| A.8.21 | Security of network services | primary | — | |
| A.8.22 | Segregation of networks | primary | 1 WARN | F-25 |
| A.8.23 | Web filtering | out-of-scope | — | |
| A.8.24 | Use of cryptography | partial | — | |
| A.8.25 | Secure development lifecycle | partial | — | |
| A.8.26 | Application security requirements | primary | — | |
| A.8.27 | Secure system architecture and engineering principles | primary | 7 CRITICAL | F-01, F-19, F-20, F-22, F-23, F-26 (+1) |
| A.8.28 | Secure coding | out-of-scope | — | |
| A.8.29 | Security testing in development and acceptance | primary | — | |
| A.8.32 | Change management | out-of-scope | — | |
| A.8.34 | Protection of information systems during audit testing | out-of-scope | — | |

Table 1. Summary of the study design and data collection.

| Study Component | Duration | Participants | Data Collection |
|---------------------------|------------|--------------|---|
| Baseline Assessment | Week 0 | 100 | Demographics, Physical Activity, Diet |
| Intervention Phase | Weeks 1-12 | 100 | Physical Activity, Diet, Blood Pressure, Heart Rate |
| Follow-up Assessment | Week 13 | 100 | Demographics, Physical Activity, Diet |
| Secondary Data Collection | Weeks 1-12 | 100 | Heart Rate Variability, Sleep Quality |
| Statistical Analysis | Week 13 | 100 | Analysis of Variance, Regression Models |
| Reporting | Week 14 | 100 | Final Report, Peer Review |

| Year | Country | Value |
|------|---------|-------|
| 2000 | China | 1.00 |
| 2001 | China | 1.00 |
| 2002 | China | 1.00 |
| 2003 | China | 1.00 |
| 2004 | China | 1.00 |
| 2005 | China | 1.00 |
| 2006 | China | 1.00 |
| 2007 | China | 1.00 |
| 2008 | China | 1.00 |
| 2009 | China | 1.00 |
| 2010 | China | 1.00 |
| 2011 | China | 1.00 |
| 2012 | China | 1.00 |
| 2013 | China | 1.00 |
| 2014 | China | 1.00 |
| 2015 | China | 1.00 |
| 2016 | China | 1.00 |
| 2017 | China | 1.00 |
| 2018 | China | 1.00 |
| 2019 | China | 1.00 |
| 2020 | China | 1.00 |
| 2021 | China | 1.00 |
| 2022 | China | 1.00 |
| 2023 | China | 1.00 |
| 2024 | China | 1.00 |
| 2025 | China | 1.00 |
| 2026 | China | 1.00 |
| 2027 | China | 1.00 |
| 2028 | China | 1.00 |
| 2029 | China | 1.00 |
| 2030 | China | 1.00 |
| 2031 | China | 1.00 |
| 2032 | China | 1.00 |
| 2033 | China | 1.00 |
| 2034 | China | 1.00 |
| 2035 | China | 1.00 |
| 2036 | China | 1.00 |
| 2037 | China | 1.00 |
| 2038 | China | 1.00 |
| 2039 | China | 1.00 |
| 2040 | China | 1.00 |
| 2041 | China | 1.00 |
| 2042 | China | 1.00 |
| 2043 | China | 1.00 |
| 2044 | China | 1.00 |
| 2045 | China | 1.00 |
| 2046 | China | 1.00 |
| 2047 | China | 1.00 |
| 2048 | China | 1.00 |
| 2049 | China | 1.00 |
| 2050 | China | 1.00 |
| 2051 | China | 1.00 |
| 2052 | China | 1.00 |
| 2053 | China | 1.00 |
| 2054 | China | 1.00 |
| 2055 | China | 1.00 |
| 2056 | China | 1.00 |
| 2057 | China | 1.00 |
| 2058 | China | 1.00 |
| 2059 | China | 1.00 |
| 2060 | China | 1.00 |
| 2061 | China | 1.00 |
| 2062 | China | 1.00 |
| 2063 | China | 1.00 |
| 2064 | China | 1.00 |
| 2065 | China | 1.00 |
| 2066 | China | 1.00 |
| 2067 | China | 1.00 |
| 2068 | China | 1.00 |
| 2069 | China | 1.00 |
| 2070 | China | 1.00 |
| 2071 | China | 1.00 |
| 2072 | China | 1.00 |
| 2073 | China | 1.00 |
| 2074 | China | 1.00 |
| 2075 | China | 1.00 |
| 2076 | China | 1.00 |
| 2077 | China | 1.00 |
| 2078 | China | 1.00 |
| 2079 | China | 1.00 |
| 2080 | China | 1.00 |
| 2081 | China | 1.00 |
| 2082 | China | 1.00 |
| 2083 | China | 1.00 |
| 2084 | China | 1.00 |
| 2085 | China | 1.00 |
| 2086 | China | 1.00 |
| 2087 | China | 1.00 |
| 2088 | China | 1.00 |
| 2089 | China | 1.00 |
| 2090 | China | 1.00 |
| 2091 | China | 1.00 |
| 2092 | China | 1.00 |
| 2093 | China | 1.00 |
| 2094 | China | 1.00 |
| 2095 | China | 1.00 |
| 2096 | China | 1.00 |
| 2097 | China | 1.00 |
| 2098 | China | 1.00 |
| 2099 | China | 1.00 |
| 2100 | China | 1.00 |

