UAE Information Assurance Standard, version 2.1 (November 2025): technical evidence

Neither Mamluk LLC-FZ nor its products are affiliated with or endorsed by the UAE Cyber Security Council.

Regime	UAE Information Assurance Standard, version 2.1 (November 2025), UAE Cyber Security Council, United Arab Emirates
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.

The mapping of each control to NIST SP 800-53 Rev. 5 is the standard's own, from its Annex D, used unchanged.

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

134 requirements: 5 enforced by a policy, 11 checked, 10 provided by the platform, 108 organisational (23 technical, outside the cluster; 76 non-technical; 9 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	4 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	108	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

18 object(s) fail at least one check: 6 cluster-wide and 12 in 1 namespace(s). They are listed under Fix first, those that fail an always applicable requirement first, then 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

6 object(s), most severe Critical.

ClusterRole **`tigera-operator`** Fails T5.2.3, T5.3.2, T5.3.4 Always applicable: T5.2.3

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 T5.2.3, T5.3.2, T5.3.4 Always applicable: T5.2.3

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 T3.1.7 Always applicable: T3.1.7

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'`

Cluster **log shipping** Fails T3.2.3 Always applicable: T3.2.3

MEDIUM no log shipper runs on the cluster

Check cluster.log-forwarding.

How to fix On a Bahriya Kubernetes Engine cluster, set components.fluent-bit.settings.output.config in config.yaml to an [OUTPUT] section naming the central store, then run apply.sh --commit. Keep the store's password out of config.yaml, as the Logging with Fluent Bit guide describes. On another cluster, install a log shipper, such as Fluent Bit, that sends the logs to a central store. Where records do not arrive, the Pod named in the finding logs each failed delivery: check that the store can be reached from the cluster and that its credentials are accepted. (Bahriya Tersane)

Full result `kubectl get daemonsets,deployments -A`

Node **node-1** Fails T3.4.1, T3.4.2 Always applicable: T3.4.1, T3.4.2

MEDIUM no cipher suites are set, so the defaults, which include CBC suites, are offered

Check node.kubelet-ciphers.

How to fix On a Bahriya Kubernetes Engine cluster, set compliance.controlPlane.enabled to true in config.yaml (the default) and upgrade each node with upgrade.sh, which writes tlsMinVersion and tlsCipherSuites into every kubelet's configuration. Elsewhere, set tlsMinVersion to VersionTLS12 and tlsCipherSuites to AES-GCM suites only in the kubelet's configuration, then restart the kubelet. (Bahriya Tersane)

MEDIUM the minimum TLS version is not set, which allows TLS 1.0

Check node.kubelet-ciphers.

How to fix On a Bahriya Kubernetes Engine cluster, set compliance.controlPlane.enabled to true in config.yaml (the default) and upgrade each node with upgrade.sh, which writes tlsMinVersion and tlsCipherSuites into every kubelet's configuration. Elsewhere, set tlsMinVersion to VersionTLS12 and tlsCipherSuites to AES-GCM suites only in the kubelet's configuration, then restart the kubelet. (Bahriya Tersane)

What was read on the node is in this run's snapshot.json, under nodes.

Platform **`API server audit log`** Fails T3.2.2 Always applicable: T3.2.2	
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 T3.1.1, T3.1.8, T6.2.3 Always applicable: T3.1.1, T6.2.3

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-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 T3.1.8, T6.2.3 Always applicable: T6.2.3

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 T3.1.8, T6.2.3 Always applicable: T6.2.3	
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 T3.1.1, T3.1.8, T6.2.3 Always applicable: T3.1.1, T6.2.3	
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-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 T3.1.1, T3.1.8, T6.2.3 Always applicable: T3.1.1, T6.2.3	
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-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 T3.1.8, T6.2.3 Always applicable: T6.2.3	
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 T3.1.8, T6.2.3 Always applicable: T6.2.3

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 T3.1.8, T6.2.3 Always applicable: T6.2.3

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 T3.1.8, T6.2.3 Always applicable: T6.2.3

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 T3.1.8, T6.2.3 Always applicable: T6.2.3

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 T3.1.8, T6.2.3 Always applicable: T6.2.3

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 T4.1.1, T4.1.3 Always applicable: T4.1.1

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

M1 Strategy and Planning

M1.1 Entity Context and Leadership

M1.1.1	The internal and external context of the security programme identified: interested parties and their requirements, the sector and national context, and the entity's capabilities.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-1 Information Security Program Plan, PM-11 Mission and Business Process Definition.	
M1.1.2	Top management leads information security: it sets policy and objectives in line with strategy, provides resources and builds security into the entity's processes.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-2 Information Security Program Leadership Role, PM-3 Information Security and Privacy Resources, PM-29 Risk Management Program Leadership Roles.	
M1.1.3	Security roles and authorities assigned and communicated, with an accountable senior leader, a security function and an Information Security Committee.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures, PM-2 Information Security Program Leadership Role, PM-6 Measures of Performance, PM-29 Risk Management Program Leadership Roles.	

M1.2 Information Security Policy

M1.2.1	An information security policy approved by top management, committed to legal compliance and improvement, communicated, and reviewed at planned intervals.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures.	
M1.2.2	Security objectives, measurable where practicable, consistent with the policy and the risk assessment, documented, approved and kept current.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-1 Information Security Program Plan, PM-3 Information Security and Privacy Resources, PM-4 Plan of Action and Milestones Process, PM-6 Measures of Performance, PM-9 Risk Management Strategy, PM-14 Testing, Training, and Monitoring, PM-28 Risk Framing, PM-30 Supply Chain Risk Management Strategy, PM-31 Continuous Monitoring Strategy.	
M1.2.3	Topic-specific security policies approved, published, acknowledged by staff and reviewed at planned intervals.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures.	

M1.3 Support

M1.3.1	Adequate people and budget for the security programme, with competences defined and evidenced.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-3 Information Security and Privacy Resources, PM-13 Security and Privacy Workforce.	
M1.3.2	A communication plan for security matters, including contact with the UAE cyber security authorities.	**Organisational evidence**
	Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PM-1 Information Security Program Plan, PM-15 Security and Privacy Groups and Associations, PM-28 Risk Framing, PM-31 Continuous Monitoring Strategy.	

M1.3.3	Security documentation approved, version-controlled, distributed and disposed of according to its classification, and compliance with the mandatory controls documented. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures, CP-2 Contingency Plan, IR-8 Incident Response Plan, PL-2 System Security and Privacy Plans, PM-4 Plan of Action and Milestones Process, PM-9 Risk Management Strategy, PM-28 Risk Framing, PM-30 Supply Chain Risk Management Strategy, PM-31 Continuous Monitoring Strategy, SA-5 System Documentation.	**Organisational evidence**
M1.3.4	Security built into project management, with risks identified early and treated throughout the project. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: SA-3 System Development Life Cycle, SA-9 External System Services, SA-15 Development Process, Standards, and Tools.	**Organisational evidence**
M1.3.5	Contact, as far as possible, with relevant security interest groups and forums, with rules on what may be shared. Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: SI-5 Security Alerts, Advisories, and Directives, PM-15 Security and Privacy Groups and Associations.	**Organisational evidence**

M2 Information Security Risk Management

M2.1 Information Security Risk Management Policy

M2.1.1	An approved risk management policy setting scope, roles, risk acceptance and the criteria for assessing risk. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: RA-1 Policy and Procedures, PM-9 Risk Management Strategy.	**Organisational evidence**

