Technology Risk Management: Notices FSM-N05 and FSM-N06 (May 2024) and Guidelines (January 2021): technical evidence

Neither Mamluk LLC-FZ nor its products are affiliated with or endorsed by the Monetary Authority of Singapore.

Regime	Technology Risk Management: Notices FSM-N05 and FSM-N06 (May 2024) and Guidelines (January 2021), Monetary Authority of Singapore (MAS)
Organisation	Example Bank
Cluster	example-production
Collected	2026-11-18T09:47:53Z
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.

MAS is the source and owner of the Technology Risk Management Notices and Guidelines. The requirement summaries in this report are Mamluk's paraphrase, not MAS's text.

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

Requirements of Notices FSM-N05 and FSM-N06 are binding. Requirements of the Guidelines are guidance that MAS expects to be adopted in proportion to an institution's risks. The notices to licensed insurers (FSM-N03, FSM-N04) and to capital markets intermediaries (FSM-N21, FSM-N22) state the same requirements; this report uses the bank notices' numbering.

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

259 requirements: 6 enforced by a policy, 21 checked, 10 provided by the platform, 222 organisational (79 technical, outside the cluster; 87 non-technical; 56 technical and non-technical).

Outcome	Requirements	Meaning
Fail	18	The cluster was checked and something does not meet the requirement. The findings say what and where.
Not provided	0	A control the requirement needs is switched off on this cluster.
Incomplete	2	Everything that could be checked passed, but part of the requirement could not be checked in this run. The reason is given.
Not evaluated	2	Nothing behind this requirement could be checked in this run. The reason is given. It is not a pass.
Pass	8	Every check behind the requirement passed on this run's date. Where coverage is partial, the pass covers the cluster's part only.
Recorded	4	Facts collected for the organisation's reviewer, such as an inventory or a list of access; no verdict.
Nothing to check	3	The cluster has nothing of this kind yet, for example no Ingress to check for TLS. Neither a pass nor a failure.
Organisational evidence	222	The organisation evidences this requirement outside the cluster; the Convoy checks nothing here.

17 object(s) fail at least one check: 5 cluster-wide and 12 in 1 namespace(s). They are listed under Fix first, those that fail a requirement marked "Notice (binding)" 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

5 object(s), most severe Critical.

ClusterRole **tigera-operator** Fails 9.1.1, 9.2.1, 11.1.3, N05 9, N06 4.1 Notice (binding): N05 9, N06 4.1

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 9.1.1, 9.2.1, 11.1.3, N05 9, N06 4.1 Notice (binding): N05 9, N06 4.1

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 8.4.1, 8.4.4

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 12.2.2

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 6.4.5, 10.1.2	
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.

Namespace payments

12 object(s), most severe High.

CronJob **nightly** Fails 7.6.2, 11.3.2, 11.3.6, 13.1.2, N06 4.1, N06 4.3(b) Notice (binding): N06 4.1, N06 4.3(b)	
HIGH	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of CronJob 'nightly' should set 'securityContext.allowPrivilegeEscalation' to false Check trivy.privileged, trivy-operator AVD-KSV-0001. **How to fix** Set containers[].securityContext.allowPrivilegeEscalation to false. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of CronJob 'nightly' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of cronjob "nightly" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
	`kubectl get policyreport 08d267bc-7735-4db3-8092-37242c730e8d -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

Deployment **legacy-batch** Fails 7.6.2, 11.3.2, 11.3.6, 13.1.2, N06 4.1, N06 4.3(b) Notice (binding): N06 4.1, N06 4.3(b)	
HIGH	no signing key covers registry.example.com/payments/checkout:3.10.1 Check policy.images-signed. **How to fix** Sign the image with cosign and add the public key, with a pattern matching the image, under signatures.keys in the Convoy's values. If the image is already signed, add the key that signed it. Then upgrade the Convoy. (Bahriya Tersane)
HIGH	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1 Check policy.registries-allowed. **How to fix** Pull the image from a registry the cluster allows, such as a mirror of your own, and update the workload to use it. To allow a further registry, add it to registries.allowed in the Convoy's values and upgrade the Convoy. (Bahriya Tersane)
MEDIUM	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.allowPrivilegeEscalation' to false Check trivy.privileged, trivy-operator AVD-KSV-0001. **How to fix** Set containers[].securityContext.allowPrivilegeEscalation to false. (Bahriya Tersane)
MEDIUM	AVD-KSV-0012: Runs as root user. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.runAsNonRoot' to true Check trivy.run-as-root, trivy-operator AVD-KSV-0012. **How to fix** Set 'containers[].securityContext.runAsNonRoot' to true. (trivy-operator)
MEDIUM	AVD-KSV-0104: Seccomp policies disabled. container "app" of replicaset "legacy-batch-5bdd998d78" in "payments" namespace should specify a seccomp profile Check trivy.seccomp, trivy-operator AVD-KSV-0104. **How to fix** Specify seccomp either by annotation or by seccomp profile type having allowed values as per pod security standards (trivy-operator)
LOW	containers without CPU and memory limits: app Check policy.resource-limits. Also failed by trivy-operator AVD-KSV-0011 (Low) and AVD-KSV-0018 (Low). **How to fix** Set resources.limits.cpu and resources.limits.memory on every container of the Pod template, at values the workload has been measured to need. (Bahriya Tersane)
LOW	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault' Check trivy.seccomp, trivy-operator AVD-KSV-0030. **How to fix** Set spec.securityContext.seccompProfile.type to RuntimeDefault on the Pod, and remove any container's seccompProfile that sets another type. (Bahriya Tersane)

Full results	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
	`kubectl get policyreport 62da526a-1c63-4fe4-b4c5-7b12ae7f4389 -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 7.6.2, 11.3.2, 11.3.6, 13.1.2, N06 4.1, N06 4.3(b) Notice (binding): N06 4.1, N06 4.3(b)

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

Full results	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`
	`kubectl get policyreport 5be8ff9f-da84-4f4d-b8a5-438e1b487f23 -n payments -o yaml`
	Kyverno names each policy report after the UID of the object it covers.

Namespace **payments** Fails 5.7.3, 11.2.2, N06 4.4 Notice (binding): N06 4.4

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 6e2f8e70-0488-43e7-b79c-5a264f16a7bc -o yaml` Kyverno names each policy report after the UID of the object it covers.

CronJob **weekly** Fails 7.6.2, 11.3.6

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 1bdd39bd-625e-4a37-8ea3-0c909f1de641 -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 7.6.2, 11.3.6

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 115b1aa4-1555-446d-9eee-2ac3dca8345f -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 **migrate-once** Fails 7.6.2, 11.3.6

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 87a6e510-c923-4cae-92bb-1e570a8122b2 -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 7.6.2, 11.3.6

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 4dae64ca-4264-4ea3-a4f0-28d6f76dc8dc -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Pod **nightly-now-zxcxw** Fails 7.6.2, 11.3.6

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 439a9e85-13f3-400c-8481-5ce4fe07efeb -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Pod **one-off** Fails 7.6.2, 11.3.6

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 06e48055-36f2-4440-8a0c-539f757e589e -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-p2qb6** Fails 7.6.2, 11.3.6

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 656f73f5-2c45-48eb-91c3-183b144fcc41 -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

ReplicaSet **unsigned-app-b5567644f** Fails 7.6.2, 11.3.6	
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 6d9b99f4-8062-4f30-b6dc-57e6fcd84a93 -n payments -o yaml` Kyverno names each policy report after the UID of the object it covers.

Requirements

N05 Notice FSM-N05: Technology Risk Management

N05 4	A framework and process to identify the institution's critical systems. Organisational, technical and non-technical. Notice (binding). NIST SP 800-53: CP-2(8) Identify Critical Assets.	**Organisational evidence**
N05 5	High availability kept for critical systems, with unscheduled downtime of each no more than four hours in total in any twelve months. Organisational, technical, outside the cluster. Notice (binding). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
N05 6	A recovery time objective of at most four hours for each critical system, with the recovery testing and the validation of the objective documented at least every twelve months. Organisational, technical, outside the cluster. Notice (binding). NIST SP 800-53: CP-4 Contingency Plan Testing, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
N05 7	The Authority notified within one hour of discovering an incident with a severe and widespread impact on operations or customer service. Organisational, non-technical. Notice (binding). NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**
N05 8	Within fourteen days of discovering such an incident, a report to the Authority on its cause and its effects, with an executive summary and the remedial measures taken. Organisational, non-technical. Notice (binding). NIST SP 800-53: IR-6 Incident Reporting, IR-4 Incident Handling.	**Organisational evidence**

N05 9 IT controls that keep customer information from being accessed or disclosed without authority. **Fail**

Checked, coverage partial. Notice (binding). NIST SP 800-53: AC-3 Access Enforcement, AC-6 Least Privilege, SC-28 Protection of Information at Rest, SC-8 Transmission Confidentiality and Integrity.

Scope of this evidence The evidence concerns access to the cluster and to the Kubernetes Secrets it holds: role-based access control, anonymous access refused, service account tokens, the encryption of Secrets at rest, and TLS on the control plane and on Ingresses. Controls over customer information in applications, databases and other systems are the financial institution'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.
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.
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.

N06 Notice FSM-N06: Cyber Hygiene

N06 4.1 Every administrative account on operating systems, databases, applications, security appliances and network devices secured against unauthorised access or use. **Fail**

Checked, coverage partial. Notice (binding). NIST SP 800-53: AC-6(5) Privileged Accounts, IA-2 Identification and Authentication (Organizational Users).

Scope of this evidence The evidence concerns administrative access to the cluster: sign-in through an identity provider, anonymous access refused, the kubelet's authentication, and the roles and containers that hold administrative privilege. Administrative accounts on operating systems, databases, applications, security appliances and network devices outside the cluster are the financial institution's to evidence.

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

node.kubelet-authn	**Pass**	The kubelet refuses anonymous requests and authenticates clients by certificate and webhook: so on all 1 node(s). Establishes: The kubelet refuses anonymous requests and authenticates clients by certificate and webhook.
platform.anonymous	**Not evaluated**	Anonymous requests restricted to the health endpoints: the platform could not observe it. Establishes: Anonymous requests to the API server are limited to the health endpoints.
platform.oidc	**Not evaluated**	The platform could not read the authentication configuration. Establishes: People sign in to the cluster through the organisation's identity provider, which enforces its own authentication factors.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
policy.no-privileged	**Pass**	Every object the policy judged passes it. Establishes: No container runs privileged or adds capabilities other than NET_BIND_SERVICE, outside named namespaces.
trivy.privileged	**Fail**	3 object(s) fail. Establishes: Containers that run privileged, may escalate privileges or add capabilities.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

N06 4.2(a) Security patches applied to every system within a time set by the risk each vulnerability poses. **Pass**

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

Scope of this evidence The verdict concerns known vulnerabilities in the images of the workloads outside the exempt namespaces, how long the critical and high ones have been open, and how recent the scans are. Patching of other systems, and the timeframes the financial institution sets by risk, are the financial institution'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 2.3.0, Kubernetes v1.36.4, observed 2026-11-18T09:43:20Z. 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.

N06 4.2(b) Controls that reduce the risk of a vulnerability for which no security patch is available. **Organisational evidence**

Organisational, technical, outside the cluster. Notice (binding). NIST SP 800-53: RA-7 Risk Response.

N06 4.3(a) Security standards, written down, for each system the institution uses. **Organisational evidence**

Organisational, technical, outside the cluster. Notice (binding). NIST SP 800-53: CM-1 Policy and Procedures.

N06 4.3(b) Every system conforms to its written security standards, except as paragraph 4.3(c) allows. **Fail**

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

Scope of this evidence The verdict concerns the configuration of the cluster's nodes, control plane and workloads against the hardening baseline the Convoy applies, which the financial institution may adopt into its written standards. Conformance of other systems, and to the financial institution's own written standards, is the financial institution's to evidence.

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

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

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

N06 4.3(c) Controls that reduce the risk where a system cannot conform to its security standards. **Organisational evidence**

Organisational, technical, outside the cluster. Notice (binding). NIST SP 800-53: RA-7 Risk Response.

N06 4.4	Controls at the network perimeter that restrict all unauthorised network traffic.	**Fail**

Checked, coverage partial. Notice (binding). NIST SP 800-53: SC-7 Boundary Protection.

Scope of this evidence The evidence concerns traffic into and within the cluster: NetworkPolicies that deny by default in each namespace, the nodes' host firewall, and Services exposed on external addresses. The financial institution's network perimeter beyond the cluster is the financial institution'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.

N06 4.5	Protection against malware on each system, wherever a protective measure exists and can be put in place.	**Organisational evidence**

Organisational, technical, outside the cluster. Notice (binding). NIST SP 800-53: SI-3 Malicious Code Protection.

N06 4.6	Multi-factor authentication for every administrative account on a critical system, and for every account used to reach customer information over the internet.	**Organisational evidence**

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

3 Technology Risk Governance and Oversight

3.1 Role of the Board of Directors and Senior Management

3.1.1	The board and senior management see that internal controls and risk management keep the IT environment secure, reliable and resilient.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-1 Information Security Program Plan, PM-9 Risk Management Strategy.