SOC2 · SOC 2 TYPE II

SOC 2 Type II — Trust Services Criteria (AICPA 2017)

21 in-scope items · 6 touched · 6 failing

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|---|---|----------------|----------------------|---|
| CC6 · Logical and Physical Access Controls | | | | |
| CC6.1 | Logical access security over protected information assets | primary | 5 CRITICAL | F-01, F-20, F-23, F-27, F-40 |
| CC6.2 | Prior to system access, credentials are registered and authorized | partial | — | |
| CC6.3 | Access to protected information assets is based on authorization | primary | — | |
| CC6.6 | Logical access security measures against threats from outside boundaries | primary | 1 WARN | F-25 |
| CC6.7 | Restricts transmission, movement and removal of information | partial | — | |
| CC6.8 | Prevents or detects against unauthorized or malicious software | primary | 6 CRITICAL | F-01, F-18, F-19, F-21, F-22, F-26 |
| CC7 · System Operations | | | | |
| CC7.1 | Detection and monitoring procedures for security events | primary | — | |
| CC7.2 | Monitoring of system components for anomalies (incidents) | primary | 15 WARN | F-02, F-03, F-04, F-05, F-06, F-07 (+9) |
| CC7.3 | Evaluation of identified events to determine incidents | partial | — | |
| CC7.4 | Procedures to respond to identified security incidents | partial | — | |
| CC7.5 | Identification and resolution of vulnerabilities | primary | — | |
| CC8 · Change Management | | | | |
| CC8.1 | Changes to infrastructure and software are authorized and managed | primary | 2 WARN | F-18, F-21 |
| A1 · Availability | | | | |
| A1.1 | Processing capacity maintained to meet availability commitments | primary | — | |
| A1.2 | Environmental protections, software, data-backup for recovery | primary | 6 WARN | F-17, F-24, F-28, F-29, F-30, F-31 |
| A1.3 | Recovery plan testing | partial | — | |
| C1 · Confidentiality | | | | |
| C1.1 | Confidential information is protected during processing and storage | primary | — | |
| C1.2 | Confidential information is disposed of in accordance with objectives | partial | — | |
| PI1 · Processing Integrity | | | | |
| PI1.1 | Obtains or generates, uses and communicates relevant quality info | partial | — | |
| PI1.2 | System processing is complete, valid, accurate, timely | partial | — | |
| PI1.4 | Inputs are processed completely, accurately and timely | partial | — | |
| PI1.5 | Outputs are reviewed for completeness and accuracy | partial | — | |

NIST-CSF · NIST CSF 2.0

NIST Cybersecurity Framework 2.0 — voluntary cybersecurity risk management guidance

19 in-scope items · 4 touched · 4 failing

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|----------------------|---|----------------|-------------------|--|
| GV · Govern | | | | |
| GV.SC-05 | Supply chain risk management requirements in agreements | partial | 2 WARN | F-18, F-21 |
| ID · Identify | | | | |
| ID.AM-01 | Inventories of hardware managed by the organization are maintained | partial | — | |
| ID.AM-02 | Inventories of software, services managed by the organization | primary | — | |
| ID.RA-01 | Vulnerabilities in assets are identified, validated and recorded | primary | 2 WARN | F-18, F-21 |
| PR · Protect | | | | |
| PR.AA-01 | Identities and credentials are issued, managed, verified, revoked | primary | — | |
| PR.AA-02 | Identities are proofed and bound to credentials based on context | partial | — | |
| PR.AA-03 | Users, services and hardware are authenticated | primary | — | |
| PR.AA-05 | Access permissions, entitlements and authorizations — least privilege | primary | — | |
| PR.DS-01 | Confidentiality, integrity and availability of data-at-rest protected | primary | — | |
| PR.DS-02 | Confidentiality, integrity and availability of data-in-transit protected | primary | — | |
| PR.IR-01 | Networks and environments are protected from unauthorized access | primary | — | |
| PR.PS-01 | Configuration management practices established and applied | primary | 9 CRITICAL | F-01, F-19, F-20, F-22, F-23, F-25 (+3) |
| PR.PS-02 | Software maintained, replaced and removed | primary | — | |
| DE · Detect | | | | |
| DE.CM-01 | Networks and network services are monitored for anomalous events | primary | — | |
| DE.CM-06 | External service provider activity and services are monitored | partial | — | |
| DE.CM-09 | Computing hardware and software are monitored for anomalies | primary | 21 WARN | F-02, F-03, F-04, F-05, F-06, F-07 (+15) |
| RS · Respond | | | | |
| RS.MA-02 | Incidents are categorized, prioritized and escalated | partial | — | |
| RC · Recover | | | | |
| RC.RP-01 | Recovery plan is executed during or after an incident | partial | — | |
| RC.RP-03 | Integrity of backups and assets is verified before use for restoring | partial | — | |