M2.2 Information Security Risk Assessment

M2.2.1	Risks to the confidentiality, integrity and availability of information identified, with an owner for each. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing, RA-3 Risk Assessment.	**Organisational evidence**
M2.2.2	Identified risks analysed for consequence and likelihood, and their levels determined. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing, RA-3 Risk Assessment.	**Organisational evidence**
M2.2.3	Analysed risks evaluated against the criteria and prioritised for treatment, with the results documented and shared with the UAE lead entities for cyber security where required. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing, RA-3 Risk Assessment.	**Organisational evidence**

M2.3 Information Security Risk Treatment

M2.3.1	A treatment option chosen for each risk, with retained risks approved by their owners. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
M2.3.2	The controls needed for each risk treatment identified, starting from this standard's controls. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
M2.3.3	A risk treatment plan with actions, resources, responsibilities and target dates. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: RA-7 Risk Response.	**Organisational evidence**
M2.3.4	A Statement of Applicability listing the controls, the reason for each, their status and the justification for any exclusion. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**

M2.4 Ongoing Information Security Risk Management

M2.4.1	The risk assessment and treatment reviewed at a defined frequency and on major change. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**
M2.4.2	Risk information shared with stakeholders and decision-makers throughout the risk management process. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**

M3 Awareness and Training

M3.1 Awareness and Training Policy

M3.1.1	An approved awareness and training policy. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AT-1 Policy and Procedures.	**Organisational evidence**

M3.2 Awareness and Training Planning

M3.2.1	An approved awareness and training programme, with its effectiveness evaluated and records kept. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

M3.3 Security Training

M3.3.1	Security skills needed identified and compared with those held, to find training gaps. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AT-3 Role-based Training, CP-3 Contingency Training, IR-2 Incident Response Training, PM-13 Security and Privacy Workforce.	**Organisational evidence**

M3.3.2	A training plan with a solution and timeline for each training need. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: AT-3 Role-based Training, CP-3 Contingency Training, IR-2 Incident Response Training, PM-13 Security and Privacy Workforce.	**Organisational evidence**
M3.3.3	Training delivered according to the plan. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: AT-3 Role-based Training, CP-3 Contingency Training, IR-2 Incident Response Training, PM-13 Security and Privacy Workforce.	**Organisational evidence**
M3.3.4	The effectiveness of training measured, and ineffective training improved or replaced. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: AT-3 Role-based Training, AT-6 Training Feedback.	**Organisational evidence**
M3.3.5	Training records kept for everyone who needs security training, and reviewed periodically. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: AT-4 Training Records.	**Organisational evidence**

M3.4 Security Awareness

M3.4.1	Security awareness campaigns for staff and third parties, planned, delivered and recorded. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**

M4 Human Resource Security

M4.1 Prior to Employment

M4.1.1	Background checks proportionate to role and risk on candidates, contractors and third-party staff. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PS-3 Personnel Screening, SA-21 Developer Screening.	**Organisational evidence**
M4.1.2	Security terms and conditions in employment and third-party contracts, signed by each person. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PL-4 Rules of Behavior, PS-6 Access Agreements.	**Organisational evidence**

M4.2 During Employment

M4.2.1	Staff, contractors and third parties informed of the security policies that apply to them, and accepting them at first access. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PL-4 Rules of Behavior, PS-6 Access Agreements, PS-7 External Personnel Security, SA-9 External System Services.	**Organisational evidence**
M4.2.2	A formal disciplinary process for breaches of security policy. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: PS-8 Personnel Sanctions.	**Organisational evidence**

M4.3 Termination or Change of Employment

M4.3.1	Security duties that continue after termination or change of employment defined and communicated. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: PS-4 Personnel Termination, PS-5 Personnel Transfer.	**Organisational evidence**
M4.3.2	Assets returned on termination or change of employment. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PS-4 Personnel Termination, PS-5 Personnel Transfer.	**Organisational evidence**

M5 Compliance

M5.1 Compliance with Information Security Legal Requirements

M5.1.1	Legal, regulatory and contractual security requirements identified, documented and reviewed periodically. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures.	**Organisational evidence**
M5.1.2	Intellectual property and software licensing requirements identified and controlled. Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: CM-10 Software Usage Restrictions.	**Organisational evidence**
M5.1.3	Records with legal or contractual protection requirements identified and protected against loss, destruction, falsification and unauthorised access or release. Organisational, technical and non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-3 Access Enforcement, AC-23 Data Mining Protection, AU-9 Protection of Audit Information, AU-10 Non-repudiation, CP-9 System Backup, SC-8 Transmission Confidentiality and Integrity, SC-8(1) Cryptographic Protection, SC-13 Cryptographic Protection, SC-28 Protection of Information at Rest, SC-28(1) Cryptographic Protection.	**Organisational evidence**
M5.1.4	Compliance with data protection and privacy law shown, through a privacy and protection policy, privacy risk assessments of processes handling personal data, controls for it and a process to detect, respond to and report breaches. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**

M5.2 Compliance with Information Policies and Standards

M5.2.1 Compliance with security policies and standards checked routinely, and non-compliance reported for remediation. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures, CA-2 Control Assessments, CA-2(1) Independent Assessors, SA-11(3) Independent Verification of Assessment Plans and Evidence.

M5.3 Information Systems Audit Considerations

M5.3.1 Audit access to operational systems approved and controlled to avoid disruption. **Organisational evidence**

Organisational, technical and non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: AU-9 Protection of Audit Information.

M6 Performance Evaluation and Improvement

M6.1 Performance Evaluation Policy

M6.1.1 A documented performance evaluation policy. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: none mapped by the regime.

M6.2 Performance Evaluation

M6.2.1 Security performance and effectiveness monitored and evaluated, with methods, timing and responsibilities defined. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: CA-1 Policy and Procedures, CA-7 Continuous Monitoring, PM-6 Measures of Performance, PM-31 Continuous Monitoring Strategy.

M6.2.2 Impartial internal audits against a documented audit programme, reported to management. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: CA-1 Policy and Procedures, CA-2 Control Assessments, CA-5 Plan of Action and Milestones, CA-7 Continuous Monitoring, PM-4 Plan of Action and Milestones Process.

M6.2.3 Top management reviews the security programme at planned intervals. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: CA-6 Authorization, PM-1 Information Security Program Plan, PM-4 Plan of Action and Milestones Process, PM-9 Risk Management Strategy, PM-10 Authorization Process, PM-29 Risk Management Program Leadership Roles.

M6.3 Improvement

M6.3.1 Nonconformities corrected, their causes analysed and corrective actions reviewed. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: CA-5 Plan of Action and Milestones, PL-2 System Security and Privacy Plans, PM-4 Plan of Action and Milestones Process, PM-31 Continuous Monitoring Strategy, RA-7 Risk Response.

M6.3.2 Security controls continually improved. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PM-1 Information Security Program Plan, PM-9 Risk Management Strategy, PM-30 Supply Chain Risk Management Strategy, PM-31 Continuous Monitoring Strategy.

T1 Information Asset Management

T1.1 Information Asset Management Policy

T1.1.1 An approved asset management policy, assigning owners and governing personal devices. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: none mapped by the regime.

T1.2 Responsibility for Assets

T1.2.1 An accurate, current inventory of information assets, with an owner for each. **Recorded**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: CM-8 System Component Inventory, PM-5 System Inventory.

Scope of this evidence The inventory of the cluster's namespaces, workloads and the images they run is recorded for review. The inventory of other assets, and their owners, are the entity's to evidence.

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.

T1.2.2 Acceptable use rules for information and assets, accepted by staff and third parties. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-20 Use of External Systems, PL-4 Rules of Behavior.