3.1.2	The board and senior management each include members able to understand and manage technology and cyber risk. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-13 Security and Privacy Workforce.	**Organisational evidence**
3.1.3	A suitably experienced head of IT and head of information security appointed, with at least the chief executive's approval. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-2 Information Security Program Leadership Role.	**Organisational evidence**
3.1.4	A technology risk management strategy established and carried out under the oversight of the board and senior management. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**
3.1.5	Key IT decisions taken within the institution's risk appetite. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing.	**Organisational evidence**
3.1.6	The board and senior management lead a culture of technology risk awareness among staff at every level. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, AT-2 Literacy Training and Awareness.	**Organisational evidence**
3.1.7	The board or its committee oversees the risk framework, an independent technology risk function, the authority and resources of those carrying out the strategy, the risk appetite and tolerance, regular strategy reviews, management competence and an independent audit function. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-2 Information Security Program Leadership Role, PM-3 Information Security and Privacy Resources, CA-2 Control Assessments.	**Organisational evidence**
3.1.8	Senior management sets up and runs the technology risk framework and strategy, keeps policies, standards and procedures in force, defines staff roles in managing technology risk and tells the board promptly of significant adverse risks and incidents. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PL-1 Policy and Procedures, PS-9 Position Descriptions.	**Organisational evidence**

3.2 Policies, Standards and Procedures

3.2.1	Policies, standards and procedures for technology risk and the protection of information assets, drawing on industry practice and reviewed regularly against changing threats. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PL-1 Policy and Procedures, PM-1 Information Security Program Plan.	**Organisational evidence**
3.2.2	The risk of each deviation from policy assessed and approved by senior management, with approved deviations reviewed periodically. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, RA-7 Risk Response, PM-9 Risk Management Strategy.	**Organisational evidence**

3.2.3 Compliance processes that verify adherence to policies, standards and procedures and follow up on non-compliance. **Organisational evidence**

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

3.3 Management of Information Assets

3.3.1 Information asset management that identifies the assets supporting the business, classifies them by security classification or criticality, assigns their owners and managers, and governs them by policy. **Pass**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-8 System Component Inventory, RA-2 Security Categorization, PM-5 System Inventory.

Scope of this evidence The inventory of the cluster's namespaces, workloads and images is recorded, and the verdict is that each namespace outside the exempt namespaces carries a classification label. Ownership, the roles of the staff managing assets, the policies that govern them, and the identification and classification of other information assets are the financial institution's to evidence.

cluster.workload-inventory	**Recorded**	13 namespaces, 22 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.
policy.namespace-classification	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries a data classification label.

3.3.2 An inventory of all information assets, reviewed periodically and updated on every change. **Recorded**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-8 System Component Inventory, CM-8(1) Updates During Installation and Removal.

Scope of this evidence The inventory of the cluster's namespaces, workloads and images is recorded. The inventory of other information assets, and its periodic review, are the financial institution's to evidence.

cluster.workload-inventory	**Recorded**	13 namespaces, 22 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.

3.4 Management of Third Party Services

3.4.1 Explanatory: third-party services that are not outsourcing can still expose the institution and its customers to IT failures and breaches at the provider. **Organisational evidence**

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

3.4.2 The technology risk to systems and data held by a third party assessed before a contract or partnership is entered into. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-9 External System Services, RA-3 Risk Assessment, SR-6 Supplier Assessments and Reviews.

3.4.3	Ongoing assurance that each third party protects the confidentiality and integrity of data and keeps its systems resilient. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**

3.5 Competency and Background Review

3.5.1	Staff, contractors and service providers competent to perform IT functions and manage technology risk. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PS-7 External Personnel Security, AT-3 Role-based Training, PM-13 Security and Privacy Workforce.	**Organisational evidence**
3.5.2	Background checks on personnel with access to the institution's data and IT systems, to reduce insider threat. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PS-3 Personnel Screening, PS-7 External Personnel Security.	**Organisational evidence**

3.6 Security Awareness and Training

3.6.1	A security awareness programme for all staff covering current cyber threats, the institution's security policies and standards, personal responsibility for information assets, and the applicable laws and regulations. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness, AT-3 Role-based Training.	**Organisational evidence**
3.6.2	Awareness training given at least once a year to all staff, contractors and service providers with access to information assets. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-2 Literacy Training and Awareness, AT-3 Role-based Training.	**Organisational evidence**
3.6.3	Training for the board on technology risks and their management. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-2 Literacy Training and Awareness, AT-3 Role-based Training.	**Organisational evidence**
3.6.4	The training programme reviewed periodically against policy changes, emerging risks and the threat landscape. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-1 Policy and Procedures, AT-2 Literacy Training and Awareness.	**Organisational evidence**

4 Technology Risk Management Framework

4.1 Risk Management Framework

4.1.1	A technology risk management framework with governance structures, defined roles and clear reporting lines. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing, PM-2 Information Security Program Leadership Role.	**Organisational evidence**
4.1.2	Risk management practices and internal controls that achieve confidentiality, integrity, security, reliability and resilience of the IT environment. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-1 Information Security Program Plan.	**Organisational evidence**

4.1.3	A risk owner, a person or function with the authority to do so, named and accountable for treating each technology risk. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing.	**Organisational evidence**
4.1.4	The framework covers risk identification, assessment, treatment, and monitoring, review and reporting to the board and senior management. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, PM-28 Risk Framing, RA-3 Risk Assessment, PM-31 Continuous Monitoring Strategy.	**Organisational evidence**
4.1.5	The adequacy and effectiveness of the framework reviewed regularly as the business, IT and threats change. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, RA-1 Policy and Procedures.	**Organisational evidence**

4.2 Risk Identification

4.2.1	The threats and vulnerabilities to the IT environment identified, including assets run or supported by third parties. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, PM-16 Threat Awareness Program.	**Organisational evidence**

4.3 Risk Assessment

4.3.1	The business impact of threats and vulnerabilities analysed, taking account of financial, legal, operational, regulatory and reputational factors. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
4.3.2	Criteria for likelihood and impact set to prioritise technology risks. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, PM-28 Risk Framing.	**Organisational evidence**

4.4 Risk Treatment

4.4.1	Mitigating controls matched to asset criticality and risk tolerance, reviewed regularly as threats and the risk profile change. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: RA-7 Risk Response, PM-9 Risk Management Strategy.	**Organisational evidence**
4.4.2	Residual risk assessed after mitigation, with defined criteria and approvers for accepting risk in line with tolerance. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: RA-7 Risk Response, PM-28 Risk Framing.	**Organisational evidence**
4.4.3	Insurance taken for insurable technology risks to limit their financial impact. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy.	**Organisational evidence**

4.5 Risk Monitoring, Review and Reporting

4.5.1	A process that assesses and monitors whether IT controls are well designed and operate effectively against the identified risks. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CA-2 Control Assessments, CA-7 Continuous Monitoring.	**Organisational evidence**
4.5.2	A risk register, with significant risks watched closely and reported to the board and senior management as often as their level warrants. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-9 Risk Management Strategy, RA-3 Risk Assessment.	**Organisational evidence**
4.5.3	Technology risk metrics that show the assets most exposed, informed by risk events, audit findings and regulation. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-6 Measures of Performance, PM-9 Risk Management Strategy.	**Organisational evidence**

5 IT Project Management and Security-by-Design

5.1 Project Management Framework

5.1.1	A project management framework of policies, standards, procedures and activities covering projects from start to close. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle.	**Organisational evidence**
5.1.2	A detailed plan for every IT project, setting scope, activities, milestones, deliverables and staff roles. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, PL-2 System Security and Privacy Plans.	**Organisational evidence**
5.1.3	Key project documents, from feasibility and business case to implementation plan, kept and approved by business and IT management. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, SA-2 Allocation of Resources.	**Organisational evidence**
5.1.4	Project risks identified, assessed, treated and monitored throughout the project. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, RA-3 Risk Assessment.	**Organisational evidence**

5.2 Project Steering Committee

5.2.1	A steering committee of business and IT stakeholders that directs and oversees large, complex projects. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle.	**Organisational evidence**
5.2.2	Unresolved risks and issues on large projects escalated to the steering committee and senior management. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, PM-9 Risk Management Strategy.	**Organisational evidence**

5.3 System Acquisition

5.3.1	Standards for evaluating and choosing vendors, with due diligence matched to the criticality of what they deliver. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-4 Acquisition Process, SR-6 Supplier Assessments and Reviews.	**Organisational evidence**
5.3.2	The vendor's development, quality and data protection practices assessed, and any vendor access to the institution's systems controlled and monitored. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-4 Acquisition Process, SA-9 External System Services, SA-15 Development Process, Standards, and Tools, AC-2(12) Account Monitoring for Atypical Usage.	**Organisational evidence**
5.3.3	An off-the-shelf product that falls short of security requirements deployed only after its risks are assessed and mitigated. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-4 Acquisition Process, RA-3 Risk Assessment.	**Organisational evidence**
5.3.4	Source code escrow considered for critical acquired software, with replacement options identified where escrow is not possible. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-4 Acquisition Process, CP-2 Contingency Plan.	**Organisational evidence**

5.4 System Development Life Cycle and Security-By-Design

5.4.1	A system development life cycle framework defining the processes, controls, standards and procedures for each phase. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, SA-15 Development Process, Standards, and Tools.	**Organisational evidence**
5.4.2	Security built into every phase of development: security in the design, continuous security evaluation and secure practice throughout. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SA-3 System Development Life Cycle, SA-17 Developer Security and Privacy Architecture and Design.	**Organisational evidence**
5.4.3	Security requirements that address at least access control, authentication and authorisation, the integrity and confidentiality of data, logging of system activity, tracking of security events, and handling of exceptions. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-4 Acquisition Process, PL-8 Security and Privacy Architectures, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
5.4.4	The IT security function involved in each phase of development where relevant. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle.	**Organisational evidence**

5.5 System Requirements Analysis

5.5.1	Functional requirements, and requirements for performance, resilience and security controls, defined and documented for each system. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-4 Acquisition Process, PL-8 Security and Privacy Architectures.	**Organisational evidence**
5.5.2	Security requirements set from an assessment of the system's threats and risks and the security level the business needs. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, SA-4 Acquisition Process.	**Organisational evidence**

5.6 System Design and Implementation

5.6.1	The proposed architecture, design and built-in controls reviewed against the requirements before implementation. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-17 Developer Security and Privacy Architecture and Design, PL-8 Security and Privacy Architectures, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
5.6.2	Design and implementation verified against the requirements, with changes or deviations endorsed by stakeholders. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-10 Developer Configuration Management, SA-4 Acquisition Process.	**Organisational evidence**
5.6.3	Domain experts, security specialists among them, take part in design reviews. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-17 Developer Security and Privacy Architecture and Design, PL-8 Security and Privacy Architectures.	**Organisational evidence**

5.7 System Testing and Acceptance

5.7.1	A testing methodology covering business logic, function, security controls and performance under load, with a test plan approved before testing. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**
5.7.2	Each requirement traced to test cases during testing. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation.	**Organisational evidence**

5.7.3	Unit, integration and acceptance testing each in its own physical or logical environment, with access to each limited to those who need it.	**Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-4(1) Separate Test Environments, AC-4 Information Flow Enforcement.

Scope of this evidence The evidence is that each application namespace carries an environment label and has network policies governing its traffic, each of which selects workloads. Separate physical environments, separation between test environments beyond the cluster's namespaces, and limiting access to each environment to those who need it are the financial institution's to evidence.

Fails in Namespace payments.

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-environment	**Pass**	Every object the policy judged passes it. Establishes: Every application namespace carries an environment label, one of the values in namespaces.environments.
policy.namespace-network-policy	**Fail**	1 object(s) fail the policy. Establishes: Every application namespace has at least one NetworkPolicy.
trivy.network-policy-selectors	**Pass**	Every object outside the exempt namespaces passes. Establishes: NetworkPolicies whose selectors select nothing.

5.7.4	Regression testing after changes to an existing system.	**Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, CM-4 Impact Analyses.

5.7.5	Defects found in testing tracked and resolved, with major ones reported to the steering committee and fixed before production.	**Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, CA-5 Plan of Action and Milestones.

5.7.6	All test results recorded in a test report signed off by stakeholders.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation.

5.8 Quality Management

5.8.1	Quality attributes and measures for deliverables defined at project planning.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-15 Development Process, Standards, and Tools.

5.8.2	Independent quality assurance of project activities and deliverables against the institution's policies and standards.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-15 Development Process, Standards, and Tools, CA-2(1) Independent Assessors.

6 Software Application Development and Management

6.1 Secure Coding, Source Code Review and Application Security Testing

6.1.1 Standards adopted for secure coding, for reviewing source code and for testing application security. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-15 Development Process, Standards, and Tools, SA-11 Developer Testing and Evaluation, SA-8 Security and Privacy Engineering Principles.

6.1.2 Coding and review standards that cover secure programming, input validation, output encoding, access control, authentication, cryptography and error handling. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-15 Development Process, Standards, and Tools, SA-8 Security and Privacy Engineering Principles, SA-11(4) Manual Code Reviews.

6.1.3 A policy that third-party and open-source code is reviewed and tested before it is built into the institution's software. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, SR-5 Acquisition Strategies, Tools, and Methods.

6.1.4 Updates and reported vulnerabilities tracked for the third-party and open-source code in the institution's software. **Pass**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, SI-5 Security Alerts, Advisories, and Directives.