Table 1. Summary of the study design and participant characteristics.

| Variable | Value |
|--|-------------|
| Number of participants | 10 |
| Age (mean ± SD) | 22.5 ± 2.1 |
| Gender (Male/Female) | 6/4 |
| Height (mean ± SD) | 175.2 ± 5.8 |
| Weight (mean ± SD) | 72.5 ± 10.2 |
| Body Mass Index (mean ± SD) | 23.8 ± 2.5 |
| Number of trials | 10 |
| Number of correct trials | 8 |
| Number of incorrect trials | 2 |
| Number of trials with error | 1 |
| Number of trials with no response | 1 |
| Number of trials with response | 9 |
| Number of trials with correct response | 8 |
| Number of trials with incorrect response | 1 |
| Number of trials with no response | 1 |

The table provides a detailed overview of the study's design and participant characteristics. It includes information on the number of participants, their demographic data (age, gender, height, weight, BMI), and the results of the trials, such as the number of correct and incorrect responses, errors, and no responses.

NSA-CISA · NSA/CISA K8S HARDENING

NSA/CISA Kubernetes Hardening Guide v1.2 — US government K8s security baseline

25 in-scope items · 7 touched · 6 failing

| ITEM | REQUIREMENT | RELEVANCE | HITS | FINDING IDS |
|--|--|--------------|-------------------|------------------|
| PS · Pod Security | | | | |
| PS-1 | Run containers as non-root user | primary | 3 WARN | F-20, F-23, F-27 |
| PS-2 | Set immutable / read-only root filesystem | primary | 3 WARN | F-19, F-22, F-26 |
| PS-3 | Disallow privileged containers | primary | 1 CRITICAL | F-01 |
| PS-4 | Disallow privilege escalation | primary | 1 INFO | F-40 |
| PS-5 | Drop unnecessary Linux capabilities | primary | — | |
| PS-6 | Block hostPath volumes and host namespaces (network/PID/IPC) | primary | 1 WARN | F-25 |
| PS-7 | Apply seccomp / AppArmor / SELinux profiles | primary | — | |
| PS-8 | Enforce Pod Security Admission baseline minimum | primary | — | |
| PS-9 | Use admission control for image scanning | partial | 2 WARN | F-18, F-21 |
| NS · Network Separation and Hardening | | | | |
| NS-1 | Default-deny NetworkPolicies in every namespace | primary | — | |
| NS-2 | Use a CNI plugin that supports NetworkPolicy | out-of-scope | — | |
| NS-3 | Restrict access to the control plane with firewall rules | partial | — | |
| NS-4 | Encrypt all traffic with TLS (cluster + ingress) | primary | — | |
| NS-5 | Encrypt etcd at rest with a KMS provider | primary | — | |
| NS-6 | Avoid NodePort and LoadBalancer services where unnecessary | primary | — | |
| AA · Authentication and Authorization | | | | |
| AA-1 | Disable anonymous authentication | primary | — | |
| AA-2 | Use strong user authentication (OIDC / IAM, MFA) | out-of-scope | — | |
| AA-3 | RBAC enabled and least-privilege ServiceAccounts | primary | — | |
| AA-4 | Disable automounting of ServiceAccount tokens by default | primary | — | |
| AA-5 | Restrict cluster-admin and wildcard permissions | primary | — | |
| LT · Audit Logging and Threat Detection | | | | |
| LT-1 | Enable Kubernetes API audit logging | primary | — | |
| LT-2 | Persist audit logs centrally; tamper-evident | partial | — | |
| LT-3 | Audit policy logs RBAC, secret, and pod-exec events | primary | — | |
| LT-4 | Runtime threat detection (Falco / Tetragon / similar) | out-of-scope | — | |
| LT-5 | Monitor for environment-specific anomalies | out-of-scope | — | |
| UA · Upgrading and Application Security Practices | | | | |
| UA-1 | Apply security patches and upgrades promptly | primary | — | |
| UA-2 | Run vulnerability scans and penetration tests periodically | partial | — | |
| UA-3 | Remove unused components and services from the cluster | partial | — | |
| UA-4 | Enforce image-signing or trust policies | partial | 2 WARN | F-18, F-21 |

Operational practices the cluster is following.

