ECC-2:2024: technical evidence

Neither Mamluk LLC-FZ nor its products are affiliated with or endorsed by the National Cybersecurity Authority (Saudi Arabia).

Regime	ECC-2:2024, National Cybersecurity Authority (NCA), Kingdom of Saudi Arabia
Organisation	Example Bank
Cluster	example-production
Collected	2026-11-19T10:53:03Z
Collector	Bahriya Tersane Compliance and Assurance Convoy, collector 1.x.y

This report records technical evidence from one Kubernetes cluster. It maps the requirements of the regime named above to what the cluster shows, through the controls of NIST SP 800-53 Rev. 5. It does not state that the organisation complies with the regime.

NCA publishes no mapping of these controls to NIST SP 800-53. The mapping in this report is Mamluk's own.

Organisational requirements are the organisation's to evidence, and the report marks them so. Where a requirement is only partly technical, the cluster evidences its part and the organisation the rest. Whether the organisation complies is determined by its assessor.

Requirement identifiers are the regulator's; each summary is Mamluk's own paraphrase, not the regulator's text. The files of this run are listed with their SHA-256 digests in manifest.sha256.

This report is the evidence. The ClusterComplianceReport tersane-compliance-nist that the cluster also holds is an indicative summary of trivy-operator's checks by NIST control, in which a check that has not run is shown as passed; it is not evidence for any regime.

Exempt namespaces: kube-system, kube-node-lease, kube-public, tigera-operator, calico-system, calico-apiserver, longhorn-system, cert-manager, kong, kuma-system, logging, netdata, bahriya-system, kyverno, trivy-system, local-path-storage, compliance, compliance-node. No policy this chart installs applies in these namespaces, and their failures are listed under each check without being counted: they hold the platform's own components (on a Bahriya Kubernetes Engine cluster, its system namespaces), the policy engine, the scanner and this Convoy, which need what the policies forbid. The namespace default is judged only while it holds a workload.

Summary

176 requirements: 7 enforced by a policy, 17 checked, 9 provided by the platform, 143 organisational (40 technical, outside the cluster; 96 non-technical; 7 technical and non-technical).

Outcome	Requirements	Meaning
Fail	13	The cluster was checked and something does not meet the requirement. The findings say what and where.
Not provided	1	A control the requirement needs is switched off on this cluster.

Incomplete	4	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	1	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	11 of which with exception: 0	Every check behind the requirement passed on this run's date. Where coverage is partial, the pass covers the cluster's part only.
Recorded	3	Facts collected for the organisation's reviewer, such as an inventory or a list of access; no verdict.
Nothing to check	0	The cluster has nothing of this kind yet, for example no Ingress to check for TLS. Neither a pass nor a failure.
Organisational evidence	143	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

16 object(s) fail at least one check: 4 cluster-wide and 12 in 1 namespace(s). They are listed under Fix first, the most severe first.

Fix first

Each object that fails a check, with the requirements it fails, what is wrong, how to fix it and the command that shows the full result. Objects are grouped by namespace; objects that belong to no namespace are cluster-wide. A group's place is set by its most severe finding, and within a group the most severe come first. Fixing an object clears its failure in every requirement listed against it. Failures in exempt namespaces are not listed here; they are listed, not counted, under each check.

Cluster-wide

4 object(s), most severe Critical.

ClusterRole **`tigera-operator`** Fails 2-2-3-3, 2-2-3-4	
CRITICAL	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator' shouldn't have access to manage resource 'secrets' Check trivy.rbac-privilege, trivy-operator AVD-KSV-0041. **How to fix** Manage secrets are not allowed. Remove resource 'secrets' from cluster role (trivy-operator)
CRITICAL	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'tigera-operator' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"] Check trivy.rbac-privilege, trivy-operator AVD-KSV-0114. **How to fix** Remove webhook configuration resources/verbs, acceptable values for verbs ['get', 'list', 'watch'] (trivy-operator)
Full result	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator -o yaml`

ClusterRole **`tigera-operator-secrets`** Fails 2-2-3-3, 2-2-3-4

CRITICAL AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator-secrets' shouldn't have access to manage resource 'secrets'

Check trivy.rbac-privilege, trivy-operator AVD-KSV-0041.

How to fix Manage secrets are not allowed. Remove resource 'secrets' from cluster role (trivy-operator)

Full result

```
kubectl get clusterrbacassessmentreport clusterrole-tigera-operator-secrets -o yaml
```

Cluster **`backups`** Fails 2-9-2, 2-9-3-1

HIGH neither Longhorn nor Velero is installed

Check cluster.backups.

How to fix On a Bahriya Kubernetes Engine cluster, set components.longhorn.settings.backup.target and credentialSecret in config.yaml, and backup.daily.enabled to true, then run apply.sh --commit, which creates the recurring job bke-daily-backup. A target that is configured but not available gives its reason in the longhorn-manager log: kubectl -n longhorn-system logs -l app=longhorn-manager --tail=200 | grep -i backup. With Velero, create a backup storage location that Velero reports Available and a Schedule that is not paused, as Velero's documentation describes; kubectl get backupstoragelocations.velero.io -A gives each location's phase. (Bahriya Tersane)

Full result

```
kubectl api-resources | grep -E 'longhorn.io|velero.io'
```

Platform **`API server audit log`** Fails 2-12-3-5

MEDIUM kept at most 30 days before rotation; the regime requires 365

Check platform.audit-rotation.

How to fix Keep the audit log for at least the period the regime requires. On BKE, which always limits the number of audit log files, forward the log to a central log store that keeps it that long, and give that store's retention setting to your assessor as evidence: from BKE 2.6.1, Fluent Bit collects the audit log on the control-plane nodes under the tag audit.*, and an output that matches that tag sends it to your store; on earlier versions, forward it with your own collector. On another cluster, either forward the log in the same way, or set --audit-log-maxage to at least that period and leave --audit-log-maxbackup unset or 0 on each API server's static Pod manifest, with enough disk on each control-plane node to hold that period. (Bahriya Tersane)

Full result

```
kubectl -n bahriya-system get configmap bke-platform -o
jsonpath='{.data.audit\.rotation}'
```

Namespace payments

12 object(s), most severe High.

CronJob **nightly** Fails 1-6-2-2, 1-6-3-2, 1-6-3-5, 2-2-3-4, 2-3-2

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of CronJob 'nightly' should set 'securityContext.allowPrivilegeEscalation' to false Check trivy.privileged, trivy-operator AVD-KSV-0001. **How to fix** Set containers[].securityContext.allowPrivilegeEscalation to false. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of CronJob 'nightly' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of cronjob "nightly" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

CronJob **weekly** Fails 1-6-3-2

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport f95320a9-ae62-47ac-8865-9ff294efe291 -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Deployment **ledger** Fails 1-6-3-2

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport dd716344-57f2-43ff-8850-cec7fbc7281f -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Deployment **legacy-batch** Fails 1-6-2-2, 1-6-3-2, 1-6-3-5, 2-2-3-4, 2-3-2	
HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.allowPrivilegeEscalation' to false Check trivy.privileged, trivy-operator AVD-KSV-0001. **How to fix** Set containers[].securityContext.allowPrivilegeEscalation to false. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "legacy-batch-5bdd998d78" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
	`kubectl get policyreport cc1c8507-d6bb-4e77-8205-1a214c884777 -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Deployment **unsigned-app** Fails 1-6-2-2, 1-6-3-2, 1-6-3-5, 2-2-3-4, 2-3-2	
HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.allowPrivilegeEscalation' to false Check trivy.privileged, trivy-operator AVD-KSV-0001. **How to fix** Set containers[].securityContext.allowPrivilegeEscalation to false. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "unsigned-app-b5567644f" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

Job **migrate-once** Fails 1-6-3-2

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport cdf45f25-40a7-4023-bc92-880235dc0c91 -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Job **nightly-now** Fails 1-6-3-2

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 6a73d7cc-01f5-42d8-9d6c-462a360b517b -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Pod **nightly-now-k7cbf** Fails 1-6-3-2

HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 4074d46b-fb0f-4ce3-8312-15270922068d -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Pod **one-off** Fails 1-6-3-2

HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
Full result	`kubectl get policyreport 157881f3-9f3d-472c-9134-201b7cf0220e -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.
	Kyverno passes an image that no signing key covers without verifying it, so no report records it.

Pod **unsigned-app-b5567644f-vpkpp** Fails 1-6-3-2

HIGH images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0

Check policy.images-signed.

How to fix Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)

Full result

```
kubectl get policyreport 3f291cbb-5fdd-4171-9ead-42230533be9f -n payments -o yaml
```

Kyverno names each policy report after the UID of the object it covers.

ReplicaSet **unsigned-app-b5567644f** Fails 1-6-3-2

HIGH images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0

Check policy.images-signed.

How to fix Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)

Full result

```
kubectl get policyreport 9f9f8242-9449-4023-a60b-aa60653c0b24 -n payments -o yaml
```

Kyverno names each policy report after the UID of the object it covers.

Namespace **payments** Fails 2-5-2, 2-5-3-1, 2-5-3-2, 2-5-3-5

MEDIUM namespace payments holds no NetworkPolicy

Check policy.namespace-network-policy.

How to fix Add NetworkPolicies to the namespace that allow only the traffic its workloads need. To start every new namespace closed, set generate.defaultDenyNetworkPolicy.enabled to true in the Convoy's values. (Bahriya Tersane)

Full result

```
kubectl get clusterpolicyreport 1bef7dc4-e354-4b6d-bc32-e548e1af4393 -o yaml
```

Kyverno names each policy report after the UID of the object it covers.

Requirements

1 Governance

1-1 Strategy

1-1-1	A documented cybersecurity strategy, approved and backed by the head of the entity. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-9 Risk Management Strategy.	**Organisational evidence**
1-1-2	An action plan that carries the strategy out. Organisational, non-technical. NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-9 Risk Management Strategy.	**Organisational evidence**
1-1-3	The strategy reviewed on a schedule and when regulation changes. Organisational, non-technical. NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

1-2 Management

1-2-1	A cybersecurity department independent of the IT department. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**

1-2-2	Cybersecurity positions held full-time by qualified Saudi professionals. Organisational, non-technical. NIST SP 800-53: PM-13 Security and Privacy Workforce.	**Organisational evidence**
1-2-3	A supervisory committee that oversees the cybersecurity programme. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-29 Risk Management Program Leadership Roles.	**Organisational evidence**

1-3 Policies and procedures

1-3-1	Cybersecurity policies and procedures documented, approved and communicated. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
1-3-2	Those policies and procedures put into practice. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
1-3-3	Technical security standards (for example, for firewalls, databases and operating systems) supporting the policies. Organisational, technical and non-technical. NIST SP 800-53: CM-6 Configuration Settings, PL-10 Baseline Selection.	**Organisational evidence**
1-3-4	Policies and procedures reviewed on a schedule, with changes recorded and approved. Organisational, non-technical. NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**

1-4 Roles and responsibilities

1-4-1	Cybersecurity governance structure, roles and responsibilities defined, approved and assigned. Organisational, non-technical. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PS-9 Position Descriptions.	**Organisational evidence**
1-4-2	Roles and responsibilities reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: PS-9 Position Descriptions.	**Organisational evidence**

1-5 Risk management

1-5-1	A documented and approved cybersecurity risk management method. Organisational, non-technical. NIST SP 800-53: RA-1 Policy and Procedures, PM-9 Risk Management Strategy.	**Organisational evidence**
1-5-2	The risk management method applied. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**

1-5-3 When risk is assessed

1-5-3-1	Risk assessed at the start of technology projects. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SA-3 System Development Life Cycle.	**Organisational evidence**
1-5-3-2	Risk assessed before major infrastructure changes. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, CM-4 Impact Analyses.	**Organisational evidence**

1-5-3-3	Risk assessed when planning to use third-party services. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SA-9 External System Services.	**Organisational evidence**
1-5-3-4	Risk assessed before new technology services and products are released. Organisational, non-technical. NIST SP 800-53: RA-3 Risk Assessment, SA-3 System Development Life Cycle.	**Organisational evidence**
1-5-4	The risk management method reviewed on a schedule, with changes recorded. Organisational, non-technical. NIST SP 800-53: RA-1 Policy and Procedures.	**Organisational evidence**

1-6 Security in projects and change

1-6-1	Cybersecurity requirements built into project and change management. Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle, CM-3 Configuration Change Control.	**Organisational evidence**

1-6-2 Requirements for projects and changes

1-6-2-1	Vulnerabilities assessed and fixed as part of projects and changes. Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SA-11 Developer Testing and Evaluation.	**Pass**

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.
cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

1-6-2-2 Secure configuration, hardening and updates reviewed before launch. **Fail**

Checked, coverage partial. NIST SP 800-53: CM-2 Baseline Configuration, CM-6 Configuration Settings.