Scope of this evidence The verdict concerns the known vulnerabilities in the packages of the images of the workloads outside the exempt namespaces, scanned against a vulnerability database refreshed every six hours, and the freshness of those scans; how long each open critical and high vulnerability has been reported is recorded beside it. Tracking updates, and the code of software that does not run in the cluster, are the financial institution'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.
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.

6.1.5 Developers trained, or otherwise skilled, to follow the institution's secure coding and application security standards. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-3 Role-based Training.

6.1.6 A strategy for application security testing, which may combine static, dynamic and interactive methods, with its rules reviewed periodically. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, SA-11(1) Static Code Analysis, SA-11(8) Dynamic Code Analysis.

6.1.7	Defects from code review and security testing tracked, with major ones fixed before production. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, CA-5 Plan of Action and Milestones.	**Organisational evidence**

6.2 Agile Software Development

6.2.1	The principles of the system development life cycle, and of building security in from the design, kept when working in Agile methods. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, SA-8 Security and Privacy Engineering Principles.	**Organisational evidence**
6.2.2	Secure coding, code review and security testing standards applied in Agile development. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, SA-15 Development Process, Standards, and Tools.	**Organisational evidence**

6.3 DevSecOps Management

6.3.1	DevSecOps activities aligned with the development life cycle framework and IT service management processes. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-3 System Development Life Cycle, SA-15 Development Process, Standards, and Tools, CM-3 Configuration Change Control.	**Organisational evidence**
6.3.2	Security measures and segregation of duties between development, testing and release in DevSecOps. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: AC-5 Separation of Duties, CM-5 Access Restrictions for Change, SA-15 Development Process, Standards, and Tools.	**Organisational evidence**

6.4 Application Programming Interface Development

6.4.1	Safeguards for developing and providing APIs, including open APIs used by third parties. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, SA-9 External System Services.	**Organisational evidence**
6.4.2	A vetting process for third parties connecting through APIs, weighing their business, security posture, reputation and record, and governing their access. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-9 External System Services, SR-6 Supplier Assessments and Reviews, AC-20 Use of External Systems.	**Organisational evidence**
6.4.3	A risk assessment before a third party connects through an API, with each API's protection matched to the sensitivity and criticality of its data. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, CA-3 Information Exchange, AC-20 Use of External Systems.	**Organisational evidence**
6.4.4	Secure API design standards that protect API keys and access tokens and enforce a set expiry for tokens. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-8 Security and Privacy Engineering Principles, IA-5 Authenticator Management, AC-12 Session Termination.	**Organisational evidence**

6.4.5 Strong encryption and key management for sensitive data sent through APIs. **Fail**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection.

Scope of this evidence The evidence is that every Ingress serves its hosts over TLS, and that the control plane and the kubelets offer only AEAD TLS cipher suites. The strength of the TLS each Ingress offers, encryption of APIs not served through the cluster's Ingresses, and the management of their keys are the financial institution'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.
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.

6.4.6 APIs security-tested with the third party before production, and third-party access sessions logged with who connected, when and what data was reached. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SA-11 Developer Testing and Evaluation, AU-2 Event Logging, AU-3 Content of Audit Records.

6.4.7 Real-time monitoring and alerting of API use, performance and suspicious activity, and prompt revocation of keys or tokens after a breach. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, AU-6 Audit Record Review, Analysis, and Reporting, IR-4 Incident Handling.

6.4.8 Enough capacity for high volumes of API calls, and protection against denial of service. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-5 Denial-of-service Protection, CP-2(2) Capacity Planning.

6.5 Management of End User Computing and Applications

6.5.1 IT not managed by the IT department, known as shadow IT, managed as part of the information assets. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CM-8 System Component Inventory, CM-11 User-installed Software.

6.5.2 Measures that control shadow IT and watch for its use. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CM-8(3) Automated Unauthorized Component Detection, CM-11 User-installed Software.

6.5.3 Applications developed or acquired by end users risk-assessed, secured, approved and tested before use. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CM-11 User-installed Software, RA-3 Risk Assessment.

7 IT Service Management

7.1 IT Service Management Framework

7.1.1 An IT service management framework of governance, processes and procedures covering configuration, refresh, patch, change, release, incident and problem management. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CM-1 Policy and Procedures, CM-9 Configuration Management Plan, IR-1 Policy and Procedures.

7.2 Configuration Management

7.2.1 A configuration management process that keeps accurate information on the hardware and software of each IT system. **Recorded**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-8 System Component Inventory, CM-2 Baseline Configuration, CM-9 Configuration Management Plan.

Scope of this evidence The inventory of the cluster's namespaces, workloads and images, and the versions of the Bahriya Kubernetes Engine and Kubernetes it runs, are recorded. The configuration information of the nodes' hardware and of other systems, and the configuration management process, are the financial institution's to evidence.

cluster.workload-inventory	**Recorded**	13 namespaces, 22 workloads, 16 distinct images. Establishes: An inventory of the cluster's namespaces, workloads and the images they run.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.3.0, Kubernetes v1.36.4, observed 2026-11-18T09:43:20Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.

7.2.2 Configuration information reviewed and verified regularly to keep it accurate and current. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CM-8 System Component Inventory, CM-9 Configuration Management Plan.

7.3 Technology Refresh Management

7.3.1 Outdated and unsupported hardware and software avoided, with end-of-support dates closely monitored. **Incomplete**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: SA-22 Unsupported System Components.

Scope of this evidence The verdict covers the cluster's Kubernetes release, judged against the end-of-life dates the Kubernetes project publishes; its Bahriya Kubernetes Engine release, judged against Mamluk's published support policy; and the operating systems of the images outside the exempt namespaces, judged against trivy's end-of-life data. A release or an image out of support fails, and the versions are recorded. The nodes' hardware and operating systems, and other hardware and software, are the financial institution's to evidence.

platform.version-support	**Pass**	Kubernetes 1.36 is supported until 2027-06-28, as https://kubernetes.io/releases/ states. Bahriya Kubernetes Engine 2.3 is one of the 5 most recent minor releases, and supported under https://bke.bahriya.cloud/faq/#release-support. Establishes: The cluster's Kubernetes minor release is within its end-of-life date as the Kubernetes project states it, and its BKE minor release within Mamluk's published BKE support policy (one of the five most recent minor releases, or six months from its release, whichever is longer); a release past either fails, as end of support. Each table is dated, and a table not reviewed in time gives no verdict.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.3.0, Kubernetes v1.36.4, observed 2026-11-18T09:43:20Z. Establishes: The BKE and Kubernetes versions the cluster runs, against which supported versions are judged.
trivy.image-os-support	**Not evaluated**	No image outside the exempt namespaces runs on an operating system trivy recognises, so none was judged. Establishes: Every workload's images are scanned for the operating system they are built on; an image whose operating system trivy holds past its end of service life fails, as end of support. An image with no operating system that trivy recognises is listed by name and not judged.

7.3.2 A refresh plan to replace hardware and software before end of support, and a risk assessment and mitigation for those nearing it. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-22 Unsupported System Components, RA-3 Risk Assessment.

7.3.3 Management dispensation, with a validity period and periodic review, for continuing to use unsupported hardware or software. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SA-22 Unsupported System Components, RA-7 Risk Response.

7.4 Patch Management

7.4.1 A patch management process that applies security and other patches within timeframes set by the criticality of the patch and the system. **Pass**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: SI-2 Flaw Remediation.

Scope of this evidence The verdict concerns open critical and high vulnerabilities in the images of the workloads outside the exempt namespaces; how long each has been reported, and the versions of the Bahriya Kubernetes Engine and Kubernetes, are recorded beside it. The patch management process and its timeframes, and the patching of the nodes' operating systems and other systems, are the financial institution's to evidence.

cluster.vulnerability-age	**Recorded**	No critical or high vulnerability is open outside the exempt namespaces. Establishes: How long each open critical and high vulnerability has been reported.
platform.versions	**Recorded**	Bahriya Kubernetes Engine 2.3.0, Kubernetes v1.36.4, observed 2026-11-18T09:43:20Z. 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.

7.4.2 Patches tested before they reach production, for compatibility and to avoid new problems. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-2 Flaw Remediation, CM-3(2) Testing, Validation, and Documentation of Changes.

7.5 Change Management

7.5.1 A change management process under which each change to an information asset is assessed, tested, reviewed and approved ahead of being made. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CM-3 Configuration Change Control, CM-4 Impact Analyses.

7.5.2 A risk and impact analysis of each change, including its security effect and its effect on other assets, before it is made. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CM-4 Impact Analyses, RA-3 Risk Assessment.

7.5.3 Changes tested in a test environment under approved test plans, with results signed off before production. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CM-3(2) Testing, Validation, and Documentation of Changes, CM-4(1) Separate Test Environments.

7.5.4 A change advisory board of business and IT management that approves and prioritises changes on their stability and security effect. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CM-3 Configuration Change Control, CM-3(4) Security and Privacy Representatives.

7.5.5 A backup taken before each change, and a rollback plan to restore the previous state. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-9 System Backup, CM-3 Configuration Change Control.

7.5.6 Defined procedures and named approvers for assessing, approving and making emergency changes. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CM-3 Configuration Change Control.

7.5.7 Logging enabled to record activities performed during changes. **Pass**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: AU-2 Event Logging, AU-12 Audit Record Generation, CM-3 Configuration Change Control.

Scope of this evidence The evidence is that the API server writes an audit log under BKE's audit policy, which records the changes made through the Kubernetes API. Logging of changes made on the nodes or to other systems is the financial institution's to evidence.

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.

7.6 Software Release Management

7.6.1 Segregation of duties in release, so that no one person can develop, compile and move code between environments. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: AC-5 Separation of Duties, CM-5 Access Restrictions for Change.

7.6.2 Controls that keep code traceable and intact as it moves between environments. **Fail**

Enforced, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-14 Signed Components, SI-7 Software, Firmware, and Information Integrity.

Scope of this evidence The verdict concerns whether each image of the workloads outside the exempt namespaces carries a signature from a configured key; the registry of the platform's own images is recorded. The traceability and integrity of source code, byte code and binaries as they move between environments before they become images are the financial institution's to evidence.

Fails in CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app, CronJob payments/weekly, Deployment payments/ledger, Job payments/migrate-once, Job payments/nightly-now, Pod payments/nightly-now-zxcxw, Pod payments/one-off, Pod payments/unsigned-app-b5567644f-p2qb6 and 1 more.

platform.image-registry	**Recorded**	The registry the control plane pulls its images from: 1x.ax/bke/kubernetes. Establishes: The platform's own images come from the registry recorded, signed.
policy.images-signed	**Fail**	11 object(s) run images that are not signed or that no signing key covers. Establishes: Every image outside the exempt namespaces carries a signature from a configured key: Kyverno verifies the images that match a key's patterns, and the collector fails any image that no key covers. A failing Pod is admitted with a warning and recorded, or refused, as policies.defaultAction sets (Warn by default).

7.7 Incident Management

7.7.1	An incident management framework aimed at restoring affected services to a secure, stable state as quickly as possible. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-1 Policy and Procedures, IR-8 Incident Response Plan.	**Organisational evidence**
7.7.2	Enough resources, internal or engaged externally, for incident response and recovery. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-7 Incident Response Assistance, IR-4 Incident Handling.	**Organisational evidence**
7.7.3	The framework covers incident handling, including cyber incidents, the keeping and protection of evidence, and the roles of staff and external parties. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: IR-8 Incident Response Plan, IR-4 Incident Handling.	**Organisational evidence**
7.7.4	System events and alerts configured and actively monitored to warn early of performance and security issues. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, SI-4(5) System-generated Alerts, AU-6 Audit Record Review, Analysis, and Reporting.	**Organisational evidence**
7.7.5	Senior management kept informed of major incidents so it can act in time, such as by invoking disaster recovery. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-6 Incident Reporting, IR-4 Incident Handling.	**Organisational evidence**
7.7.6	A communications plan for informing customers and handling the media, naming spokespersons, experts and channels. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-8 Incident Response Plan, IR-7 Incident Response Assistance.	**Organisational evidence**
7.7.7	Timely updates to customers on incident handling and protective measures, with advice on steps they should take. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-6 Incident Reporting, IR-7 Incident Response Assistance.	**Organisational evidence**

7.8 Problem Management

7.8.1	A problem management process that finds and resolves the root causes of incidents to prevent recurrence. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-4 Incident Handling, IR-8 Incident Response Plan.	**Organisational evidence**
7.8.2	A record of past incidents and their lessons, to help resolve similar incidents. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-5 Incident Monitoring, IR-4 Incident Handling.	**Organisational evidence**
7.8.3	Trend analysis of past incidents to find patterns, confirm root causes were resolved and decide on further measures. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: IR-5 Incident Monitoring, IR-4 Incident Handling.	**Organisational evidence**

8 IT Resilience

8.1 System Availability

8.1.1	Systems designed and built for the availability the business needs. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-2 Contingency Plan, PL-8 Security and Privacy Architectures.	**Organisational evidence**
8.1.2	Redundancy or fault tolerance for systems needing high availability, periodic architecture reviews that map dependencies and single points of failure, and regular resilience testing. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-2 Contingency Plan, SC-36 Distributed Processing and Storage, CP-4 Contingency Plan Testing.	**Organisational evidence**
8.1.3	Resource utilisation monitored continuously against set thresholds, to support capacity management. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-2(2) Capacity Planning, SI-4 System Monitoring.	**Organisational evidence**
8.1.4	Procedures for responding when resource or performance thresholds are breached. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-2(2) Capacity Planning, IR-4 Incident Handling.	**Organisational evidence**

8.2 System Recoverability

8.2.1	Recovery time and recovery point objectives set in line with business recovery priorities. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution, CP-2(3) Resume Mission and Business Functions.	**Organisational evidence**
8.2.2	A disaster recovery plan with procedures for various scenarios and recovery roles, reviewed at least once a year and on material change. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-2 Contingency Plan, CP-10 System Recovery and Reconstitution.	**Organisational evidence**
8.2.3	Recovery follows the tested, approved plan, with untested measures used only after a risk assessment and senior management approval. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-10 System Recovery and Reconstitution, CP-2 Contingency Plan.	**Organisational evidence**
8.2.4	An endeavour to run operations from the recovery or alternate site periodically, to show it can sustain the business. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-7 Alternate Processing Site, CP-4 Contingency Plan Testing.	**Organisational evidence**

8.3 Testing of Disaster Recovery Plan

8.3.1	Regular disaster recovery tests, with business and IT taking part, that show the recovery objectives can be met. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-4 Contingency Plan Testing, CP-4(1) Coordinate with Related Plans.	**Organisational evidence**

8.3.2 A disaster recovery test plan with objectives, scope, scenarios, scripts, recovery procedures and success criteria. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-4 Contingency Plan Testing.