T1.3 Information Protection

T1.3.1 A classification scheme for information, implemented across the entity and kept current. **Pass**

Enforced, coverage partial. Always applicable, priority P1. NIST SP 800-53: RA-2 Security Categorization.

Scope of this evidence The evidence is that each namespace outside the exempt namespaces carries a classification label. The scheme, its communication and the classification of other information are the entity's to evidence.

policy.namespace-classification	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries a data classification label.

T1.3.2 Information and related assets labelled according to their classification. **Pass**

Enforced, coverage partial. Always applicable, priority P2. NIST SP 800-53: MP-3 Media Marking, PE-22 Component Marking.

Scope of this evidence The evidence is that each namespace outside the exempt namespaces carries a classification label. Labelling other information and assets is the entity's to evidence.

policy.namespace-classification	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries a data classification label.

T1.3.3 Information processed, stored and communicated according to its classification. **Incomplete**

Platform, coverage partial. Always applicable, priority P2. NIST SP 800-53: MP-2 Media Access, MP-4 Media Storage, MP-5 Media Transport, MP-6 Media Sanitization, MP-7 Media Use, PE-16 Delivery and Removal, PE-18 Location of System Components, PE-20 Asset Monitoring and Tracking, SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

Scope of this evidence The evidence is TLS on traffic into the cluster and to its control plane, and the encryption of Kubernetes Secrets at rest. Handling procedures, and the handling of other information, are the entity's to evidence.

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.secret-encryption	**Not evaluated**	The platform could not observe Secret encryption. Establishes: Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.
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.

T1.3.4 Rules for transferring information inside and outside the entity, by classification, and only authorised information released on social media and other public platforms. **Incomplete**

Platform, coverage partial. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-4 Information Flow Enforcement, AC-17 Remote Access, AC-18 Wireless Access, AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems, CA-3 Information Exchange, PE-17 Alternate Work Site, SC-7 Boundary Protection, SC-8 Transmission Confidentiality and Integrity, SC-15 Collaborative Computing Devices and Applications, PS-6 Access Agreements, SA-9 External System Services. Evidence counted: platform.control-plane-tls, policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is the encryption in transit of traffic into the cluster and to its control plane. The rules, agreements and other channels of transfer are the entity's to evidence.

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.

T1.3.5 Data leakage prevention that detects and blocks the disclosure of classified information. **Organisational evidence**

Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: PE-19 Information Leakage.

T1.3.6	Information deleted securely when no longer needed, by classification and law, and the deletion process reviewed periodically. Organisational, technical, outside the cluster. Always applicable, priority P2. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**

T1.4 Storage Media

T1.4.1	Removable media managed through their life cycle, restricted and monitored. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: MP-2 Media Access, MP-4 Media Storage, MP-5 Media Transport, MP-6 Media Sanitization, MP-7 Media Use.	**Organisational evidence**
T1.4.2	Media holding classified information re-used or disposed of securely, with disposals logged. Organisational, technical and non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

T1.5 User Endpoint Devices

T1.5.1	User endpoint devices secured, with automatic lock, management of personal devices and logging. Organisational, technical, outside the cluster. Always applicable, priority P1. NIST SP 800-53: AC-17 Remote Access, AC-18 Wireless Access, AC-19 Access Control for Mobile Devices, AC-3 Access Enforcement, PE-17 Alternate Work Site, AC-11 Device Lock.	**Organisational evidence**

T2 Physical and Environmental Security

T2.1 Physical and Environmental Security Policy

T2.1.1	An approved physical and environmental security policy. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: PE-1 Policy and Procedures.	**Organisational evidence**

T2.2 Secure Areas

T2.2.1	Secure areas classified by what they hold, each with a defined perimeter and protection. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: PE-3 Physical Access Control.	**Organisational evidence**
T2.2.2	Entry to secure areas authenticated and logged, with visible identification, visitors and contractors escorted, and delivery areas controlled. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control, PE-4 Access Control for Transmission, PE-5 Access Control for Output Devices, PE-16 Delivery and Removal.	**Organisational evidence**
T2.2.3	The public kept away from key facilities, which carry no sign of what they hold. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: PE-3 Physical Access Control, PE-5 Access Control for Output Devices.	**Organisational evidence**

T2.2.4	Physical protection against natural disasters, attack and accident, based on site risk assessments. Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: CP-6 Alternate Storage Site, CP-7 Alternate Processing Site, PE-9 Power Equipment and Cabling, PE-13 Fire Protection, PE-14 Environmental Controls, PE-15 Water Damage Protection, PE-18 Location of System Components, PE-19 Information Leakage, PE-23 Facility Location.	**Organisational evidence**
T2.2.5	Rules for working in secure areas, with activity supervised, devices controlled and the areas under surveillance. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-19(4) Restrictions for Classified Information, SC-42 Sensor Capability and Data.	**Organisational evidence**

T2.3 Equipment Security

T2.3.1	Equipment protected against unauthorised access and damage, with environmental conditions monitored. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: PE-9 Power Equipment and Cabling, PE-13 Fire Protection, PE-14 Environmental Controls, PE-15 Water Damage Protection, PE-18 Location of System Components, PE-19 Information Leakage, PE-23 Facility Location.	**Organisational evidence**
T2.3.2	Uninterruptible power and emergency lighting for information systems. Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: CP-8 Telecommunications Services, PE-9 Power Equipment and Cabling, PE-10 Emergency Shutoff, PE-11 Emergency Power, PE-12 Emergency Lighting, PE-14 Environmental Controls, PE-15 Water Damage Protection.	**Organisational evidence**
T2.3.3	Power and telecommunication cables protected and segregated. Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: PE-4 Access Control for Transmission, PE-9 Power Equipment and Cabling.	**Organisational evidence**
T2.3.4	Equipment maintained as its supplier recommends, with maintenance logged and classified data protected. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P3. NIST SP 800-53: MA-2 Controlled Maintenance, MA-6 Timely Maintenance.	**Organisational evidence**
T2.3.5	Equipment used off the premises protected. Organisational, technical and non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems, MP-5 Media Transport, PE-17 Alternate Work Site, MA-2 Controlled Maintenance, PE-16 Delivery and Removal.	**Organisational evidence**
T2.3.6	Equipment disposed of or re-used securely, with disposals recorded. Organisational, technical and non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**
T2.3.7	A clear desk and clear screen policy. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-11 Device Lock, MP-2 Media Access, MP-4 Media Storage.	**Organisational evidence**

T3 Operations Management

T3.1 Operational Procedures and Responsibilities

T3.1.1 Minimum security configurations defined for common technology, implemented, monitored for deviation and reviewed periodically. **Fail**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: CM-1 Policy and Procedures, CM-2 Baseline Configuration, CM-3 Configuration Change Control, CM-6 Configuration Settings, CM-9 Configuration Management Plan.

Scope of this evidence The verdict concerns the configuration of the cluster's nodes, control plane and workloads against a hardening baseline; the platform's versions and the inventory are recorded beside it. Configurations of other technology are the entity's to evidence.

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.

T3.1.2 Operating procedures documented, reviewed periodically and available to those who need them. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: AC-1 Policy and Procedures, AT-1 Policy and Procedures, AU-1 Policy and Procedures, CA-1 Policy and Procedures, CM-1 Policy and Procedures, CP-1 Policy and Procedures, IA-1 Policy and Procedures, IR-1 Policy and Procedures, MA-1 Policy and Procedures, MP-1 Policy and Procedures, PE-1 Policy and Procedures, PL-1 Policy and Procedures, PM-1 Information Security Program Plan, PS-1 Policy and Procedures, PT-1 Policy and Procedures, RA-1 Policy and Procedures, SA-1 Policy and Procedures, SC-1 Policy and Procedures, SI-1 Policy and Procedures, SR-1 Policy and Procedures, SA-5 System Documentation.