Fails in CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app.

cluster.workload-inventory	**Recorded**	13 namespaces, 21 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.
node.etcd-data	**Pass**	etcd's data directory is owned by root and closed to other users: so on all 1 node(s). Establishes: etcd's data directory on each control-plane node is owned by root and closed to other users (700).
node.file-permissions	**Pass**	Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s). Establishes: The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.
node.kubelet-hardening	**Pass**	The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s). Establishes: The kubelet keeps its read-only port closed and rotates its client certificates.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
platform.mesh-cni	**Not evaluated**	The service mesh CNI plugin: the platform could not observe it. Establishes: Meshed Pods run without elevated privileges, through the mesh's CNI plugin.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.
policy.resource-limits	**Fail**	3 object(s) fail the policy. Establishes: Every container declares memory and CPU limits.

trivy.limits	**Fail**	3 object(s) fail. Establishes: Containers without CPU or memory limits.
trivy.run-as-root	**Fail**	3 object(s) fail. Establishes: Containers that run as the root user.
trivy.seccomp	**Fail**	3 object(s) fail. Establishes: Containers without the runtime's default seccomp profile.

1-6-3 Requirements for software development

1-6-3-1 Secure coding standards followed. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SA-15 Development Process, Standards, and Tools.

1-6-3-2 Development tools and libraries taken only from trusted, licensed sources. **Fail**

Enforced, coverage partial. NIST SP 800-53: SR-3 Supply Chain Controls and Processes, CM-14 Signed Components.

Scope of this evidence The verdict covers the images of the workloads outside the exempt namespaces: that they come from the registries the organisation allows, by a fixed tag or digest, and carry a signature from a configured key (an image no key covers fails). By default a failing Pod is admitted with a warning and recorded, not refused. Whether the sources are trusted and licensed, and tools and libraries outside the images, are the organisation's to evidence.

Fails in CronJob payments/nightly, CronJob payments/weekly, Deployment payments/ledger, Deployment payments/legacy-batch, Deployment payments/unsigned-app, Job payments/migrate-once, Job payments/nightly-now, Pod payments/nightly-now-k7cbf, Pod payments/one-off, Pod payments/unsigned-app-b5567644f-vpkpp and 1 more.

platform.image-registry	**Recorded**	The registry the control plane pulls its images from: 1x.ax/bke/kubernetes. Establishes: The platform's own images come from the registry recorded, signed.
policy.images-signed	**Fail**	11 object(s) run images that are not signed or that no signing key covers. Establishes: Every image outside the exempt namespaces carries a signature from a configured key: Kyverno verifies the images that match a key's patterns, and the collector fails any image that no key covers. A failing Pod is admitted with a warning and recorded, or refused, as policies.defaultAction sets (Warn by default).
policy.no-latest-tag	**Pass**	Every object the policy judged passes it. Establishes: Images are referenced by a fixed tag or digest, never by a moving tag.
policy.registries-allowed	**Fail**	7 object(s) fail the policy. Establishes: Containers run images only from the registries the customer allows.
trivy.image-sources	**Pass**	Every object outside the exempt namespaces passes. Establishes: Images from public registries (AVD-KSV-0034), or referenced by a moving tag (AVD-KSV-0013). AVD-KSV-0125 is not used: its list trusts only three cloud providers' registries, and policy.registries-allowed judges the registries against your own list instead. See https://tersane.bahriya.cloud/docs/charts/compliance/#checks-the-convoy-does-not-use-and-why.

1-6-3-3	Software tested against the entity's cybersecurity requirements. Organisational, technical, outside the cluster. NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
1-6-3-4	Applications integrated with each other securely. Organisational, technical, outside the cluster. NIST SP 800-53: SA-9 External System Services, SC-8 Transmission Confidentiality and Integrity.	**Organisational evidence**

1-6-3-5 Secure configuration, hardening and updates reviewed before software is launched. **Fail**

Checked, coverage partial. NIST SP 800-53: CM-6 Configuration Settings, CM-7 Least Functionality.

Fails in CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app.

node.etcd-data	**Pass**	etcd's data directory is owned by root and closed to other users: so on all 1 node(s). Establishes: etcd's data directory on each control-plane node is owned by root and closed to other users (700).
node.file-permissions	**Pass**	Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s). Establishes: The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.
node.kubelet-hardening	**Pass**	The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s). Establishes: The kubelet keeps its read-only port closed and rotates its client certificates.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
platform.mesh-cni	**Not evaluated**	The service mesh CNI plugin: the platform could not observe it. Establishes: Meshed Pods run without elevated privileges, through the mesh's CNI plugin.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
policy.no-host-namespaces	**Pass**	Every object the policy judged passes it. Establishes: No Pod shares the host's network, process or IPC namespace, outside named namespaces.

policy.no-host-path	**Pass**	Every object the policy judged passes it. Establishes: No Pod mounts a host path, outside named namespaces.
policy.no-host-ports	**Pass**	Every object the policy judged passes it. Establishes: No container binds a host port, outside named namespaces.
policy.resource-limits	**Fail**	3 object(s) fail the policy. Establishes: Every container declares memory and CPU limits.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.host-access	**Pass**	Every object outside the exempt namespaces passes. Establishes: Workloads that use the host's namespaces, paths or ports.
trivy.limits	**Fail**	3 object(s) fail. Establishes: Containers without CPU or memory limits.
trivy.run-as-root	**Fail**	3 object(s) fail. Establishes: Containers that run as the root user.
trivy.seccomp	**Fail**	3 object(s) fail. Establishes: Containers without the runtime's default seccomp profile.

1-6-4 Project management security requirements reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-3 System Development Life Cycle.

1-7 Compliance

1-7-1 Cybersecurity obligations from nationally approved international agreements identified and met. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PM-1 Information Security Program Plan.

1-8 Review and audit

1-8-1 The cybersecurity department reviews how the controls are applied, on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.

1-8-2 Independent parties outside the cybersecurity department audit the controls. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CA-2(1) Independent Assessors.

1-8-3 Audit results, with scope, findings and corrective actions, reported to the committee and the head of the entity. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CA-2 Control Assessments, CA-5 Plan of Action and Milestones.

1-9 Human resources

1-9-1 Personnel security requirements set for before, during and after employment. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PS-1 Policy and Procedures.

1-9-2 Those personnel requirements applied. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PS-1 Policy and Procedures.

1-9-3 Before employment

1-9-3-1 Security and confidentiality duties written into employment contracts, lasting beyond employment. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PS-6 Access Agreements.

1-9-3-2 Screening of people in security roles and in technical roles with privileged access. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PS-3 Personnel Screening.

1-9-4 During employment

1-9-4-1 Security awareness at joining and throughout employment. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.

1-9-4-2 Personnel follow the entity's security policies and procedures. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.

1-9-5 Access rights reviewed and removed at once when employment ends. **Recorded**

Checked, coverage partial. NIST SP 800-53: PS-4 Personnel Termination, AC-2 Account Management. Evidence counted: cluster.access-review; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The cluster's role bindings, the record of who holds which rights, are recorded for the review. Removing a leaver's rights, at the identity provider and elsewhere, is the entity's to evidence.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.

1-9-6 Personnel security requirements reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PS-1 Policy and Procedures.

1-10 Awareness and training

1-10-1 An approved awareness programme delivered through several channels. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.

1-10-2 The awareness programme carried out. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.

1-10-3 What awareness covers

1-10-3-1 Handling email safely, especially phishing. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AT-2(1) Practical Exercises.

1-10-3-2	Handling mobile devices and storage media safely. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
1-10-3-3	Browsing the internet safely. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
1-10-3-4	Using social media safely. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

1-10-4 Specialist training

1-10-4-1	Specialist training for the cybersecurity department. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
1-10-4-2	Specialist training for software developers and those who run technology assets. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
1-10-4-3	Specialist training for executives and supervisors. Organisational, non-technical. NIST SP 800-53: AT-3 Role-based Training.	**Organisational evidence**
1-10-5	The awareness programme reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: AT-1 Policy and Procedures.	**Organisational evidence**

2 Defence

2-1 Asset management

2-1-1	Asset management security requirements documented and approved. Organisational, non-technical. NIST SP 800-53: CM-8 System Component Inventory, PM-5 System Inventory.	**Organisational evidence**
2-1-2	Asset management security requirements applied, with an accurate inventory. Checked, coverage partial. NIST SP 800-53: CM-8 System Component Inventory. cluster.workload-inventory — **Recorded** — 13 namespaces, 21 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.	**Recorded**
2-1-3	An acceptable use policy for assets, approved and communicated. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
2-1-4	The acceptable use policy applied. Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.	**Organisational evidence**
2-1-5	Assets classified, labelled and handled as regulation requires. Enforced, coverage partial. NIST SP 800-53: RA-2 Security Categorization, MP-3 Media Marking. **Scope of this evidence** The evidence is that each namespace outside the exempt namespaces carries a classification label. Classifying, labelling and handling other assets, and the data the workloads hold, are the organisation's to evidence. policy.namespace-classification — **Pass** — Every object the policy judged passes it. Establishes: Every application namespace carries a data classification label.	**Pass**

2-1-6	Asset management security requirements reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: CM-8 System Component Inventory.	**Organisational evidence**

2-2 Identity and access management

2-2-1	Identity and access management requirements documented and approved. Organisational, non-technical. NIST SP 800-53: AC-1 Policy and Procedures, IA-1 Policy and Procedures.	**Organisational evidence**
2-2-2	Identity and access management requirements applied. Platform, coverage partial. NIST SP 800-53: AC-2 Account Management, IA-2 Identification and Authentication (Organizational Users).	**Incomplete**

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.
node.kubelet-authn	**Pass**	The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: so on all 1 node(s). Establishes: The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
platform.oidc	**Not evaluated**	The platform could not read the authentication configuration. Establishes: People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.

2-2-3 Identity and access minimums

2-2-3-1 Authentication of users by name and password, at the least. **Incomplete**

Platform, coverage partial. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), IA-5 Authenticator Management.

node.kubelet-authn	**Pass**	The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: so on all 1 node(s). Establishes: The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
platform.oidc	**Not evaluated**	The platform could not read the authentication configuration. Establishes: People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.
trivy.config-secrets	**Pass**	Every object outside the exempt namespaces passes. Establishes: ConfigMaps that hold secrets.

2-2-3-2 Multi-factor authentication for remote and privileged access, with factors chosen by the impact of their failure. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts, AC-17 Remote Access.

2-2-3-3 Access granted by need to know, least privilege and separation of duties. **Fail**

Checked, coverage partial. NIST SP 800-53: AC-3 Access Enforcement, AC-5 Separation of Duties, AC-6 Least Privilege.

Fails in ClusterRole tigera-operator, ClusterRole tigera-operator-secrets.

node.kubelet-authz	**Pass**	The kubelet authorises requests through the API server: so on all 1 node(s). Establishes: The kubelet authorises requests through the API server (Webhook mode).
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
policy.no-default-token	**Pass**	Every object the policy judged passes it. Establishes: Pods say whether they mount a service account token, so that none receives one by default.
trivy.rbac-exec	**Pass**	Every object outside the exempt namespaces passes. Establishes: Roles that allow executing into Pods or impersonating privileged groups.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.
trivy.token-automount	**Pass**	Every object outside the exempt namespaces passes. Establishes: Pods that mount a service account token.

2-2-3-4 Privileged access managed. **Fail**

Checked, coverage partial. NIST SP 800-53: AC-6(1) Authorize Access to Security Functions, AC-6(5) Privileged Accounts, AC-2(7) Privileged User Accounts.

Fails in ClusterRole tigera-operator, ClusterRole tigera-operator-secrets, CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
policy.no-privileged	**Pass**	Every object the policy judged passes it. Establishes: No container runs privileged or adds capabilities other than NET_BIND_SERVICE, outside named namespaces.
trivy.privileged	**Fail**	3 object(s) fail. Establishes: Containers that run privileged, may escalate privileges or add capabilities.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

2-2-3-5 Identities and access rights reviewed periodically. **Recorded**

Checked, coverage partial. NIST SP 800-53: AC-2(3) Disable Accounts, AC-6(7) Review of User Privileges.

cluster.access-review	**Recorded**	109 role bindings to subjects; 2 to cluster-admin across the cluster. Establishes: Every subject bound to a role, with what it may do, for the periodic access review.