This section measures the cluster against **168** practitioner best practices distilled from the kubernetes.io security and configuration guides, the OWASP Kubernetes cheat sheet, the CIS Kubernetes Benchmark, vendor production checklists (Wiz, Sysdig, Palark, Pulumi, Devtron, learnk8s) and the OPA Gatekeeper + Kyverno policy libraries. Of these, **115** are auto-checkable from cluster state — the rest are organisational practices that must be evidenced elsewhere.

| | | | | |
|---|---|---|--|--|
| <p>BP-1 · Cluster & Infrastructure</p> <p>100%</p> <p>3 met of 3 in-scope · 0 failing</p> | <p>BP-2 · Namespaces & Multi-Tenancy</p> <p>100%</p> <p>7 met of 7 in-scope · 0 failing</p> | <p>BP-3 · Workload Security & Pod Hardening</p> <p>68%</p> <p>13 met of 19 in-scope · 5 failing</p> | <p>BP-4 · RBAC & Identity</p> <p>100%</p> <p>13 met of 13 in-scope · 0 failing</p> | <p>BP-5 · Network & Ingress</p> <p>100%</p> <p>10 met of 10 in-scope · 0 failing</p> |
| <p>BP-6 · Secrets & Data Protection</p> <p>100%</p> <p>9 met of 9 in-scope · 0 failing</p> | <p>BP-7 · Images & Supply Chain</p> <p>80%</p> <p>8 met of 10 in-scope · 2 failing</p> | <p>BP-8 · Resources, Limits & Quotas</p> <p>90%</p> <p>9 met of 10 in-scope · 0 failing</p> | <p>BP-9 · Reliability & Resilience</p> <p>92%</p> <p>12 met of 13 in-scope · 1 failing</p> | <p>BP-10 · Observability & Monitoring</p> <p>100%</p> <p>7 met of 7 in-scope · 0 failing</p> |
| <p>BP-11 · Lifecycle, Deployment & GitOps</p> <p>83%</p> <p>5 met of 6 in-scope · 1 failing</p> | <p>BP-12 · Cost Optimization</p> <p>100%</p> <p>5 met of 5 in-scope · 0 failing</p> | <p>BP-13 · Governance & Policy</p> <p>100%</p> <p>3 met of 3 in-scope · 0 failing</p> | | |

Per-category breakdown follows. **Met** = the practice is in scope, no findings hit it. **Failing** = at least one CRITICAL or WARN finding evidences it is not being followed. **Out-of-scope** items are hidden from the per-category tables — they appear in `legal/kubernetes-best-practices-checklist.md` with the organisational evidence they require.

Table 1. Summary of the study design and data collection.

| Phase | Duration | Activities | Data Collected |
|----------------------------|----------|-----------------------------|--|
| Phase 1: Baseline | 4 weeks | Rest and observation | Heart rate, blood pressure, body temperature |
| Phase 2: Intervention | 8 weeks | Physical training (3x/week) | Heart rate, blood pressure, body temperature, energy expenditure |
| Phase 3: Post-intervention | 4 weeks | Rest and observation | Heart rate, blood pressure, body temperature |
| Phase 4: Follow-up | 12 weeks | Rest and observation | Heart rate, blood pressure, body temperature |

Physical training consisted of aerobic and resistance exercises performed 3 times per week.