T3.1.3 A change management process recording each change, its security impact and approval, with rollback and recovery plans. **Organisational evidence**

Organisational, technical, outside the cluster. Always applicable, priority P2. NIST SP 800-53: CM-3 Configuration Change Control, CM-5 Access Restrictions for Change, SA-10 Developer Configuration Management.

T3.1.4 Development, test and production environments separated, with rules for access and promotion between them. **Pass**

Enforced, coverage partial. Applicable by risk assessment, priority P2. NIST SP 800-53: CM-4(1) Separate Test Environments, CM-5 Access Restrictions for Change.

Scope of this evidence The evidence is that each namespace outside the exempt namespaces carries an environment label, so production can be told apart. Separate environments, and the rules for access and promotion, are the entity's to evidence.

policy.namespace-environment	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries an environment label, one of the values in namespaces.environments.

T3.1.5 Capacity measured, future needs estimated and capacity adjusted. **Organisational evidence**

Organisational, technical, outside the cluster. Applicable by risk assessment, priority P4. NIST SP 800-53: AU-4 Audit Log Storage Capacity, CP-2(2) Capacity Planning, SC-5(2) Capacity, Bandwidth, and Redundancy.

T3.1.6 Up-to-date protection against malware on servers and endpoints, with scans, logging and alerts. **Organisational evidence**

Organisational, technical, outside the cluster. Always applicable, priority P1. NIST SP 800-53: AT-2 Literacy Training and Awareness, SI-3 Malicious Code Protection.

T3.1.7 Backup scope, frequency and protection set, procedures documented and backups tested. **Fail**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: CP-9 System Backup.

Scope of this evidence The verdict concerns whether Longhorn has an available backup target and a recurring backup job, or Velero an available storage location and an active schedule; the last backup of each volume or schedule is recorded beside it. The scope, protection and documentation of backups, testing restores, 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.

T3.1.8 Software installed only by authorised administrators, originals of installed software kept, installations logged and unauthorised software removed. **Fail**

Enforced, coverage partial. Applicable by risk assessment, priority P3. NIST SP 800-53: CM-5 Access Restrictions for Change, CM-7(4) Unauthorized Software — Deny-by-exception, CM-7(5) Authorized Software — Allow-by-exception, CM-11 User-installed Software.

Scope of this evidence The evidence is that the cluster runs only images from the registries the entity allows, signed by a configured key. Who may install software, keeping its originals, logging installations and removing unauthorised software elsewhere are the entity'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.

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.registries-allowed	**Fail**	7 object(s) fail the policy. Establishes: Containers run images only from the registries the customer allows.

T3.2 Monitoring

T3.2.1 A monitoring policy setting what is monitored, how and how often, and the requirements for logging and clock synchronisation. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: AU-1 Policy and Procedures.

T3.2.2 Auditable events and log content defined for all systems, with a minimum review frequency and retention, logs reviewed by trained staff, and critical logs protected. **Fail**

Platform, coverage partial. Always applicable, priority P1. NIST SP 800-53: AU-3 Content of Audit Records, AU-6 Audit Record Review, Analysis, and Reporting, AU-11 Audit Record Retention, AU-12 Audit Record Generation, AU-14 Session Audit, AU-9 Protection of Audit Information.

Scope of this evidence The evidence is the cluster's API audit log and how long it is kept locally, judged against a default of one year that the entity may change, and the protection of its directory and files on each control-plane node, which admit no user but root. The protection of other logs, logging by other systems and applications, and the review of logs are the entity's to evidence.

Fails in Platform API server audit log.

node.audit-log-permissions	**Pass**	The API server's audit log directory is owned by root and no more open than 700, and each file in it no more open than 600: so on all 1 node(s). Establishes: On each control-plane node, the API server's audit log directory is owned by root and no more open than 700, and each file directly in it no more open than 600, so that no user but root can change or read the audit log. Judged where the API server writes its audit log to a directory on the node, held in a host-path volume; on a Bahriya Kubernetes Engine cluster, from release 2.5.0. Where the directory cannot be examined, the check is not evaluated and states why. The node collector runs as an unprivileged user and examines modes alone: where the directory admits no other user, it cannot list the files, and that directory is the evidence for them, since on the node's local filesystem no user but root can then reach them, whatever their modes or any POSIX ACL.
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.
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.

T3.2.3 Networks, systems and applications monitored for anomalous behaviour, with what is gathered, how often it is reviewed and by whom, and how long it is kept, defined; potential incidents evaluated. **Fail**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, AU-7 Audit Record Reduction and Report Generation, SI-4 System Monitoring.

Scope of this evidence The verdict concerns whether the cluster's logs leave its nodes for a central store, where they can be monitored: Fluent Bit sending them there, or another log shipper, named, whose destination the entity evidences. The monitoring and its review, what is gathered and how long it is kept, and other systems are the entity's to evidence.

Fails in Cluster log shipping.

cluster.log-forwarding	**Fail**	No log shipper runs on the cluster, so its logs stay on its nodes. Establishes: The cluster's logs leave its nodes and arrive: Fluent Bit sends them to a central store (an output with a host, or an s3 output with a bucket), and its own counters show records delivered there since the last run with no error, failed retry or dropped record; or another log shipper runs, which is named and whose destination the organisation evidences.

T3.2.4 One date and time format across systems, with clock synchronisation checked regularly. **Not provided**

Platform, coverage partial. Applicable by risk assessment, priority P3. NIST SP 800-53: AU-8 Time Stamps.

Scope of this evidence The evidence is the time source of the cluster's nodes and their synchronisation. Other systems, and the date and time format, are the entity's to evidence.

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.

T3.3 Threat and Vulnerability Management

T3.3.1 Threat information gathered from chosen sources, analysed and acted upon. **Organisational evidence**

Organisational, technical, outside the cluster. Applicable by risk assessment, priority P3. NIST SP 800-53: RA-10 Threat Hunting.

T3.3.2 Vulnerabilities in new systems found and planned for before production, production systems tested, and vulnerabilities addressed. **Pass**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: RA-3 Risk Assessment, RA-5 Vulnerability Monitoring and Scanning, SI-2 Flaw Remediation, SI-5 Security Alerts, Advisories, and Directives.

Scope of this evidence The verdict concerns the images of the workloads outside the exempt namespaces and the freshness of their scans; the platform's versions and the age of open vulnerabilities are recorded beside it. Testing the nodes, the platform and other systems is the entity's to evidence.

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.

T3.4 Cryptography and Key Management

T3.4.1 Cryptographic governance, with encryption requirements set from risk and weak or outdated algorithms replaced promptly. **Fail**

Checked, coverage partial. Always applicable, priority P2. NIST SP 800-53: IA-7 Cryptographic Module Authentication, SC-12 Cryptographic Key Establishment and Management, SC-13 Cryptographic Protection, SC-17 Public Key Infrastructure Certificates.

Scope of this evidence The verdict concerns the TLS settings of the cluster's control plane and kubelets; the provider of the key that encrypts Secrets is recorded beside it. The policy, and cryptography elsewhere, are the entity's to evidence.

Fails in Node node-1.

node.kubelet-ciphers	**Fail**	The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 1 node(s). Establishes: The kubelet offers TLS 1.2 or later with AEAD cipher suites only.
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.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).