2-2-4 Identity and access management reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: AC-1 Policy and Procedures.

2-3 Systems and processing facilities

2-3-1 Protection requirements for systems and processing facilities documented and approved. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SC-1 Policy and Procedures, SI-1 Policy and Procedures.

2-3-2 Those protection requirements applied. **Fail**

Platform, coverage partial. NIST SP 800-53: CM-6 Configuration Settings, CM-7 Least Functionality.

Fails in CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app.

node.etcd-data	**Pass**	etcd's data directory is owned by root and closed to other users: so on all 1 node(s). Establishes: etcd's data directory on each control-plane node is owned by root and closed to other users (700).
node.file-permissions	**Pass**	Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s). Establishes: The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.
node.kubelet-hardening	**Pass**	The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s). Establishes: The kubelet keeps its read-only port closed and rotates its client certificates.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
platform.mesh-cni	**Not evaluated**	The service mesh CNI plugin: the platform could not observe it. Establishes: Meshed Pods run without elevated privileges, through the mesh's CNI plugin.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
policy.no-host-namespaces	**Pass**	Every object the policy judged passes it. Establishes: No Pod shares the host's network, process or IPC namespace, outside named namespaces.

policy.no-host-path	**Pass**	Every object the policy judged passes it. Establishes: No Pod mounts a host path, outside named namespaces.
policy.no-host-ports	**Pass**	Every object the policy judged passes it. Establishes: No container binds a host port, outside named namespaces.
policy.resource-limits	**Fail**	3 object(s) fail the policy. Establishes: Every container declares memory and CPU limits.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.host-access	**Pass**	Every object outside the exempt namespaces passes. Establishes: Workloads that use the host's namespaces, paths or ports.
trivy.limits	**Fail**	3 object(s) fail. Establishes: Containers without CPU or memory limits.
trivy.run-as-root	**Fail**	3 object(s) fail. Establishes: Containers that run as the root user.
trivy.seccomp	**Fail**	3 object(s) fail. Establishes: Containers without the runtime's default seccomp profile.

2-3-3 System protection minimums

2-3-3-1	Up-to-date, centrally managed protection against malware on servers and workstations. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
2-3-3-2	Use of removable storage strictly restricted and secured. Organisational, technical, outside the cluster. NIST SP 800-53: MP-7 Media Use.	**Organisational evidence**

2-3-3-3 Systems, applications and devices kept patched. **Pass**

Checked, coverage partial. NIST SP 800-53: SI-2 Flaw Remediation.

Scope of this evidence The verdict concerns the images of the workloads outside the exempt namespaces. The versions of the Bahriya Kubernetes Engine and Kubernetes are recorded beside it. Patching the nodes' operating systems, and other systems and devices, are the organisation's to evidence.

cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

2-3-3-4 Clocks synchronised centrally with an accurate, trusted time source. **Not provided**

Platform, coverage full. NIST SP 800-53: AU-8 Time Stamps, SC-45 System Time Synchronization.

node.time-sync	**Not evaluated**	The platform names no time servers, so there is nothing to compare the nodes with. Establishes: Each node runs a time service configured with the servers the platform names.
platform.time-servers	**Not provided**	No time servers are set for the cluster; each node keeps its own. Establishes: The time servers each node synchronises with.

2-3-4 System protection requirements reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SC-1 Policy and Procedures.

2-4 Email protection

2-4-1 Email protection requirements documented and approved. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SI-8 Spam Protection.

2-4-2 Email protection requirements applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection.

2-4-3 Email protection minimums

2-4-3-1 Incoming mail filtered for phishing and spam. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection.

2-4-3-2 Multi-factor authentication for email, with factors chosen by impact. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts.

2-4-3-3 Email archived and backed up. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-9 System Backup.

2-4-3-4	Email protected against advanced persistent threats and zero-day malware. Organisational, technical, outside the cluster. NIST SP 800-53: SI-3 Malicious Code Protection, SI-8 Spam Protection.	**Organisational evidence**
2-4-3-5	The entity's mail domains validated with SPF, DKIM and DMARC. Organisational, technical, outside the cluster. NIST SP 800-53: SI-8 Spam Protection.	**Organisational evidence**
2-4-4	Email protection reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: SI-8 Spam Protection.	**Organisational evidence**

2-5 Network security

2-5-1	Network security requirements documented and approved. Organisational, non-technical. NIST SP 800-53: SC-1 Policy and Procedures.	**Organisational evidence**
2-5-2	Network security requirements applied. Checked, coverage partial. NIST SP 800-53: SC-7 Boundary Protection. Fails in Namespace payments.	**Fail**

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.

2-5-3 Network security minimums

2-5-3-1 Networks segmented by firewalls, with defence in depth. **Fail**

Enforced, coverage partial. NIST SP 800-53: SC-7 Boundary Protection, AC-4 Information Flow Enforcement.

Fails in Namespace payments.

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

2-5-3-2	Production networks kept apart from test and development.	**Fail**

Enforced, coverage partial. NIST SP 800-53: SC-7 Boundary Protection.

Fails in Namespace payments.

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.

2-5-3-3	Internet browsing restricted, especially to suspicious, file-sharing and remote access sites.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SI-4 System Monitoring.

2-5-3-4	Wireless networks authenticated and encrypted, and kept off the internal network unless assessed.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: AC-18 Wireless Access.

2-5-3-5 Network services, protocols and ports restricted and managed. **Fail**

Enforced, coverage partial. NIST SP 800-53: CM-7 Least Functionality, SC-7 Boundary Protection.

Fails in Namespace payments.

platform.host-firewall	**Not evaluated**	The platform could not count the host endpoints. Establishes: The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.
policy.default-deny-generated	**Not provided**	The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed. Establishes: A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
policy.no-host-namespaces	**Pass**	Every object the policy judged passes it. Establishes: No Pod shares the host's network, process or IPC namespace, outside named namespaces.
policy.no-host-path	**Pass**	Every object the policy judged passes it. Establishes: No Pod mounts a host path, outside named namespaces.
policy.no-host-ports	**Pass**	Every object the policy judged passes it. Establishes: No container binds a host port, outside named namespaces.
trivy.external-ip	**Pass**	Every object outside the exempt namespaces passes. Establishes: Services with external IP addresses.
trivy.host-access	**Pass**	Every object outside the exempt namespaces passes. Establishes: Workloads that use the host's namespaces, paths or ports.

2-5-3-6 Intrusion prevention in place. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-4 System Monitoring.

2-5-3-7 DNS secured. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-20 Secure Name/Address Resolution Service (Authoritative Source), SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver).

2-5-3-8 The browsing channel protected against advanced persistent threats. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SI-3 Malicious Code Protection.

2-5-3-9 Protection against distributed denial of service attacks. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-5 Denial-of-service Protection.

2-5-4	Network security reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: SC-1 Policy and Procedures.	**Organisational evidence**

2-6 Mobile devices

2-6-1	Mobile and personal device security requirements documented and approved. Organisational, non-technical. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**
2-6-2	Those mobile device requirements applied. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**

2-6-3 Mobile device minimums

2-6-3-1	The entity's data kept separate and encrypted on mobile and personal devices. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19(5) Full Device or Container-based Encryption.	**Organisational evidence**
2-6-3-2	Mobile device use limited to business need. Organisational, technical, outside the cluster. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**
2-6-3-3	The entity's data wiped from devices that are lost or whose user leaves. Organisational, technical, outside the cluster. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
2-6-3-4	Security awareness for device users. Organisational, non-technical. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
2-6-4	Mobile device security reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: AC-19 Access Control for Mobile Devices.	**Organisational evidence**

2-7 Data protection

2-7-1	Data protection requirements documented and approved, as regulation requires. Organisational, non-technical. NIST SP 800-53: SC-28 Protection of Information at Rest, PM-5 System Inventory.	**Organisational evidence**
2-7-2	Data protected according to its classification. Organisational, technical, outside the cluster. NIST SP 800-53: SC-28 Protection of Information at Rest.	**Organisational evidence**
2-7-3	Data protection reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: SC-28 Protection of Information at Rest.	**Organisational evidence**

2-8 Cryptography

2-8-1	Cryptography requirements documented and approved. Organisational, non-technical. NIST SP 800-53: SC-13 Cryptographic Protection.	**Organisational evidence**
2-8-2	Cryptography requirements applied. Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection.	**Organisational evidence**

2-8-3 Cryptography minimums (National Cryptographic Standards)

2-8-3-1 Only approved cryptographic algorithms and solutions used. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-13 Cryptographic Protection.

2-8-3-2 Cryptographic keys managed securely through their life. **Not evaluated**

Platform, coverage partial. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

platform.key-provider	**Not evaluated**	The platform could not observe the encryption provider. Establishes: Where the encryption key is held (a local key, or a key management service through KMS v2).

2-8-3-3 Data encrypted in transit and at rest, according to its classification. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

2-8-4 Cryptography reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SC-13 Cryptographic Protection.

2-9 Backup and recovery

2-9-1 Backup and recovery requirements documented and approved. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CP-9 System Backup.

2-9-2 Backup and recovery requirements applied. **Fail**

Checked, coverage partial. NIST SP 800-53: CP-9 System Backup.

Scope of this evidence The verdict concerns whether the cluster is backed up: Longhorn, the cluster's storage, with an available backup target and a recurring backup job, or Velero with an available storage location and an active schedule; the last backup of each volume or schedule is recorded beside it. Recovery, and the backups of other systems, are the entity's to evidence.

Fails in Cluster backups.

cluster.backups	**Fail**	Nothing backs the cluster up: neither Longhorn nor Velero is installed. Establishes: The cluster is backed up: Longhorn has an available backup target and a recurring backup job, or Velero has an available backup storage location and an active schedule. The last backup of each volume and schedule is recorded beside the verdict.

2-9-3 Backup minimums

2-9-3-1 Backups cover the critical assets. **Fail**

Checked, coverage partial. NIST SP 800-53: CP-9 System Backup.

Scope of this evidence The verdict concerns the cluster: whether Longhorn has an available backup target and a recurring backup job, or Velero an available storage location and an active schedule, with the last backup of each volume or schedule recorded beside it. Other critical assets are the entity's to evidence.

Fails in Cluster backups.

cluster.backups	**Fail**	Nothing backs the cluster up: neither Longhorn nor Velero is installed. Establishes: The cluster is backed up: Longhorn has an available backup target and a recurring backup job, or Velero has an available backup storage location and an active schedule. The last backup of each volume and schedule is recorded beside the verdict.

2-9-3-2 Data and systems can be restored quickly after an incident. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-10 System Recovery and Reconstitution.

2-9-3-3 Restoring from backup tested periodically. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-9(1) Testing for Reliability and Integrity.

2-9-4 Backup and recovery reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CP-9 System Backup.

2-10 Vulnerability management

2-10-1 Vulnerability management requirements documented and approved. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

2-10-2 Vulnerability management requirements applied. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.
cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

2-10-3 Vulnerability management minimums

2-10-3-1 Vulnerabilities assessed and detected periodically. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.
cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

2-10-3-2 Vulnerabilities classified by severity. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.
cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

2-10-3-3 Vulnerabilities fixed in an order set by their severity and risk. **Pass**

Checked, coverage partial. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SI-2 Flaw Remediation.

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.
cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.
trivy.vulnerabilities	**Pass**	No container outside the exempt namespaces runs an image with a critical or high vulnerability. Establishes: Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

2-10-3-4 Patches tested outside production before they are applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: SI-2 Flaw Remediation, CM-4(1) Separate Test Environments.

2-10-3-5 Current vulnerability information received from trusted sources. **Pass**

Checked, coverage partial. NIST SP 800-53: SI-5 Security Alerts, Advisories, and Directives, RA-5(2) Update Vulnerabilities to Be Scanned.

cluster.scan-freshness	**Pass**	Every workload outside the exempt namespaces was scanned within 48 hours. Establishes: When each workload was last scanned and how current the vulnerability database was.

2-10-4 Vulnerability management reviewed on a schedule. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning.

2-11 Penetration testing

2-11-1 Penetration testing requirements documented and approved. **Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CA-8 Penetration Testing.