8.3.3 Recovery tests covering plausible disruptions, including loss of the primary site and major failures, and dependencies between assets, third-party ones included. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-4 Contingency Plan Testing, CP-4(1) Coordinate with Related Plans.

8.3.4 The disaster recovery capability of service providers assessed, with arrangements tested jointly with them. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CP-4 Contingency Plan Testing, SA-9 External System Services, CP-4(1) Coordinate with Related Plans.

8.4 System Backup and Recovery

8.4.1 A backup strategy and a plan for regular backups from which systems and data can be restored after disruption, corruption or deletion. **Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CP-9 System Backup, CP-10 System Recovery and Reconstitution.

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 backup strategy and plan, and the backups of other systems and data, are the financial institution'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.

8.4.2 A policy for the backup data life cycle: frequency, retention, storage and secure destruction. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CP-9 System Backup, MP-6 Media Sanitization.

8.4.3 Restoration from backups tested periodically. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CP-9(1) Testing for Reliability and Integrity, CP-4 Contingency Plan Testing.

8.4.4	Confidential data in backups protected, for example by encryption, and backup media kept offline or off site.	**Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CP-9(8) Cryptographic Protection, CP-9 System Backup, CP-6 Alternate Storage Site.

Scope of this evidence The verdict concerns whether each backed-up Longhorn volume outside the exempt namespaces is encrypted, and whether Longhorn has an available backup target, which is outside the cluster, and a recurring backup job, or Velero an available storage location, also outside it, and an active schedule. Whether that location is offline or off site, and the backups of other systems, are the financial institution's to evidence.

Fails in Cluster backups.

cluster.backup-encryption	**Nothing to check**	Neither Longhorn nor Velero is installed, so no backup leaves the site. Establishes: Every backed-up Longhorn volume is encrypted, so that its backups leave the site encrypted.
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.

8.5 Data Centre Resilience

8.5.1	A threat and vulnerability risk assessment of each data centre covering physical, environmental, political and economic threats, reviewed on material change.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, PE-18 Location of System Components, PE-23 Facility Location.

8.5.2	Redundant power, network paths, and cooling, electrical and mechanical systems in the data centre, with no single point of failure.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PE-9 Power Equipment and Cabling, PE-11 Emergency Power, PE-14 Environmental Controls, CP-8 Telecommunications Services.

8.5.3	Fire detection and suppression in the data centre.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PE-13 Fire Protection.

8.5.4	A secondary data centre far enough from the primary that one local disruption cannot affect both.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CP-7 Alternate Processing Site, CP-7(1) Separation from Primary Site, CP-6 Alternate Storage Site.

8.5.5	Physical security and environmental controls monitored around the clock, with tested escalation and response procedures.	**Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PE-6 Monitoring Physical Access, PE-14 Environmental Controls, IR-8 Incident Response Plan.

8.5.6 Physical access controls in the data centre: need-based access promptly revoked, escorted visitors, monitored entry points and racks, controlled keys, and delivery areas kept apart from sensitive areas. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PE-2 Physical Access Authorizations, PE-3 Physical Access Control, PE-8 Visitor Access Records, PE-6 Monitoring Physical Access.

9 Access control

9.1 User access management

9.1.1 No single person able to carry out a sensitive function alone: two-person control, segregation of duties and least privilege, with access granted by each person's role. **Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: AC-5 Separation of Duties, AC-6 Least Privilege, AC-6(1) Authorize Access to Security Functions.

Scope of this evidence The verdict covers the cluster's RBAC: subjects and workloads with administrative, wildcard, exec or Secret access, and service account tokens. Two-person control, segregation of duties, and access to other systems are the financial institution's to evidence.

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

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.

9.1.2 A process to grant, change and remove access rights, with each grant approved by a suitable party such as the asset owner. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: AC-2 Account Management.

9.1.3 User access and the administration of users recorded, each record uniquely attributable, for audit and investigation. **Pass**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: AU-2 Event Logging, AU-3 Content of Audit Records, AU-12 Audit Record Generation, AC-2(4) Automated Audit Actions.

Scope of this evidence The evidence is the cluster's API audit log, which records the authenticated user, the verb, the source address and the time of each request, changes to roles and bindings included. Logging of access and user administration on other systems is the financial institution's to evidence.

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.

9.1.4	A password policy, and a process that enforces strong passwords for access to IT systems. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: IA-5(1) Password-based Authentication.	**Organisational evidence**
9.1.5	Multi-factor authentication for users who can perform sensitive system functions. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-2(1) Multi-factor Authentication to Privileged Accounts, IA-2(2) Multi-factor Authentication to Non-privileged Accounts.	**Organisational evidence**
9.1.6	Periodic review of users' privileges by suitable parties such as asset owners, finding dormant, redundant and inappropriate access and resolving exceptions promptly. Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: AC-2(3) Disable Accounts, AC-6(7) Review of User Privileges. **Scope of this evidence** The cluster's role bindings, with what each subject may do, are recorded for the review. The review itself, resolving its exceptions, and accounts on other systems are the financial institution'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.	**Recorded**
9.1.7	Access granted only where it is needed, and removed or disabled promptly when a user's role or employment changes. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: AC-2 Account Management, PS-4 Personnel Termination, PS-5 Personnel Transfer.	**Organisational evidence**
9.1.8	Service providers with access to the institution's information assets monitored and restricted as its own staff are. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: PS-7 External Personnel Security, SA-9 External System Services.	**Organisational evidence**

9.2 Privileged access management

9.2.1 Privileged accounts, which can do severe harm, granted only where needed, with their activity logged and reviewed in ongoing monitoring. **Fail**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: AC-6(5) Privileged Accounts, AC-6(9) Log Use of Privileged Functions, AU-2 Event Logging, AU-6 Audit Record Review, Analysis, and Reporting. Evidence counted: platform.audit, trivy.rbac-privilege; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The verdict covers the roles and bindings in the cluster that grant administrative, wildcard or Secret access, and the API server's audit log, which records privileged users' requests. The review of that activity, and privileged accounts on other systems, are the financial institution's to evidence.

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

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

9.2.2 A process to manage system and service accounts and to watch their use for suspicious or unauthorised activity. **Pass**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: AC-2 Account Management, AC-2(12) Account Monitoring for Atypical Usage, AU-2 Event Logging. Evidence counted: platform.audit; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is the API server's audit log, which records the requests made by the cluster's service accounts. Managing those accounts, watching their use for suspicious activity, and system and service accounts on other systems are the financial institution's to evidence.

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.

9.3 Remote access management

9.3.1 Remote connections into the institution's network encrypted against eavesdropping, and remote users strongly authenticated, for example by multi-factor authentication. **Incomplete**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: AC-17 Remote Access, AC-17(2) Protection of Confidentiality and Integrity Using Encryption, SC-8 Transmission Confidentiality and Integrity.

Scope of this evidence The evidence is TLS into the cluster and to its control plane, the host firewall on the nodes, and sign-in to the cluster delegated to the institution's identity provider. Whether that provider requires multi-factor authentication, SSH access to the nodes, and remote access to the institution's internal network are the financial institution'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.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.
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.

9.3.2 Remote access permitted only from devices secured to the institution's standards. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: AC-17 Remote Access, AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems.

10 Cryptography

10.1 Cryptographic algorithm and protocol

10.1.1 Explains that cryptography protects the confidentiality, integrity and authenticity of data and supports authentication. **Organisational evidence**

Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: SC-13 Cryptographic Protection.

10.1.2 Cryptographic algorithms drawn from recognised international standards, with algorithm and key length chosen to meet the institution's security objectives. **Fail**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: SC-13 Cryptographic Protection.

Scope of this evidence The verdict concerns the TLS cipher suites offered by the cluster's control plane and kubelets, which must be AEAD suites at TLS 1.2 or later. Algorithms and key lengths used elsewhere, and their fit with the institution's objectives, are the financial institution'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.

10.1.3 Random seeds and numbers on which an algorithm's security depends long and random enough. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

10.1.4 Every cryptographic algorithm in use tested or vetted against the institution's security objectives. **Organisational evidence**

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

10.1.5 Developments in cryptanalysis followed, with algorithms changed or key lengths increased where needed. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-13 Cryptographic Protection, PM-16 Threat Awareness Program.

10.2 Cryptographic key management

10.2.1 A policy, standards and procedures for managing keys through each stage of their life, from generation to expiry. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.

10.2.2 Keys generated securely and kept from disclosure, with the material used to derive them protected or destroyed afterwards. **Not evaluated**

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

Scope of this evidence The provider of the key that encrypts the cluster's Secrets, a local key or a key management service, is recorded for review. The generation and protection of that and every other key, and the destruction of the material used to derive keys, are the financial institution's to evidence.

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).

10.2.3	A lifespan set for each key according to data sensitivity, system criticality and threats, with the key replaced securely before it expires. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**
10.2.4	Sensitive keys handled and stored in hardened, tamper-resistant systems such as a hardware security module. Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management. **Scope of this evidence** The evidence records whether the key that encrypts the cluster's Secrets is held on the control-plane nodes or in a key management service through KMS v2. Whether that service is a hardened, tamper-resistant system such as a hardware security module, and the storage of every other key, are the financial institution's to evidence. 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).	**Not evaluated**
10.2.5	Sensitive keys kept from exposure in transit, delivered out of band or by other secure means. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**
10.2.6	Each key used for one purpose only, for example separate keys for encryption and for signing. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**
10.2.7	A compromised key revoked and replaced, together with every key whose security depends on it. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management, IR-4 Incident Handling.	**Organisational evidence**
10.2.8	Expired or revoked keys destroyed so that they cannot be recovered. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**
10.2.9	A replacement key generated so that knowing the old key, wholly or in part, does not reveal the new one. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management.	**Organisational evidence**
10.2.10	Keys backed up for recovery, with the backups strongly protected. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-12 Cryptographic Key Establishment and Management, SC-12(1) Availability.	**Organisational evidence**

11 Data and infrastructure security

11.1 Data security

11.1.1 Data loss prevention policies, with measures that detect and stop unauthorised access to, change, copying or sending of confidential data in transit, at rest and in use. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: AC-4 Information Flow Enforcement, SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest.

11.1.2 Data theft and unauthorised change on systems and endpoint devices prevented and detected, with systems run by service providers held to the same standards. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, SI-7 Software, Firmware, and Information Integrity, SA-9 External System Services.

11.1.3 Confidential data held on systems and endpoint devices encrypted, with strong controls on who can reach it. **Fail**

Platform, coverage partial. Guidelines (guidance). NIST SP 800-53: SC-28 Protection of Information at Rest, AC-3 Access Enforcement.

Scope of this evidence The evidence is that Kubernetes Secrets are encrypted at rest in etcd, that anonymous requests to the API server are limited to the health endpoints, that kubelets authorise requests through the API server, and the roles that grant administrative or Secret access. Encryption of the applications' stored data, of endpoint devices and of other systems is the financial institution'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.
platform.secret-encryption	**Not evaluated**	The platform could not observe Secret encryption. Establishes: Secrets, and optionally ConfigMaps, are encrypted at rest in etcd.
trivy.rbac-privilege	**Fail**	2 object(s) fail. Establishes: Roles and bindings that grant administrative access, wildcard access, access to Secrets, or anonymous access.

11.1.4 Only authorised storage media, systems and endpoint devices used to send, transfer or hold confidential data. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: MP-7 Media Use, AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems.

11.1.5 Use of unauthorised internet services, such as social media, file sharing, email and messaging, for confidential data prevented and detected. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-7 Boundary Protection, AC-4 Information Flow Enforcement.