T3.4.2 All classified data, credentials included, encrypted at rest and in transit on every device and medium. **Fail**

Platform, coverage partial. Always applicable, priority P1. NIST SP 800-53: SC-13 Cryptographic Protection.

Scope of this evidence The verdict concerns the strength of the TLS cipher suites the cluster's control plane and kubelets offer. The encryption at rest of Kubernetes Secrets and TLS on Ingress traffic are reported under T1.3.3. Encryption of other classified data at rest and in transit, and on devices and media, is the entity's to evidence.

Fails in Node node-1.

node.kubelet-ciphers	**Fail**	The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 1 node(s). Establishes: The kubelet offers TLS 1.2 or later with AEAD cipher suites only.
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.

T3.4.3	Cryptographic keys managed securely through their life cycle, stored securely and recoverable. Platform, coverage partial. Always applicable, priority P1. NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management, SC-17 Public Key Infrastructure Certificates. **Scope of this evidence** The provider of the key that encrypts the cluster's Secrets is recorded for review. The management of other keys is the entity's to evidence.	**Not evaluated**
	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).
T3.4.4	An inventory of systems using public key cryptography, with post-quantum standards tested before use and staff prepared for the transition. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**

T4 Network Security

T4.1 Network Security Management

T4.1.1 Networks controlled: an approved policy, a diagram, authentication of connecting devices, risk-assessed network components, and filtering and monitoring of traffic in and out. **Fail**

Platform, coverage partial. Always applicable, priority P1. NIST SP 800-53: AC-3 Access Enforcement, AC-17 Remote Access, AC-18 Wireless Access, AC-20 Use of External Systems, SC-7 Boundary Protection, SC-8 Transmission Confidentiality and Integrity, SC-10 Network Disconnect. Evidence counted: platform.host-firewall, policy.default-deny-generated, policy.namespace-network-policy, trivy.external-ip; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is the cluster's host firewall and its network policies; the verdict requires the Convoy's generated default-deny network policy. The policy, the diagram, authentication of connecting devices, monitoring of traffic, the risk assessment of network components and other networks are the entity's to evidence.

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.

T4.1.2 Security requirements set and met for each network service, and written into service agreements. **Organisational evidence**

Organisational, technical and non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: CA-3 Information Exchange, SA-9 External System Services.

T4.1.3 Networks segregated by defined criteria, with segregation built in and evaluated periodically. **Fail**

Platform, coverage partial. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-4 Information Flow Enforcement, SC-7 Boundary Protection.

Scope of this evidence The evidence is the cluster's host firewall and its network policies, which separate namespaces; the verdict requires the Convoy's generated default-deny network policy. Segregation of other networks, and its periodic evaluation, are the entity's to evidence.

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.

T4.1.4 Wireless networks surveyed and controlled, with guest access kept apart. **Organisational evidence**

Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-18 Wireless Access.

T4.1.5 Access to illegal, malicious and phishing websites blocked. **Organisational evidence**

Organisational, technical, outside the cluster. Applicable by risk assessment, priority P3. NIST SP 800-53: SC-7 Boundary Protection.

T5 Identity and Access Management

T5.1 Identity and Access Management

T5.1.1 An identity and access management policy. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-1 Policy and Procedures.

T5.2 User Access Management

T5.2.1 A unique identity and account for each user, never shared, identities removed promptly when no longer needed, and activity of restricted identities logged. **Incomplete**

Platform, coverage partial. Always applicable, priority P1. NIST SP 800-53: AC-2 Account Management.

Scope of this evidence The verdict concerns whether sign-in to the cluster is delegated to the entity's identity provider; the cluster's role bindings are recorded beside it. Whether shared credentials, such as kubeadm's admin.conf, are still in use, the removal of identities and the logging of restricted identities' activity are 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.
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.

T5.2.2 Access rights granted and removed through a formal procedure, with approval and implementation by different people, records of all rights, removal at once on change of role or departure, and temporary and inactive accounts checked periodically. **Recorded**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: AC-2 Account Management, IA-2 Identification and Authentication (Organizational Users), IA-4 Identifier Management, IA-5 Authenticator Management, IA-8 Identification and Authentication (Non-organizational Users). 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 review. The procedure, and the removal of rights, are 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.

T5.2.3 Privileged rights restricted and recorded, administrators using separate accounts with multi-factor authentication, and their activity logged. **Fail**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: AC-2 Account Management, AC-3 Access Enforcement, AC-6 Least Privilege, CM-5 Access Restrictions for Change.

Scope of this evidence The verdict concerns which subjects and workloads hold privileged access in the cluster, and that sign-in is delegated to the identity provider; the role bindings are recorded beside it. Whether that provider requires a second factor, and the logging and review of administrators' activity, are the entity's to evidence.

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

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-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.
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.
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.

T5.2.4 User access rights reviewed periodically and on any change in a user's status. **Recorded**

Checked, coverage partial. Always applicable, priority P1. NIST SP 800-53: AC-2 Account Management, PE-2 Physical Access Authorizations. 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 are recorded for the review. The review itself 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.

T5.3 Secure Authentication and Authorization

T5.3.1 Strong authentication on every system, secure log-on and log-off, session limits on sensitive systems and idle sessions ended. **Organisational evidence**

Organisational, technical, outside the cluster. Always applicable, priority P1. NIST SP 800-53: AC-7 Unsuccessful Logon Attempts, AC-8 System Use Notification, AC-9 Previous Logon Notification, IA-6 Authentication Feedback.

T5.3.2 Access to information and assets restricted by role and business need. **Fail**

Checked, coverage partial. Applicable by risk assessment, priority P2. NIST SP 800-53: AC-3 Access Enforcement, AC-24 Access Control Decisions.

Scope of this evidence The verdict concerns the cluster's role-based access control: privileged bindings, the kubelet's authorisation and anonymous access. Access to other systems is the entity's to evidence.

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.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

T5.3.3 Remote access only over secure channels with authentication, and remote administration approved and monitored. **Incomplete**

Platform, coverage partial. Always applicable, priority P1. NIST SP 800-53: AC-17 Remote Access, AC-18 Wireless Access, AC-20 Use of External Systems, CA-3 Information Exchange, IA-2 Identification and Authentication (Organizational Users), IA-8 Identification and Authentication (Non-organizational Users).

Scope of this evidence The evidence is that sign-in to the cluster is delegated to the identity provider, anonymous access is refused, kubelets authenticate their callers and the host firewall restricts access. Authentication and encryption of SSH access to the nodes, other remote access to the entity's systems, and the approval and monitoring of remote administration are the entity's to evidence.

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.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.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.

T5.3.4 Utility programs that can override controls restricted to authorised people, and their use monitored. **Fail**

Checked, coverage partial. Applicable by risk assessment, priority P4. NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege. Evidence counted: trivy.rbac-exec, trivy.rbac-privilege; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict concerns which subjects may run commands inside containers or hold privileged rights in the cluster. Monitoring their use, and other utility programs, are the entity's to evidence.

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

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.