2-11-2 Penetration testing requirements applied. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-8 Penetration Testing.

2-11-3 Penetration testing minimums

2-11-3-1 Testing covers every service exposed to the internet and its components. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-8 Penetration Testing.

2-11-3-2 Penetration tests carried out periodically. **Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CA-8 Penetration Testing.

2-11-4	Penetration testing reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**

2-12 Event logs and monitoring

2-12-1	Logging and monitoring requirements documented and approved. Organisational, non-technical. NIST SP 800-53: AU-1 Policy and Procedures.	**Organisational evidence**
2-12-2	Logging and monitoring requirements applied. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.	**Pass**

platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

2-12-3 Logging and monitoring minimums

2-12-3-1	Security event logging turned on for critical assets. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation.	**Pass**

platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

2-12-3-2	Logging turned on for privileged accounts and remote access. Platform, coverage partial. NIST SP 800-53: AU-2 Event Logging, AC-17(1) Monitoring and Control.	**Pass**

platform.audit	**Pass**	API audit logging: in effect on every control-plane node. Establishes: The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

2-12-3-3	The security information and event management (SIEM) approach for collecting logs identified. Organisational, technical, outside the cluster. NIST SP 800-53: AU-6(3) Correlate Audit Record Repositories, SI-4 System Monitoring.	**Organisational evidence**
2-12-3-4	Security event logs monitored continuously. Organisational, technical, outside the cluster. NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, SI-4 System Monitoring.	**Organisational evidence**

2-12-3-5	Security event logs kept for at least twelve months. Platform, coverage partial. NIST SP 800-53: AU-11 Audit Record Retention. Fails in Platform API server audit log.	**Fail**

platform.audit-rotation	**Fail**	The API server keeps its audit log for at most 30 days, fewer than the 365 the regime requires. A log collected to a central store may meet the requirement; that store is the customer's to evidence. Establishes: How long the API server keeps its audit log on the node. The API server deletes a rotated file at its age limit or its file-count limit, whichever comes first, so the age limit is an upper bound: it is the retention only where no file-count limit applies. An absent --audit-log-maxbackup is taken as Kubernetes' documented default, 0, no limit on the number of files. Where a file-count limit applies, the days kept depend on how much is logged, and the regime's period is evidenced by the central log store the audit log is forwarded to.

2-12-4	Logging and monitoring reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: AU-1 Policy and Procedures.	**Organisational evidence**

2-13 Incident and threat management

2-13-1	Incident and threat management requirements documented and approved. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures.	**Organisational evidence**
2-13-2	Incident and threat management requirements applied. Organisational, technical and non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**

2-13-3 Incident management minimums

2-13-3-1	Incident response plans and escalation procedures. Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan.	**Organisational evidence**
2-13-3-2	Incidents classified. Organisational, non-technical. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
2-13-3-3	Incidents reported to NCA. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
2-13-3-4	Incident notifications, threat intelligence, indicators and reports shared with NCA. Organisational, non-technical. NIST SP 800-53: IR-6 Incident Reporting, PM-16 Threat Awareness Program.	**Organisational evidence**
2-13-3-5	Threat intelligence feeds collected and handled. Organisational, technical, outside the cluster. NIST SP 800-53: PM-16 Threat Awareness Program, SI-5 Security Alerts, Advisories, and Directives.	**Organisational evidence**
2-13-4	Incident and threat management reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: IR-1 Policy and Procedures.	**Organisational evidence**

2-14 Physical security

2-14-1	Physical protection requirements documented and approved. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures.	**Organisational evidence**

2-14-2	Physical protection requirements applied. Organisational, non-technical. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**

2-14-3 Physical security minimums

2-14-3-1	Access to critical areas, such as data centres and network rooms, limited to authorised people. Organisational, non-technical. NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control.	**Organisational evidence**
2-14-3-2	Access logged and monitored, including by CCTV. Organisational, non-technical. NIST SP 800-53: PE-6 Monitoring Physical Access, PE-8 Visitor Access Records.	**Organisational evidence**
2-14-3-3	Access and surveillance records protected. Organisational, non-technical. NIST SP 800-53: PE-8 Visitor Access Records.	**Organisational evidence**
2-14-3-4	Assets and media holding classified information destroyed or reused securely. Organisational, technical and non-technical. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
2-14-3-5	Equipment protected inside and outside the entity's premises. Organisational, technical and non-technical. NIST SP 800-53: PE-17 Alternate Work Site, PE-20 Asset Monitoring and Tracking.	**Organisational evidence**
2-14-4	Physical protection reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: PE-1 Policy and Procedures.	**Organisational evidence**

2-15 External web applications

2-15-1	Web application protection requirements documented and approved. Organisational, non-technical. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
2-15-2	Web application protection requirements applied. Enforced, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity.	**Incomplete**

platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.

2-15-3 Web application minimums

2-15-3-1	A web application firewall in front of external applications. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SI-4 System Monitoring.	**Organisational evidence**
2-15-3-2	Applications built in separate tiers. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**

2-15-3-3	Secure protocols, such as HTTPS.	**Incomplete**

Enforced, coverage partial. NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-23 Session Authenticity.

platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
policy.ingress-tls	**Nothing to check**	The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge. Establishes: Every Ingress serves its hosts over TLS.

2-15-3-4	A secure use policy made clear to users.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: PL-4 Rules of Behavior.

2-15-3-5	User authentication with factors chosen by the impact of their failure.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: IA-2 Identification and Authentication (Organizational Users), IA-8 Identification and Authentication (Non-organizational Users).

2-15-4	Web application protection reviewed on a schedule.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.

3 Resilience

3-1 Business continuity

3-1-1	Cybersecurity requirements for business continuity documented and approved.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CP-1 Policy and Procedures.

3-1-2	Those continuity requirements applied.	**Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CP-2 Contingency Plan.

3-1-3 Business continuity minimums

3-1-3-1	Cybersecurity systems and procedures kept running through disruption.	**Organisational evidence**

Organisational, technical and non-technical. NIST SP 800-53: CP-2 Contingency Plan.

3-1-3-2	Plans for responding to incidents that threaten business continuity.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: IR-8 Incident Response Plan, CP-2 Contingency Plan.

3-1-3-3	Disaster recovery plans.	**Organisational evidence**

Organisational, technical, outside the cluster. NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.

3-1-4	Business continuity requirements reviewed on a schedule.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: CP-2 Contingency Plan.

4 Third parties and cloud

4-1 Third parties

4-1-1	Cybersecurity requirements for contracts with third parties documented and approved. Organisational, non-technical. NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services.	**Organisational evidence**

4-1-2 Contract minimums

4-1-2-1	Confidentiality, and secure removal of the entity's data when the service ends. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, PS-7 External Personnel Security.	**Organisational evidence**
4-1-2-2	How the third party communicates a cybersecurity incident. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, IR-6 Incident Reporting.	**Organisational evidence**
4-1-2-3	The third party bound to the entity's security requirements and to regulation. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**

4-1-3 Outsourced and managed services

4-1-3-1	Risk assessed and mitigations confirmed before contracts are signed or changed. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
4-1-3-2	Managed security centres that operate by remote access located wholly in the Kingdom. Organisational, non-technical. NIST SP 800-53: SA-9(5) Processing, Storage, and Service Location.	**Organisational evidence**
4-1-4	Third-party requirements reviewed on a schedule. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**

4-2 Cloud computing and hosting

4-2-1	Cloud and hosting security requirements documented and approved. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**
4-2-2	Cloud and hosting security requirements applied. Organisational, technical and non-technical. NIST SP 800-53: SA-9 External System Services.	**Organisational evidence**

4-2-3 Cloud and hosting minimums

4-2-3-1	The provider protects the entity's data by its classification and returns it in usable form at the end. Organisational, non-technical. NIST SP 800-53: SA-9 External System Services, SC-28 Protection of Information at Rest.	**Organisational evidence**
4-2-3-2	The entity's environment kept separate from other customers' at the provider. Organisational, technical, outside the cluster. NIST SP 800-53: SC-7 Boundary Protection, SC-39 Process Isolation.	**Organisational evidence**

4-2-4	Cloud and hosting requirements reviewed on a schedule.	**Organisational evidence**

Organisational, non-technical. NIST SP 800-53: SA-9 External System Services.

Checks

cluster.access-review Recorded

Every subject bound to a role, with what it may do, for the periodic access review.

109 role bindings to subjects; 2 to cluster-admin across the cluster.

- cluster-admin: Group kubeadm:cluster-admins (kubeadm:cluster-admins)
- cluster-admin: Group system:masters (cluster-admin)

Scope	Subject	Role
cluster	Group kubeadm:cluster-admins	ClusterRole cluster-admin
cluster	Group system:authenticated	ClusterRole calico-tiered-policy-passthrough
cluster	Group system:authenticated	ClusterRole system:basic-user
cluster	Group system:authenticated	ClusterRole system:discovery
cluster	Group system:authenticated	ClusterRole system:public-info-viewer
cluster	Group system:bootstrappers:kubeadm:default-node-token	ClusterRole kubeadm:get-nodes
cluster	Group system:bootstrappers:kubeadm:default-node-token	ClusterRole system:certificates.k8s.io:certificatesigningrequests:nodec
cluster	Group system:bootstrappers:kubeadm:default-node-token	ClusterRole system:node-bootstrapper
cluster	Group system:masters	ClusterRole cluster-admin
cluster	Group system:monitoring	ClusterRole system:monitoring
cluster	Group system:nodes	ClusterRole system:certificates.k8s.io:certificatesigningrequests:selfno
cluster	Group system:serviceaccounts	ClusterRole system:service-account-issuer-discovery
cluster	Group system:unauthenticated	ClusterRole system:public-info-viewer
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole calico-crds
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole calico-extension-apiserver-auth-access
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole calico-webhook-reader
cluster	ServiceAccount calico-system/calico-apiserver	ClusterRole system:auth-delegator
cluster	ServiceAccount calico-system/calico-cni-plugin	ClusterRole calico-cni-plugin
cluster	ServiceAccount calico-system/calico-kube-controllers	ClusterRole calico-kube-controllers

cluster	ServiceAccount calico-system/calico-node	ClusterRole calico-node
cluster	ServiceAccount calico-system/calico-typha	ClusterRole calico-typha
cluster	ServiceAccount compliance/compliance-collector	ClusterRole compliance-collector
cluster	ServiceAccount kube-system/attachdetach-controller	ClusterRole system:controller:attachdetach-controller
cluster	ServiceAccount kube-system/certificate-controller	ClusterRole system:controller:certificate-controller
cluster	ServiceAccount kube-system/clusterrole-aggregation-controller	ClusterRole system:controller:clusterrole-aggregation-cont
cluster	ServiceAccount kube-system/coredns	ClusterRole system:coredns
cluster	ServiceAccount kube-system/cronjob-controller	ClusterRole system:controller:cronjob-controller
cluster	ServiceAccount kube-system/daemon-set-controller	ClusterRole system:controller:daemon-set-controller
cluster	ServiceAccount kube-system/deployment-controller	ClusterRole system:controller:deployment-controller
cluster	ServiceAccount kube-system/device-taint-eviction-controller	ClusterRole system:controller:device-taint-eviction-controll
cluster	ServiceAccount kube-system/disruption-controller	ClusterRole system:controller:disruption-controller
cluster	ServiceAccount kube-system/endpoint-controller	ClusterRole system:controller:endpoint-controller
cluster	ServiceAccount kube-system/endpointslice-controller	ClusterRole system:controller:endpointslice-controller
cluster	ServiceAccount kube-system/endpointslicemirroring-controller	ClusterRole system:controller:endpointslicemirroring-contr
cluster	ServiceAccount kube-system/ephemeral-volume-controller	ClusterRole system:controller:ephemeral-volume-controlle
cluster	ServiceAccount kube-system/expand-controller	ClusterRole system:controller:expand-controller
cluster	ServiceAccount kube-system/generic-garbage-collector	ClusterRole system:controller:generic-garbage-collector
cluster	ServiceAccount kube-system/horizontal-pod-autoscaler	ClusterRole system:controller:horizontal-pod-autoscaler
cluster	ServiceAccount kube-system/job-controller	ClusterRole system:controller:job-controller
cluster	ServiceAccount kube-system/kube-dns	ClusterRole system:kube-dns
cluster	ServiceAccount kube-system/kube-proxy	ClusterRole system:node-proxier
cluster	ServiceAccount kube-system/legacy-service-account-token-cleaner	ClusterRole system:controller:legacy-service-account-token cleaner