BP-3 · WORKLOAD SECURITY & POD HARDENING

Pod securityContext, capabilities, host-namespace isolation, SA hygiene

19 in-scope items · 13 met · 5 failing

| ITEM | PRACTICE | RELEVANCE | HITS | FINDING IDS |
|------|---|---------------------|-------------------|------------------|
| 3.1 | <code>`privileged: false`</code> on every container | primary | 1 CRITICAL | F-01 |
| 3.2 | <code>`allowPrivilegeEscalation: false`</code> on every container | primary | 1 INFO | F-40 |
| 3.3 | <code>`runAsNonRoot: true`</code> (or <code>`runAsUser > 0`</code>) on every container | primary | 3 WARN | F-20, F-23, F-27 |
| 3.4 | <code>`readOnlyRootFilesystem: true`</code> ; writable paths via <code>`emptyDir`</code> only | primary | 3 WARN | F-19, F-22, F-26 |
| 3.5 | <code>`capabilities.drop: ["ALL"]`</code> ; capabilities re-added explicitly | primary | — | |
| 3.6 | Forbid dangerous caps (NET_ADMIN, SYS_ADMIN, ...) | primary | — | |
| 3.7 | <code>`hostNetwork: false`</code> | primary | 1 WARN | F-25 |
| 3.8 | <code>`hostPID: false`</code> | primary | — | |
| 3.9 | <code>`hostIPC: false`</code> | primary | — | |
| 3.10 | No <code>`hostPath`</code> mounts to sensitive paths | primary | — | |
| 3.11 | <code>`seccompProfile.type: RuntimeDefault`</code> (or custom) on every container | primary | — | |
| 3.12 | AppArmor / SELinux profile annotation set per workload | primary | — | |
| 3.13 | Unsafe sysctls blocked | partial | — | |
| 3.14 | <code>`automountServiceAccountToken: false`</code> unless workload calls API | primary | — | |
| 3.15 | No <code>`kubectl exec`</code> / debug containers in production unless audited | partial | — | |
| 3.16 | Non-root build user in the Dockerfile (defence in depth) | partial | 3 WARN | F-20, F-23, F-27 |
| 3.17 | <i>Dedicated runtime sandbox (gVisor / Kata) for high-risk workloads</i> | <i>out-of-scope</i> | — | |
| 3.18 | No naked Pods — workloads created via Deployment / StatefulSet | primary | — | |
| 3.19 | Use Deployments instead of bare Pods for stateless apps | primary | — | |
| 3.20 | Deny pods that mount the container runtime socket | primary | — | |

BP-4 · RBAC & IDENTITY

Authn / authz, ServiceAccount hygiene, cluster-admin minimisation

13 in-scope items · 13 met · 0 failing

| ITEM | PRACTICE | RELEVANCE | HITS | FINDING IDS |
|------|---|---------------------|------|-------------|
| 4.1 | RBAC enabled (<code>--authorization-mode=Node,RBAC</code>) | primary | — | |
| 4.2 | Cluster-admin bound to ≤ 2 named subjects post-bootstrap | primary | — | |
| 4.3 | No wildcard verbs/resources in any Role / ClusterRole | primary | — | |
| 4.4 | Cluster-wide <code>`secrets`</code> read access restricted to platform controllers | primary | — | |
| 4.5 | <code>`escalate`/`bind`/`impersonate`</code> verbs granted only when needed | primary | — | |
| 4.6 | <code>`pods/exec`</code>, <code>`pods/portforward`</code>, <code>`pods/attach`</code> restricted | primary | — | |
| 4.7 | Each workload has a dedicated <code>`ServiceAccount`</code> (never <code>`default`</code>) | primary | — | |
| 4.8 | <code>`automountServiceAccountToken: false`</code> at the SA level when unused | primary | — | |
| 4.9 | Bound, projected, short-lived SA tokens — no long-lived <code>`Secret`</code> -backed tokens | partial | — | |
| 4.10 | <code>`system:masters`</code> not used outside cluster bootstrap / break-glass | partial | — | |
| 4.11 | <i>External OIDC / IAM identity provider for human cluster access</i> | <i>out-of-scope</i> | — | |
| 4.12 | <i>MFA enforced for every human cluster identity</i> | <i>out-of-scope</i> | — | |
| 4.13 | <i>Quarterly access review; offboarding revokes grants $\leq 24h$</i> | <i>out-of-scope</i> | — | |
| 4.14 | RBAC inventory tooling run on every audit | partial | — | |
| 4.15 | <code>`NodeRestriction`</code> admission plugin enabled | primary | — | |
| 4.16 | Anonymous access disabled on the API server | primary | — | |