T5.4 Authentication Information

T5.4.1	Credentials issued, revoked and re-issued through a secure process. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**
T5.4.2	Good practice for using credentials set and communicated to users. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**
T5.4.3	A credential management system that automates verified credential changes, enforces strength, lifetime and reuse limits, forces a change of default passwords at first login, and stores credentials hashed or encrypted. Organisational, technical, outside the cluster. Always applicable, priority P1. NIST SP 800-53: IA-5 Authenticator Management.	**Organisational evidence**

T6 Third Party Security

T6.1 Third Party Security Policy

T6.1.1	An approved third-party security policy. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: SR-1 Policy and Procedures.	**Organisational evidence**

T6.2 Management of Third Party and Supply Chain Risks

T6.2.1	Suppliers classified by risk, supply chain risks assessed and mitigated, and monitored. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: SR-2 Supply Chain Risk Management Plan.	**Organisational evidence**
T6.2.2	Criteria for assessing suppliers' security, applied in selecting them. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: SR-6 Supplier Assessments and Reviews.	**Organisational evidence**

T6.2.3 Security requirements for procured hardware and software, products evaluated and tested before use, and upgrades applied promptly. **Fail**

Enforced, coverage partial. Always applicable, priority P2. NIST SP 800-53: SR-3 Supply Chain Controls and Processes, SR-7 Supply Chain Operations Security, SR-9 Tamper Resistance and Detection, SR-10 Inspection of Systems or Components, SR-11 Component Authenticity.

Scope of this evidence The evidence is that the images of the workloads outside the exempt namespaces come from the registries the entity 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. Evaluating and testing products, applying upgrades and maintenance promptly, and other procurement are the entity'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.

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.

T6.2.4 Security requirements, including compliance with applicable law, written into contracts with suppliers. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: SA-4 Acquisition Process, SR-3 Supply Chain Controls and Processes.

T6.2.5 Suppliers' adherence to their security obligations monitored, and changes to their services managed. **Organisational evidence**

Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews, RA-9 Criticality Analysis, SR-7 Supply Chain Operations Security.

T7 Information Systems Acquisition, Development and Maintenance

T7.1 Information Systems Acquisition, Development and Maintenance Policy

T7.1.1	An approved policy for secure acquisition, development and maintenance of systems. Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: SA-3 System Development Life Cycle, SA-15 Development Process, Standards, and Tools, SA-17 Developer Security and Privacy Architecture and Design.	**Organisational evidence**

T7.2 Security Requirements of Information Systems

T7.2.1	Security requirements identified when developing or acquiring applications. Organisational, technical, outside the cluster. Always applicable, priority P1. NIST SP 800-53: SA-4 Acquisition Process.	**Organisational evidence**
T7.2.2	Secure engineering principles documented and applied. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P4. NIST SP 800-53: SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**

T7.3 Secure Software Development

T7.3.1	Approved secure coding practices, automated security testing and developer training. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: SI-3 Malicious Code Protection.	**Organisational evidence**
T7.3.2	Outsourced development governed by quality assurance, contract terms and checks of the delivered code. Organisational, technical and non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: SA-4 Acquisition Process, SA-10 Developer Configuration Management, SA-11 Developer Testing and Evaluation, SA-15 Development Process, Standards, and Tools, SR-2 Supply Chain Risk Management Plan, SR-4 Provenance.	**Organisational evidence**
T7.3.3	Access to source code, development tools and libraries controlled, reviewed and logged. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P3. NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege, CM-5 Access Restrictions for Change.	**Organisational evidence**

T7.4 Secure Testing and Deployment

T7.4.1	Changes controlled: tracked, every version kept and verified, rollback defined and changes tested before production. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: CM-3 Configuration Change Control, SA-10 Developer Configuration Management, SI-2 Flaw Remediation.	**Organisational evidence**
T7.4.2	Test data protected: production data copied to test only with approval and erased after testing. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P3. NIST SP 800-53: SA-3(2) Use of Live or Operational Data.	**Organisational evidence**

T7.4.3	Security testing of new or changed systems, with acceptance criteria, before they go into operation. Organisational, technical, outside the cluster. Applicable by risk assessment, priority P2. NIST SP 800-53: CM-3 Configuration Change Control, CM-4 Impact Analyses, SI-2 Flaw Remediation, CA-2 Control Assessments, SA-11 Developer Testing and Evaluation, SA-4 Acquisition Process, SR-5(2) Assessments Prior to Selection, Acceptance, Modification, or Update.	**Organisational evidence**

T8 Information Security Incident Management

T8.1 Information Security Incident Management Policy

T8.1.1	An incident management policy, with the Emirate, sector and national reporting requirements. Organisational, non-technical. Applicable by risk assessment, priority P2. NIST SP 800-53: IR-1 Policy and Procedures.	**Organisational evidence**
T8.1.2	Staff and third parties aware of their duty to report security events, and of how to do so. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: AU-6 Audit Record Review, Analysis, and Reporting, IR-6 Incident Reporting, SI-2 Flaw Remediation.	**Organisational evidence**

T8.2 Management of Information Security Incidents and Improvements

T8.2.1	An approved incident response plan and an Incident Response Team. Organisational, non-technical. Always applicable, priority P1. NIST SP 800-53: IR-4 Incident Handling, IR-7 Incident Response Assistance, IR-8 Incident Response Plan.	**Organisational evidence**
T8.2.2	Incidents classified and prioritised taking account of the Cyber Security Council's issuances, and those to be reported to national agencies identified. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: none mapped by the regime.	**Organisational evidence**
T8.2.3	Training and certification for incident response staff. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: IR-2 Incident Response Training.	**Organisational evidence**
T8.2.4	Incident response tested periodically and gaps remedied. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: IR-3 Incident Response Testing.	**Organisational evidence**
T8.2.5	The data to collect about each incident defined, recorded and protected. Organisational, non-technical. Always applicable, priority P2. NIST SP 800-53: IR-5 Incident Monitoring.	**Organisational evidence**
T8.2.6	Records of incidents and their lessons kept, with controls added to prevent recurrence. Organisational, non-technical. Applicable by risk assessment, priority P4. NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
T8.2.7	Procedures for identifying, collecting and preserving evidence, with chain of custody. Organisational, technical and non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: AU-4 Audit Log Storage Capacity, AU-9 Protection of Audit Information, AU-10(3) Chain of Custody, AU-11 Audit Record Retention.	**Organisational evidence**

T9 Information Systems Continuity Management

T9.1 ICT Readiness for Business Continuity

T9.1.1 ICT readiness for continuity planned and tested, with continuity plans for response and recovery. **Organisational evidence**

Organisational, technical, outside the cluster. Always applicable, priority P2. NIST SP 800-53: CP-2 Contingency Plan, CP-6 Alternate Storage Site, CP-7 Alternate Processing Site, CP-8 Telecommunications Services, CP-9 System Backup, CP-10 System Recovery and Reconstitution, CP-11 Alternate Communications Protocols, CP-13 Alternative Security Mechanisms.

T9.1.2 Security controls kept working during disruption, with compensating controls where they cannot be. **Organisational evidence**

Organisational, technical and non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: CP-2 Contingency Plan, CP-6 Alternate Storage Site, CP-7 Alternate Processing Site.

T9.2 Testing, Maintaining and Reassessing Plans

T9.2.1 Continuity plans tested periodically and kept current from the lessons learned. **Organisational evidence**

Organisational, non-technical. Applicable by risk assessment, priority P3. NIST SP 800-53: CP-4 Contingency Plan Testing.

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-toke 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.log-forwarding Fail

The cluster's logs leave its nodes and arrive: Fluent Bit sends them to a central store (an output with a host, or an s3 output with a bucket), and its own counters show records delivered there since the last run with no error, failed retry or dropped record; or another log shipper runs, which is named and whose destination the organisation evidences.

No log shipper runs on the cluster, so its logs stay on its nodes.