cluster	ServiceAccount kube-system/namespace-controller	ClusterRole system:controller:namespace-controller
cluster	ServiceAccount kube-system/node-controller	ClusterRole system:controller:node-controller
cluster	ServiceAccount kube-system/persistent-volume-binder	ClusterRole system:controller:persistent-volume-binder
cluster	ServiceAccount kube-system/pod-garbage-collector	ClusterRole system:controller:pod-garbage-collector
cluster	ServiceAccount kube-system/pv-protection-controller	ClusterRole system:controller:pv-protection-controller
cluster	ServiceAccount kube-system/pvc-protection-controller	ClusterRole system:controller:pvc-protection-controller
cluster	ServiceAccount kube-system/replicaset-controller	ClusterRole system:controller:replicaset-controller
cluster	ServiceAccount kube-system/replication-controller	ClusterRole system:controller:replication-controller
cluster	ServiceAccount kube-system/resource-claim-controller	ClusterRole system:controller:resource-claim-controller
cluster	ServiceAccount kube-system/resourcequota-controller	ClusterRole system:controller:resourcequota-controller
cluster	ServiceAccount kube-system/root-ca-cert-publisher	ClusterRole system:controller:root-ca-cert-publisher
cluster	ServiceAccount kube-system/route-controller	ClusterRole system:controller:route-controller
cluster	ServiceAccount kube-system/selinux-warning-controller	ClusterRole system:controller:selinux-warning-controller
cluster	ServiceAccount kube-system/service-account-controller	ClusterRole system:controller:service-account-controller
cluster	ServiceAccount kube-system/service-cidrs-controller	ClusterRole system:controller:service-cidrs-controller
cluster	ServiceAccount kube-system/service-controller	ClusterRole system:controller:service-controller
cluster	ServiceAccount kube-system/statefulset-controller	ClusterRole system:controller:statefulset-controller
cluster	ServiceAccount kube-system/ttl-after-finished-controller	ClusterRole system:controller:ttl-after-finished-controller
cluster	ServiceAccount kube-system/ttl-controller	ClusterRole system:controller:ttl-controller
cluster	ServiceAccount kube-system/validatingadmissionpolicy-status-controller	ClusterRole system:controller:validatingadmissionpolicy-st controller
cluster	ServiceAccount kube-system/volumeattributesclass-protection-controller	ClusterRole system:controller:volumeattributesclass-protec controller
cluster	ServiceAccount kyverno/engine-admission-controller	ClusterRole kyverno:admission-controller

cluster	ServiceAccount kyverno/engine-admission-controller	ClusterRole view
cluster	ServiceAccount kyverno/engine-background-controller	ClusterRole kyverno:background-controller
cluster	ServiceAccount kyverno/engine-background-controller	ClusterRole view
cluster	ServiceAccount kyverno/engine-cleanup-controller	ClusterRole kyverno:cleanup-controller
cluster	ServiceAccount kyverno/engine-reports-controller	ClusterRole kyverno:reports-controller
cluster	ServiceAccount kyverno/engine-reports-controller	ClusterRole view
cluster	ServiceAccount local-path-storage/local-path-provisioner-service-account	ClusterRole local-path-provisioner-role
cluster	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator
cluster	ServiceAccount trivy-system/trivy-operator-engine	ClusterRole trivy-operator
cluster	User kube-apiserver-kubelet-client	ClusterRole system:kubelet-api-admin
cluster	User system:kube-controller-manager	ClusterRole calico-tier-getter
cluster	User system:kube-controller-manager	ClusterRole system:kube-controller-manager
cluster	User system:kube-proxy	ClusterRole system:node-proxier
cluster	User system:kube-scheduler	ClusterRole system:kube-scheduler
cluster	User system:kube-scheduler	ClusterRole system:volume-scheduler
bahriya-system	ServiceAccount compliance/compliance-collector	ClusterRole bke-platform-reader
calico-system	ServiceAccount calico-system/goldmane	Role goldmane
calico-system	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator-secrets
compliance-node	ServiceAccount compliance/compliance-collector	Role compliance-node-collector
kube-public	ServiceAccount kube-system/bootstrap-signer	Role system:controller:bootstrap-signer
kube-public	User system:anonymous	Role kubeadm:bootstrap-signer-clusterinfo
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kube-proxy
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kubeadm:kubelet-config
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kubeadm:nodes-kubeadm-config

kube-system	Group system:nodes	Role kubeadm:kubelet-config
kube-system	Group system:nodes	Role kubeadm:nodes-kubeadm-config
kube-system	ServiceAccount calico-system/calico-apiserver	Role extension-apiserver-authentication-reader
kube-system	ServiceAccount kube-system/bootstrap-signer	Role system:controller:bootstrap-signer
kube-system	ServiceAccount kube-system/cloud-provider	Role system:controller:cloud-provider
kube-system	ServiceAccount kube-system/kube-controller-manager	Role system::leader-locking-kube-controller-manager
kube-system	ServiceAccount kube-system/kube-scheduler	Role system::leader-locking-kube-scheduler
kube-system	ServiceAccount kube-system/leader-election-controller	Role system::leader-locking-kube-controller-manager
kube-system	ServiceAccount kube-system/token-cleaner	Role system:controller:token-cleaner
kube-system	User system:kube-controller-manager	Role extension-apiserver-authentication-reader
kube-system	User system:kube-controller-manager	Role system::leader-locking-kube-controller-manager
kube-system	User system:kube-scheduler	Role extension-apiserver-authentication-reader
kube-system	User system:kube-scheduler	Role system::leader-locking-kube-scheduler
kyverno	ServiceAccount kyverno/engine-admission-controller	Role kyverno:admission-controller
kyverno	ServiceAccount kyverno/engine-background-controller	Role kyverno:background-controller
kyverno	ServiceAccount kyverno/engine-cleanup-controller	Role kyverno:cleanup-controller
kyverno	ServiceAccount kyverno/engine-reports-controller	Role kyverno:reports-controller
local-path-storage	ServiceAccount local-path-storage/local-path-provisioner-service-account	Role local-path-provisioner-role
tigera-operator	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator-secrets
trivy-system	ServiceAccount trivy-system/trivy-operator-engine	Role trivy-operator-engine
trivy-system	ServiceAccount trivy-system/trivy-operator-engine	Role trivy-operator-engine-leader-election

cluster.backups Fail

The cluster is backed up: Longhorn has an available backup target and a recurring backup job, or Velero has an available backup storage location and an active schedule. The last backup of each volume and schedule is recorded beside the verdict.

Nothing backs the cluster up: neither Longhorn nor Velero is installed.

- no longhorn.io API group
- no velero.io API group

How to fix On a Bahriya Kubernetes Engine cluster, set components.longhorn.settings.backup.target and credentialSecret in config.yaml, and backup.daily.enabled to true, then run apply.sh --commit, which creates the recurring job bke-daily-backup. A target that is configured but not available gives its reason in the longhorn-manager log: kubectl -n longhorn-system logs -l app=longhorn-manager --tail=200 | grep -i backup. With Velero, create a backup storage location that Velero reports Available and a Schedule that is not paused, as Velero's documentation describes; kubectl get backupstoragelocations.velero.io -A gives each location's phase. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Cluster backups	neither Longhorn nor Velero is installed	`kubectl api-resources | grep -E 'longhorn.io|velero.io'`

cluster.scan-freshness Pass

When each workload was last scanned and how current the vulnerability database was.

Every workload outside the exempt namespaces was scanned within 48 hours.

- scans older than 48 hours fail
- 7 workload(s) outside the exempt namespaces

cluster.vulnerability-age Recorded

How long each open critical and high vulnerability has been reported.

No critical or high vulnerability is open outside the exempt namespaces.

- ages are counted from the first run of this collector that reported each one

cluster.workload-inventory Recorded

An inventory of the cluster's namespaces, workloads and the images they run.

13 namespaces, 21 workloads, 16 distinct images.

Namespace	Workload	Images
compliance	CronJob compliance-collect-nca-ecc	registry.example.com/tersane/convoy/compliance/core/collector:1.x.y@sha256:c6258
compliance	Deployment compliance-web-view	registry.example.com/tersane/core/nginxinc/nginx-unprivileged:1.x.y@sha256:f5116e
compliance	Pod reader	registry.example.com/tersane/core/nginxinc/nginx-unprivileged@sha256:f5116ed460

compliance-node	Job node-facts-gtn4z	registry.example.com/tersane/convoy/compliance/core/collector:1.x.y@sha256:c6258
kube-system	DaemonSet kube-proxy	registry.k8s.io/kube-proxy:v1.36.4
kube-system	Deployment coredns	registry.k8s.io/coredns/coredns:v1.14.2
kyverno	Deployment engine-admission-controller	registry.example.com/tersane/core/kyverno/kyvernopre:1.x.y@sha256:27f3cc52e628 registry.example.com/tersane/core/kyverno/kyverno:1.x.y@sha256:c8c4dd09e720d2
kyverno	Deployment engine-background-controller	registry.example.com/tersane/core/kyverno/background-controller:1.x.y@sha256:c46e124f21ef8a6bb4b48de57106808b1007edcd5ddd4ff7df5
kyverno	Deployment engine-cleanup-controller	registry.example.com/tersane/core/kyverno/cleanup-controller:1.x.y@sha256:d7340a
kyverno	Deployment engine-reports-controller	registry.example.com/tersane/core/kyverno/reports-controller:1.x.y@sha256:5fb6d3e
local-path-storage	Deployment local-path-provisioner	registry.example.com/storage/local-path-provisioner:1.x.y
payments	CronJob nightly	registry.example.com/payments/legacy-batch:1.0.0
payments	CronJob weekly	registry.example.com/payments/checkout:3.10.1
payments	Deployment ledger	registry.example.com/payments/checkout:3.10.1
payments	Deployment legacy-batch	registry.example.com/payments/checkout:3.10.1
payments	Deployment unsigned-app	registry.example.com/payments/legacy-batch:1.0.0
payments	Job migrate-once	registry.example.com/payments/checkout:3.10.1
payments	Pod one-off	registry.example.com/payments/checkout:3.10.1
tigera-operator	Deployment tigera-operator	quay.io/tigera/operator:v1.44.0
trivy-system	Deployment trivy-operator-engine	registry.example.com/tersane/core/aquasecurity/trivy-operator:1.x.y@sha256:05191a

trivy-system	StatefulSet trivy-server	registry.example.com/tersane/core/aquasecurity/trivy:1.x.y@sha256:790fd66d16973

node.etcd-data Pass

etcd's data directory on each control-plane node is owned by root and closed to other users (700).

etcd's data directory is owned by root and closed to other users: so on all 1 node(s).

- node-1: 1 path(s) examined

node.file-permissions Pass

The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.

Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s).

- node-1: 33 path(s) examined

node.kubelet-authn Pass

The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.

The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: so on all 1 node(s).

- Read from the kubelet's configuration and flag files: a change made after the kubelet last started is not yet in effect, and is not visible to the node collector.

node.kubelet-authz Pass

The kubelet authorises requests through the API server (Webhook mode).

The kubelet authorises requests through the API server: so on all 1 node(s).

- Read from the kubelet's configuration and flag files: a change made after the kubelet last started is not yet in effect, and is not visible to the node collector.

node.kubelet-hardening Pass

The kubelet keeps its read-only port closed and rotates its client certificates.

The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s).

- Read from the kubelet's configuration and flag files: a change made after the kubelet last started is not yet in effect, and is not visible to the node collector.
- node-1: protectKernelDefaults is false (recorded, not judged: turning it on requires kernel settings the platform does not yet apply)

node.time-sync Not evaluated

Each node runs a time service configured with the servers the platform names.

The platform names no time servers, so there is nothing to compare the nodes with.

platform.anonymous Not evaluated

Anonymous requests to the API server are limited to the health endpoints.

Anonymous requests restricted to the health endpoints: the platform could not observe it.

- compliance.anonymous.configured: unknown
- compliance.anonymous.observed: unknown

platform.audit Pass

The API server writes an audit log under BKE's audit policy, which records requests by authenticated users, including privileged ones.

API audit logging: in effect on every control-plane node.