Table 1. Summary of the study

| Study | Year | Country | Sample Size | Design | Outcome |
|-------|------|-------------|-------------|--------------|---------|
| 1 | 2010 | USA | 1000 | Case-control | High |
| 2 | 2011 | UK | 2000 | Cohort | High |
| 3 | 2012 | Canada | 1500 | Case-control | High |
| 4 | 2013 | Australia | 1200 | Cohort | High |
| 5 | 2014 | France | 1800 | Case-control | High |
| 6 | 2015 | Germany | 1600 | Cohort | High |
| 7 | 2016 | Italy | 1400 | Case-control | High |
| 8 | 2017 | Spain | 1700 | Cohort | High |
| 9 | 2018 | Japan | 1900 | Case-control | High |
| 10 | 2019 | South Korea | 1300 | Cohort | High |
| 11 | 2020 | India | 1100 | Case-control | High |
| 12 | 2021 | Brazil | 1000 | Cohort | High |
| 13 | 2022 | China | 1200 | Case-control | High |
| 14 | 2023 | USA | 1500 | Cohort | High |
| 15 | 2024 | UK | 1800 | Case-control | High |
| 16 | 2025 | Canada | 1600 | Cohort | High |
| 17 | 2026 | Australia | 1400 | Case-control | High |
| 18 | 2027 | France | 1700 | Cohort | High |
| 19 | 2028 | Germany | 1500 | Case-control | High |
| 20 | 2029 | Italy | 1600 | Cohort | High |
| 21 | 2030 | Spain | 1400 | Case-control | High |
| 22 | 2031 | Japan | 1700 | Cohort | High |
| 23 | 2032 | South Korea | 1500 | Case-control | High |
| 24 | 2033 | India | 1300 | Cohort | High |
| 25 | 2034 | Brazil | 1100 | Case-control | High |
| 26 | 2035 | China | 1200 | Cohort | High |
| 27 | 2036 | USA | 1400 | Case-control | High |
| 28 | 2037 | UK | 1600 | Cohort | High |
| 29 | 2038 | Canada | 1500 | Case-control | High |
| 30 | 2039 | Australia | 1300 | Cohort | High |
| 31 | 2040 | France | 1700 | Case-control | High |
| 32 | 2041 | Germany | 1500 | Cohort | High |
| 33 | 2042 | Italy | 1600 | Case-control | High |
| 34 | 2043 | Spain | 1400 | Cohort | High |
| 35 | 2044 | Japan | 1700 | Case-control | High |
| 36 | 2045 | South Korea | 1500 | Cohort | High |
| 37 | 2046 | India | 1300 | Case-control | High |
| 38 | 2047 | Brazil | 1100 | Cohort | High |
| 39 | 2048 | China | 1200 | Case-control | High |
| 40 | 2049 | USA | 1400 | Cohort | High |
| 41 | 2050 | UK | 1600 | Case-control | High |
| 42 | 2051 | Canada | 1500 | Cohort | High |
| 43 | 2052 | Australia | 1300 | Case-control | High |
| 44 | 2053 | France | 1700 | Cohort | High |
| 45 | 2054 | Germany | 1500 | Case-control | High |
| 46 | 2055 | Italy | 1600 | Cohort | High |
| 47 | 2056 | Spain | 1400 | Case-control | High |
| 48 | 2057 | Japan | 1700 | Cohort | High |
| 49 | 2058 | South Korea | 1500 | Case-control | High |
| 50 | 2059 | India | 1300 | Cohort | High |
| 51 | 2060 | Brazil | 1100 | Case-control | High |
| 52 | 2061 | China | 1200 | Cohort | High |
| 53 | 2062 | USA | 1400 | Case-control | High |
| 54 | 2063 | UK | 1600 | Cohort | High |
| 55 | 2064 | Canada | 1500 | Case-control | High |
| 56 | 2065 | Australia | 1300 | Cohort | High |
| 57 | 2066 | France | 1700 | Case-control | High |
| 58 | 2067 | Germany | 1500 | Cohort | High |
| 59 | 2068 | Italy | 1600 | Case-control | High |
| 60 | 2069 | Spain | 1400 | Cohort | High |
| 61 | 2070 | Japan | 1700 | Case-control | High |
| 62 | 2071 | South Korea | 1500 | Cohort | High |
| 63 | 2072 | India | 1300 | Case-control | High |
| 64 | 2073 | Brazil | 1100 | Cohort | High |
| 65 | 2074 | China | 1200 | Case-control | High |
| 66 | 2075 | USA | 1400 | Cohort | High |
| 67 | 2076 | UK | 1600 | Case-control | High |
| 68 | 2077 | Canada | 1500 | Cohort | High |
| 69 | 2078 | Australia | 1300 | Case-control | High |
| 70 | 2079 | France | 1700 | Cohort | High |
| 71 | 2080 | Germany | 1500 | Case-control | High |
| 72 | 2081 | Italy | 1600 | Cohort | High |
| 73 | 2082 | Spain | 1400 | Case-control | High |
| 74 | 2083 | Japan | 1700 | Cohort | High |
| 75 | 2084 | South Korea | 1500 | Case-control | High |
| 76 | 2085 | India | 1300 | Cohort | High |
| 77 | 2086 | Brazil | 1100 | Case-control | High |
| 78 | 2087 | China | 1200 | Cohort | High |
| 79 | 2088 | USA | 1400 | Case-control | High |
| 80 | 2089 | UK | 1600 | Cohort | High |
| 81 | 2090 | Canada | 1500 | Case-control | High |
| 82 | 2091 | Australia | 1300 | Cohort | High |
| 83 | 2092 | France | 1700 | Case-control | High |
| 84 | 2093 | Germany | 1500 | Cohort | High |
| 85 | 2094 | Italy | 1600 | Case-control | High |
| 86 | 2095 | Spain | 1400 | Cohort | High |
| 87 | 2096 | Japan | 1700 | Case-control | High |
| 88 | 2097 | South Korea | 1500 | Cohort | High |
| 89 | 2098 | India | 1300 | Case-control | High |
| 90 | 2099 | Brazil | 1100 | Cohort | High |
| 91 | 2100 | China | 1200 | Case-control | High |