- no Fluent Bit DaemonSet or Deployment in namespace logging
- no other log shipper found: Fluent Bit, Vector, Fluentd, Promtail, Grafana Alloy, Filebeat, OpenTelemetry Collector, Datadog Agent

How to fix On a Bahriya Kubernetes Engine cluster, set components.fluent-bit.settings.output.config in config.yaml to an [OUTPUT] section naming the central store, then run apply.sh --commit. Keep the

store's password out of config.yaml, as the Logging with Fluent Bit guide describes. On another cluster, install a log shipper, such as Fluent Bit, that sends the logs to a central store. Where records do not arrive, the Pod named in the finding logs each failed delivery: check that the store can be reached from the cluster and that its credentials are accepted. (Bahriya Tersane)

Fails (1)

Object	What is wrong	Full result
Cluster log shipping	no log shipper runs on the cluster	`kubectl get daemonsets,deployments -A`

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.audit-log-permissions **Pass**

On each control-plane node, the API server's audit log directory is owned by root and no more open than 700, and each file directly in it no more open than 600, so that no user but root can change or read the audit log. Judged where the API server writes its audit log to a directory on the node, held in a host-path volume; on a Bahriya Kubernetes Engine cluster, from release 2.5.0. Where the directory cannot be examined, the check is not evaluated and states why. The node collector runs as an unprivileged user and examines modes alone: where the directory admits no other user, it cannot list the files, and that directory is the evidence for them, since on the node's local filesystem no user but root can then reach them, whatever their modes or any POSIX ACL.

The API server's audit log directory is owned by root and no more open than 700, and each file in it no more open than 600: so on all 1 node(s).

- node-1: files in /var/log/kubernetes/audit not examinable: the directory admits no other user (mode 700, owner root). This is the expected, secure state: no user but root can reach the files, whatever their modes, so the directory is the evidence for them.
- node-1: audit log directory /var/log/kubernetes/audit examined

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-ciphers Fail

The kubelet offers TLS 1.2 or later with AEAD cipher suites only.

The kubelet offers TLS 1.2 or later with AEAD cipher suites only: not so on 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: minimum not set, suites not set

How to fix On a Bahriya Kubernetes Engine cluster, set compliance.controlPlane.enabled to true in config.yaml (the default) and upgrade each node with upgrade.sh, which writes tlsMinVersion and tlsCipherSuites into every kubelet's configuration. Elsewhere, set tlsMinVersion to VersionTLS12 and tlsCipherSuites to AES-GCM suites only in the kubelet's configuration, then restart the kubelet. (Bahriya

Tersane)

Fails (2)

Object	What is wrong	Full result
Node node-1	the minimum TLS version is not set, which allows TLS 1.0	`What was read on the node is in this run's snapshot.json, under nodes.`
Node node-1	no cipher suites are set, so the defaults, which include CBC suites, are offered	`What was read on the node is in this run's snapshot.json, under nodes.`

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.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.secret-encryption Not evaluated

Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.

The platform could not observe Secret encryption.

- encryption.observed: unknown
- encryption.resources.configured: 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-environment Pass

Every application namespace carries an environment label, one of the values in namespaces.environments.

Every object the policy judged passes it.

- tersane-compliance-namespace-environment: 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/environment, one of: production, staging, test, development	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-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.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.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.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.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-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-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-7 Unsuccessful Logon Attempts	a. Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period] ; and b. Automatically [Selection (one or more): lock the account or node for [Assignment: organization-defined time period] ; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm] ; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.

AC-8 System Use Notification	a. Display [Assignment: organization-defined system use notification] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that: 1. Users are accessing a U.S. Government system; 2. System usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. Use of the system indicates consent to monitoring and recording; b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and c. For publicly accessible systems: 1. Display system use information [Assignment: organization-defined conditions] , before granting further access to the publicly accessible system; 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system.
AC-9 Previous Logon Notification	Notify the user, upon successful logon to the system, of the date and time of the last logon.
AC-11 Device Lock	a. Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended] ; and b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.
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-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(4) Restrictions for Classified Information	(a) Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and (b) Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information: (1) Connection of unclassified mobile devices to classified systems is prohibited; (2) Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official; (3) Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and (4) Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials] , and if classified information is found, the incident handling policy is followed. (c) Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies].

AC-20 Use of External Systems	a. [Selection (one or more): establish [Assignment: organization-defined terms and conditions] ; identify [Assignment: organization-defined controls asserted]] , consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: 1. Access the system from external systems; and 2. Process, store, or transmit organization-controlled information using external systems; or b. Prohibit the use of [Assignment: organization-defined prohibited types of external systems].
AC-23 Data Mining Protection	Employ [Assignment: organization-defined techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
AC-24 Access Control Decisions	[Selection (one or more): establish procedures; implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.
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-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.
AT-4 Training Records	a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b. Retain individual training records for [Assignment: organization-defined time period].
AT-6 Training Feedback	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].

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-3 Content of Audit Records	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.
AU-4 Audit Log Storage Capacity	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].
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-7 Audit Record Reduction and Report Generation	Provide and implement an audit record reduction and report generation capability that: a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and b. Does not alter the original content or time ordering of audit records.
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-9 Protection of Audit Information	a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and b. Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.
AU-10 Non-repudiation	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions].
AU-10(3) Chain of Custody	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.
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).

AU-14 Session Audit	a. Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances] ; and b. Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
CA-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] assessment, authorization, and monitoring 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 assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and c. Review and update the current assessment, authorization, and monitoring: 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].
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-3 Information Exchange	a. Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; non-disclosure agreements; [Assignment: organization-defined type of agreement]]; b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c. Review and update the agreements [Assignment: organization-defined frequency].
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-6 Authorization	a. Assign a senior official as the authorizing official for the system; b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c. Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; e. Update the authorizations [Assignment: organization-defined frequency].
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].
CM-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] configuration management 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 configuration management policy and the associated configuration management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c. Review and update the current configuration management: 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].
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-5 Access Restrictions for Change	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
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(4) Unauthorized Software — Deny-by-exception	(a) Identify [Assignment: organization-defined software programs]; (b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and (c) Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].
CM-7(5) Authorized Software — Allow-by-exception	(a) Identify [Assignment: organization-defined software programs]; (b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and (c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].
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-9 Configuration Management Plan	Develop, document, and implement a configuration management plan for the system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c. Defines the configuration items for the system and places the configuration items under configuration management; d. Is reviewed and approved by [Assignment: organization-defined personnel or roles] ; and e. Protects the configuration management plan from unauthorized disclosure and modification.
CM-10 Software Usage Restrictions	a. Use software and associated documentation in accordance with contract agreements and copyright laws; b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CM-11 User-installed Software	a. Establish [Assignment: organization-defined policies] governing the installation of software by users; b. Enforce software installation policies through the following methods: [Assignment: organization-defined methods] ; and c. Monitor policy compliance [Assignment: organization-defined frequency].

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-2(2) Capacity Planning	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
CP-3 Contingency Training	a. Provide contingency training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and b. Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-4 Contingency Plan Testing	a. Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined organization-defined tests]. b. Review the contingency plan test results; and c. Initiate corrective actions, if needed.
CP-6 Alternate Storage Site	a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

CP-7 Alternate Processing Site	a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable; b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and c. Provide controls at the alternate processing site that are equivalent to those at the primary site.
CP-8 Telecommunications Services	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
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-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.
CP-11 Alternate Communications Protocols	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.
CP-13 Alternative Security Mechanisms	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.
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-4 Identifier Management	Manage system identifiers by: a. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b. Selecting an identifier that identifies an individual, group, role, service, or device; c. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for [Assignment: organization-defined time period].
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-6 Authentication Feedback	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.
IA-7 Cryptographic Module Authentication	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.
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-2 Incident Response Training	a. Provide incident response training to system users consistent with assigned roles and responsibilities: 1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access; 2. When required by system changes; and 3. [Assignment: organization-defined frequency] thereafter; and b. Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-3 Incident Response Testing	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].