11.1.6	Sensitive production data kept out of non-production environments, used there only with senior management's approval, under access and removal controls and masked where possible. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SA-3(2) Use of Live or Operational Data, PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research.	**Organisational evidence**
11.1.7	Confidential data erased beyond recovery before storage media, systems or devices are disposed of or reused. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: MP-6 Media Sanitization.	**Organisational evidence**

11.2 Network security

11.2.1	Firewalls and similar devices protecting the network at its connections to the Internet and to third parties. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-7 Boundary Protection.	**Organisational evidence**

11.2.2 Mechanisms against lateral movement and insider threat; one way is to place information assets in network segments by criticality, role or data sensitivity. **Fail**

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

Scope of this evidence Segmentation within the cluster only: the host firewall on the nodes and the network policies of each application namespace. The verdict can be Pass only when the Convoy's generated default-deny network policy is turned on (it is off by default). Segmentation of the institution's wider network is the financial institution'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.

11.2.3 Network intrusion prevention that detects and blocks malicious traffic. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, SI-4(4) Inbound and Outbound Communications Traffic.

11.2.4 Network access control that detects and stops unauthorised devices from joining the network. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-3 Device Identification and Authentication.

11.2.5 Rules on firewalls, routers, switches and access points reviewed regularly, with obsolete rules and insecure protocols removed promptly. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CM-7(1) Periodic Review, SC-7 Boundary Protection.

11.2.6	Separating web browsing from endpoint devices by physical or logical means, or equivalent controls, considered to reduce exposure to attack. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-7 Boundary Protection, SC-44 Detonation Chambers.	**Organisational evidence**
11.2.7	Protection that detects and responds to denial-of-service attacks, possibly with a mitigation provider filtering traffic upstream. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-5 Denial-of-service Protection.	**Organisational evidence**
11.2.8	Periodic review of the network architecture, its security design and interconnections, to find vulnerabilities. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: PL-8 Security and Privacy Architectures, CA-2 Control Assessments.	**Organisational evidence**

11.3 System security

11.3.1	Security standards setting hardened configurations for hardware and software, reviewed periodically. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CM-2 Baseline Configuration, CM-6 Configuration Settings.	**Organisational evidence**

11.3.2 A process confirming that security standards are applied uniformly across systems, finding deviations and dealing with their risk promptly. **Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-6 Configuration Settings, CA-7 Continuous Monitoring.

Scope of this evidence The verdict concerns the cluster's configuration against its hardening baseline: Pod Security defaults, the TLS and settings of the control plane and kubelets, file permissions on the nodes, and whether workloads run as root, without seccomp or without resource limits. Applying the institution's standards to other systems, and dealing with deviations, are the financial institution's to evidence.

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

node.etcd-data	**Pass**	etcd's data directory is owned by root and closed to other users: so on all 1 node(s). Establishes: etcd's data directory on each control-plane node is owned by root and closed to other users (700).
node.file-permissions	**Pass**	Kubernetes' configuration, credentials and keys are owned by root and no more open than their limits: so on all 1 node(s). Establishes: The Kubernetes configuration, credentials, certificates and keys on each node are owned by root and no more open than their limits (600 for credentials, keys and manifests, 644 for certificates). The API server's audit log directory is judged by node.audit-log-permissions, not here.
node.kubelet-hardening	**Pass**	The kubelet keeps its read-only port closed and rotates its certificates: so on all 1 node(s). Establishes: The kubelet keeps its read-only port closed and rotates its client certificates.
platform.control-plane-tls	**Not evaluated**	The control-plane TLS and profiling settings: the platform could not observe it. Establishes: Profiling is off and only AEAD TLS cipher suites are offered by the control plane and the kubelets.
platform.mesh-cni	**Not evaluated**	The service mesh CNI plugin: the platform could not observe it. Establishes: Meshed Pods run without elevated privileges, through the mesh's CNI plugin.
platform.pod-security	**Not evaluated**	Pod Security admission defaults: the platform could not observe it. Establishes: Pod Security Admission defaults are applied to namespaces, with the exemptions listed.
policy.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.

11.3.3 Endpoint protection, behavioural and signature-based, against malware and its usual routes such as links, websites, attachments and removable media. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-3 Malicious Code Protection.

11.3.4 Anti-malware signatures kept current and systems scanned regularly for malicious files or anomalous activity. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-3 Malicious Code Protection.

11.3.5 Detection and response that scans promptly for indicators of compromise and watches system and endpoint processes for anomalies. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.

11.3.6 Measures such as application allowlisting so that only authorised software can be installed on systems. **Fail**

Enforced, coverage partial. Guidelines (guidance). NIST SP 800-53: CM-7(5) Authorized Software — Allow-by-exception, CM-11 User-installed Software.

Scope of this evidence The evidence is that the workloads outside the exempt namespaces run images only from the registries the institution allows, signed by a configured key; a failing Pod is admitted with a warning and recorded, or refused where the institution sets the policies to deny. Software installed on the nodes and on other systems is the financial institution's to evidence.

Fails in CronJob payments/nightly, Deployment payments/legacy-batch, Deployment payments/unsigned-app, CronJob payments/weekly, Deployment payments/ledger, Job payments/migrate-once, Job payments/nightly-now, Pod payments/nightly-now-zxcxw, Pod payments/one-off, Pod payments/unsigned-app-b5567644f-p2qb6 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.

11.3.7 A risk assessment and suitable safeguards before staff may reach the corporate network from personal devices. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: AC-19 Access Control for Mobile Devices, AC-20 Use of External Systems, RA-3 Risk Assessment.

11.4 Virtualisation security

11.4.1	Security standards for every component of a virtualisation solution, since a failure in one virtual machine can spread to others. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CM-6 Configuration Settings.	**Organisational evidence**
11.4.2	Administrative access to hypervisors and host operating systems tightly restricted. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: AC-6(5) Privileged Accounts, AC-3 Access Enforcement.	**Organisational evidence**
11.4.3	Policies and standards governing virtual images and snapshots from creation to destruction, protecting them from unauthorised access or change. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CM-2 Baseline Configuration, MP-4 Media Storage.	**Organisational evidence**

11.5 Internet of Things

11.5.1	An inventory of IoT devices, recording the networks they join and where they are located. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CM-8 System Component Inventory.	**Organisational evidence**
11.5.2	The risks of IoT devices, often built with little security, assessed and mitigated by processes and controls. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
11.5.3	The network hosting IoT devices secured, with their traffic restricted and the devices kept in a segment apart from core systems and confidential data. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-7 Boundary Protection, AC-4 Information Flow Enforcement.	**Organisational evidence**
11.5.4	Unauthorised access to IoT devices prevented. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-3 Device Identification and Authentication, AC-3 Access Enforcement.	**Organisational evidence**
11.5.5	IoT devices monitored for suspicious activity so that compromised ones can be isolated promptly. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**

12 Cyber security operations

12.1 Cyber threat intelligence and information sharing

12.1.1	A process to gather and analyse cyber events, threat intelligence and vulnerability information for their relevance and impact. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: PM-16 Threat Awareness Program, SI-5 Security Alerts, Advisories, and Directives.	**Organisational evidence**

12.1.2	Cyber intelligence monitoring services procured, and active participation in trusted threat-sharing arrangements. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-16 Threat Awareness Program, PM-15 Security and Privacy Groups and Associations.	**Organisational evidence**
12.1.3	A process for detecting and answering online misinformation about the institution, possibly aided by external media monitoring. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: PM-16 Threat Awareness Program, IR-4 Incident Handling.	**Organisational evidence**

12.2 Cyber event monitoring and detection

12.2.1	A security operations centre or managed security service for continuous monitoring and prompt response, with defined processes, roles and responsibilities. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, IR-4 Incident Handling.	**Organisational evidence**

12.2.2 A process for gathering, processing, reviewing and keeping system logs for security monitoring, with the logs protected from unauthorised access. **Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: AU-4 Audit Log Storage Capacity, AU-6 Audit Record Review, Analysis, and Reporting, AU-9 Protection of Audit Information.

Scope of this evidence The verdict concerns whether the cluster's logs leave its nodes for a central store, and whether only root can read or change the API server's audit log directory and files on each control-plane node. Reviewing and retaining logs, protecting the central store and every other log, and the logs of other systems are the financial institution's to evidence.

Not examined Audit log location not examined: this Bahriya Kubernetes Engine release does not set the audit log's modes; upgrade to 2.5.0 or later.

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.
node.audit-log-permissions	**Not evaluated**	Audit log location not examined: this Bahriya Kubernetes Engine release does not set the audit log's modes; upgrade to 2.5.0 or later. 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.

12.2.3 A baseline of each system's routine activity, kept current, against which activity is analysed for anomalies. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, SI-4(13) Analyze Traffic and Event Patterns.

12.2.4 User behaviour analytics considered to strengthen security monitoring. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring, AC-2(12) Account Monitoring for Atypical Usage.

12.2.5	Events across system logs correlated to reveal suspicious patterns. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: AU-6(3) Correlate Audit Record Repositories, SI-4(16) Correlate Monitoring Information.	**Organisational evidence**
12.2.6	A process for escalating suspicious system activity or user behaviour to the relevant stakeholders promptly. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-6 Incident Reporting, SI-4 System Monitoring.	**Organisational evidence**

12.3 Cyber incident response and management

12.3.1	A cyber incident response plan to contain threats and restore services securely, setting out communication, coordination and response for plausible scenarios. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-8 Incident Response Plan, IR-4 Incident Handling.	**Organisational evidence**
12.3.2	A process within the plan to find the control weaknesses behind a breach and assess its full impact. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
12.3.3	Threat intelligence and the lessons of incidents used to improve controls and the incident plan. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-4 Incident Handling, PM-16 Threat Awareness Program.	**Organisational evidence**

13 Cyber security assessment

13.1 Vulnerability assessment

13.1.1 Regular vulnerability assessment of IT systems, at a frequency set by criticality and exposure, with the gaps found addressed promptly. **Pass**

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

Scope of this evidence The verdict concerns the images of the workloads outside the exempt namespaces: open critical and high vulnerabilities, and the freshness of their scans; the age of each open vulnerability and the platform's versions are recorded beside it. Assessing the nodes, the platform and other systems, and setting the frequency by criticality, are the financial institution'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 2.3.0, Kubernetes v1.36.4, observed 2026-11-18T09:43:20Z. 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.

13.1.2 Vulnerability assessment covering at least vulnerability discovery, weak configurations, open ports and application flaws, and common web flaws for web systems. **Fail**

Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: RA-5 Vulnerability Monitoring and Scanning, CM-6 Configuration Settings.

Scope of this evidence The verdict concerns the images of the workloads outside the exempt namespaces, scanned for known vulnerabilities, and the cluster's configuration against its hardening baseline. Finding open network ports, testing applications and web systems for flaws of their own, and assessing other systems are the financial institution's to evidence.

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

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.
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.
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.
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.

13.2 Penetration testing

13.2.1	Penetration testing for an in-depth evaluation of defences, with both black-box and grey-box tests for online financial services. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**
13.2.2	A bug bounty programme considered to complement penetration testing. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-5(11) Public Disclosure Program.	**Organisational evidence**
13.2.3	Penetration testing done in production, with suitable safeguards, for a truer picture of the defences. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**
13.2.4	Penetration testing at a frequency set by criticality and exposure, and for Internet-facing systems at least yearly and after major changes. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CA-8 Penetration Testing.	**Organisational evidence**

13.3 Cyber exercises

13.3.1	Regular scenario-based cyber exercises, such as social engineering, table-top or cyber range exercises, that test response, recovery and communication plans. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: IR-3 Incident Response Testing, CP-4 Contingency Plan Testing.	**Organisational evidence**

13.3.2	The relevant stakeholders involved in each exercise as its objectives require, from senior management to service providers and technical staff. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-3 Incident Response Testing.	**Organisational evidence**

13.4 Adversarial attack simulation exercise

13.4.1	An adversarial attack simulation that tests cyber defences and the response plan against prevalent threats. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CA-8(2) Red Team Exercises.	**Organisational evidence**
13.4.2	Objectives, scope and rules of engagement agreed before the exercise, which is run under close supervision so that the red team does not disrupt production. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: CA-8(2) Red Team Exercises, CA-8 Penetration Testing.	**Organisational evidence**

13.5 Intelligence-based scenario design

13.5.1	Assessment scenarios built on challenging but plausible threats. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: CA-8(2) Red Team Exercises, PM-16 Threat Awareness Program.	**Organisational evidence**
13.5.2	Relevant threat intelligence could be used to identify the likeliest threat actors and their tactics, techniques and procedures when designing scenarios. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: PM-16 Threat Awareness Program, CA-8(2) Red Team Exercises.	**Organisational evidence**

13.6 Remediation management

13.6.1	A remediation process that tracks and resolves the issues assessments and exercises find, covering severity classification, deadlines by severity, and the handling of deviations. Checked, coverage partial. Guidelines (guidance). NIST SP 800-53: CA-5 Plan of Action and Milestones, RA-7 Risk Response, SI-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions. **Scope of this evidence** The age of each open vulnerability in the images of the workloads outside the exempt namespaces is recorded by severity, for the financial institution to compare with its own deadlines. The remediation process, its deadlines and the handling of deviations, and the findings of other assessments and exercises, are the financial institution's to evidence.	**Recorded**

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.

14 Online financial services

14.1 Security of online financial services

14.1.1 Security measures for online financial services proportionate to their risk. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment, PL-8 Security and Privacy Architectures.