BP-7 · IMAGES & SUPPLY CHAIN

Image pinning, scanning, signing, SBOM, registry hygiene

10 in-scope items · 8 met · 2 failing

| ITEM | PRACTICE | RELEVANCE | HITS | FINDING IDS |
|------|---|--------------|------------------|-------------|
| 7.1 | Production images pinned by <code>@sha256:</code> digest | primary | — | |
| 7.2 | No <code>:latest</code> (or <code>unset</code>) tag in any production manifest | primary | 2 WARN | F-18, F-21 |
| 7.3 | <code>imagePullPolicy: Always</code> for re-pushable tags | primary | — | |
| 7.4 | Allow-listed registries only — block <code>docker.io/*</code> wildcards | partial | — | |
| 7.5 | Image vulnerability scan gates promotion to prod | partial | — | |
| 7.6 | CRITICAL CVEs block deploy; HIGH CVEs require ticket + SLA | partial | — | |
| 7.7 | Image signatures verified at admission (Cosign / Notation) | partial | — | |
| 7.8 | SBOM generated and stored for every production image | partial | — | |
| 7.9 | Multi-stage builds; minimal base (<code>scratch</code> / <code>distroless</code> / <code>alpine</code>) | out-of-scope | — | |
| 7.10 | No build tools, shells, or package managers in the runtime image | out-of-scope | — | |
| 7.11 | OCI metadata labels populated | partial | — | |
| 7.12 | <code>.dockerignore</code> excludes <code>.git</code> , secrets, build artefacts, and tests | out-of-scope | — | |
| 7.13 | Vulnerability remediation SLA documented (CRIT $\leq 7d$, HIGH $\leq 30d$) | out-of-scope | — | |
| 7.14 | Coordinated Vulnerability Disclosure policy published | out-of-scope | — | |
| 7.15 | Private registry with retention + replication | out-of-scope | — | |
| 7.16 | Image promotion uses commit-SHA tags or semver — never floating tags | partial | 2 WARN | F-18, F-21 |

BP-8 · RESOURCES, LIMITS & QUOTAS

Right-sizing, capacity, headroom, ResourceQuota / LimitRange

10 in-scope items · 9 met · 0 failing

| ITEM | PRACTICE | RELEVANCE | HITS | FINDING IDS |
|------|--|----------------|-------------------------|------------------------------------|
| 8.1 | Every container has CPU and memory `requests` | primary | 6 INFO | F-33, F-34, F-36, F-37, F-41, F-42 |
| 8.2 | Every container has memory `limits` | primary | — | |
| 8.3 | CPU `limits` set only when isolation is required | primary | — | |
| 8.4 | Requests sized via profiling / load testing / VPA | partial | — | |
| 8.5 | Aggregate requests across all workloads \leq80% of node-pool allocatable | primary | — | |
| 8.6 | `LimitRange` provides defaults so missing fields don't slip through | primary | — | |
| 8.7 | `ResourceQuota` per namespace caps total CPU / memory / pod count | primary | — | |
| 8.8 | Ephemeral storage requests + limits set for scratch-writing workloads | partial | — | |
| 8.9 | Default `StorageClass` defined; PVCs always reference one | partial | — | |
| 8.10 | Node pools sized so a single node loss does not breach quota | partial | — | |

Table 1. Demographic characteristics of the study population

| Characteristic | Number (n) | Percentage (%) |
|---------------------|------------|----------------|
| Age (years) | | |
| < 18 | 12 | 12.0 |
| 18-24 | 28 | 28.0 |
| 25-34 | 35 | 35.0 |
| 35-44 | 22 | 22.0 |
| 45-54 | 13 | 13.0 |
| 55-64 | 10 | 10.0 |
| 65-74 | 8 | 8.0 |
| 75-84 | 5 | 5.0 |
| 85+ | 3 | 3.0 |
| Gender | | |
| Male | 45 | 45.0 |
| Female | 55 | 55.0 |
| Ethnicity | | |
| White | 60 | 60.0 |
| Black | 20 | 20.0 |
| Hispanic | 15 | 15.0 |
| Asian | 10 | 10.0 |
| Other | 5 | 5.0 |
| Marital status | | |
| Married | 40 | 40.0 |
| Single | 30 | 30.0 |
| Divorced | 15 | 15.0 |
| Widowed | 15 | 15.0 |
| Education level | | |
| High school or less | 30 | 30.0 |
| Some college | 25 | 25.0 |
| Bachelor's degree | 20 | 20.0 |
| Master's degree | 10 | 10.0 |
| PhD | 5 | 5.0 |
| Income (annual) | | |
| < \$10,000 | 15 | 15.0 |
| \$10,000-\$20,000 | 25 | 25.0 |
| \$20,000-\$30,000 | 20 | 20.0 |
| \$30,000-\$40,000 | 15 | 15.0 |
| > \$40,000 | 25 | 25.0 |

Note: Percentages may not sum to 100% due to rounding.