- compliance.audit.configured: yes
- compliance.audit.observed: yes
- audit.policy: bke

platform.audit-rotation Fail

How long the API server keeps its audit log on the node. The API server deletes a rotated file at its age limit or its file-count limit, whichever comes first, so the age limit is an upper bound: it is the retention only where no file-count limit applies. An absent --audit-log-maxbackup is taken as Kubernetes' documented default, 0, no limit on the number of files. Where a file-count limit applies, the days kept depend on how much is logged, and the regime's period is evidenced by the central log store the audit log is forwarded to.

The API server keeps its audit log for at most 30 days, fewer than the 365 the regime requires. A log collected to a central store may meet the requirement; that store is the customer's to evidence.

- audit.rotation: maxage=30 maxbackup=10 maxsize=100
- the regime's log-retention-days: 365

How to fix Keep the audit log for at least the period the regime requires. On BKE, which always limits the number of audit log files, forward the log to a central log store that keeps it that long, and give that store's retention setting to your assessor as evidence: from BKE 2.6.1, Fluent Bit collects the audit log on the control-plane nodes under the tag audit.*, and an output that matches that tag sends it to your store; on earlier versions, forward it with your own collector. On another cluster, either forward the log in the same way, or set --audit-log-maxage to at least that period and leave --audit-log-maxbackup unset or 0 on each API server's static Pod manifest, with enough disk on each control-plane node to hold that period. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Platform API server audit log	kept at most 30 days before rotation; the regime requires 365	`kubectl -n bahriya-system get configmap bke-platform -o jsonpath='{.data.audit\.rotation}'`

platform.control-plane-tls Not evaluated

Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.

The control-plane TLS and profiling settings: the platform could not observe it.

- compliance.control-plane.configured: unknown
- compliance.control-plane.observed: unknown

platform.host-firewall Not evaluated

The nodes' own ports are filtered by the cluster's host firewall. The collector reads that BKE has declared host endpoints for the nodes; what they admit from outside the cluster (the API server, SSH, the NodePorts and ICMP) is BKE's host firewall policy (SR-2026-010), which the collector does not read.

The platform could not count the host endpoints.

- host-network.host-endpoints: unknown
- host-network.ssh-ports: unknown

platform.image-registry Recorded

The platform's own images come from the registry recorded, signed.

The registry the control plane pulls its images from: 1x.ax/bke/kubernetes.

- image-registry: 1x.ax/bke/kubernetes

platform.key-provider Not evaluated

Where the encryption key is held (a local key, or a key management service through KMS v2).

The platform could not observe the encryption provider.

- encryption.provider: unknown

platform.mesh-cni Not evaluated

Meshed Pods run without elevated privileges, through the mesh's CNI plugin.

The service mesh CNI plugin: the platform could not observe it.

- compliance.mesh-cni.configured: unknown
- compliance.mesh-cni.observed: unknown

platform.oidc Not evaluated

People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.

The platform could not read the authentication configuration.

- authentication.oidc-issuers: unknown

platform.pod-security Not evaluated

Pod Security Admission defaults are applied to namespaces, with the exemptions listed.

Pod Security admission defaults: the platform could not observe it.

- compliance.pod-security.configured: unknown
- compliance.pod-security.observed: unknown
- pod-security.defaults: unknown
- pod-security.exemptions: unknown

platform.time-servers Not provided

The time servers each node synchronises with.

No time servers are set for the cluster; each node keeps its own.

- compliance.time-servers.configured: unknown

How to fix Name the organisation's time servers in compliance.time.servers in /etc/bke/config.yaml and run apply.sh --commit, then upgrade.sh --node-settings --commit on every node. That command moves no version and restarts only the time service. (Bahriya Tersane)

platform.versions Recorded

The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.

Bahriya Kubernetes Engine 2.6.1, Kubernetes v1.36.4, observed 2026-11-19T10:47:57Z.

- bke-version: 2.6.1
- kubernetes-version: v1.36.4
- observed-at: 2026-11-19T10:47:57Z

policy.default-deny-generated Not provided

A default-deny NetworkPolicy is generated in every application namespace (when the customer turns it on).

The policy tersane-compliance-default-deny is not in the cluster: it is set to Off, or the Convoy's policies are not installed.

How to fix Set generate.defaultDenyNetworkPolicy.enabled to true in the Convoy's values and upgrade the Convoy. Where the policy is present but not ready, Kyverno's own status for it says why: kubectl describe generatingpolicy tersane-compliance-default-deny. (Bahriya Tersane)

policy.images-signed Fail

Every image outside the exempt namespaces carries a signature from a configured key: Kyverno verifies the images that match a key's patterns, and the collector fails any image that no key covers. A failing Pod is admitted with a warning and recorded, or refused, as policies.defaultAction sets (Warn by default).

11 object(s) run images that are not signed or that no signing key covers.

- tersane-compliance-images-signed: ready
- tersane-compliance-images-signed-organisation: ready
- 9 object(s) passed, 6 failed
- not judged while it holds no workload: namespace default
- signing keys cover: 1x.ax/*, registry.example.com/payments/legacy-batch*

How to fix Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)

Fails (11)

Object	What is wrong	Full result
CronJob payments/nightly	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
Deployment payments/unsigned-app	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`

Job payments/nightly-now	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6a73d7cc-01f5-42d8-9d6c-462a360b517b -n payments -o yaml`
Pod payments/nightly-now-k7cbf	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 4074d46b-fb0f-4ce3-8312-15270922068d -n payments -o yaml`
Pod payments/unsigned-app-b5567644f-vpkpp	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 3f291cbb-5fdd-4171-9ead-42230533be9f -n payments -o yaml`
ReplicaSet payments/unsigned-app-b5567644f	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 9f9f8242-9449-4023-a60b-aa60653c0b24 -n payments -o yaml`
Deployment payments/ledger	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
Deployment payments/legacy-batch	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
CronJob payments/weekly	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
Job payments/migrate-once	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`
Pod payments/one-off	no signing key covers registry.example.com/payments/checkout:3.10.1	`Kyverno passes an image that no signing key covers without verifying it, so no report records it.`

policy.ingress-tls Nothing to check

Every Ingress serves its hosts over TLS.

The cluster has no Ingress outside the exempt namespaces, so the policy has nothing to judge.

- tersane-compliance-ingress-tls: ready
- 0 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.namespace-classification Pass

Every application namespace carries a data classification label.

Every object the policy judged passes it.

- tersane-compliance-namespace-classification: ready
- 1 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

Fails in exempt namespaces, not counted (1)

Object	What is wrong	Full result
Namespace default	holds no workload, so not judged; the namespace needs the label tersane.bahriya.cloud/data-classification, one of: top-secret, secret, restricted, public	`kubectl get clusterpolicyreport 64c20931-22c4-4dab-a1fd-bf2b33cddf86 -o yaml`

policy.namespace-network-policy Fail

Every application namespace has at least one NetworkPolicy.

1 object(s) fail the policy.

- tersane-compliance-namespace-network-policy: ready
- 0 object(s) passed, 1 failed
- not judged while it holds no workload: namespace default

How to fix Add NetworkPolicies to the namespace that allow only the traffic its workloads need. To start every new namespace closed, set generate.defaultDenyNetworkPolicy.enabled to true in the Convoy's values. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Namespace payments	namespace payments holds no NetworkPolicy	`kubectl get clusterpolicyreport 1bef7dc4-e354-4b6d-bc32-e548e1af4393 -o yaml`

Fails in exempt namespaces, not counted (1)

Object	What is wrong	Full result
Namespace default	holds no workload, so not judged; namespace default holds no NetworkPolicy	`kubectl get clusterpolicyreport 64c20931-22c4-4dab-a1fd-bf2b33cddf86 -o yaml`

policy.no-default-token Pass

Pods say whether they mount a service account token, so that none receives one by default.

Every object the policy judged passes it.

- tersane-compliance-no-default-token: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.no-host-namespaces Pass

No Pod shares the host's network, process or IPC namespace, outside named namespaces.

Every object the policy judged passes it.

- tersane-compliance-no-host-namespaces: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.no-host-path Pass

No Pod mounts a host path, outside named namespaces.

Every object the policy judged passes it.

- tersane-compliance-no-host-path: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.no-host-ports Pass

No container binds a host port, outside named namespaces.

Every object the policy judged passes it.

- tersane-compliance-no-host-ports: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.no-latest-tag Pass

Images are referenced by a fixed tag or digest, never by a moving tag.

Every object the policy judged passes it.

- tersane-compliance-no-latest-tag: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.no-privileged Pass

No container runs privileged or adds capabilities other than NET_BIND_SERVICE, outside named namespaces.

Every object the policy judged passes it.

- tersane-compliance-no-privileged: ready
- 7 object(s) passed, 0 failed
- not judged while it holds no workload: namespace default

policy.registries-allowed Fail

Containers run images only from the registries the customer allows.

7 object(s) fail the policy.

- tersane-compliance-registries-allowed: ready
- 0 object(s) passed, 7 failed
- not judged while it holds no workload: namespace default

How to fix Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)

Fails (7)

Object	What is wrong	Full result

CronJob payments/nightly	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
CronJob payments/weekly	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport f95320a9-ae62-47ac-8865-9ff294efe291 -n payments -o yaml`
Deployment payments/ledger	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport dd716344-57f2-43ff-8850-cec7fbc7281f -n payments -o yaml`
Deployment payments/legacy-batch	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport cc1c8507-d6bb-4e77-8205-1a214c884777 -n payments -o yaml`
Deployment payments/unsigned-app	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`
Job payments/migrate-once	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport cdf45f25-40a7-4023-bc92-880235dc0c91 -n payments -o yaml`
Pod payments/one-off	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport 157881f3-9f3d-472c-9134-201b7cf0220e -n payments -o yaml`

policy.resource-limits Fail

Every container declares memory and CPU limits.

3 object(s) fail the policy.

- tersane-compliance-resource-limits: ready
- 4 object(s) passed, 3 failed
- not judged while it holds no workload: namespace default

How to fix Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)

Fails (3)

Object	What is wrong	Full result
CronJob payments/nightly	containers without CPU and memory limits: app	`kubectl get policyreport 6c214e3c-3f4f-4d99-8099-f6228f4cc31c -n payments -o yaml`
Deployment payments/legacy-batch	containers without CPU and memory limits: app	`kubectl get policyreport cc1c8507-d6bb-4e77-8205-1a214c884777 -n payments -o yaml`
Deployment payments/unsigned-app	containers without CPU and memory limits: app	`kubectl get policyreport 22981270-ecca-417b-8654-00a3545f8d5f -n payments -o yaml`

trivy.config-secrets Pass

ConfigMaps that hold secrets.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0109
- 29 object(s) with a passing result, 0 failing, 3 failing in exempt namespaces

Fails in exempt namespaces, not counted (3)

Object	What is wrong	Full result
ConfigMap trivy-system/trivy-operator	AVD-KSV-0109: ConfigMap with secrets. ConfigMap 'trivy-operator' in 'trivy-system' namespace stores secrets in key(s) or value(s) '{"node.collector.imagePullSecret"}'	`kubectl get configauditreport configmap-trivy-operator -n trivy-system -o yaml`
ConfigMap trivy-system/trivy-operator-config	AVD-KSV-0109: ConfigMap with secrets. ConfigMap 'trivy-operator-config' in 'trivy-system' namespace stores secrets in key(s) or value(s) '{"OPERATOR_ACCESS_GLOBAL_SECRETS_SERVICE_ACCOUNTS", "OPERATOR_EXPOSED_SECRET_SCANNER_ENABLED", "OPERATOR_METRICS_EXPOSED_SECRET_INFO_ENABLED", "OPERATOR_PRIVATE_REGISTRY_SCAN_SECRETS_NAMES"}'	`kubectl get configauditreport configmap-trivy-operator-config -n trivy-system -o yaml`
ConfigMap trivy-system/trivy-operator-trivy-config	AVD-KSV-0109: ConfigMap with secrets. ConfigMap 'trivy-operator-trivy-config' in 'trivy-system' namespace stores secrets in key(s) or value(s) '{"trivy.imagePullSecret"}'	`kubectl get configauditreport configmap-trivy-operator-trivy-config -n trivy-system -o yaml`

trivy.external-ip Pass

Services with external IP addresses.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0108
- 15 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

trivy.host-access Pass

Workloads that use the host's namespaces, paths or ports.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0008, AVD-KSV-0009, AVD-KSV-0010, AVD-KSV-0023, AVD-KSV-0024
- 22 object(s) with a passing result, 0 failing, 3 failing in exempt namespaces

Fails in exempt namespaces, not counted (7)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0009: Access to host network. ReplicaSet 'tigera-operator-686489b657' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0023: hostPath volumes mounted. ReplicaSet 'tigera-operator-686489b657' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`

Installation calico-system/default	AVD-KSV-0009: Access to host network. DaemonSet 'calico-node' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0009: Access to host network. ReplicaSet 'calico-typha-5f45dc8cf9' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport replicaset-calico-typha-5f45dc8cf9 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0023: hostPath volumes mounted. DaemonSet 'calico-node' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0023: hostPath volumes mounted. DaemonSet 'csi-node-driver' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Job compliance-node/node-facts-gtn4z	AVD-KSV-0023: hostPath volumes mounted. Job 'node-facts-gtn4z' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport job-node-facts-gtn4z -n compliance-node -o yaml`

trivy.image-sources Pass

Images from public registries (AVD-KSV-0034), or referenced by a moving tag (AVD-KSV-0013). AVD-KSV-0125 is not used: its list trusts only three cloud providers' registries, and policy.registries-allowed judges the registries against your own list instead. See https://tersane.bahriya.cloud/docs/charts/compliance/#checks-the-convoy-does-not-use-and-why.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0013, AVD-KSV-0034
- 22 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

trivy.limits Fail

Containers without CPU or memory limits.