14.1.2 Communication channels carrying customer data secured, for example by encryption and digital signatures. **Nothing to check**

Enforced, coverage partial. Guidelines (guidance). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-13 Cryptographic Protection. Evidence counted: policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence is that every Ingress serves its hosts over TLS. Digital signatures, and the protection of customer data on channels beyond the Ingress, are the financial institution's to evidence.

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.

14.1.3 Online services protected against common attacks such as code injection, cross-site scripting, interception, DNS hijacking, distributed denial of service, malware and spoofing. **Nothing to check**

Enforced, coverage partial. Guidelines (guidance). NIST SP 800-53: SI-10 Information Input Validation, SC-5 Denial-of-service Protection, SC-8 Transmission Confidentiality and Integrity, SC-20 Secure Name/Address Resolution Service (Authoritative Source). Evidence counted: policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster.

Scope of this evidence The evidence concerns interception only: every Ingress serves its hosts over TLS. Protection against code injection, cross-site scripting, DNS hijacking, denial of service, malware and spoofing is the financial institution's to evidence.

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.

14.1.4 The particular risks of mobile applications understood and addressed by specific measures (Annex C). **Organisational evidence**

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

14.1.5 Mobile applications and software offered to customers only through official app stores or other secure channels. **Organisational evidence**

Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SR-4 Provenance.

14.1.6 Phishing aimed at the institution or its customers monitored, reported to providers for takedown, and customers warned and advised. **Organisational evidence**

Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: PM-16 Threat Awareness Program, IR-6 Incident Reporting.

14.1.7	Rooted or jailbroken devices barred from financial transactions in the mobile app, unless the app runs in a sandbox that shields it from malware. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: AC-19 Access Control for Mobile Devices, SI-7 Software, Firmware, and Information Integrity.	**Organisational evidence**

14.2 Customer authentication and transaction signing

14.2.1	Multi-factor authentication when customers log in to online financial services. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).	**Organisational evidence**
14.2.2	Customer passwords encrypted end to end from the app or browser to the verifying system, and verified only inside hardened, tamper-resistant equipment. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, IA-5(1) Password-based Authentication.	**Organisational evidence**
14.2.3	Transaction signing, such as digital signatures, to authorise high-risk activities like changes to customer details, new payees and large transfers. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: AU-10 Non-repudiation.	**Organisational evidence**
14.2.4	Risk-based or adaptive authentication that matches the options offered to the risk of each transaction may be used. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-10 Adaptive Authentication.	**Organisational evidence**
14.2.5	Time-based one-time passwords valid for as short a period as practicable. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-5 Authenticator Management, IA-8 Identification and Authentication (Non-organizational Users).	**Organisational evidence**
14.2.6	Biometric data and customer credentials encrypted in storage and in transmission. Enforced, coverage partial. Guidelines (guidance). NIST SP 800-53: SC-8 Transmission Confidentiality and Integrity, SC-28 Protection of Information at Rest. Evidence counted: policy.ingress-tls; the rest of the regime's mapping is not evidenced by the cluster. **Scope of this evidence** The evidence is that every Ingress serves its hosts over TLS, which encrypts customer credentials on their way into the cluster. Their encryption beyond the Ingress and in storage, biometric data included, is the financial institution's to evidence. 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.	**Nothing to check**
14.2.7	Biometric false acceptance and false rejection rates set in proportion to the risk of the online activity. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users).	**Organisational evidence**

14.2.8	Soft tokens provisioned with safeguards such as customer identity checks, blocking of rooted or jailbroken devices, and device binding. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-8 Identification and Authentication (Non-organizational Users), IA-12 Identity Proofing.	**Organisational evidence**
14.2.9	Authenticated customer sessions and their encryption kept intact, hijacked sessions detected and ended, and idle sessions ended after a set time. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SC-23 Session Authenticity, AC-12 Session Termination, SC-10 Network Disconnect.	**Organisational evidence**
14.2.10	Alternative authorisation controls for corporate customers, such as maker-checker, risk-assessed to confirm they suit the activities' risk. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: RA-3 Risk Assessment.	**Organisational evidence**
14.2.11	Authentication credentials stored in a form that resists reverse engineering, with a process to revoke and replace compromised credentials. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: IA-5 Authenticator Management, SC-28 Protection of Information at Rest.	**Organisational evidence**

14.3 Fraud monitoring

14.3.1	Real-time fraud monitoring that identifies and blocks suspicious online transactions. Organisational, technical, outside the cluster. Guidelines (guidance). NIST SP 800-53: SI-4 System Monitoring.	**Organisational evidence**
14.3.2	A process to investigate suspicious transactions and resolve issues promptly. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: IR-4 Incident Handling.	**Organisational evidence**
14.3.3	Customers notified of suspicious activity or transfers above a set threshold, with the transaction's details and how to report a problem. Organisational, technical and non-technical. Guidelines (guidance). NIST SP 800-53: IR-6 Incident Reporting.	**Organisational evidence**

14.4 Customer education and communication

14.4.1	Customers told of good security practice for online financial services, including securing their own devices. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
14.4.2	Customers warned promptly of new cyber threats, so they can take precautions. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-2 Literacy Training and Awareness.	**Organisational evidence**
14.4.3	Customers advised how to spot unauthorised transactions and report security issues or suspected fraud promptly. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: AT-2 Literacy Training and Awareness, IR-7 Incident Response Assistance.	**Organisational evidence**

15 IT audit

15.1 Audit function

15.1.1	IT audit giving the board and senior management an independent opinion on the adequacy and effectiveness of technology risk management, governance and controls. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CA-2 Control Assessments, CA-2(1) Independent Assessors.	**Organisational evidence**
15.1.2	A complete set of auditable areas covering all IT operations, functions and processes, for risk-based audit planning. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
15.1.3	IT audits at a frequency matched to the criticality and risk of each asset, function or process. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CA-2 Control Assessments.	**Organisational evidence**
15.1.4	IT auditors with the competence and skills to assess IT policies, procedures, processes and controls. Organisational, non-technical. Guidelines (guidance). NIST SP 800-53: CA-2(1) Independent Assessors.	**Organisational evidence**

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-controller
cluster	ServiceAccount kube-system/expand-controller	ClusterRole system:controller:expand-controller
cluster	ServiceAccount kube-system/generic-garbage-collector	ClusterRole system:controller:generic-garbage-collector
cluster	ServiceAccount kube-system/horizontal-pod-autoscaler	ClusterRole system:controller:horizontal-pod-autoscaler
cluster	ServiceAccount kube-system/job-controller	ClusterRole system:controller:job-controller
cluster	ServiceAccount kube-system/kube-dns	ClusterRole system:kube-dns
cluster	ServiceAccount kube-system/kube-proxy	ClusterRole system:node-proxier
cluster	ServiceAccount kube-system/legacy-service-account-token-cleaner	ClusterRole system:controller:legacy-service-account-token-cleaner
cluster	ServiceAccount kube-system/namespace-controller	ClusterRole system:controller:namespace-controller
cluster	ServiceAccount kube-system/node-controller	ClusterRole system:controller:node-controller
cluster	ServiceAccount kube-system/persistent-volume-binder	ClusterRole system:controller:persistent-volume-binder
cluster	ServiceAccount kube-system/pod-garbage-collector	ClusterRole system:controller:pod-garbage-collector
cluster	ServiceAccount kube-system/pv-protection-controller	ClusterRole system:controller:pv-protection-controller
cluster	ServiceAccount kube-system/pvc-protection-controller	ClusterRole system:controller:pvc-protection-controller
cluster	ServiceAccount kube-system/replicaset-controller	ClusterRole system:controller:replicaset-controller
cluster	ServiceAccount kube-system/replication-controller	ClusterRole system:controller:replication-controller
cluster	ServiceAccount kube-system/resource-claim-controller	ClusterRole system:controller:resource-claim-controller
cluster	ServiceAccount kube-system/resourcequota-controller	ClusterRole system:controller:resourcequota-controller
cluster	ServiceAccount kube-system/root-ca-cert-publisher	ClusterRole system:controller:root-ca-cert-publisher
cluster	ServiceAccount kube-system/route-controller	ClusterRole system:controller:route-controller
cluster	ServiceAccount kube-system/selinux-warning-controller	ClusterRole system:controller:selinux-warning-controller
cluster	ServiceAccount kube-system/service-account-controller	ClusterRole system:controller:service-account-controller
cluster	ServiceAccount kube-system/service-cidrs-controller	ClusterRole system:controller:service-cidrs-controller

cluster	ServiceAccount kube-system/service-controller	ClusterRole system:controller:service-controller
cluster	ServiceAccount kube-system/statefulset-controller	ClusterRole system:controller:statefulset-controller
cluster	ServiceAccount kube-system/ttl-after-finished-controller	ClusterRole system:controller:ttl-after-finished-controller
cluster	ServiceAccount kube-system/ttl-controller	ClusterRole system:controller:ttl-controller
cluster	ServiceAccount kube-system/validatingadmissionpolicy-status-controller	ClusterRole system:controller:validatingadmissionpolicy-st controller
cluster	ServiceAccount kube-system/volumeattributesclass-protection-controller	ClusterRole system:controller:volumeattributesclass-protec controller
cluster	ServiceAccount kyverno/engine-admission-controller	ClusterRole kyverno:admission-controller
cluster	ServiceAccount kyverno/engine-admission-controller	ClusterRole view
cluster	ServiceAccount kyverno/engine-background-controller	ClusterRole kyverno:background-controller
cluster	ServiceAccount kyverno/engine-background-controller	ClusterRole view
cluster	ServiceAccount kyverno/engine-cleanup-controller	ClusterRole kyverno:cleanup-controller
cluster	ServiceAccount kyverno/engine-reports-controller	ClusterRole kyverno:reports-controller
cluster	ServiceAccount kyverno/engine-reports-controller	ClusterRole view
cluster	ServiceAccount local-path-storage/local-path-provisioner-service-account	ClusterRole local-path-provisioner-role
cluster	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator
cluster	ServiceAccount trivy-system/trivy-operator-engine	ClusterRole trivy-operator
cluster	User kube-apiserver-kubelet-client	ClusterRole system:kubelet-api-admin
cluster	User system:kube-controller-manager	ClusterRole calico-tier-getter
cluster	User system:kube-controller-manager	ClusterRole system:kube-controller-manager
cluster	User system:kube-proxy	ClusterRole system:node-proxier
cluster	User system:kube-scheduler	ClusterRole system:kube-scheduler
cluster	User system:kube-scheduler	ClusterRole system:volume-scheduler
bahriya-system	ServiceAccount compliance/compliance-collector	ClusterRole bke-platform-reader
calico-system	ServiceAccount calico-system/goldmane	Role goldmane

calico-system	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator-secrets
compliance-node	ServiceAccount compliance/compliance-collector	Role compliance-node-collector
kube-public	ServiceAccount kube-system/bootstrap-signer	Role system:controller:bootstrap-signer
kube-public	User system:anonymous	Role kubeadm:bootstrap-signer-clusterinfo
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kube-proxy
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kubeadm:kubelet-config
kube-system	Group system:bootstrappers:kubeadm:default-node-token	Role kubeadm:nodes-kubeadm-config
kube-system	Group system:nodes	Role kubeadm:kubelet-config
kube-system	Group system:nodes	Role kubeadm:nodes-kubeadm-config
kube-system	ServiceAccount calico-system/calico-apiserver	Role extension-apiserver-authentication-reader
kube-system	ServiceAccount kube-system/bootstrap-signer	Role system:controller:bootstrap-signer
kube-system	ServiceAccount kube-system/cloud-provider	Role system:controller:cloud-provider
kube-system	ServiceAccount kube-system/kube-controller-manager	Role system::leader-locking-kube-controller-manager
kube-system	ServiceAccount kube-system/kube-scheduler	Role system::leader-locking-kube-scheduler
kube-system	ServiceAccount kube-system/leader-election-controller	Role system::leader-locking-kube-controller-manager
kube-system	ServiceAccount kube-system/token-cleaner	Role system:controller:token-cleaner
kube-system	User system:kube-controller-manager	Role extension-apiserver-authentication-reader
kube-system	User system:kube-controller-manager	Role system::leader-locking-kube-controller-manager
kube-system	User system:kube-scheduler	Role extension-apiserver-authentication-reader
kube-system	User system:kube-scheduler	Role system::leader-locking-kube-scheduler
kyverno	ServiceAccount kyverno/engine-admission-controller	Role kyverno:admission-controller
kyverno	ServiceAccount kyverno/engine-background-controller	Role kyverno:background-controller

kyverno	ServiceAccount kyverno/engine-cleanup-controller	Role kyverno:cleanup-controller
kyverno	ServiceAccount kyverno/engine-reports-controller	Role kyverno:reports-controller
local-path-storage	ServiceAccount local-path-storage/local-path-provisioner-service-account	Role local-path-provisioner-role
tigera-operator	ServiceAccount tigera-operator/tigera-operator	ClusterRole tigera-operator-secrets
trivy-system	ServiceAccount trivy-system/trivy-operator-engine	Role trivy-operator-engine
trivy-system	ServiceAccount trivy-system/trivy-operator-engine	Role trivy-operator-engine-leader-election

cluster.backup-encryption Nothing to check

Every backed-up Longhorn volume is encrypted, so that its backups leave the site encrypted.