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-5 Incident Monitoring	Track and document incidents.
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-7 Incident Response Assistance	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
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.
MA-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] maintenance 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 maintenance policy and the associated maintenance controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c. Review and update the current maintenance: 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].

MA-2 Controlled Maintenance	a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; c. Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information]; e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and f. Include the following information in organizational maintenance records: [Assignment: organization-defined information].
MA-6 Timely Maintenance	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.
MP-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] media 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 media protection policy and the associated media protection controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and c. Review and update the current media 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].
MP-2 Media Access	Restrict access to [Assignment: organization-defined organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined organization-defined personnel or roles].
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-4 Media Storage	a. Physically control and securely store [Assignment: organization-defined organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined organization-defined controlled areas] ; and b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
MP-5 Media Transport	a. Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined organization-defined controls]; b. Maintain accountability for system media during transport outside of controlled areas; c. Document activities associated with the transport of system media; and d. Restrict the activities associated with the transport of system media to authorized personnel.

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-4 Access Control for Transmission	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].
PE-5 Access Control for Output Devices	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.

PE-9 Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.
PE-10 Emergency Shutoff	a. Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations; b. Place emergency shutoff switches or devices in [Assignment: organization-defined location] to facilitate access for authorized personnel; and c. Protect emergency power shutoff capability from unauthorized activation.
PE-11 Emergency Power	Provide an uninterruptible power supply to facilitate [Selection: an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.
PE-12 Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
PE-13 Fire Protection	Employ and maintain fire detection and suppression systems that are supported by an independent energy source.
PE-14 Environmental Controls	a. Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels] ; and b. Monitor environmental control levels [Assignment: organization-defined frequency].
PE-15 Water Damage Protection	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
PE-16 Delivery and Removal	a. Authorize and control [Assignment: organization-defined organization-defined types of system components] entering and exiting the facility; and b. Maintain records of the system components.
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-18 Location of System Components	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.
PE-19 Information Leakage	Protect the system from information leakage due to electromagnetic signals emanations.
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].
PE-22 Component Marking	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.
PE-23 Facility Location	a. Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b. For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.

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-2 System Security and Privacy Plans	a. Develop security and privacy plans for the system that: 1. Are consistent with the organization’s enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of mission and business processes; 4. Identify the individuals that fulfill system roles and responsibilities; 5. Identify the information types processed, stored, and transmitted by the system; 6. Provide the security categorization of the system, including supporting rationale; 7. Describe any specific threats to the system that are of concern to the organization; 8. Provide the results of a privacy risk assessment for systems processing personally identifiable information; 9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components; 10. Provide an overview of the security and privacy requirements for the system; 11. Identify any relevant control baselines or overlays, if applicable; 12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; 13. Include risk determinations for security and privacy architecture and design decisions; 14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups] ; and 15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation. b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]; c. Review the plans [Assignment: organization-defined frequency]; d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and e. Protect the plans from unauthorized disclosure and modification.
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].

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-4 Plan of Action and Milestones Process	a. Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b. Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-5 System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
PM-6 Measures of Performance	Develop, monitor, and report on the results of information security and privacy measures of performance.
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-10 Authorization Process	a. Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b. Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Integrate the authorization processes into an organization-wide risk management program.

PM-11 Mission and Business Process Definition	a. Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c. Review and revise the mission and business processes [Assignment: organization-defined frequency].
PM-13 Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.
PM-14 Testing, Training, and Monitoring	a. Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b. Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-15 Security and Privacy Groups and Associations	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a. To facilitate ongoing security and privacy education and training for organizational personnel; b. To maintain currency with recommended security and privacy practices, techniques, and technologies; and c. To share current security and privacy information, including threats, vulnerabilities, and incidents.
PM-28 Risk Framing	a. Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; b. Distribute the results of risk framing activities to [Assignment: organization-defined personnel] ; and c. Review and update risk framing considerations [Assignment: organization-defined frequency].
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.
PM-30 Supply Chain Risk Management Strategy	a. Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; b. Implement the supply chain risk management strategy consistently across the organization; and c. Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.
PM-31 Continuous Monitoring Strategy	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a. Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b. Establishing [Assignment: organization-defined monitoring frequencies] and [Assignment: organization-defined assessment frequencies] for control effectiveness; c. Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d. Correlation and analysis of information generated by control assessments and monitoring; e. Response actions to address results of the analysis of control assessment and monitoring information; and f. Reporting the security and privacy status of organizational systems to [Assignment: organization-defined organization-defined personnel or roles] [Assignment: organization-defined organization-defined frequency].

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-5 Personnel Transfer	a. Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b. Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action]; c. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].
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-8 Personnel Sanctions	a. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b. Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

PT-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] personally identifiable information processing and transparency 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 personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personally identifiable information processing and transparency policy and procedures; and c. Review and update the current personally identifiable information processing and transparency: 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-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-7 Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
RA-9 Criticality Analysis	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].
RA-10 Threat Hunting	a. Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and b. Employ the threat hunting capability [Assignment: organization-defined frequency].
SA-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 services acquisition 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 services acquisition policy and the associated system and services acquisition controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c. Review and update the current system and services acquisition: 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].
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-3(2) Use of Live or Operational Data	(a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and (b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

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-5 System Documentation	a. Obtain or develop administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b. Obtain or develop user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and d. Distribute documentation to [Assignment: organization-defined personnel or roles].
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-10 Developer Configuration Management	Require the developer of the system, system component, or system service to: a. Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items]; c. Implement only organization-approved changes to the system, component, or service; d. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

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-11(3) Independent Verification of Assessment Plans and Evidence	(a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and (b) Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.
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].
SA-17 Developer Security and Privacy Architecture and Design	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization’s security and privacy architecture that is an integral part the organization’s enterprise architecture; b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.
SA-21 Developer Screening	Require that the developer of [Assignment: organization-defined system, systems component, or system service]: a. Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties] ; and b. Satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria].

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(2) Capacity, Bandwidth, and Redundancy	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks.
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-8(1) Cryptographic Protection	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.
SC-10 Network Disconnect	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.
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-15 Collaborative Computing Devices and Applications	a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed] ; and b. Provide an explicit indication of use to users physically present at the devices.
SC-17 Public Key Infrastructure Certificates	a. Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.
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-28(1) Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].
SC-42 Sensor Capability and Data	a. Prohibit [Selection (one or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems] ; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]] ; and b. Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].
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.
SR-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] supply chain risk management 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 supply chain risk management policy and the associated supply chain risk management controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c. Review and update the current supply chain risk management: 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].
SR-2 Supply Chain Risk Management Plan	a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]; b. Review and update the supply chain risk management plan [Assignment: organization-defined frequency] or as required, to address threat, organizational or environmental changes; and c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

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-4 Provenance	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].
SR-5(2) Assessments Prior to Selection, Acceptance, Modification, or Update	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.
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].
SR-7 Supply Chain Operations Security	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined OPSEC controls].
SR-9 Tamper Resistance and Detection	Implement a tamper protection program for the system, system component, or system service.
SR-10 Inspection of Systems or Components	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency] ; upon [Assignment: organization-defined indications of need for inspection]] to detect tampering: [Assignment: organization-defined systems or system components].
SR-11 Component Authenticity	a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b. Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations] ; [Assignment: organization-defined personnel or roles]].