3 object(s) fail.

- trivy checks: AVD-KSV-0011, AVD-KSV-0018
- 13 object(s) with a passing result, 3 failing, 6 failing in exempt namespaces

How to fix AVD-KSV-0011 Set a limit value under 'containers[].resources.limits.cpu'. (trivy-operator)

How to fix AVD-KSV-0018 Set a limit value under 'containers[].resources.limits.memory'. (trivy-operator)

Fails (6)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0011: CPU not limited. Container 'app' of CronJob 'nightly' should set 'resources.limits.cpu' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
CronJob payments/nightly	AVD-KSV-0018: Memory not limited. Container 'app' of CronJob 'nightly' should set 'resources.limits.memory' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`

Deployment payments/legacy-batch	AVD-KSV-0011: CPU not limited. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'resources.limits.cpu' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0018: Memory not limited. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'resources.limits.memory' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0011: CPU not limited. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'resources.limits.cpu' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0018: Memory not limited. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'resources.limits.memory' Listed under Fix first with policy.resource-limits.	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (30)

Object	What is wrong	Full result
APIServer calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-apiserver' of ReplicaSet 'calico-apiserver-6b7f4598c7' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-apiserver-6b7f4598c7 -n calico-system -o yaml`
APIServer calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-apiserver' of ReplicaSet 'calico-apiserver-6b7f4598c7' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-apiserver-6b7f4598c7 -n calico-system -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0011: CPU not limited. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0018: Memory not limited. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Goldmane calico-system/default	AVD-KSV-0011: CPU not limited. Container 'goldmane' of ReplicaSet 'goldmane-7d6f669648' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-goldmane-7d6f669648 -n calico-system -o yaml`
Goldmane calico-system/default	AVD-KSV-0018: Memory not limited. Container 'goldmane' of ReplicaSet 'goldmane-7d6f669648' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-goldmane-7d6f669648 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-kube-controllers' of ReplicaSet 'calico-kube-controllers-697bdf6d74' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-kube-controllers-697bdf6d74 -n calico-system -o yaml`

Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-node' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'calico-typha' of ReplicaSet 'calico-typha-5f45dc8cf9' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-typha-5f45dc8cf9 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0011: CPU not limited. Container 'install-cni' of DaemonSet 'calico-node' should set 'resources.limits.cpu'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-kube-controllers' of ReplicaSet 'calico-kube-controllers-697bdf6d74' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-kube-controllers-697bdf6d74 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-node' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-typha' of ReplicaSet 'calico-typha-5f45dc8cf9' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-typha-5f45dc8cf9 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`

Installation calico-system/default	AVD-KSV-0018: Memory not limited. Container 'install-cni' of DaemonSet 'calico-node' should set 'resources.limits.memory'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Pod compliance/reader	AVD-KSV-0011: CPU not limited. Container 'reader' of Pod 'reader' should set 'resources.limits.cpu'	`kubectl get configauditreport pod-reader -n compliance -o yaml`
Pod compliance/reader	AVD-KSV-0018: Memory not limited. Container 'reader' of Pod 'reader' should set 'resources.limits.memory'	`kubectl get configauditreport pod-reader -n compliance -o yaml`
Whisker calico-system/default	AVD-KSV-0011: CPU not limited. Container 'whisker' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0011: CPU not limited. Container 'whisker-backend' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0018: Memory not limited. Container 'whisker' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0018: Memory not limited. Container 'whisker-backend' of ReplicaSet 'whisker-7bcf464c86' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-whisker-7bcf464c86 -n calico-system -o yaml`

trivy.network-policy-selectors Pass

NetworkPolicies whose selectors select nothing.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0038
- 188 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

trivy.privileged Fail

Containers that run privileged, may escalate privileges or add capabilities.

3 object(s) fail.

- trivy checks: AVD-KSV-0017, AVD-KSV-0001, AVD-KSV-0005, AVD-KSV-0022
- 22 object(s) with a passing result, 3 failing, 2 failing in exempt namespaces

How to fix AVD-KSV-0001 Set containers[].securityContext.allowPrivilegeEscalation to false. (Bahriya Tersane)

Fails (3)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of CronJob 'nightly' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`

Deployment payments/unsigned-app	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (15)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0001: Can elevate its own privileges. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'calico-node' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'install-cni' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'calico-node' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`

Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'install-cni' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`

trivy.rbac-exec Pass

Roles that allow executing into Pods or impersonating privileged groups.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0053, AVD-KSV-0043
- 188 object(s) with a passing result, 0 failing, 3 failing in exempt namespaces

Fails in exempt namespaces, not counted (3)

Object	What is wrong	Full result
ClusterRole admin	Kubernetes default role; AVD-KSV-0053: Exec into Pods. ClusterRole 'admin' should not have access to resource '["pods/exec"]' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-admin -o yaml`
ClusterRole edit	Kubernetes default role; AVD-KSV-0053: Exec into Pods. ClusterRole 'edit' should not have access to resource '["pods/exec"]' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-edit -o yaml`
ClusterRole system:aggregate-to-edit	Kubernetes default role; AVD-KSV-0053: Exec into Pods. ClusterRole 'system:aggregate-to-edit' should not have access to resource '["pods/exec"]' for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-7b884bc5d8 -o yaml`

trivy.rbac-privilege Fail

Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

2 object(s) fail.

- trivy checks: AVD-KSV-0041, AVD-KSV-0044, AVD-KSV-0045, AVD-KSV-0047, AVD-KSV-0051, AVD-KSV-0052, AVD-KSV-0111, AVD-KSV-0112, AVD-KSV-0113, AVD-KSV-0114, AVD-KSV-0122, AVD-KSV-0123
- 188 object(s) with a passing result, 2 failing, 17 failing in exempt namespaces

How to fix AVD-KSV-0041 Manage secrets are not allowed. Remove resource 'secrets' from cluster role (trivy-operator)

How to fix AVD-KSV-0114 Remove webhook configuration resources/verbs, acceptable values for verbs ['get', 'list', 'watch'] (trivy-operator)

Fails (3)

Object	What is wrong	Full result
ClusterRole tigera-operator	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator -o yaml`
ClusterRole tigera-operator	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'tigera-operator' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator -o yaml`
ClusterRole tigera-operator-secrets	AVD-KSV-0041: Manage secrets. ClusterRole 'tigera-operator-secrets' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-tigera-operator-secrets -o yaml`

Fails in exempt namespaces, not counted (18)

Object	What is wrong	Full result
ClusterRole admin	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'admin' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-admin -o yaml`
ClusterRole cluster-admin	Kubernetes default role; AVD-KSV-0044: No wildcard verb and resource roles. Role permits wildcard verb on wildcard resource	`kubectl get clusterrbacassessmentreport clusterrole-cluster-admin -o yaml`
ClusterRole edit	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'edit' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-edit -o yaml`
ClusterRole kyverno:admission-controller	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:admission-controller' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-78fb9f7b45 -o yaml`

ClusterRole kyverno:admission-controller:core	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:admission-controller:core' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-66dd849fcd -o yaml`
ClusterRole kyverno:cleanup-controller	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:cleanup-controller' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-5fc98dd666 -o yaml`
ClusterRole kyverno:cleanup-controller:core	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:cleanup-controller:core' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-757c5df67 -o yaml`
ClusterRole system:aggregate-to-edit	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:aggregate-to-edit' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-7b884bc5d8 -o yaml`
ClusterRole system:controller:legacy-service-account-token-cleaner	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:controller:legacy-service-account-token-cleaner' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-864fd65956 -o yaml`
ClusterRole system:kube-controller-manager	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:kube-controller-manager' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-b754c4cc6 -o yaml`
ClusterRole system:node	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:node' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-54cdc9b678 -o yaml`
ClusterRole trivy-operator	AVD-KSV-0041: Manage secrets. ClusterRole 'trivy-operator' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-trivy-operator -o yaml`

ClusterRole trivy-operator	AVD-KSV-0047: Do not allow privilege escalation from node proxy. Role permits privilege escalation from node proxy	`kubectl get clusterrbacassessmentreport clusterrole-trivy-operator -o yaml`
Role kyverno/kyverno:admission-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:admission-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-78fb9f7b45 -n kyverno -o yaml`
Role kyverno/kyverno:background-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:background-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-586b8c778d -n kyverno -o yaml`
Role kyverno/kyverno:cleanup-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:cleanup-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-5fc98dd666 -n kyverno -o yaml`
Role kyverno/kyverno:reports-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:reports-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-899885f55 -n kyverno -o yaml`
Role trivy-system/trivy-operator-engine	AVD-KSV-0113: Manage namespace secrets. Role 'trivy-operator-engine' shouldn't have access to manage secrets in namespace 'trivy-system'	`kubectl get rbacassessmentreport role-trivy-operator-engine -n trivy-system -o yaml`

trivy.run-as-root Fail

Containers that run as the root user.

3 object(s) fail.

- trivy checks: AVD-KSV-0012, AVD-KSV-0105
- 188 object(s) with a passing result, 3 failing, 2 failing in exempt namespaces

How to fix AVD-KSV-0012 Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)

Fails (3)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0012: Runs as root user. Container 'app' of CronJob 'nightly' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (10)

Object	What is wrong	Full result

Deployment tigera-operator/tigera-operator	AVD-KSV-0012: Runs as root user. Container 'tigera-operator' of ReplicaSet 'tigera-operator-686489b657' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'calico-node' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0012: Runs as root user. Container 'install-cni' of DaemonSet 'calico-node' should set 'securityContext.runAsNonRoot' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0105: Containers must not set runAsUser to 0. securityContext.runAsUser should be set to a value greater than 0	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0105: Containers must not set runAsUser to 0. securityContext.runAsUser should be set to a value greater than 0	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`

trivy.seccomp Fail

Containers without the runtime's default seccomp profile.

3 object(s) fail.

- trivy checks: AVD-KSV-0030, AVD-KSV-0104
- 18 object(s) with a passing result, 3 failing, 1 failing in exempt namespaces

How to fix AVD-KSV-0030 Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

How to fix AVD-KSV-0104 Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)

Fails (6)

Object	What is wrong	Full result

CronJob payments/nightly	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
CronJob payments/nightly	AVD-KSV-0104: Seccomp policies disabled. container "app" of cronjob "nightly" in "payments" namespace should specify a seccomp profile	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "legacy-batch-5bdd998d78" in "payments" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "unsigned-app-b5567644f" in "payments" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (2)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0104: Seccomp policies disabled. container "tigera-operator" of replicaset "tigera-operator-686489b657" in "tigera-operator" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`

trivy.token-automount Pass

Pods that mount a service account token.

Every object outside the exempt namespaces passes.

- trivy checks: AVD-KSV-0036
- 188 object(s) with a passing result, 0 failing, 0 failing in exempt namespaces

trivy.vulnerabilities Pass

Every workload's images are scanned for known vulnerabilities, classified by severity, against a vulnerability database refreshed every six hours.

No container outside the exempt namespaces runs an image with a critical or high vulnerability.