BP-11 · LIFECYCLE, DEPLOYMENT & GITOPS

GitOps, IaC, admission policy, progressive delivery, upgrades

6 in-scope items · 5 met · 1 failing

| ITEM | PRACTICE | RELEVANCE | HITS | FINDING IDS |
|-------|--|----------------|------------------|-------------|
| 11.1 | All manifests in version control; no out-of-band `kubectl apply` | out-of-scope | — | |
| 11.2 | Two-person review rule for prod-targeting PRs | out-of-scope | — | |
| 11.3 | GitOps controller (Argo CD / Flux) reconciles desired state | out-of-scope | — | |
| 11.4 | Manifest linting in CI | partial | — | |
| 11.5 | Policy-as-Code admission (Kyverno / OPA Gatekeeper) | partial | — | |
| 11.6 | Progressive delivery for high-blast-radius services | out-of-scope | — | |
| 11.7 | Deployment strategy chosen per workload | out-of-scope | — | |
| 11.8 | Rollback path tested; `kubectl rollout undo` rehearsed | out-of-scope | — | |
| 11.9 | Deprecated-API detection before upgrade | primary | — | |
| 11.10 | Removed-API findings always block upgrade | primary | — | |
| 11.11 | Standard recommended labels populated | partial | — | |
| 11.12 | ConfigMap / Secret hot-reload configured | out-of-scope | — | |
| 11.13 | Kustomize / Helm with environment overlays | out-of-scope | — | |
| 11.14 | Production data never used unmasked in lower environments | out-of-scope | — | |
| 11.15 | Image tag carried as commit SHA so every deploy is traceable | partial | 2 WARN | F-18, F-21 |

BP-12 · COST OPTIMIZATION

Right-sizing, idle workloads, autoscaling, node-pool strategy

5 in-scope items · 5 met · 0 failing

| ITEM | PRACTICE | RELEVANCE | HITS | FINDING IDS |
|------|--|---------------------|------|-------------|
| 12.1 | Right-size requests against observed usage | primary | — | |
| 12.2 | Identify and shut down idle workloads | primary | — | |
| 12.3 | Top-N most expensive namespaces reviewed monthly | primary | — | |
| 12.4 | <i>Spot / preemptible node pools for fault-tolerant batch / dev</i> | <i>out-of-scope</i> | — | |
| 12.5 | <i>Committed-use / savings-plan discounts for steady workloads</i> | <i>out-of-scope</i> | — | |
| 12.6 | Cluster Autoscaler / Karpenter scales node pool down at low traffic | partial | — | |
| 12.7 | <i>Region selection considers data-egress and regulation, not just price</i> | <i>out-of-scope</i> | — | |
| 12.8 | Avoid CPU limits where throttling worsens latency | partial | — | |
| 12.9 | <i>Monitoring stack cost is itself tracked</i> | <i>out-of-scope</i> | — | |

What are the components of the OSI model?

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

QUESTION 101

What is the purpose of the OSI model?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 102

What is the difference between a protocol and a standard?

1. A protocol is a set of rules that governs the communication between two devices, while a standard is a set of rules that governs the communication between multiple devices.
2. A protocol is a set of rules that governs the communication between two devices, while a standard is a set of rules that governs the communication between multiple devices.
3. A protocol is a set of rules that governs the communication between two devices, while a standard is a set of rules that governs the communication between multiple devices.

QUESTION 103
What is the purpose of the OSI model's top three layers?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 104

What is the purpose of the OSI model's bottom three layers?

1. To provide a common framework for describing and analyzing network protocols
2. To provide a common framework for describing and analyzing network protocols
3. To provide a common framework for describing and analyzing network protocols

QUESTION 105

What is the purpose of the OSI model's top layer?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 106

What is the purpose of the OSI model's bottom layer?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 107

What is the purpose of the OSI model's top two layers?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 108

What is the purpose of the OSI model's bottom two layers?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 109

What is the purpose of the OSI model's top layer?

1. To provide a common framework for describing and analyzing network protocols

QUESTION 110

```
# flagged by: config scan
# Set readOnlyRootFilesystem to true in the container securityContext.

# [11] F-27 · kube-system · container "kube-proxy" is not set to runAsNonRoot
# affects: DaemonSet/kube-proxy
# flagged by: config scan
# Set runAsUser to a non-zero number and runAsNonRoot to true in your pod or container securityContext.
Refer to https://kubernetes.io/docs/tasks/configure-pod-container/security-context/ for details.
```

Re-run the scan pipeline after remediation. The score, trend line, and confidence distribution all update on the next pass.