Neither Longhorn nor Velero is installed, so no backup leaves the site.

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, 22 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
compliance	Deployment compliance-web-view	registry.example.com/tersane/core/nginxinc/nginx-unprivileged:1.x.y@sha256:
compliance	Pod reader	registry.example.com/tersane/core/nginxinc/nginx-unprivileged@sha256:f5116
compliance-node	Job node-facts-flz54	registry.example.com/tersane/convoy/compliance/core/collector:1.x.y@sha256
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@sha256:27f3cc5 registry.example.com/tersane/core/kyverno/kyverno:1.x.y@sha256:c8c4dd09e

kyverno	Deployment engine-background-controller	registry.example.com/tersane/core/kyverno/background-controller:1.x.y@sha256:c46e124f21ef8a6bb4b48de57106808b1007edcd5ddd
kyverno	Deployment engine-cleanup-controller	registry.example.com/tersane/core/kyverno/cleanup-controller:1.x.y@sha256:c
kyverno	Deployment engine-reports-controller	registry.example.com/tersane/core/kyverno/reports-controller:1.x.y@sha256:5
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:(
trivy-system	Job scan-vulnerabilityreport-7fcd456b4f	registry.example.com/tersane/core/aquasecurity/trivy:1.x.y@sha256:790fd66d
trivy-system	StatefulSet trivy-server	registry.example.com/tersane/core/aquasecurity/trivy:1.x.y@sha256:790fd66d

node.audit-log-permissions Not evaluated

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.

Audit log location not examined: this Bahriya Kubernetes Engine release does not set the audit log's modes; upgrade to 2.5.0 or later.

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)

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.control-plane-tls Not evaluated

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

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

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

platform.host-firewall Not evaluated

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

The platform could not count the host endpoints.

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

platform.image-registry Recorded

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

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

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

platform.key-provider Not evaluated

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

The platform could not observe the encryption provider.

- encryption.provider: unknown

platform.mesh-cni Not evaluated

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

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

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

platform.oidc Not evaluated

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

The platform could not read the authentication configuration.

- authentication.oidc-issuers: unknown

platform.pod-security Not evaluated

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

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

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

platform.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.version-support Pass

The cluster's Kubernetes minor release is within its end-of-life date as the Kubernetes project states it, and its BKE minor release within Mamluk's published BKE support policy (one of the five most recent minor releases, or six months from its release, whichever is longer); a release past either fails, as end of support. Each table is dated, and a table not reviewed in time gives no verdict.

Kubernetes 1.36 is supported until 2027-06-28, as https://kubernetes.io/releases/ states. Bahriya Kubernetes Engine 2.3 is one of the 5 most recent minor releases, and supported under https://bke.bahriya.cloud/faq/#release-support.

- kubernetes-version: v1.36.4
- Kubernetes support table: https://kubernetes.io/releases/, published, as of 2026-11-10, to be reviewed by 2027-02-08
- bke-version: 2.3.0
- Bahriya Kubernetes Engine support table: https://bke.bahriya.cloud/faq/#release-support, published, as of 2026-11-10, to be reviewed by 2027-02-08

platform.versions Recorded

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

Bahriya Kubernetes Engine 2.3.0, Kubernetes v1.36.4, observed 2026-11-18T09:43:20Z.

- bke-version: 2.3.0
- kubernetes-version: v1.36.4
- observed-at: 2026-11-18T09:43:20Z

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 08d267bc-7735-4db3-8092-37242c730e8d -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 5be8ff9f-da84-4f4d-b8a5-438e1b487f23 -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 4dae64ca-4264-4ea3-a4f0-28d6f76dc8dc -n payments -o yaml`

Pod payments/nightly-now-zxcxw	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 439a9e85-13f3-400c-8481-5ce4fe07efeb -n payments -o yaml`
Pod payments/unsigned-app-b5567644f-p2qb6	images not signed by organisation: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 656f73f5-2c45-48eb-91c3-183b144fcc41 -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 6d9b99f4-8062-4f30-b6dc-57e6fcd84a93 -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 70ce6bcd-83ad-4175-992e-c8e11628ae7e -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 70ce6bcd-83ad-4175-992e-c8e11628ae7e -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 6e2f8e70-0488-43e7-b79c-5a264f16a7bc -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 70ce6bcd-83ad-4175-992e-c8e11628ae7e -o yaml`

policy.no-default-token Pass

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

Every object the policy judged passes it.

- tersane-compliance-no-default-token: ready
- 7 object(s) passed, 0 failed

- not judged while it holds no workload: namespace default

policy.no-host-namespaces Pass

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

Every object the policy judged passes it.

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

policy.no-host-path Pass

No Pod mounts a host path, outside named namespaces.

Every object the policy judged passes it.

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

policy.no-host-ports Pass

No container binds a host port, outside named namespaces.

Every object the policy judged passes it.

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

policy.no-privileged Pass

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

Every object the policy judged passes it.

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

policy.registries-allowed Fail

Containers run images only from the registries the customer allows.

7 object(s) fail the policy.

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

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

Fails (7)

Object	What is wrong	Full result

CronJob payments/nightly	images not from an allowed registry: registry.example.com/payments/legacy-batch:1.0.0	`kubectl get policyreport 08d267bc-7735-4db3-8092-37242c730e8d -n payments -o yaml`
CronJob payments/weekly	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport 1bdd39bd-625e-4a37-8ea3-0c909f1de641 -n payments -o yaml`
Deployment payments/ledger	images not from an allowed registry: registry.example.com/payments/checkout:3.10.1	`kubectl get policyreport 115b1aa4-1555-446d-9eee-2ac3dca8345f -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 62da526a-1c63-4fe4-b4c5-7b12ae7f4389 -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 5be8ff9f-da84-4f4d-b8a5-438e1b487f23 -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 87a6e510-c923-4cae-92bb-1e570a8122b2 -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 06e48055-36f2-4440-8a0c-539f757e589e -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 08d267bc-7735-4db3-8092-37242c730e8d -n payments -o yaml`
Deployment payments/legacy-batch	containers without CPU and memory limits: app	`kubectl get policyreport 62da526a-1c63-4fe4-b4c5-7b12ae7f4389 -n payments -o yaml`
Deployment payments/unsigned-app	containers without CPU and memory limits: app	`kubectl get policyreport 5be8ff9f-da84-4f4d-b8a5-438e1b487f23 -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.host-access Pass

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

Every object outside the exempt namespaces passes.

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

Fails in exempt namespaces, not counted (7)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0009: Access to host network. ReplicaSet 'tigera-operator-686489b657' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Deployment tigera-operator/tigera-operator	AVD-KSV-0023: hostPath volumes mounted. ReplicaSet 'tigera-operator-686489b657' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`
Installation calico-system/default	AVD-KSV-0009: Access to host network. DaemonSet 'calico-node' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0009: Access to host network. ReplicaSet 'calico-typha-5bd879cc96' should not set 'spec.template.spec.hostNetwork' to true	`kubectl get configauditreport replicaset-calico-typha-5bd879cc96 -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0023: hostPath volumes mounted. DaemonSet 'calico-node' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0023: hostPath volumes mounted. DaemonSet 'csi-node-driver' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Job compliance-node/node-facts-flz54	AVD-KSV-0023: hostPath volumes mounted. Job 'node-facts-flz54' should not set 'spec.template.volumes.hostPath'	`kubectl get configauditreport job-node-facts-flz54 -n compliance-node -o yaml`

trivy.image-os-support Not evaluated

Every workload's images are scanned for the operating system they are built on; an image whose operating system trivy holds past its end of service life fails, as end of support. An image with no operating system that trivy recognises is listed by name and not judged.

No image outside the exempt namespaces runs on an operating system trivy recognises, so none was judged.

- 27 container image(s) scanned
- 0 outside the exempt namespaces on an operating system trivy recognises, 7 on none it recognises

- Images with no operating system trivy recognises (scratch, static or unrecognised), not judged by this check: registry.example.com/payments/checkout:3.10.1, registry.example.com/payments/legacy-batch:1.0.0

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-75f57fdd4' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-apiserver-75f57fdd4 -n calico-system -o yaml`
APIServer calico-system/default	AVD-KSV-0018: Memory not limited. Container 'calico-apiserver' of ReplicaSet 'calico-apiserver-75f57fdd4' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-apiserver-75f57fdd4 -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-6b8c8bf84b' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-kube-controllers-6b8c8bf84b -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-5bd879cc96' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-calico-typha-5bd879cc96 -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-6b8c8bf84b' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-kube-controllers-6b8c8bf84b -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-5bd879cc96' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-calico-typha-5bd879cc96 -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-6bcd685fcd' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-whisker-6bcd685fcd -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0011: CPU not limited. Container 'whisker-backend' of ReplicaSet 'whisker-6bcd685fcd' should set 'resources.limits.cpu'	`kubectl get configauditreport replicaset-whisker-6bcd685fcd -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0018: Memory not limited. Container 'whisker' of ReplicaSet 'whisker-6bcd685fcd' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-whisker-6bcd685fcd -n calico-system -o yaml`
Whisker calico-system/default	AVD-KSV-0018: Memory not limited. Container 'whisker-backend' of ReplicaSet 'whisker-6bcd685fcd' should set 'resources.limits.memory'	`kubectl get configauditreport replicaset-whisker-6bcd685fcd -n calico-system -o yaml`

trivy.network-policy-selectors Pass

NetworkPolicies whose selectors select nothing.

Every object outside the exempt namespaces passes.

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

trivy.privileged Fail

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

3 object(s) fail.

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

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

Fails (3)

Object	What is wrong	Full result
CronJob payments/nightly	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of CronJob 'nightly' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport cronjob-nightly -n payments -o yaml`
Deployment payments/legacy-batch	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'legacy-batch-5bdd998d78' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport replicaset-legacy-batch-5bdd998d78 -n payments -o yaml`
Deployment payments/unsigned-app	AVD-KSV-0001: Can elevate its own privileges. Container 'app' of ReplicaSet 'unsigned-app-b5567644f' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport replicaset-unsigned-app-b5567644f -n payments -o yaml`

Fails in exempt namespaces, not counted (15)

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

Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0001: Can elevate its own privileges. Container 'install-cni' of DaemonSet 'calico-node' should set 'securityContext.allowPrivilegeEscalation' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'calico-csi' of DaemonSet 'csi-node-driver' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'calico-node' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'cni-plugins' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'csi-node-driver-registrar' of DaemonSet 'csi-node-driver' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'ebpf-bootstrap' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'flexvol-driver' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`
Installation calico-system/default	AVD-KSV-0017: Privileged. Container 'install-cni' of DaemonSet 'calico-node' should set 'securityContext.privileged' to false	`kubectl get configauditreport daemonset-calico-node -n calico-system -o yaml`

trivy.rbac-exec **Pass**

Roles that allow executing into Pods or impersonating privileged groups.

Every object outside the exempt namespaces passes.

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

Fails in exempt namespaces, not counted (3)

Object	What is wrong	Full result

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

trivy.rbac-privilege Fail

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

2 object(s) fail.

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

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

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

Fails (3)

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

Fails in exempt namespaces, not counted (18)

Object	What is wrong	Full result

ClusterRole admin	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'admin' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-admin -o yaml`
ClusterRole cluster-admin	Kubernetes default role; AVD-KSV-0044: No wildcard verb and resource roles. Role permits wildcard verb on wildcard resource	`kubectl get clusterrbacassessmentreport clusterrole-cluster-admin -o yaml`
ClusterRole edit	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'edit' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-edit -o yaml`
ClusterRole kyverno:admission-controller	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:admission-controller' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-78fb9f7b45 -o yaml`
ClusterRole kyverno:admission-controller:core	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:admission-controller:core' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-66dd849fcd -o yaml`
ClusterRole kyverno:cleanup-controller	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:cleanup-controller' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-5fc98dd666 -o yaml`
ClusterRole kyverno:cleanup-controller:core	AVD-KSV-0114: Manage webhookconfigurations. ClusterRole 'kyverno:cleanup-controller:core' should not have access to resources ["mutatingwebhookconfigurations", "validatingwebhookconfigurations"] for verbs ["create", "update", "patch", "delete", "deletecollection", "impersonate", "*"]	`kubectl get clusterrbacassessmentreport clusterrole-757c5df67 -o yaml`

ClusterRole system:aggregate-to-edit	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:aggregate-to-edit' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-7b884bc5d8 -o yaml`
ClusterRole system:controller:legacy-service-account-token-cleaner	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:controller:legacy-service-account-token-cleaner' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-864fd65956 -o yaml`
ClusterRole system:kube-controller-manager	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:kube-controller-manager' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-b754c4cc6 -o yaml`
ClusterRole system:node	Kubernetes default role; AVD-KSV-0041: Manage secrets. ClusterRole 'system:node' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-54cdc9b678 -o yaml`
ClusterRole trivy-operator	AVD-KSV-0041: Manage secrets. ClusterRole 'trivy-operator' shouldn't have access to manage resource 'secrets'	`kubectl get clusterrbacassessmentreport clusterrole-trivy-operator -o yaml`
ClusterRole trivy-operator	AVD-KSV-0047: Do not allow privilege escalation from node proxy. Role permits privilege escalation from node proxy	`kubectl get clusterrbacassessmentreport clusterrole-trivy-operator -o yaml`
Role kyverno/kyverno:admission-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:admission-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-78fb9f7b45 -n kyverno -o yaml`
Role kyverno/kyverno:background-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:background-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-586b8c778d -n kyverno -o yaml`
Role kyverno/kyverno:cleanup-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:cleanup-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-5fc98dd666 -n kyverno -o yaml`
Role kyverno/kyverno:reports-controller	AVD-KSV-0113: Manage namespace secrets. Role 'kyverno:reports-controller' shouldn't have access to manage secrets in namespace 'kyverno'	`kubectl get rbacassessmentreport role-899885f55 -n kyverno -o yaml`
Role trivy-system/trivy-operator-engine	AVD-KSV-0113: Manage namespace secrets. Role 'trivy-operator-engine' shouldn't have access to manage secrets in namespace 'trivy-system'	`kubectl get rbacassessmentreport role-trivy-operator-engine -n trivy-system -o yaml`

trivy.run-as-root Fail

Containers that run as the root user.