- 29 container image(s) scanned
- oldest scan of a workload outside the exempt namespaces: 2026-11-19T10:52:08Z

Fails in exempt namespaces, not counted (8)

Object	What is wrong	Full result
Deployment compliance/compliance-web-view (nginx)	container nginx: 1 critical, 3 high	`kubectl get vulnerabilityreport replicaset-compliance-web-view-79cb6dfddf-nginx -n compliance -o yaml`
Deployment kyverno/engine-background-controller (controller)	container controller: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-background-controller-849b6675fd-controller -n kyverno -o yaml`
Deployment kyverno/engine-cleanup-controller (controller)	container controller: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-cleanup-controller-6f84876bfc-controller -n kyverno -o yaml`
Deployment kyverno/engine-reports-controller (controller)	container controller: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-reports-controller-86d87f4465-controller -n kyverno -o yaml`
Installation calico-system/default (calico-node)	container calico-node: 1 critical, 8 high	`kubectl get vulnerabilityreport daemonset-calico-node-calico-node -n calico-system -o yaml`
Installation calico-system/default (ebpf-bootstrap)	container ebpf-bootstrap: 1 critical, 8 high	`kubectl get vulnerabilityreport daemonset-calico-node-ebpf-bootstrap -n calico-system -o yaml`
Pod compliance/reader (reader)	container reader: 1 critical, 3 high	`kubectl get vulnerabilityreport pod-reader-reader -n compliance -o yaml`
StatefulSet trivy-system/trivy-server (trivy-server)	container trivy-server: 1 critical, 4 high	`kubectl get vulnerabilityreport statefulset-trivy-server-trivy-server -n trivy-system -o yaml`

NIST SP 800-53 controls

Each control of NIST SP 800-53 Rev. 5 that a requirement in this report names, with its statement as NIST publishes it. Text in square brackets is for the organisation to define. Each link opens the control in NIST's Cybersecurity and Privacy Reference Tool.

Control	Statement
AC-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

AC-2 Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.
AC-2(3) Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
AC-2(7) Privileged User Accounts	(a) Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme; an attribute-based access scheme]; (b) Monitor privileged role or attribute assignments; (c) Monitor changes to roles or attributes; and (d) Revoke access when privileged role or attribute assignments are no longer appropriate.
AC-3 Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-4 Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
AC-5 Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals] ; and b. Define system access authorizations to support separation of duties.
AC-6 Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
AC-6(1) Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals and roles] to: (a) [Assignment: organization-defined organization-defined security functions (deployed in hardware, software, and firmware)] ; and (b) [Assignment: organization-defined security-relevant information].
AC-6(5) Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
AC-6(7) Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles and classes] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

AC-17 Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
AC-17(1) Monitoring and Control	Employ automated mechanisms to monitor and control remote access methods.
AC-18 Wireless Access	a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b. Authorize each type of wireless access to the system prior to allowing such connections.
AC-19 Access Control for Mobile Devices	a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b. Authorize the connection of mobile devices to organizational systems.
AC-19(5) Full Device or Container-based Encryption	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].
AT-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] awareness and training policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c. Review and update the current awareness and training: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AT-2 Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined organization-defined frequency] thereafter; and 2. When required by system changes or following [Assignment: organization-defined organization-defined events]; b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques]; c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
AT-2(1) Practical Exercises	Provide practical exercises in literacy training that simulate events and incidents.
AT-3 Role-based Training	a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined organization-defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes; b. Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AU-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] audit and accountability policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c. Review and update the current audit and accountability: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AU-2 Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined organization-defined event types (subset of the event types defined in [AU-2a.](#au-2_smt.a)) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
AU-6 Audit Record Review, Analysis, and Reporting	a. Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity; b. Report findings to [Assignment: organization-defined personnel or roles] ; and c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.
AU-6(3) Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
AU-8 Time Stamps	a. Use internal system clocks to generate time stamps for audit records; and b. Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.
AU-11 Audit Record Retention	Retain audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.
AU-12 Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in [AU-2a](#au-2_smt.a) on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in [AU-2c](#au-2_smt.c) that include the audit record content defined in [AU-3](#au-3).

CA-2 Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined assessment frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
CA-2(1) Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.
CA-5 Plan of Action and Milestones	a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
CA-7 Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to [Assignment: organization-defined organization-defined personnel or roles] [Assignment: organization-defined organization-defined frequency].
CA-8 Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined system(s) or system components].
CM-2 Baseline Configuration	a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b. Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment: organization-defined circumstances] ; and 3. When system components are installed or upgraded.

CM-3 Configuration Change Control	a. Determine and document the types of changes to the system that are configuration-controlled; b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c. Document configuration change decisions associated with the system; d. Implement approved configuration-controlled changes to the system; e. Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period]; f. Monitor and review activities associated with configuration-controlled changes to the system; and g. Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency] ; when [Assignment: organization-defined configuration change conditions]].
CM-4 Impact Analyses	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(1) Separate Test Environments	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-6 Configuration Settings	a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations]; b. Implement the configuration settings; c. Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements] ; and d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
CM-7 Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission-essential capabilities] ; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].
CM-8 System Component Inventory	a. Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Does not include duplicate accounting of components or components assigned to any other system; 4. Is at the level of granularity deemed necessary for tracking and reporting; and 5. Includes the following information to achieve system component accountability: [Assignment: organization-defined information] ; and b. Review and update the system component inventory [Assignment: organization-defined frequency].
CM-14 Signed Components	Prevent the installation of [Assignment: organization-defined organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CP-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] contingency planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c. Review and update the current contingency planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-2 Contingency Plan	a. Develop a contingency plan for the system that: 1. Identifies essential mission and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; 6. Addresses the sharing of contingency information; and 7. Is reviewed and approved by [Assignment: organization-defined organization-defined personnel or roles]; b. Distribute copies of the contingency plan to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the system [Assignment: organization-defined frequency]; e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to [Assignment: organization-defined organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
CP-9 System Backup	a. Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency]; b. Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency]; c. Conduct backups of system documentation, including security- and privacy-related documentation [Assignment: organization-defined frequency] ; and d. Protect the confidentiality, integrity, and availability of backup information.
CP-9(1) Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined organization-defined frequency] to verify media reliability and information integrity.
CP-10 System Recovery and Reconstitution	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

IA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] identification and authentication policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and c. Review and update the current identification and authentication: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IA-2 Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-2(1) Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.
IA-2(2) Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.
IA-5 Authenticator Management	Manage system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b. Establishing initial authenticator content for any authenticators issued by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e. Changing default authenticators prior to first use; f. Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur; g. Protecting authenticator content from unauthorized disclosure and modification; h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and i. Changing authenticators for group or role accounts when membership to those accounts changes.
IA-8 Identification and Authentication (Non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

IR-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] incident response policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c. Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-4 Incident Handling	a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinate incident handling activities with contingency planning activities; c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
IR-6 Incident Reporting	a. Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period] ; and b. Report incident information to [Assignment: organization-defined authorities].
IR-8 Incident Response Plan	a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Addresses the sharing of incident information; 9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency] ; and 10. Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles]. b. Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel]; c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d. Communicate incident response plan changes to [Assignment: organization-defined organization-defined incident response personnel (identified by name and/or by role) and organizational elements] ; and e. Protect the incident response plan from unauthorized disclosure and modification.
MP-3 Media Marking	a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempt [Assignment: organization-defined types of media exempted from marking] from marking if the media remain within [Assignment: organization-defined controlled areas].

MP-6 Media Sanitization	a. Sanitize [Assignment: organization-defined organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined organization-defined sanitization techniques and procedures] ; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
MP-7 Media Use	a. [Selection: restrict; prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls] ; and b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.
PE-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] physical and environmental protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c. Review and update the current physical and environmental protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PE-2 Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency] ; and d. Remove individuals from the facility access list when access is no longer required.
PE-3 Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined systems or devices] ; guards]; b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]; d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances]; e. Secure keys, combinations, and other physical access devices; f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency] ; and g. Change combinations and keys [Assignment: organization-defined organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
PE-6 Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events] ; and c. Coordinate results of reviews and investigations with the organizational incident response capability.
PE-8 Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]; b. Review visitor access records [Assignment: organization-defined frequency] ; and c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].

PE-17 Alternate Work Site	a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees; b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls]; c. Assess the effectiveness of controls at alternate work sites; and d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.
PE-20 Asset Monitoring and Tracking	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].
PL-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] planning policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and c. Review and update the current planning: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PL-4 Rules of Behavior	a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c. Review and update the rules of behavior [Assignment: organization-defined frequency] ; and d. Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency] ; when the rules are revised or updated].
PL-10 Baseline Selection	Select a control baseline for the system.
PM-1 Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and c. Protect the information security program plan from unauthorized disclosure and modification.
PM-2 Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

PM-3 Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.
PM-5 System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
PM-9 Risk Management Strategy	a. Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b. Implement the risk management strategy consistently across the organization; and c. Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.
PM-13 Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.
PM-16 Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PM-29 Risk Management Program Leadership Roles	a. Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b. Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.
PS-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] personnel security policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c. Review and update the current personnel security: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PS-3 Personnel Screening	a. Screen individuals prior to authorizing access to the system; and b. Rescreen individuals in accordance with [Assignment: organization-defined organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].
PS-4 Personnel Termination	Upon termination of individual employment: a. Disable system access within [Assignment: organization-defined time period]; b. Terminate or revoke any authenticators and credentials associated with the individual; c. Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d. Retrieve all security-related organizational system-related property; and e. Retain access to organizational information and systems formerly controlled by terminated individual.

PS-6 Access Agreements	a. Develop and document access agreements for organizational systems; b. Review and update the access agreements [Assignment: organization-defined frequency] ; and c. Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].
PS-7 External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements; d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period] ; and e. Monitor provider compliance with personnel security requirements.
PS-9 Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.
RA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
RA-2 Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
RA-3 Risk Assessment	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles] ; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

RA-5 Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-5(2) Update Vulnerabilities to Be Scanned	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency] ; prior to a new scan; when new vulnerabilities are identified and reported].
SA-3 System Development Life Cycle	a. Acquire, develop, and manage the system using [Assignment: organization-defined system-development life cycle] that incorporates information security and privacy considerations; b. Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c. Identify individuals having information security and privacy roles and responsibilities; and d. Integrate the organizational information security and privacy risk management process into system development life cycle activities.
SA-4 Acquisition Process	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service: a. Security and privacy functional requirements; b. Strength of mechanism requirements; c. Security and privacy assurance requirements; d. Controls needed to satisfy the security and privacy requirements. e. Security and privacy documentation requirements; f. Requirements for protecting security and privacy documentation; g. Description of the system development environment and environment in which the system is intended to operate; h. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i. Acceptance criteria.
SA-8 Security and Privacy Engineering Principles	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined organization-defined systems security and privacy engineering principles].
SA-9 External System Services	a. Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].
SA-9(5) Processing, Storage, and Service Location	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements].

SA-11 Developer Testing and Evaluation	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to: a. Develop and implement a plan for ongoing security and privacy control assessments; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency to conduct] at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.
SA-15 Development Process, Standards, and Tools	a. Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and 4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b. Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined organization-defined security and privacy requirements].
SC-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business-process-level; system-level] system and communications protection policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and c. Review and update the current system and communications protection: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SC-5 Denial-of-service Protection	a. [Selection: protect against; limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events] ; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].
SC-7 Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
SC-8 Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-12 Cryptographic Key Establishment and Management	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements].

SC-13 Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses] ; and b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography].
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
SC-23 Session Authenticity	Protect the authenticity of communications sessions.
SC-28 Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-39 Process Isolation	Maintain a separate execution domain for each executing system process.
SC-45 System Time Synchronization	Synchronize system clocks within and between systems and system components.
SI-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] system and information integrity policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and c. Review and update the current system and information integrity: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SI-2 Flaw Remediation	a. Identify, report, and correct system flaws; b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and d. Incorporate flaw remediation into the organizational configuration management process.

SI-3 Malicious Code Protection	a. Implement [Selection (one or more): signature-based; non-signature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]] ; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
SI-4 System Monitoring	a. Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives] ; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c. Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Analyze detected events and anomalies; e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f. Obtain legal opinion regarding system monitoring activities; and g. Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
SI-5 Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles] ; [Assignment: organization-defined elements] ; [Assignment: organization-defined external organizations]] ; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
SI-8 Spam Protection	a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
SR-3 Supply Chain Controls and Processes	a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls] ; and c. Document the selected and implemented supply chain processes and controls in [Selection (one or more): security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].

SR-6 Supplier Assessments and Reviews	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].