3 object(s) fail.

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

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

Fails (3)

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

Fails in exempt namespaces, not counted (10)

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

Installation calico-system/default	AVD-KSV-0105: Containers must not set runAsUser to 0. securityContext.runAsUser should be set to a value greater than 0	`kubectl get configauditreport daemonset-csi-node-driver -n calico-system -o yaml`

trivy.seccomp Fail

Containers without the runtime's default seccomp profile.

3 object(s) fail.

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

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

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

Fails (6)

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

Fails in exempt namespaces, not counted (2)

Object	What is wrong	Full result
Deployment tigera-operator/tigera-operator	AVD-KSV-0030: Runtime/Default Seccomp profile not set. Either Pod or Container should set 'securityContext.seccompProfile.type' to 'RuntimeDefault'	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`

Deployment tigera-operator/tigera-operator	AVD-KSV-0104: Seccomp policies disabled. container "tigera-operator" of replicaset "tigera-operator-686489b657" in "tigera-operator" namespace should specify a seccomp profile	`kubectl get configauditreport replicaset-tigera-operator-686489b657 -n tigera-operator -o yaml`

trivy.token-automount Pass

Pods that mount a service account token.

Every object outside the exempt namespaces passes.

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

trivy.vulnerabilities Pass

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

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

- 27 container image(s) scanned
- oldest scan of a workload outside the exempt namespaces: 2026-11-18T09:46:20Z

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-7d86b7d9d5-nginx -n compliance -o yaml`
Deployment kyverno/engine-admission-controller (kyverno)	container kyverno: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-admission-controller-6dfcc4ff8-kyverno -n kyverno -o yaml`
Deployment kyverno/engine-admission-controller (kyverno-pre)	container kyverno-pre: 0 critical, 1 high	`kubectl get vulnerabilityreport replicaset-engine-admission-controller-6dfcc4ff8-kyverno-pre -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`
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-2 Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes.
AC-2(3) Disable Accounts	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
AC-2(4) Automated Audit Actions	Automatically audit account creation, modification, enabling, disabling, and removal actions.
AC-2(12) Account Monitoring for Atypical Usage	(a) Monitor system accounts for [Assignment: organization-defined atypical usage] ; and (b) Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].
AC-3 Access Enforcement	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-4 Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
AC-5 Separation of Duties	a. Identify and document [Assignment: organization-defined duties of individuals] ; and b. Define system access authorizations to support separation of duties.
AC-6 Least Privilege	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
AC-6(1) Authorize Access to Security Functions	Authorize access for [Assignment: organization-defined individuals and roles] to: (a) [Assignment: organization-defined organization-defined security functions (deployed in hardware, software, and firmware)] ; and (b) [Assignment: organization-defined security-relevant information].

AC-6(5) Privileged Accounts	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
AC-6(7) Review of User Privileges	(a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles and classes] to validate the need for such privileges; and (b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
AC-6(9) Log Use of Privileged Functions	Log the execution of privileged functions.
AC-12 Session Termination	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events].
AC-17 Remote Access	a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize each type of remote access to the system prior to allowing such connections.
AC-17(2) Protection of Confidentiality and Integrity Using Encryption	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
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-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].
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.
AU-2 Event Logging	a. Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types]; b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged; c. Specify the following event types for logging within the system: [Assignment: organization-defined organization-defined event types (subset of the event types defined in [AU-2a.](#au-2_smt.a)) along with the frequency of (or situation requiring) logging for each identified event type]; d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e. Review and update the event types selected for logging [Assignment: organization-defined frequency].
AU-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-6(3) Correlate Audit Record Repositories	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
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-12 Audit Record Generation	a. Provide audit record generation capability for the event types the system is capable of auditing as defined in [AU-2a](#au-2_smt.a) on [Assignment: organization-defined system components]; b. Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c. Generate audit records for the event types defined in [AU-2c](#au-2_smt.c) that include the audit record content defined in [AU-3](#au-3).
CA-2 Control Assessments	a. Select the appropriate assessor or assessment team for the type of assessment to be conducted; b. Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; d. Assess the controls in the system and its environment of operation [Assignment: organization-defined assessment frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; e. Produce a control assessment report that document the results of the assessment; and f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
CA-2(1) Independent Assessors	Employ independent assessors or assessment teams to conduct control assessments.
CA-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-7 Continuous Monitoring	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes: a. Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics]; b. Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c. Ongoing control assessments in accordance with the continuous monitoring strategy; d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e. Correlation and analysis of information generated by control assessments and monitoring; f. Response actions to address results of the analysis of control assessment and monitoring information; and g. Reporting the security and privacy status of the system to [Assignment: organization-defined organization-defined personnel or roles] [Assignment: organization-defined organization-defined frequency].

CA-8 Penetration Testing	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined system(s) or system components].
CA-8(2) Red Team Exercises	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].
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-3(2) Testing, Validation, and Documentation of Changes	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(4) Security and Privacy Representatives	Require [Assignment: organization-defined organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].
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 Least Functionality	a. Configure the system to provide only [Assignment: organization-defined mission-essential capabilities] ; and b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].
CM-7(1) Periodic Review	(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and (b) Disable or remove [Assignment: organization-defined organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].
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-8(1) Updates During Installation and Removal	Update the inventory of system components as part of component installations, removals, and system updates.
CM-8(3) Automated Unauthorized Component Detection	(a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined organization-defined automated mechanisms] [Assignment: organization-defined frequency] ; and (b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by unauthorized components; isolate unauthorized components; notify [Assignment: organization-defined personnel or roles]].
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-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].

CM-14 Signed Components	Prevent the installation of [Assignment: organization-defined organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.
CP-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-2(3) Resume Mission and Business Functions	Plan for the resumption of [Selection: all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.
CP-2(8) Identify Critical Assets	Identify critical system assets supporting [Selection: all; essential] mission and business functions.
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-4(1) Coordinate with Related Plans	Coordinate contingency plan testing with organizational elements responsible for related plans.
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-7(1) Separation from Primary Site	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.
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-9(1) Testing for Reliability and Integrity	Test backup information [Assignment: organization-defined organization-defined frequency] to verify media reliability and information integrity.
CP-9(8) Cryptographic Protection	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined 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.
IA-2 Identification and Authentication (Organizational Users)	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-2(1) Multi-factor Authentication to Privileged Accounts	Implement multi-factor authentication for access to privileged accounts.
IA-2(2) Multi-factor Authentication to Non-privileged Accounts	Implement multi-factor authentication for access to non-privileged accounts.
IA-3 Device Identification and Authentication	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

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-5(1) Password-based Authentication	For password-based authentication: (a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly; (b) Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a); (c) Transmit passwords only over cryptographically-protected channels; (d) Store passwords using an approved salted key derivation function, preferably using a keyed hash; (e) Require immediate selection of a new password upon account recovery; (f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; (g) Employ automated tools to assist the user in selecting strong password authenticators; and (h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].
IA-8 Identification and Authentication (Non-organizational Users)	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
IA-10 Adaptive Authentication	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].
IA-12 Identity Proofing	a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b. Resolve user identities to a unique individual; and c. Collect, validate, and verify identity evidence.
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-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.
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-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-2 Physical Access Authorizations	a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b. Issue authorization credentials for facility access; c. Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency] ; and d. Remove individuals from the facility access list when access is no longer required.
PE-3 Physical Access Control	a. Enforce physical access authorizations at [Assignment: organization-defined entry and exit points] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined systems or devices] ; guards]; b. Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]; c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls]; d. Escort visitors and control visitor activity [Assignment: organization-defined circumstances]; e. Secure keys, combinations, and other physical access devices; f. Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency] ; and g. Change combinations and keys [Assignment: organization-defined organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
PE-6 Monitoring Physical Access	a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b. Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events] ; and c. Coordinate results of reviews and investigations with the organizational incident response capability.
PE-8 Visitor Access Records	a. Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period]; b. Review visitor access records [Assignment: organization-defined frequency] ; and c. Report anomalies in visitor access records to [Assignment: organization-defined personnel].
PE-9 Power Equipment and Cabling	Protect power equipment and power cabling for the system from damage and destruction.
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-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-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-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-8 Security and Privacy Architectures	a. Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals; 3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b. Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.

PM-1 Information Security Program Plan	a. Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and c. Protect the information security program plan from unauthorized disclosure and modification.
PM-2 Information Security Program Leadership Role	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
PM-3 Information Security and Privacy Resources	a. Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b. Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and c. Make available for expenditure, the planned information security and privacy resources.
PM-5 System Inventory	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
PM-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-13 Security and Privacy Workforce	Establish a security and privacy workforce development and improvement program.
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-16 Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.

PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research	a. Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b. Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes; c. Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d. Review and update policies and procedures [Assignment: organization-defined organization-defined frequency].
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-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-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-7 External Personnel Security	a. Establish personnel security requirements, including security roles and responsibilities for external providers; b. Require external providers to comply with personnel security policies and procedures established by the organization; c. Document personnel security requirements; d. Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period] ; and e. Monitor provider compliance with personnel security requirements.

PS-9 Position Descriptions	Incorporate security and privacy roles and responsibilities into organizational position descriptions.
RA-1 Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system-level] risk assessment policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c. Review and update the current risk assessment: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] ; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
RA-2 Security Categorization	a. Categorize the system and information it processes, stores, and transmits; b. Document the security categorization results, including supporting rationale, in the security plan for the system; and c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
RA-3 Risk Assessment	a. Conduct a risk assessment, including: 1. Identifying threats to and vulnerabilities in the system; 2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments; c. Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d. Review risk assessment results [Assignment: organization-defined frequency]; e. Disseminate risk assessment results to [Assignment: organization-defined personnel or roles] ; and f. Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
RA-5 Vulnerability Monitoring and Scanning	a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyze vulnerability scan reports and results from vulnerability monitoring; d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

RA-5(11) Public Disclosure Program	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.
RA-7 Risk Response	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.
SA-2 Allocation of Resources	a. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and c. Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.
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-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(1) Static Code Analysis	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.
SA-11(4) Manual Code Reviews	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].
SA-11(8) Dynamic Code Analysis	Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.
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-22 Unsupported System Components	a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b. Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].

SC-5 Denial-of-service Protection	a. [Selection: protect against; limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events] ; and b. Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].
SC-7 Boundary Protection	a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system; b. Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
SC-8 Transmission Confidentiality and Integrity	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-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-12(1) Availability	Maintain availability of information in the event of the loss of cryptographic keys by users.
SC-13 Cryptographic Protection	a. Determine the [Assignment: organization-defined cryptographic uses] ; and b. Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography].
SC-20 Secure Name/Address Resolution Service (Authoritative Source)	a. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
SC-23 Session Authenticity	Protect the authenticity of communications sessions.
SC-28 Protection of Information at Rest	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-36 Distributed Processing and Storage	Distribute the following processing and storage components across multiple [Selection: physical locations; logical domains]: [Assignment: organization-defined organization-defined processing and storage components].
SC-44 Detonation Chambers	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].
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-2(3) Time to Remediate Flaws and Benchmarks for Corrective Actions	(a) Measure the time between flaw identification and flaw remediation; and (b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].
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-4(4) Inbound and Outbound Communications Traffic	(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic; (b) Monitor inbound and outbound communications traffic [Assignment: organization-defined organization-defined frequency] for [Assignment: organization-defined organization-defined unusual or unauthorized activities or conditions].
SI-4(5) System-generated Alerts	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].
SI-4(13) Analyze Traffic and Event Patterns	(a) Analyze communications traffic and event patterns for the system; (b) Develop profiles representing common traffic and event patterns; and (c) Use the traffic and event profiles in tuning system-monitoring devices.
SI-4(16) Correlate Monitoring Information	Correlate information from monitoring tools and mechanisms employed throughout the system.

SI-5 Security Alerts, Advisories, and Directives	a. Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; b. Generate internal security alerts, advisories, and directives as deemed necessary; c. Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles] ; [Assignment: organization-defined elements] ; [Assignment: organization-defined external organizations]] ; and d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
SI-7 Software, Firmware, and Information Integrity	a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined organization-defined software, firmware, and information] ; and b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined organization-defined actions].
SI-10 Information Input Validation	Check the validity of the following information inputs: [Assignment: organization-defined information inputs].
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 Acquisition Strategies, Tools, and Methods	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined strategies, tools, and methods].
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].